UNIVERSIDAD SIMÓN BOLÍVAR
BARRANQUILLA Y CÚCUTA - COLOMBIA | VIGILADA MINEDUCACIÓN

ACREDITACIÓN INSTITUCIONAL EN ALTA CALIDAD
RENOVACIÓN - 8 AÑOS • 2021 - 2029
Resolución 015867 - MINEDUCACIÓN

FACULTAD CIENCIAS JURIDICAS Y SOCIALES

PROGRAMA DERECHO

CIBERDELITOS EN LA LOCALIDAD DE SUBA EN BOGOTÁ

Línea de investigación:

COMPORTAMIENTO HUMANO, CONDUCTA PUNIBLE Y ORDENAMIENTO JURÍDICO PENAL.

Presentan:

LUIS FERNANDO PARRA ROSALES

LUIS DANIEL MOLINA CORONEL

MARÍA PAZ TODARO PEDROZO

ALFREDO MELGOSA FIGUEROA

GABRIELA DEL CARMEN BARRETO ANGULO

MARÍA ISABEL PADILLA CASTILLA

Profesor Tutor:

Sandra Viviana Díaz Rincón

Trabajo de investigación

18/05/2023

BARRANQUILLA, ATLÁNTICO
REPÚBLICA DE COLOMBIA

INTRODUCCIÓN

El presente trabajo es producto de la investigación sobre todo lo concerniente al Ciberdelito precisamente en Bogotá. Según el coronel Julián Buitrago, del centro cibernético de la Dirección de Investigación Criminal, esta es la ciudad capital donde los delitos informáticos que más ocurren son el hurto de información, suplantación de identidad y hurto de páginas web; vulnerando y afectando directamente a las víctimas en su intimidad documental, revelando los secretos, las conversaciones o simplemente comunicaciones privadas que deber ser respetadas. Asimismo, se desarrolla un odio interno con aquella persona o aquella empresa en la cual se llevará a cabo este acto tan atroz.

Es de vital importancia mencionar que la inseguridad cibernética se ha convertido en un flagelo no solo en Colombia, sino en todos los países del mundo, problema bastante complejo que requiere de la intervención de los gobiernos, situación que se ha vuelto dramática perjudicando a muchas personas que han sido víctimas de este tipo de delitos. Es importante mencionar que el nacimiento de las redes informáticas conllevó a la proliferación de esta forma de delinquir, por lo cual es imprescindible analizar y profundizar acerca de los motivos por los que se han proliferado este tipo de delitos, donde las redes de la información han contribuido mucho a la proliferación de estos. Es de anotar que el internet ha pasado por diversas etapas, y de acuerdo con su evolución y desarrollo esto ha permitido que aparezcan las nuevas formas de delinquir relacionadas con la sistematización.

Debido al surgimiento de nuevas tecnologías, los ciberdelincuentes han buscado la manera de delinquir en redes sociales y en todas las plataformas informáticas, valiéndose de cualquier medio con fines delictivos, frente a la ventaja que tiene cada persona de contar con un dispositivo electrónico, existe el riesgo de que se pueda materializar un delito, no obstante, los ciberdelitos están más sesgados hacia los menores de edad, debido a la vulnerabilidad a los que estos se encuentran expuestos.

Por lo anterior es de suma importancia la investigación expuesta en el presente trabajo, ya que permite analizar de una manera más profunda y sobre todo detallada, las técnicas preventivas frente a los delitos informáticos, así como lo referente a la

punibilidad de estos, buscando la protección tanto de las victimas como de las plataformas en juego.

Asimismo, pretende explicar la posición, avances y la normatividad en general de la legislatura colombiana frente al ciberdelito; que a medida que ha avanzado el tiempo y las tecnologías, se ha tenido que adaptar a un contexto jurídico-informático para poder regular el alta en los delitos informáticos.

Con el desarrollo de esta investigación se busca analizar a fondo las causas y efectos de los ciberdelitos, previniendo las conductas ilícitas que afectan los datos informáticos de las víctimas, utilizando las nuevas tecnologías que avanzan día a día. De esta manera, se hace necesario la actualización de estos ciberdelitos para garantizar la seguridad y combatir la ciberdelincuencia que ataca constantemente en la sociedad.

A nivel nacional, se puede destacar la evolución que ha tenido la legislación colombiana, frente a la regulación y tratamiento que se les ha dado a los delitos informáticos; esto debido al acelerado incremento en la masificación y utilización de medios electrónicos para adelantar las distintas actividades cotidianas. Las políticas públicas que han mejorado en gran medida el acercamiento de elementos de cómputo e informáticos, la necesidad de interactuar y expandir el campo de acción de diferentes sectores públicos y privados, la apertura económica que trae consigo la facilidad de obtener distintas herramientas tecnológicas, generan una mayor disponibilidad para que todo tipo de información sea más accesible, incluyendo aplicaciones, medios y métodos para llevar a cabo un ataque informático (Montañez, 2017).

Sabiendo que el delito del ciberdelito está tipificado en el ordenamiento jurídico colombiano, los accionantes de este injusto continúan con realizando dichos actos, esto gracias a la alta demanda que han tenido los aparatos electrónicos los cuales han sido adquiridos por muchos nacionales a lo largo de estos 3 años post pandemia. La obtención de estos productos genera más entusiasmo para los trasgresores de la ley a delinquir con más facilidad debido a la poca seguridad informática que los adquisidores tienen en su conocimiento, la gran no tienen la capacidad cognitiva de instalar un programa con el cual mantengan a salvo toda la información que guardan, las contraseñas de sus redes sociales, de sus correos electrónicos, etc.

Según Blu Radio, en uno de sus artículos, afirman que Colombia es el país con más ciber-extorsiones en la región. De igual manera, explican uno de los métodos más recurrentes por los cuales los ciberdelincuentes actúan; un simple enlace enviado a cualquier dirección de correo electrónico puede llevar a colapsar y bloquear los sistemas que se consideran más seguros.

> Desde el Departamento Administrativo Nacional de Estadística (DANE), el Invima, por el cual los ciberdelincuentes pedían un pago de cinco millones de dólares en criptomonedas, hasta EPS Sanitas y la más reciente víctima, EPM, demuestran el alto riesgo que representa un malware de rescate o ransomware, que impide a los usuarios acceder a su sistema o a sus archivos personales, exigiendo el pago de un rescate para poder acceder de nuevo a ellos (Maldonado, 2022, p. 34).

PLANTEAMIENTO DEL PROBLEMA

El Ciberdelito en la localidad de Suba en Bogotá-Colombia refleja un crecimiento gradual en el número de incidentes cibernéticos reportados a las autoridades del ecosistema de ciberseguridad. Este se ha convertido en la tipología criminal de mayor crecimiento en Bogotá durante los últimos tres años; impulsado por aceleradores como la pandemia y el consecuente incremento del comercio electrónico que conllevó la situación. Respecto a eso, ¿Cómo afecta el ciberdelito a la comunidad bogotana?

El principal interés de los Cibercriminales en Bogotá se basa en la motivación económica y la posterior monetización de las ganancias generadas en cada Ciberataque; El delito informático más denunciado en Colombia es el Hurto por medios informáticos; los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banco.

Si bien la cifra obedece a los centros urbanos con mayor densidad poblacional y penetración de internet en el país, el factor de desarrollo económico influye en los objetivos de los cibercriminales, que enfocan su actuar con entidades financieras y grandes compañías. (Tanque de Análisis y Creatividad de las TIC, 2020).

Los sistemas informáticos y la tecnología a medida que evolucionan son más indispensables para la sociedad, ya que los usuarios centran sus actividades en estos

medios y les facilita la realización de diferentes funciones; sin embargo, existen problemas de seguridad que se han evidenciado por que los intrusos aprovechan la confianza, el descuido o falta de conocimiento de los usuarios para lograr obtener información confidencial o ingresar a los sistemas que los usuarios utilizan. A partir de lo anterior, se llega a generar el siguiente interrogante: ¿Cómo afecta el ciberdelito a las personas y empresas de Colombia y como minimizar los riesgos?

JUSTIFICACIÓN

El ciberdelito en Bogotá es un tema que debe ser abordado y requiere la obligación de comprender cómo se afectan los derechos de las víctimas del ciberdelito en Bogotá, como la protección de datos personales, la seguridad financiera, los bienes y propiedades e incluso la sexualidad, esto siempre basado en el análisis legal relevante bajo la legislación colombiana. Asimismo, pretende identificar los grupos con mayor susceptibilidad al ciberdelito, si existe un rango de edad establecido, o si los internautas presentan conductas o portales recurrentes que los hacen más vulnerables que otros, frente al uso y consumo de internet.

De igual manera, se pretende observar su evolución y tendencias, tanto como de la ley expedida que se le aplica a este acto delictivo, cuya regulación y normatividad se encuentra en la Ley 1273 de 2009, para entender de alguna manera como se ven vulnerados los sistemas de información de las personas que habitan en la ciudad capital, como consecuencia, señalar distintos procedimientos para la prevención y tratamiento de los riesgos que afectan la infraestructura tecnológica y la integridad, confiabilidad y disponibilidad de la información de esas entidades.

El ciberdelito se incrementa en la misma medida que evoluciona la tecnología, las víctimas pueden llegar a ser usuarios comunes que realizan tareas básicas, que por falta de conocimiento reciben un ataque o grandes empresas con información confidencial son vulnerables a los fraudes, virus informáticos, o cualquier tipo de delito que se encuentre en la red, lo cual puede causarles grandes pérdidas.

OBJETIVOS

OBJETIVO GENERAL:

- Analizar la conducta criminal de los habitantes de la localidad de Suba-Bogotá desde la criminología y el Derecho.

OBJETIVOS ESPECÍFICOS:

- Identificar en el ordenamiento jurídico penal, los delitos informáticos en Colombia.
- Interpretar la jurisprudencia de la Corte Suprema de Justicia entorno a la tipificación de los delitos informáticos en Colombia.

DELIMITACIÓN DEL PROBLEMA

El Ciberdelito es una problemática que afecta cada vez más a los ciudadanos en Colombia, especialmente en Bogotá, ciudad en la que los dichos incidentes cibernéticos se reflejan en mayor continuidad, incluyendo ataques de phishing a empresas y usuarios individuales, la creación y distribución de programas malignos y virus informáticos, y la explotación sexual infantil en línea. Además, las autoridades también están luchando contra el uso ilegal de criptomonedas para actividades delictivas.

De acuerdo con las investigaciones y los reportes obtenidos por las autoridades de ciberseguridad, la metodología que utilizan estos cibercriminales se basa en la vulneración y afectación de la víctima a nivel monetario tanto como de su intimidad; dentro de los delitos informáticos más concurrentes se encuentran la suplantación de identidad, el hurto de información como también, el hurto de páginas web, por lo que para prevenir el ciberdelito, es importante que los usuarios de internet tomen medidas de seguridad, como mantener sus contraseñas seguras y no compartir información personal en línea.

Las empresas también deben tomar medidas para proteger sus sistemas y datos, incluyendo el uso de software de seguridad y la capacitación del personal en seguridad en línea. Las autoridades están trabajando para combatir el ciberdelito, incluyendo la creación de unidades especializadas de investigación y la promoción de la colaboración entre las agencias de aplicación de la ley y las empresas privadas. Sin embargo, todavía

hay mucho trabajo por hacer para proteger a los ciudadanos de Bogotá y de Colombia en general contra el ciberdelito.

Por medio de esta investigación se permite dar a conocer las afectaciones que traen consigo los delitos informáticos a las víctimas y como crear prevención teniendo como base la práctica y metodología ya utilizada por dichos cibercriminales; de igual manera conocer dentro del ámbito jurídico el Ciberdelito e identificar la normativa que se encuentra tipificada para éstos.

DELIMITACIÓN ESPACIAL

Bogotá – Colombia.

DELIMITACIÓN TEMPORAL

Desde el año 2000 al presente año.

ESTADO DEL ARTE

La investigación a la que se hace referencia en el presente trabajo de grado se enmarca en el estudio de la tipicidad de los delitos informáticos en la dinámica del ecosistema digital sobre el cibercrimen y la ciberseguridad, en concordancia con las características que identifican la era del nuevo conocimiento que se ha fundamentado en los beneficios derivados de los avances tecnológicos; aunque la tecnología también ha sido utilizada con fines delictivos mediante los cuales han buscado infringir la normatividad penal y en consecuencia los bienes jurídicos tutelados a partir de la Ley 1273 de 2009, sin embargo, la evolución de la teoría del delito ha propiciado la generación de las conductas delictivas tendientes a la creación de nuevos delitos ciber en todas las áreas que aún no han sido reguladas por el Derecho Penal.

Respecto al plan metodológico de esta investigación; transcurre por medio de un enfoque paradigmático, bajo un enfoque cualitativo, que genera la posibilidad de establecer el desarrollo legislativo. Con el análisis ya generado a lo largo del trabajo investigativo, se generan distintas conclusiones, de las cuales puedo empezar indicando que se debe resaltar el esfuerzo generado por Colombia, con la creación de la ley 1273 de 2009, la cual fortalece el sistema jurídico frente a la nueva tendencia global, que se

basa en el tratamiento digital de la información; sin embargo, al generar un análisis detallado del articulado, se puede constatar vacíos, que pueden generar contradicciones, ya que si bien la ley pretende proteger la integridad, disponibilidad y confidencialidad de la información, se pueden generar errores en la interpretación, como se puede evidenciar en el artículo 269D, el cual indica: “Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes”. (Ley 1273, 2009).

Para dar la bienvenida al lector, y como primera medida se indica que el punto inicial de este trabajo es referente al concepto sociológico, dado para significar la base fundamental del problema; el ser humano entendido como un ser social que a lo largo de la historia ha evolucionado en cuanto a sus gustos, intereses, tendencias artísticas, literarias, gastronómicas, expectativas y prioridades; que dan origen y fin a distintas épocas, los cambios sociales han dado origen a distintas generaciones; inicio, para entender los fenómenos y eventos que están ligados a características culturales, éticas, y emocionales de personas que comparten una temporalidad similar a su fecha de nacimiento. Generación x, y, entre otras, hasta llegar finalmente la generación z; generaciones que empiezan con la llegada del internet, la generación del milenio; generación en la cual su vida gira alrededor de un mundo virtual.

Estados Unidos, España, México, Uruguay, y Chile, países que han sido ejemplo en cuanto a legislación informática, hasta llegar a nuestro país Colombia; que se posicionó como líder en la región al tener indiscutiblemente una de las más completas leyes en cuanto a delitos informáticos se refiere.

“Es posible afirmar que el objeto de esta es adquirir conocimientos de verdades ya descubiertas y procurar la solución de problemas prácticos mediante la aplicación de los principios generales de la ciencia jurídica” (Restrepo, 2012, p. 3). Por esta razón, se considera esta investigación de carácter jurídico, y a su vez responde a una investigación de tipo jurídico con un enfoque sistémico debido a que su objeto de conocimiento se fundamenta en el ordenamiento normativo y las falencias que de ello se han identificado

en el ecosistema digital; por lo que el problema de investigación se instituye a partir del análisis normativo de los delitos informáticos desde una perspectiva restrictiva y del sistema jurídico desde una visión extensiva. De igual manera, corresponde a una investigación de tipo cualitativo – exploratoria teniendo en cuenta la ausencia de estudios previos y de planteamientos metodológicos mediante los cuales se busque brindar solución al problema de investigación sub examine.

En relación con el método de investigación se utilizará el método teórico de tipo dialectico por medio del cual se busca el conocimiento y la transformación de la sociedad y del pensamiento. De igual manera, en relación con la técnica de recolección de información se analizarán e identificarán a través de una búsqueda generalizada en los informes 23 evaluativos sobre el informe de “Amenazas del cibercrimen en Colombia” que de manera anualizada presenta la Dirección de Investigación Criminal en cooperación con la Interpol. Finalmente, en relación con las fuentes de información se utilizarán de tipo secundario correspondiente a un estudio bibliográfico y normativo sobre los delitos informáticos desde un contexto nacional e internacional (Caso España).

Sin embargo, en virtud de la protección de los derechos fundamentales al habeas data, privacidad, intimidad e información se ha de constituir un sistema normativo efectivo de defensa judicial en lo que respecta a las políticas criminales del nuevo derecho penal que le corresponde crear al Estado para brindar y garantizar amparo a la seguridad de la información y los datos online. No obstante, so pena de existir en el ordenamiento un bien jurídico de carácter especial se ha de identificar únicamente nueve conductas punibles en el contexto de los delitos informáticos y frente a las cuales los continuos avances tecnológicos las ha evolucionado y desactualizado eminentemente. Jurídica de orden nacional para combatir a los delincuentes de cuello blanco denominados «hackers/crackers» quienes en las últimas décadas sin temor alguno han accedido sin autorización previa y fraudulentamente a las medidas de seguridad de la información, dejando de esta manera una gran afectación económica y social. Por lo que en observancia del evidente escenario en el cual se fundamentó el problema de investigación se ha de cimentar la propuesta de un modelo integral de protección de la

información y los datos en el área del derecho penal, debido a la necesidad de adecuar el sistema jurídico con el sistema digital y tecnológico.

En el presente trabajo de investigación se da por sentado la evolución y el marco conceptual de los delitos informáticos planteados por diferentes autores nacionales e internacionales, y establece la relación con la reciente Ley 1273 de 2009, mediante la cual la legislación colombiana se equipará con la de otros países en cuanto a la normatividad sobre el cibercrimen, que ha venido vulnerando distintos campos de las relaciones y comunicaciones personales, empresariales e institucionales. El ciberdelito, como tendencia que incide no sólo en el campo tecnológico sino también en el económico, político y social, debe ser conocido, evaluado y enfrentado, por lo cual el análisis de la norma, su aporte y alcance puede dar otros elementos de juicio para entender la realidad de nuestras organizaciones y visualizar sus políticas y estrategias, a la luz de la misma norma y de los estándares mundiales sobre seguridad informática.

La variedad, amplitud y complejidad de los sistemas de información que adquieren, requieren o encuentran disponibles las organizaciones actuales, junto a la dinámica del permanente cambio observado en las tecnologías de la información y las comunicaciones, han impulsado de múltiples formas y, al mismo tiempo, condicionado las grandes transformaciones de las organizaciones, los mercados y el mundo de la modernidad y de la posmodernidad. Son cambios que, además de sus innegables ventajas, han traído simultáneamente para las personas y las organizaciones, amenazas, riesgos y espectros de incertidumbre en los escenarios de internet, intranet, desarrollo tecnológico, gestión de la información, la comunicación y los sistemas.

Con cada vez mayor frecuencia y mayor impacto, los dispositivos de almacenamiento y procesamiento de información -llámense servidores, estaciones de trabajo o simplemente PC- son vulnerados en sus elementos más sensibles, dejando expuestos no sólo múltiples y significativos datos de distinto valor, sino los mismos patrimonios reales de personas y organizaciones y, aún más, su dignidad, su honra y su vida.

Con los sistemas informáticos ha ocurrido algo similar a lo observado en la historia. Pocas personas, en la actualidad, pueden abstraerse del contacto directo o

indirecto con un sistema de cómputo, lo cual muestra de distintas maneras el poder y alcance de la tecnología informática en las sociedades del mundo.

El importante y dinámico cambio que ha condicionado los nuevos comportamientos sociales, económicos, políticos y éticos de las personas y los pueblos, ha venido acompañado de un no menos dinámico y, a la vez, peligroso proceso de una nueva delincuencia que, al utilizar o impactar los sistemas de información y comunicación de las organizaciones y el mundo, ha llegado a posicionarse como uno de los cada vez mayores peligros para la seguridad, la honra, vida y bienes de las personas y las organizaciones de todos los países.

Como consecuencia, se han diseñado, divulgado y aplicado no sólo modelos, sistemas, herramientas y procedimientos de seguridad informática, sino también el necesario complemento legal para combatir el delito, además de la capacitación y preparación especializada para manejar estos componentes de seguridad, de manera integrada y cada vez más generalizada entre la sociedad. Por esta misma razón, sus condiciones de vulnerabilidad y gestión del riesgo informático pueden señalar un derrotero para orientar las normas, políticas, estrategias y procedimientos que permitan enfrentar tal amenaza y velar por la seguridad de toda la Sociedad.

En este ítem está inmerso el concepto de espionaje no es unívoco y se vincula con distintos comportamientos. En cambio, la noción de espionaje en un sentido jurídico penal encuentra sus principales raíces en el delito del mismo nombre, figura atentatoria de la seguridad del Estado, que se regula en el artículo 109 del Código Penal y en los artículos 252 y ss. del Código de Justicia Militar. Se trata de una conducta relacionada con el concepto de “violación de secretos”, que puede expresarse ya sea mediante la introducción indebida en la esfera del secreto (intromisión), o bien, a través de la difusión indebida del secreto al que se ha tenido acceso legítimamente.

El delito de espionaje informático genera una serie de dificultades interpretativas y de delimitación de su injusto. Ellas se hacen más patentes si se considera que el análisis dogmático de la delincuencia informática es aún incipiente y que el espionaje informático ha tenido un escaso tratamiento doctrinal, si se lo compara con otras figuras que integran este sector de la criminalidad, en especial con el fraude informático. En

primer lugar, el sentido y alcance de aquello que denominamos «espionaje informático» no es evidente.

En segundo lugar, tampoco es claro cómo castigar el espionaje informático de acuerdo con el derecho penal vigente en todos los supuestos que pueden calificarse de tales. Así, ya que no todos los casos constitutivos de espionaje informático se ejecutan de igual forma ni tienen idéntica gravedad, pueden surgir dudas al momento de aplicar una misma hipótesis legal a casos que efectivamente son disímiles. Si se considera, además, el bien jurídico subyacente al espionaje informático, es posible que a las normas de la Ley 19.223 se superpongan otras de penalidad no necesariamente equivalente, como los delitos contra la intimidad o privacidad regulados en el Código Penal. En tercer lugar, no debe perderse de vista que vivimos en una «sociedad de la información», caracterizada por la disponibilidad y el intercambio constante de datos entre los individuos a través del uso de tecnologías.

Lo señalado no sólo plantea desafíos en cuanto a la necesidad de identificar de manera adecuada el injusto del comportamiento a castigar, sino también respecto de qué vamos a exigir de una persona, que es titular de información o está a cargo de ella, para salvaguardar esa información del acceso indebido de otros.

El espionaje informático provoca diversos problemas interpretativos y de delimitación de su injusto. Por otro lado, el hecho de que se viva en una sociedad de la información, en la que existe disponibilidad e intercambio permanente de datos, puede generar dificultades al momento de sancionar el acceso a los mismos.

De tal manera, implica un acceso a y conocimiento indebido de datos. Se trata de un concepto estrechamente relacionado con el de intromisión relativa a datos que no han de ser revelados, pues existen intereses contrarios a que ellos sean conocidos. Tratándose de casos en los que se verifica un acceso indebido a datos, tal conexión puede dar lugar a relaciones concursales, sin perjuicio de que el espionaje informático sirva para colmar vacíos de punibilidad existentes en ciertas descripciones típicas.

Por último; para definir el injusto del espionaje informático, resulta clave analizar el concepto de información penalmente relevante. La tipificación del espionaje

informático en la Ley 19.223 es fuente de inconvenientes, que deberían ser revisados en una futura reforma legislativa. Por último, la propuesta de reforma del espionaje informático en actual trámite parlamentario presenta algunos avances respecto de la regulación contenida en la Ley 19.223, en especial en lo que se refiere a la superación de barreras técnicas o medidas tecnológicas de seguridad.

En este ítem como referente se tiene a Colombia, el desarrollo académico referente a los temas de ciberseguridad y ciberdefensa se ha centrado en un análisis de la regulación normativa e institucional de dinámicas variadas presentes en el ciberespacio, y ha dejado de lado el nivel de autonomía que han tenido las fuerzas militares en la gestión de seguridad y defensa en el ciberespacio. dicha autonomía siempre ha estado supeditada a un control por parte del poder civil, que se establece por medio de instituciones jurídicas y políticas que garantizan un equilibrio para la conducción del estado y la especialidad de sus funciones correspondientes. sin embargo, debido a que las nuevas amenazas debilitan el marco establecido, estas reglas requieren de un proceso constante de revisión y construcción con el fin de hacer frente de manera oportuna a dichas amenazas.

La investigación que se hace en este artículo se propone explorar el desarrollo institucional acerca del dominio del ciberespacio en Colombia y su incidencia sobre las relaciones cívico-militares en el país. para ello, recurre a un análisis de fuentes primarias y secundarias, con el propósito de definir el ciberespacio y las ciber amenazas que surgen en él, así como describir las relaciones cívico-militares en Colombia y explicar el marco institucional referente a la seguridad y defensa del ciberespacio en el país. en este caso, y en contraste con la tradición del país, se evidencia que la iniciativa surgió del sector civil, lo que promovió una mayor participación de este sector en el campo de la seguridad y defensa. así, la agenda de ciberseguridad y ciberdefensa puede ser la punta de lanza para replantear las relaciones cívico-militares.

La definición de la política de ciberseguridad y ciberdefensa en Colombia constituye un interesante punto de análisis en el marco de las relaciones cívico-militares en el país, dado que tradicionalmente fueron las fuerzas militares, en su espacio de autonomía, las encargadas de definir las prioridades y lineamientos en materia de

seguridad y defensa. esa autonomía debe ser redefinida en atención al contexto actual de surgimiento de nuevas amenazas y de necesidad de una política de ciberdefensa y ciberseguridad del estado. es en esta política donde se observa un intento de redefinir las relaciones cívico-militares, ya que los civiles se han involucrado más en la definición de prioridades al respecto.

Se realiza un análisis detallado de la situación actual de la ciberseguridad y ciberdelincuencia en Colombia, destacando los principales desafíos y retos que enfrenta el país en este ámbito, en la investigación llevada a cabo, el autor destaca la falta de conciencia y cultura de seguridad informática en la sociedad, la falta de recursos y capacitación en el ámbito de la ciberseguridad, la ausencia de una estrategia nacional de ciberseguridad, y la necesidad de fortalecer la cooperación y coordinación entre las diferentes entidades públicas y privadas involucradas en la prevención y sanción de los ciberdelitos como los principales desafíos, Ramírez propone una serie de recomendaciones para abordar estos desafíos, entre las cuales destacan la necesidad de aumentar la inversión en ciberseguridad y fortalecer la formación y capacitación en este ámbito, el establecimiento de una estrategia nacional de ciberseguridad, la creación de un marco legal actualizado y eficaz en materia de ciberdelincuencia, y la promoción de la cooperación y coordinación entre los diferentes actores involucrados en la lucha contra los ciberdelitos.

Los autores destacan que la ciberdelincuencia en Colombia es un fenómeno en aumento, y que ha sido impulsado por el rápido crecimiento de la tecnología y la conectividad en el país. Además, señalan que los ciberdelitos más comunes en Colombia incluyen el robo de identidad, el fraude electrónico y el phishing, Bernal y Núñez también analizan los factores que contribuyen al aumento de la ciberdelincuencia en Colombia, entre los cuales destacan la falta de cultura de seguridad informática en la sociedad, la falta de regulación y control en el uso de la tecnología, y la falta de coordinación entre las diferentes entidades encargadas de prevenir y sancionar los ciberdelitos, los autores proponen una serie de recomendaciones para abordar la problemática de la ciberdelincuencia en Colombia, incluyendo la necesidad de promover la cultura de seguridad informática en la sociedad, la implementación de medidas de regulación y

control en el uso de la tecnología, la mejora de la coordinación y cooperación entre las diferentes entidades involucradas en la prevención y sanción de los ciberdelitos, y la implementación de políticas y estrategias específicas para combatir la ciberdelincuencia.

En la siguiente sección se tiene como referente el sector de servicios financieros y como enfrenta desafíos en el desarrollo de actividades que requieren la utilización de tecnologías de la información y las comunicaciones, debido a que están expuestas a una serie de riesgos como cibercrimen, que pueden afectar la confianza en la marca de la empresa y en el servicio. con el fin de hacer frente a estos desafíos, ACH Colombia desarrolló un proyecto para anticipar y prevenir los riesgos relacionados con los crímenes informáticos, utilizando herramientas que faciliten el análisis de información para la toma de decisiones. adicionalmente, ha diseñado e implementado un modelo de prevención especial para el botón de pagos, que es uno de los servicios que esta compañía presta a las entidades financieras, personas jurídicas y naturales y entidades públicas. el presente artículo pretende presentar algunos resultados del proyecto.

Se han considerado focos de vulnerabilidad aquellas situaciones que permiten mayores actividades de fraude, condiciones o actividades que atentan contra las entidades del sistema financiero, y en el caso de los bancos que ponen entre dicho la imagen de entidades seguras y confiables. haciendo una analogía, en el pasado, las entidades bancarias basaban su prestigio en la protección de sus valores con grandes cajas fuertes y recintos con altos estándares de seguridad e impenetrabilidad. de esta manera, la entidad bancaria protegía su principal activo de ataques de criminales y en la actualidad, esa relación entre recinto físico “seguro” y seguridad de los valores del banco, ha evolucionado. aquellos esquemas de seguridad han cambiado, de la misma forma que el concepto de valor que tienen los clientes. actualmente, aquellos elementos físicos que contenían el dinero de los clientes son grupos de datos virtuales, los cuales pueden ser administrados a través de la internet.

Los valores se han convertido en datos que migran a nuevos sistemas de contención; la caja fuerte se ha transformado en un disco duro, o espacio en la nube. esto representa un nuevo reto en términos de seguridad en el sector financiero y bancario. los sistemas de pago han sufrido el mismo tipo de transformación de tal forma

que actualmente el servicio que se prestaba por medios análogos como el dinero, o a través de tarjetas débito y crédito, hoy en día se realizan a través de medios computarizados. en el mercado diariamente se realizan cantidades importantes de transacciones financieras a través sistemas de pago electrónicos o por medios informáticos que tienen diferentes características de seguridad y posibilidad de acceso. uno de esos sistemas es el botón de pago electrónico, que permite realizar pagos en línea como un servicio alternativo a las tradicionales tarjetas de crédito.

Las estrategias de reducción a nivel de sistema pueden tener un impacto más grande en la disminución de fraude, que las estrategias individuales. es decir, al desarrollar este tipo de actividades de manera colaborativa, es posible tener un mayor nivel de impacto con respecto a los posibles resultados de la implementación a nivel de bancos, comercios o incluso a Colombia a nivel individual. a pesar de tener una estrategia de sistema, se hace necesario que cada entidad financiera, así como el prestador del servicio de pago (ACH Colombia) implemente estrategias individuales que tengan en cuenta el tipo de mercado, la diferencia entre clientes, las particularidades de su negocio, de tal forma que sea posible cerrar los focos de fraude a nivel individual y posteriormente, facilitar la identificación y cierre entre comercios y bancos.

La implementación del proyecto ha permitido detectar y generar disminuciones en la ocurrencia del fraude. sin embargo, la tipología de fraude varía de manera constante. por esta causa, la alimentación prolongada de los sistemas de información es fundamental para identificar patrones que antes no eran evidentes, de manera que sea posible seguir afinando las reglas y el modelo establecido para prevención de fraude.

La presente investigación se desarrolla para analizar e identificar las falencias existentes en la legislación colombiana en cuanto a delitos informáticos y el impacto que ha tenido en las empresas con respecto a los países de Latinoamérica, desde la perspectiva y lineamientos del “convenio de ciberdelincuencia de 2001, convenios existentes sobre ciberdelincuencia y ciberdelito en Colombia y las leyes colombianas implementadas que los tipifiquen, porque el especialista de seguridad informática necesita conocer la posición que ha tomado su país en la defensa y preservación integral de los sistemas informáticos en contra de los ciberdelincuentes, como personas y desde

cualquier campo de la ciencia, cada colombiano está llamado a realizar aportes que contribuyan al fortalecimiento de la seguridad, y desde la ingeniería de sistemas, aún más, desde el punto de vista de los especialistas en seguridad informática debe existir una preocupación más alta por formular alternativas de mejora y es que, seguridad cibernética debería no ser algo de cada país individual ya que una nación por sí sola no puede asegurar adecuadamente sus redes.

El presente proyecto es una investigación que se basa en la revisión bibliográfica y analítica, por medio del desarrollo del tema de delitos informáticos y el cibercrimen a través de comparativos a partir de una línea base de investigación sobre el tema escogido. por otro lado, se tomó como herramienta de recolección y análisis de información el análisis documental, desde las normas de tipificación de delitos informáticos, normatividad y revisión de convenios internacionales como el conpes, comparativos de los distintos delitos y casos reales, análisis de la ley colombiana contra las leyes de Latinoamérica y otros países externos.

Este documento al ser de carácter analítico, y por medio de generación de cuadros comparativos, sobre la normatividad en Colombia, la tipificación de los delitos informáticos ubicados en Latinoamérica y Colombia, y dentro del desarrollo de este proyecto se muestran y analizan las diversas técnicas de cibercriminalidad que se cometen con más frecuencia en Colombia; por lo que es posible evidenciar que Colombia aún tiene huecos y baches en los que se pueden cometer delitos difícilmente tipificarles y no contemplados en la ley actual, pero que son bastante graves y delicados por sus características en los ámbitos de seguridad informática y que se puedan sancionar correctamente, algunos que pueden incluso dejar daños irreparables en todos los entornos de desarrollo y crecimiento de los diferentes países de Latinoamérica y Colombia y sus usuarios. de este modo, se puede concluir que la ley 1273 de 2009 esta desactualizada y requiere que se le dé un estudio por parte de las autoridades responsables, en el cual se pueda contemplar adiciones, ajustes tanto a los actuales artículos como la generación de los faltantes, con el fin de dar una tipificación acorde al delito, afección y perjuicio, estas mejoras a la ley de delitos informáticos podría establecer un bien reglamentario y judicial que vaya de la mano con las necesidades,

penalizaciones que cada delito realmente se merezca, y es que un factor de ciberdelincuencia actual es que se dejan pasar muchas cosas que aunque mínimas son el inicio de delitos más graves.

La aparición de los delitos en el espacio cibernético ha planteado nuevos desafíos al derecho tradicional. este nuevo escenario delictivo exhorta a la doctrina especializada a plantearse si son adecuadas para la ciberdelincuencia las respuestas penales creadas para cubrir el espacio físico tradicional.

> Son solo muestras de ello las novedosas características técnicas, lógicas y de uso del tic (tecnologías de la información y la comunicación), la cuestión de la cifra negra en los ciberdelitos, la contribución de la víctima desde un plano victimológico, la reinterpretación de las reglas espaciotemporales, la superior capacidad lesiva de estos injustos o la pluralidad de potenciales víctimas existentes (Gorostidi, 2020, p. 5).

Desde el momento en que se entra al ciberespacio ya sea desde un celular, un televisor inteligente o un reloj, toda persona es vulnerable de convertirse en una posible víctima de los ciberdelincuentes, debido a que este espacio brinda muchas oportunidades para que se materialice un ciberdelito.

En esta investigación se eligió utilizar la investigación cualitativa, la cual atraviesa varias etapas en su desarrollo uno de ellos es la recolección productiva de datos, a partir de estos y secuencialmente se establecen otras etapas como el análisis de estos , es decir que partiendo del problema es necesario establecer que información relevante aporta el problema de investigación , se analizan estos datos para poder luego hacer una entrada al campo que no es más que observar e identificar otros rasgos que no fueron definidos en la recogida de datos y que resultan más sensibles a la observación para finalmente analizar cada uno de estos datos suministrados y hacer difusión de estos (Rodríguez-Gómez et al, 1996).

Debido al surgimiento de nuevas tecnologías, los ciberdelincuentes han buscado la manera de delinquir en redes sociales y en todas las plataformas informáticas, valiéndose de cualquier medio con fines delictivos, frente a la ventaja que tiene cada

persona de contar con un dispositivo electrónico, existe el riesgo de que se pueda materializar un delito, no obstante, los ciberdelitos están más sesgados hacia los menores de edad, debido a la vulnerabilidad a los que estos se encuentran expuestos.

Colombia cuenta con la normatividad suficiente en materia preventiva y sancionatoria frente a la comisión de delitos informáticos, empezando con la constitución política de 1991 la cual es garante de los derechos fundamentales vulnerados a causa de estos delitos además de la Ley No. 1273 de 2009, en la que se tipificaron los ciberdelitos, complementado el código penal, sin embargo, es necesario establecer los mecanismos de control para la vigilancia y la aplicabilidad del marco legal.

Secuencialmente en este acápite se dará a conocer por primera vez lo que se ha detallado con cada una de las modalidades de mayor afectación e Impacto señalando los actores que intervienen en la cadena criminal e identificando cuáles son los principales métodos de engaño que emplean los criminales a la hora de facilitar y acometer los ataques. Es claro que para enfrentar una amenaza es importante conocer cómo actúa y que puntos débiles internos de la organización aprovecha. Identificar las vulnerabilidades oportunamente permite entonces corregir los fallos en la seguridad e infraestructura e implementar planes de mejoramiento que abarquen desde los recursos tecnológicos, humanos y del proceso mismo afectado en el incidente presentado. La dinámica actual del Cibercrimen en Colombia refleja un crecimiento gradual en el número de incidentes cibernéticos reportados a las autoridades del ecosistema de ciberseguridad A través de los canales de atención a empresas y ciudadanos dispuestos por la Policía Nacional fueron registrados 28.827 casos durante el 2019 (Tanque de Análisis y Creatividad de las TIC, 2020).

Sin importar el escenario del Ciberataque y la complejidad que este signifique para la empresa, todas las organizaciones deben prepararse para gestionar un incidente cibernético y esa labor previa involucra a todos los empleados y directivos, por lo que es muy importante saber cuáles son los roles y responsabilidades que tiene cada uno de los actores involucrados en el plan de respuesta y gestión de un incidente cibernético. La formación y concienciación en ciberseguridad contribuyen en esencia a que cada integrante de la organización identifique los riesgos y las amenazas a las que está

expuesta la compañía y como se convierte en la primera barrera de contención de un ataque. La Ciberseguridad es un compromiso de todos.

En el presente capitulo se evidencia las múltiples posibilidades que brindan las nuevas tecnologías de la comunicación y la aparición en escena de un nuevo espacio, el virtual o ciberespacio, en materia de delincuencia, facilitando la afectación de bienes jurídicos a una distancia y con una velocidad impensadas, resulta un lugar común la afirmación de estar en presencia de una problemática frente a la que el proceso de homogeneización legislativa y de cooperación en los ámbitos sustantivos y adjetivos, es una necesidad ineludible si se quiere evitar la existencia de "paraísos" de impunidad.

> El Delito informático es la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software" (Davara, 2002, p. 23).

Se hará un análisis de nuestra carta magna, existen normas que se relacionan directamente con la información y por ende se convierten en el sustento de firmeza superior para fundar los llamados delitos informáticos. Es así como encontramos en el artículo 15 de la Carta Política, en lo concerniente a la intimidad de las personas y el artículo 20 relativo al derecho de información. La Constitución Política de Colombia si otorga a través de sus principales normas que consagran como derechos fundamentales, tales como los artículos 15 y 20, un respaldo suficiente como para que el legislador consagre normas tendientes a desarrollar.

La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos, se deben adoptar mejores medidas para tener mayores conocimientos en tecnologías de la información; a través de ellas se permitirá tener un marco de referencia aceptable para el manejo de dichas situaciones, ello porque, se poseen pocos conocimientos y experiencias en el manejo de entornos en donde se puede ser fácilmente sujeto pasivo de los ciberdelincuentes. Con la normatividad creada por Colombia respecto a los delitos informáticos y el Convenio de Budapest se buscó blindar a las Instituciones públicas o privadas y a las personas en contra ataques de la ciberdelincuencia.

Este documento, tiene como propósito generar conciencia, una visión clara a los consumidores acerca del conjunto de problemas al usar esta tecnología, por ejemplo; la seguridad de los datos, seguridad física, seguridad lógica, ataques, intrusiones en el hogar, comunicación con niños, ataques personales, grabación remota, se realiza una serie de recomendaciones acerca del uso adecuado de la red, sea cableada o wifi, evidenciando algunos métodos de seguridad y criptografía.

Dentro de esta nueva tecnología de los dispositivos inteligentes IoT, en las viviendas y edificios inteligentes, es de vital importancia de conocer sus usos, beneficios que trae, facilita la tarea, reduce tiempos, permite controlar todo desde el celular, las luces, cerraduras, cámaras, audio doméstico, puerta de garaje, persianas de las ventanas, y cualquier cosa con un enchufe. Estos nuevos dispositivos son geniales, pero es bueno conocer todos los riesgos asociados al implementar esta tecnología.

Estas nuevas tecnologías se caracterizan en primer lugar por la inmaterialidad e intangibilidad de las mismas es decir no se pueden tocar están basadas en software, que por la naturaleza de dichas tecnologías en muchas oportunidades solo se pueden ver en un ordenador, pero no palpar, un ejemplo de ellos se evidencia en que la mayoría de las personas tiene conocimiento del internet, como funciona, pero no lo puede tocar, así funcionan la mayoría de aplicaciones mediante las cuales se efectúan las actividades del ser humano.

En este sentido, se aborda el tema del Ciberdelito y su tipificación en el COIP, por cuanto se considera un tema sensible y factible de vulnerabilidad dado el uso frecuente y esencial en que se ha convertido el uso de las TIC actualmente en distintas áreas del quehacer cotidiano. Constituyendo así, un medio por el cual todos los seres humanos han podido realizar actividades que con anterioridad le eran imposibles, y que en estos tiempos se pueden efectuar de una manera más rápida y eficaz. Por tanto, la tecnología ha tenido un impacto global, en materia de salud, en materia bancaria, en materia informática y en todos los aspectos de la vida del ser humano. Es por esta razón, que el sistema informático debe ser debidamente regulado ante la ola de criminalidad digital que puede observarse a través de diversas plataformas virtuales, las cuales es

responsabilidad del Estado establecer las bases jurídicas adecuadamente para sancionar a los infractores de delitos cibernéticos.

En este ítem se ha realizado en torno a los riesgos y la prevención del uso de internet en niños y adolescentes. Así mismo, se pretende indagar, conocer y clasificar herramientas y estrategias formativas, que sirvan como punto de partida para el fomento de una educación continua que promueva la práctica de valores y el uso de normas que les permitan a los niños y jóvenes, protegerse de los peligros que se dan, en el uso del mundo digital.

Para los niños y adolescentes, el mundo gira en torno a lo digital, tanto en el plano académico, como en el social: amistades, entretenimiento y ocio. Los más jóvenes manejan la tecnología como verdaderos expertos, pero en muchos casos no han desarrollado completamente el sentido crítico para reconocer riesgos y abordarlos de forma eficaz, por esta razón constituyen un grupo de alta vulnerabilidad, especialmente frente al uso incontrolado del mundo digital, puesto que, a su edad, en las actuales condiciones, aún no cuentan con la madurez y una educación adecuada para un uso responsable de los entornos digitales.

En este ítem se desarrolla de La justificación de llevar a cabo esta investigación se planteó debido a la necesidad de contribuir a la consolidación y referenciación sobre la tipificación y tratamiento jurídico-legal por parte de organismos internacionales generadores de soft law en la materia y los avances de hard law por parte de países de manera individualizada y comunidad de países ante diferentes tratados y acuerdos comerciales de carácter bilateral y multilateral. Igualmente, la proliferación de diferentes tipologías de ciberdelitos, dado el auge del uso del Internet y las TICs en todos los ámbitos de la sociedad global y la existencia de vacíos teóricos y uniformes para castigar, prevenir y penalizar el delito informático, son razones que justifican este tipo de investigaciones. El delito informático no sólo afecta Colombia sino a todos los países, puesto que en la medida del crecimiento de la sociedad de la información, el uso de las TIC, las redes sociales en todos los ámbitos económicos, sociales, políticos y culturales, obliga a los organismos internacionales y estados nacionales a realizar un frente común a través de la modificación de las leyes que protejan y castiguen la ciberdelincuencia,

que ha traspasado fronteras y se vuelve cada vez más compleja en su identificación y aplicación de la normatividad en esta materia.

En este ítem sé analizar y observar la investigación que tiene un amplio punto de partida, y es que a raíz de la interacción humana a través de los medios de comunicación e información relacionados con las redes que comparten datos, se ha dado pie a un sin número de nuevas conductas que afectan a esos, también nuevos, bienes jurídicos tutelados en los ordenamientos penales relacionados con la información, la intimidad y los datos, o en otras ocasiones, la utilización de los medios informáticos, electrónicos y de las telecomunicaciones se han convertido en herramientas para la comisión de los tipos penales tradicionales. Son estas situaciones, las que nos han llevado a los diferentes planteamientos y cuestionamientos que han permitido el nacimiento de esta investigación. Analizando un caso aleatorio de una conducta ilícita realizada en cualquiera de las modalidades descritas anteriormente, nos encontramos con que los sujetos activos y pasivos del delito pueden encontrarse a miles de kilómetros de distancia, no solo con culturas, idiomas y costumbres diferentes, sino con sistemas legales y de justicia penales que pueden tornarse completamente contradictorios donde no logre realizarse una correcta persecución de la conducta que ha vulnerado los bienes jurídicos tutelados y que de esta forma pueda materializarse uno de los preceptos de reparación para la víctima.

El presente documento hace referencia a la importancia de la ciberseguridad en Bogotá, viéndose como un factor de riesgo muy grave donde hay que atacar y combatirlo. Es decir, para lograr mantener la integridad, confidencialidad y disponibilidad en la información, es básico si se pretenden lograr los objetivos corporativos. Para que los anteriores principios sean efectivos, se requiere la implementación de pautas que sean adoptadas como cultura en las entidades, lo cual implica un compromiso verdadero de todas las personas involucradas en su gestión. Este documento dará un enfoque para conocer algunos lineamientos de política de ciberseguridad en Colombia, legislación relacionada, antecedentes y conceptos propios de la ciberseguridad.

En este documento está evidenciado el desarrollo en proyectos que benefician y ayudan con la ciberdefensa. De tal manera, este proyecto incluye solo información de

fuentes abiertas, es decir, datos públicos difundidos en redes sociales y no información privada. Es decir, el mismo ejercicio que vienen haciendo de tiempo atrás las empresas de marketing para conocer el impacto de una nueva marca. Hacia el futuro, aseguran (Ramirez Sanchez & Campo-Archbold, 2021), el proyecto de investigación planea aumentar las características consideradas en el análisis de tuits. Esto permitirá hacer una evaluación más profunda de la información obtenida y detectar patrones avanzados de amenazas especializadas contra las próximas víctimas, cuidando y deteniendo estos ciberdelitos.

En este documento tiene como propósito dar a conocer recomendaciones para prevenir un ciberdelito, refiriéndose a:

- Inspeccionar el mensaje, corroborar el dominio y la gramática del contenido cuando utilices alguna aplicación.
- Usar una red segura al momento de buscar ofertas, evitar las redes públicas.
- Configuración de alertas bancarias en caso de efectuarse alguna sin permiso, la autenticación sigue siendo un aliado en este sentido.

Hay que verificar que la URL de la página en cuestión tenga el candado de sitio seguro.

- Control sobre las cookies, y es que al aceptarlas le está abriendo la puerta para que internet conozca los hábitos de consulta, los gustos, entre otros.

Artículo en el cual se da a conocer de manera numérica/porcentual los ciber delitos cometidos entre el año 2021 y lo corrido del presente año, 2022, en donde teniendo en cuenta los estudios y estadísticas presentadas, el costo que abarcará el cibercrimen alcanzarían los 10.5 billones de dólares para el 2025; de igual manera este artículo nos presenta a CISOS y C2User conocidos como lo dice Alberto Samuel Yohai, presidente de la CCIT, como un espacio que trabajará bajo un enfoque metodológico innovador de ciberseguridad centrado en el usuario en el cual podremos encontrar las tendencias relacionadas al ciber delito.

En otras instancias este ítem muestra el informe anual de las tendencias del ciberdelito utilizado en Colombia y qué mecanismos de prevención serían los mejores a tomar frente a un altercado como estos, entre ellos, recomienda a las organizaciones en general la implementación de medidas de seguridad en cuanto a las redes informáticas.

El enfoque principal de este artículo es dar a conocer cuáles son los ciberdelitos más comunes en Colombia según el esquema de la Policía Nacional; como también el aviso y recomendaciones realizadas a la ciudadanía mediante los cuales se busca que disminuyan estos, y denunciar sin temor los posibles ciberdelitos.

– Estafa por compra o venta de productos: Este delito hace referencia al engaño por medio de productos que se desean adquirir o si bien por parte del delincuente, lograr su venta, en ambos puntos de vista, hallamos al delincuente como quien cumple el objetivo de incentivar o inducir a la víctima para ya sea la compra de un producto, teniendo como herramientas virtuales, imágenes de referencia no propios y originales que buscan atraer al público haciéndoles creer que dicho producto y sus asesores son de total confianza. Es importante tener precaución y estar alerta a posibles señales de alerta cuando se realice transacciones de compra o venta.

– Phishing (correos electrónicos falsos para pescar información confidencial): El Phishing es conocido como un método usual de ciberdelito, debido a que este resulta muy efectivo, debido a que por medio de sus datos electrónicos como es el correo personal y de más datos los cuales son sumamente importantes, los ciberdelincuentes logran crear en algunos casos vínculos que los conllevan a un acercamiento con la víctima, consecuente a ello, realizan el delito con mucha más eficacia y facilidad.

– Suplantación de identidad: Su función y objetivo consiste en hacerse pasar por una persona o en cuyo caso, victima, con finalidades como estafa, fraude u obtención de datos e información personal y confidencial. Los atacantes suelen hacerse pasar por una institución legítima como un banco, una empresa de correo electrónico o una red social. La suplantación de identidad puede ser una forma efectiva de engañar a las personas para que den información crítica y puede ser la primera etapa de un ataque más grande.

– Vishing: Consiste en las llamadas fraudulentas, estas van dirigidas a todo tipo de persona, pero, en su mayoría y por el monto monetario, sus principales víctimas son personas con un estatus alto, como empresarios, políticos, o personas del común pero estudiadas por estos mismos ciberdelincuentes, para lograr un engaño y consigo una ganancia exitosa, son 1.087 los casos registrados.

– Malware: El malware o también llamado software malicioso, está programado y diseñado para realizar daños a un sistema informático/operativo, en el que se pueden observar perdidas de datos importantes en las bases de dichos sistemas. El malware se puede clasificar en diferentes subtipos como virus informáticos, gusanos, troyanos, ransomware, spyware, adware, software malicioso falso, eliminador y keyloggers.

– Amenaza a través de redes sociales: este tipo de ciber delito se ha vuelto muy común en la actualidad, puesto que la obtención de datos por redes sociales ha sido un proceso muy sencillo, en especial para los ciber criminales, puesto que hace falta de políticas de privacidad y prevención en dichas redes que sean puestas en práctica de manera eficaz, en dicho delito encontramos en múltiples casos, la violación al derecho a la intimidad de toda persona. Las personas pueden tomar medidas de prevención para protegerse de amenazas en línea, como revisar periódicamente su perfil de redes sociales y configurar la privacidad, ser cuidadosos con la información personal que publican en línea, evitar aceptar solicitudes de amistad de personas desconocidas y establecer medidas de seguridad en sus dispositivos electrónicos para evitar hackeos.

– Injuria o calumnia a través de redes sociales: Dicho delito se presenta en igual magnitud a las amenazas vía redes sociales, en este caso los ciberdelincuentes se encargan de sembrar el temor y en múltiples de casos, calumnias sobre la víctima, por lo que es esta misma y su temor, quien da el paso a seguir a lo ciberdelincuentes para continuar su acción, aprovechándose así de manera, en mayoría, monetaria de la víctima, o consigo, favores especiales. La injuria en estos casos consiste en atribuir a alguien un hecho o cualidad que le menoscaba en su consideración o estima, mientras que la calumnia se refiere a la atribución a alguien de un hecho falso y perjudicial para su honor o reputación.

El presente artículo de investigación tiene como objetivo mostrar los lineamientos adoptados de Ciberseguridad y Ciberdefensa, para la gestión, protección, procesamiento, almacenamiento y transmisión de datos e información; a través de Tecnologías de Información y Comunicaciones (TIC). Así como el rol que desempeña la informática forense en la Seguridad Nacional, tal como se ha declarado y planteado en diversos textos diseñados por diferentes entes del sector público y privado y la relación de estos temas identificando que hay, que falta y cómo vamos en materia de Informática Forense. Finalmente, se estará en capacidad de conocer el estado actual de seguridad informática, Ciberseguridad y Ciberdefensa y que se tiene en materia especifica de Informática Forense.

Las tecnologías al ser aplicadas en distintos campos de acción, ha logrado posicionarse en diferentes sectores de la economía, hasta hace un par de décadas se realizaban tareas netamente manuales. Al haberse realizado esta evolución de lo manual a lo tecnológico, no solo se han obtenido ventajas y desventajas, sino también se han adquirido factores de riesgo, convirtiéndose en amenazas y vulnerabilidades que ameritan un cuidado especial y un tratamiento integral.

Un ejemplo de aplicación de tecnologías modernas, son implementación de las tecnologías de información y telecomunicaciones, en aplicaciones electrónicas de control, administración y gestión en infraestructura critica, convirtiéndose en puntos claves para la economía de un país, y al mismo tiempo en objetivos estratégicos, para la realización y ejecución de Ciberdelitos.

El objetivo es realizar una revisión en materia de prevención del cibercrimen en el ámbito europeo. De acuerdo con los datos estadísticos, Europa es el segundo territorio con mayor número de ciber usuarios a nivel mundial; se destaca el Reino Unido, por ser uno de los países que han destinado más entidades a la prevención del ciberdelito. Por este motivo, por ser el segundo país de la Unión Europea con mayor número de ciber usuarios en la red -y el primero en relación con Facebook-, se ha decidido realizar un exhaustivo análisis sobre los organismos y entidades que orientan sus fines a evitar la ciber victimización, y se menciona los menores como víctimas especialmente vulnerables. No cabe duda de los beneficios aportados por parte de los nuevos medios

de información y comunicación a la sociedad moderna, pero igual que las ventajas son innumerables, los efectos negativos adheridos a su desarrollo y proliferación también son notorios.

Sin embargo, la posibilidad de realizar comportamientos criminales al margen del espacio físico se hace presente con el desarrollo de las nuevas tecnologías, y se crea de este modo una compleja problemática en el ámbito jurisdiccional. De este modo, la justificación del presente análisis se basa en sus implicaciones sociales, y se demuestra cuantitativamente que se trata de un fenómeno creciente, cuyos fines últimos debieran orientarse a la prevención; aspecto deducible del número de usuarios con acceso a las Tecnologías de la Información y la Comunicación (TIC), y que delimita, en última instancia, la motivación y modalidad de actuación del ciberdelincuente.

El trabajo examina algunos elementos criminológicos que pueden contribuir al análisis jurídico-penal de los delitos informáticos. El estudio se centra en los delitos que inciden en el soporte lógico de un sistema informático e implican el uso de redes computacionales, distinguiendo medios y contextos de comisión, sujetos y consecuencias.

En la actualidad se encuentra muy arraigada la idea de que el análisis del Derecho penal no puede ceñirse a lo estrictamente jurídico y debe, en cambio, incorporar el aporte de otras áreas del conocimiento, en especial de la criminología en tanto ciencia interdisciplinaria y empírica. Con más o menos matices, y con independencia del delito que se examine, los estudios criminológicos permiten establecer, entre otras cosas, cuáles son los medios y contextos de ejecución, quiénes son los autores y víctimas, así como cuáles son las consecuencias de un específico delito. Gracias a ellos se favorece una creación, revisión, interpretación y aplicación de los tipos penales más vinculada con la realidad y, en estrecha relación con ello, una mejor comprensión y explicación de un determinado fenómeno delictivo. Respecto del análisis de los delitos informáticos, son varios los factores que refuerzan la importancia de considerar los resultados de estudios criminológicos. Dichos delitos se vinculan con la informática, y ella presenta una serie de notas distintivas, que dificultan la comprensión de este sector de la criminalidad.

La problemática del abuso sexual contra niños, niñas y adolescentes en Colombia sigue aumentando, incluyendo en el emergente ciberespacio donde los ciberdelitos sexuales son una realidad. Este artículo busca analizar si la política criminal jurídica actual del Estado colombiano es suficiente para afrontar esta problemática, considerando el ciberespacio como nuevo escenario y ofreciendo una relación elemental de las principales conductas constitutivas de ciberdelitos sexuales. La conclusión es que se necesita un nuevo paradigma de política criminal que priorice la prevención y no el populismo punitivo.

El nacimiento y la evolución de las tecnologías de la información y la comunicación han transformado la forma en que se relacionan los integrantes de la aldea global, generando un nuevo escenario digital conocido como ciberespacio que ha traído beneficios, pero también ha generado nuevas oportunidades para la comisión de conductas punibles en línea o ciberdelitos.

En Colombia, el ciberdelito es un problema complejo y multifacético que requiere medidas diversas. Se propone fortalecer las capacidades técnicas y tecnológicas de las autoridades encargadas de la investigación y persecución del ciberdelito, sensibilizar y educar a la población sobre los riesgos del uso inadecuado de las tecnologías de la información y la comunicación, implementar medidas de protección de datos personales y de seguridad informática en las empresas y organizaciones, y actualizar constantemente la legislación y las políticas públicas relacionadas con el ciberdelito para adaptarse a los cambios tecnológicos y garantizar la protección de los derechos humanos en la era digital.

El ciberdelito ha aumentado en Colombia en los últimos años, incluyendo delitos informáticos como phishing, fraude en línea, malware y ransomware, así como amenazas más complejas como el cibercrimen organizado y los ataques patrocinados por el estado. Esto tiene un impacto significativo en la privacidad, seguridad, sociedad y economía de Colombia, lo que ha llevado al gobierno a tomar medidas para prevenir y combatir el ciberdelito en el país, incluyendo la creación de la Unidad de Ciberdelincuencia de la fiscalía general de la Nación y el desarrollo del Plan Nacional de Ciberseguridad para proteger la infraestructura crítica del país.

Actualmente, las cifras de la fiscalía general de la Nación son cada día más alarmantes, toda vez que el delito de acceso abusivo a un sistema informático es el tercer delito, respecto a los delitos informáticos, en el que más incurren los delincuentes. En ese sentido cabe resaltar que, desde el año 2019, las denuncias por el delito de acceso abusivo a un sistema informático corresponden al 0,59 % del total de denuncias presentadas.

Ahora, desde el año 2019, antes de la pandemia, se presentaron 8.204 denuncias por este delito, lo que muestra un aumento del 41,7 % en 2020 y del 55,7 % en 2021. Así mismo, comparando enero y abril de 2021 y 2022, el incremento en presentación de denuncias, en relación con este delito, es del 47,6 %. (DialogosPunitivos.com, 2021).

En cuanto a la naturaleza del delito de acceso abusivo a un sistema informático, se ha considerado dogmáticamente como un delito de mera conducta, es decir, que no requiere necesariamente un resultado en sí mismo, debido a que el verbo rector utilizado en la norma es "acceder". Esto implica la idea de ingresar o adentrarse en un sistema de datos informáticos con o sin autorización del propietario. No obstante, sí se necesita que se produzca un diálogo coherente entre el autor de la acción y el sistema al que se accede, para poder establecer una relación o interacción lógica.

En cuanto a la técnica legislativa empleada en nuestro ordenamiento jurídico para tipificar el delito de acceso abusivo a un sistema informático, es destacable que el legislador ha generado una discusión, ya que este delito fue consagrado en un solo tipo penal, lo cual difiere de las sugerencias de la doctrina en algunos aspectos. Por ejemplo, en la redacción de este delito, la figura de la auto-puesta en peligro debe ser evaluada antes del análisis de la imputación objetiva, debido a que parece que el principio de autorresponsabilidad del titular del sistema no se ha tomado en cuenta. Esto se debe a que, en este caso, el poseedor de la información asume voluntaria y libremente el riesgo cuando entrega información a un tercero, y asume las consecuencias de sus acciones. No obstante, respecto a la protección del bien jurídico y a la calificación del tipo penal, la Corte Suprema de Justicia acertó cuando recalcó que este delito es pluriofensivo, es decir, “lesiona simultáneamente varios intereses que el legislador concibe como dignos

de tutela jurídica", como, por ejemplo, los datos personales, el patrimonio económico, la seguridad de la información y el peligro indirecto de la información almacenada en ellos.

A pesar de esto, la Corte Suprema de Justicia pudo ser más contundente respecto a la pronunciación sobre este delito, pues, en distintas oportunidades, las demandas de casación que llegan a la Sala Penal no han sido discutidas de forma amplia porque la Corte consideró en su momento que no tenía los elementos jurisprudenciales y dogmáticos suficientes para tomar una decisión de fondo.

En tales circunstancias, es paradójico pensar que probablemente se deba esperar otra cantidad de tiempo para que la Corte Suprema de Justicia pueda realizar un análisis aún más exhaustivo de ese delito, cuando tuvo la oportunidad de hacerlo ahora y, sobre todo, teniendo en cuenta que la comisión de los delitos informáticos está en auge por la necesidad de la virtualidad desde la pandemia por COVID-19.

MARCO TEÓRICO

El ciberdelito es una amenaza cada vez más presente en la sociedad actual, y Bogotá no es la excepción. Para entender el fenómeno del ciberdelito en Bogotá, es necesario tener en cuenta algunos conceptos clave del marco teórico, como se menciona a continuación:

- Definición de ciberdelito: el ciberdelito se refiere a la comisión de delitos utilizando las tecnologías de la información y comunicación (TIC). Estos delitos pueden incluir el robo de datos, la estafa en línea, el ciberacoso, la pornografía infantil, el grooming, entre otros.
- Factores que contribuyen al aumento del ciberdelito: en la actualidad, el aumento del ciberdelito se debe en parte al creciente uso de las TIC, la falta de regulación adecuada, la escasa educación sobre seguridad informática y la facilidad de acceso a la tecnología.
- Impacto del ciberdelito: el ciberdelito puede tener un impacto significativo en la sociedad, incluyendo la pérdida de datos personales, la interrupción de los servicios en línea, la violación de la privacidad, el daño a la reputación, la pérdida financiera y la afectación psicológica.

- Prevención y lucha contra el ciberdelito: para prevenir y combatir el ciberdelito en Bogotá, es necesario contar con una regulación efectiva y actualizada, campañas de educación sobre seguridad informática, mecanismos de denuncia y atención a las víctimas, y una colaboración efectiva entre las autoridades y los proveedores de servicios en línea.
- Marco legal en Colombia: en Colombia, el marco legal para combatir el ciberdelito incluye la Ley 1273 de 2009, que establece los delitos informáticos y las penas correspondientes, y la Ley 1581 de 2012, que regula la protección de datos personales.

En conclusión, el ciberdelito es un problema cada vez más relevante en Bogotá y en el mundo, que requiere de una regulación efectiva y actualizada, educación y conciencia sobre seguridad informática, y una colaboración efectiva entre las autoridades y los proveedores de servicios en línea.

> La aparición de los delitos en el espacio cibernético ha planteado nuevos desafíos al derecho tradicional. este nuevo escenario delictivo exhorta a la doctrina especializada a plantearse si son adecuadas para la ciberdelincuencia las respuestas penales creadas para cubrir el espacio físico tradicional. son solo muestras de ello las novedosas características técnicas, lógicas y de uso del tic (tecnologías de la información y la comunicación), la cuestión de la cifra negra en los ciberdelitos, la contribución de la víctima desde un plano victimológico, la reinterpretación de las reglas espaciotemporales, la superior capacidad lesiva de estos injustos o la pluralidad de potenciales víctimas existentes (Gorostidi, 2020, p. 13).

Gorostidi (2020) es un experto en ciberseguridad y en su obra "Ciberseguridad, riesgos y amenazas en el mundo digital" aborda el tema de los ciberdelitos desde una perspectiva técnica y legal. En su obra, Gorostidi destaca que los ciberdelitos son una amenaza real y creciente en el mundo digital, y que las empresas y organizaciones deben tomar medidas para protegerse contra ellos. También destaca que los ciberdelitos pueden tener graves consecuencias para las víctimas, como la pérdida de datos, la interrupción del negocio, el robo de propiedad intelectual y el daño a la reputación.

Gorostidi (2020) también señala que los ciberdelitos no son un problema que pueda ser resuelto solo por la tecnología o la ley. En cambio, argumenta que una estrategia efectiva de ciberseguridad debe abordar no solo la tecnología y la ley, sino también la cultura de seguridad, la formación de los empleados y la conciencia de los riesgos cibernéticos. En resumen, Gorostidi destaca la importancia de reconocer la amenaza que representan los ciberdelitos y tomar medidas para protegerse contra ellos, y aboga por un enfoque integral de la ciberseguridad que aborde la tecnología, la ley, la cultura de seguridad y la formación de los empleados.

Desde el momento en que se entra al ciberespacio ya sea desde un celular, un televisor inteligente o un reloj, toda persona es vulnerable de convertirse en una posible víctima de los ciberdelincuentes, debido a que este espacio brinda muchas oportunidades para que se materialice un ciberdelito.

De tal manera, también plantea que los delitos incluyen un artículo referido a la comisión del mismo a través de las TIC, salvo casos concretos como el derecho a la vida. Otro aspecto que ha estudiado es si para ver si era necesario crear nuevos bienes jurídicos a proteger, como la ciberseguridad, la libertad informática o la protección de datos. Pero llegó a la conclusión que no, porque todo lo que hacemos en el ciberespacio tiene siempre su reflejo en el mundo físico y afecta a bienes jurídicos que ya existen y están protegidos en el Código Penal. Además, el derecho penal tiene vocación de estabilidad, así que cuanto menos lo cambiemos, mejor. Si podemos utilizar lo que ya existe para dar respuesta a los problemas actuales siempre es mejor que cambiar la ley, que debería ser lo último. En otras ramas del derecho no, pero en derecho penal sí. Ahí está el ejemplo de la ley del ‘solo sí es sí’.

MARCO CONCEPTUAL

El ciberdelito es un término amplio que se refiere a cualquier delito que se comete utilizando tecnología informática o de comunicaciones, como Internet, redes sociales, correo electrónico o dispositivos móviles. El ciberdelito puede ser llevado a cabo por individuos o grupos de manera malintencionada o por motivaciones financieras, políticas, sociales o personales. Las actividades de ciberdelincuencia pueden tener consecuencias

graves para los individuos y las empresas afectadas, incluyendo la pérdida de datos, la violación de la privacidad y la exposición financiera.

Respecto a los ciberdelincuentes, estos son individuos o grupos que utilizan la tecnología informática y las redes de comunicaciones para llevar a cabo actividades delictivas en línea. Los motivos de los ciberdelincuentes pueden variar desde el beneficio económico a la venganza personal, el hacktivismo, la curiosidad, entre otros. Estos individuos pueden utilizar diversas técnicas, herramientas y prácticas que les permiten robar información, infectar sistemas informáticos, extorsionar a empresas, robar identidades e incluso afectar la seguridad nacional. A continuación, se presentan algunas definiciones de ciberdelito de diferentes autores:

El ciberdelito es "cualquier delito cometido utilizando una computadora o red de computadoras como medio, objetivo o lugar del delito" (UNODC, 2019). Para esta organización, el ciberdelito incluye una amplia gama de actividades ilícitas que se realizan en línea, como el fraude electrónico, el robo de identidad, la extorsión, la difusión de contenido violento y explotación infantil, el ciberespionaje y el ciberterrorismo. La UNODC trabaja para prevenir y combatir el ciberdelito mediante la promoción de normas y acuerdos internacionales, la cooperación y asistencia técnica a nivel nacional e internacional, y la promoción del desarrollo de capacidades en materia de ciberseguridad.

El NIST es una agencia federal del Departamento de Comercio de los Estados Unidos que se dedica a desarrollar estándares y guías técnicas para la industria y el gobierno en los Estados Unidos. El NIST ha desarrollado pautas y marcos para la ciberseguridad y es considerado un líder en el campo de la ciberseguridad.

En la literatura académica, algunos autores definen el ciberdelito como "delitos cometidos contra la propiedad o la privacidad de las personas utilizando tecnología informática o de comunicaciones" (Wall, 2007, p. 23). Otros autores lo definen como "delitos en los que la tecnología juega un papel central, ya sea como medio, como objetivo o como instrumento" (Brenner, 2009, 23).

> Los ciberataques son una categoría más amplia que los delitos informáticos porque incluyen acciones que pueden no ser ilegales en sí mismas, pero que pueden tener consecuencias negativas para la seguridad y privacidad de las personas y organizaciones. Por ejemplo, un ciberataque puede ser un intento malintencionado de acceder a una red o sistema informático sin autorización, mientras que un delito informático específico como el fraude electrónico implica la manipulación ilegal de información en línea para obtener ganancias. (Rayón y Gómez, 2014, p. 12).

Además, los autores distinguen entre el ciberdelito y el cibercrimen. Mientras que el ciberdelito se enfoca en actividades ilegales que involucran el uso indebido de la tecnología, el cibercrimen se refiere a una gama más amplia de actividades criminales que utilizan tecnologías de la información y comunicación como medio o instrumento. Por lo tanto, el cibercrimen puede incluir no solo delitos informáticos específicos, sino también actividades como el terrorismo cibernético, la propaganda en línea y la ciberguerra.

Por otro lado, Choi y Toro Álvarez (2017) enfatizan en que el cibercrimen es un problema global y complejo en la actualidad, debido a la creciente dependencia de las tecnologías de la información y comunicación en todo el mundo. Estos autores también señalan que el cibercrimen no solo afecta a individuos y organizaciones, sino también a gobiernos y sistemas políticos. Por lo tanto, es importante desarrollar soluciones efectivas para prevenir y combatir el cibercrimen a nivel internacional.

En cuanto a los aspectos psicológicos y los comportamientos humanos detrás del cibercrimen, la academia ha explorado temas como el anonimato en línea, la motivación de los cibercriminales y los factores que influyen en la conducta en línea. Por ejemplo, algunos estudios han demostrado que la sensación de anonimato en línea puede llevar a comportamientos más agresivos y arriesgados, mientras que la presión de grupo en línea puede influir en la adopción de comportamientos criminales. La comprensión de estos factores puede ayudar a desarrollar mejores estrategias de prevención y combate del cibercrimen.

En resumen, el ciberdelito es cualquier actividad ilegal que se comete utilizando tecnología informática o de comunicaciones como medio, objetivo o instrumento del delito. Hay muchos tipos diferentes de ciberdelitos que se pueden cometer utilizando tecnología informática o de comunicaciones. A continuación, se presentan algunos de los tipos de ciberdelitos más comunes según diversos autores:

- Delitos informáticos: incluyen cualquier actividad ilegal que se realiza utilizando una computadora o red de computadoras, como el robo de datos, la distribución de virus informáticos, la creación de programas maliciosos, el phishing y el hacking. Los delitos informáticos atentan contra la integridad de datos, propiedad intelectual, entre otros derechos, dichos delitos son de carácter penal por lo que se encuentran sujetos a las leyes y regulaciones específicas.
- Delitos contra la propiedad intelectual: incluyen la piratería informática, la violación de derechos de autor, el uso no autorizado de marcas registradas y la falsificación de productos y servicios. Algunos de los delitos contra la propiedad intelectual incluyen la distribución ilegal de contenido protegido por derechos de autor, la falsificación y la utilización no autorizada de marcas registradas y la venta de productos falsificados.
- Delitos contra la privacidad: incluyen la interceptación ilegal de comunicaciones, la publicación no autorizada de información personal, el acoso en línea y el espionaje. Las personas afectadas por este tipo de delitos acuden a las autoridades competentes, puesto que dicho delito es de carácter penal y los culpables serán investigados y debidamente procesados.
- Delitos financieros: incluyen el fraude en línea, el robo de identidad con la finalidad de realizar operaciones financieras no autorizadas, el robo de tarjetas de crédito, el lavado de dinero en línea, como también los esquemas fraudulentos de inversión.
- Delitos sexuales: incluyen la explotación sexual en línea, la pornografía infantil que involucra el uso de tecnologías de la información y la comunicación para conectar a menores de edad y otros individuos

vulnerables con el fin de obtener imágenes o videos sexuales o para perpetrar otras formas del abuso sexual, el grooming y el sexting que hace referencia al intercambio de mensajes y fotografías sexualmente explicitas a través de dispositivos electrónicos.

El phishing es una técnica de ciberdelito utilizada para obtener información confidencial, como nombres de usuario, contraseñas, información de tarjetas de crédito y otra información personal, haciéndose pasar por una entidad legítima en línea. Esta técnica se lleva a cabo a través de la creación de correos electrónicos, mensajes de texto, sitios web, o incluso llamadas telefónicas falsas que parecen provenir de empresas u organizaciones legítimas como bancos, empresas de servicios públicos, proveedores de servicios en línea, etc.

El objetivo del phishing es engañar a la víctima para que revele información personal o financiera confidencial. Los correos electrónicos de phishing suelen contener enlaces que dirigen a los usuarios a sitios web falsos que parecen legítimos, pero que en realidad están diseñados para capturar la información del usuario. Los mensajes también pueden contener archivos adjuntos maliciosos que, cuando se descargan, pueden infectar el sistema del usuario con malware.

El phishing es una de las técnicas de ciberdelito más comunes y efectivas debido a su naturaleza engañosa y su capacidad para imitar sitios web y correos electrónicos legítimos. Para protegerse contra el phishing, es importante verificar la dirección de correo electrónico y el sitio web antes de ingresar información personal o financiera, no hacer clic en enlaces sospechosos, mantener actualizado el software de seguridad y antivirus y estar alerta a cualquier actividad sospechosa.

El carding es una técnica de ciberdelito que implica el uso de tarjetas de crédito o débito robadas o falsificadas para hacer compras ilegales en línea. Los carders a menudo roban la información de la tarjeta de crédito de las víctimas a través de técnicas de phishing, malware o skimming. Luego, utilizan esta información para hacer compras en línea o vender la información a otros criminales.

El vishing, por otro lado, es una técnica de ciberdelito que implica la utilización de llamadas telefónicas para engañar a las víctimas y obtener información confidencial, como números de tarjetas de crédito, contraseñas y otra información personal. Los delincuentes que realizan el vishing se hacen pasar por representantes de empresas legítimas, como bancos, empresas de servicios públicos o proveedores de servicios en línea, y engañan a las víctimas para que revelen información personal o financiera.

Ambas técnicas son formas de fraude financiero y pueden tener graves consecuencias para las víctimas, incluyendo la pérdida de dinero y el robo de identidad. Es importante que los usuarios de tarjetas de crédito y débito estén alerta a estas técnicas y tomen medidas para proteger su información personal y financiera, como no compartir información confidencial por teléfono o en línea, verificar la autenticidad de los sitios web antes de ingresar información de pago, y monitorear sus cuentas bancarias para detectar cualquier actividad sospechosa.

En cuanto a las consecuencias legales, las leyes y regulaciones varían de un país a otro en cuanto a la definición de ciberdelito y las sanciones correspondientes. En algunos casos, las leyes existentes para delitos offline también se aplican al ciberdelito, mientras que otros países han desarrollado leyes específicas para abordar el cibercrimen, en cualquier caso, la prevención y el combate al cibercrimen requieren de la cooperación y colaboración entre los gobiernos, las empresas, la sociedad civil y otros actores relevantes. La promoción de normas y acuerdos internacionales, la inversión en capacidades y tecnologías de ciberseguridad, la educación y concientización sobre la seguridad en línea, así como la colaboración entre los distintos sectores son elementos clave en la lucha contra el ciberdelito.

MARCO JURÍDICO

El marco jurídico colombiano sobre los ciberdelitos se establece en la Ley 1273 de 2009, la cual fue creada para regular los delitos informáticos y electrónicos en Colombia. Esta ley establece las normas y principios necesarios para prevenir, investigar y sancionar los delitos informáticos, y establece penas para las personas que cometan estos delitos.

A continuación, se describen algunos aspectos importantes de la Ley 1273 de 2009:

- Definición de delitos informáticos: La ley establece que un delito informático es cualquier acción ilegal que se cometa mediante el uso de tecnologías de la información y la comunicación, como computadoras, redes y sistemas de información. Estos delitos pueden incluir el acceso no autorizado a sistemas informáticos, la suplantación de identidad en línea, el fraude informático y la difusión de virus o malware.
- Penas: La ley establece penas para las personas que cometan delitos informáticos, las cuales pueden variar desde multas hasta la prisión, dependiendo de la gravedad del delito. Por ejemplo, el acceso no autorizado a un sistema informático puede ser castigado con una pena de hasta 96 meses de prisión y una multa de hasta 1.500 salarios mínimos mensuales.
- Responsabilidad de los proveedores de servicios de internet: La ley establece que los proveedores de servicios de internet son responsables por los delitos informáticos que se cometan a través de sus redes, y deben tomar medidas para prevenirlos. Además, se les exige que conserven los registros de actividad de sus usuarios por un período mínimo de cinco años.
- Investigación y procesamiento de delitos informáticos: La ley establece que la fiscalía general de la Nación es la encargada de investigar y procesar los delitos informáticos en Colombia. Para ello, se creó la Unidad de Delitos Informáticos, que tiene la responsabilidad de coordinar y llevar a cabo las investigaciones relacionadas con estos delitos.
- Cooperación internacional: La ley establece que Colombia puede cooperar con otros países para investigar y procesar delitos informáticos que afecten a más de un país. Además, se establece que las autoridades colombianas pueden solicitar la extradición de personas que hayan cometido delitos informáticos en Colombia y se encuentren en otro país.

En resumen, la Ley 1273 de 2009 establece un marco jurídico completo para la prevención, investigación y sanción de los delitos informáticos en Colombia. Esta ley define los delitos informáticos, establece penas para los delincuentes, responsabiliza a los proveedores de servicios de internet, establece la autoridad encargada de investigar y procesar estos delitos, y permite la cooperación internacional para combatirlos.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito. En este artículo se establece que aquellos que, con el fin de obtener datos personales de manera ilícita, creen sitios web falsos o suplanten sitios web auténticos, serán castigados con penas de prisión y mulas. Estas penas serán en consecuencia más severas si la conducta es realizada en grupo o asociación ilícita, tal como lo establece el artículo 269 de dicho mismo Código Penal.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO II - De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Aquí se establece que todos aquellos que, mediante el uso de tecnologías de la información y la comunicación, y de manera fraudulenta, obtengan datos personales o información comercial de otros, de terceros con el fin de apropiarse de bienes, estos serán castigados con penas de prisión y multas. Esta conducta es considerada como una forma de hurto y puede ser castigada aún más severamente si se realiza en grupo o asociación ilegal.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se

le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad. (Código Penal Colombiano,1273 - 2009, pg. 131-135). En dicho artículo se establece que aquellos que mediante el uso de tecnologías de la información y las comunicaciones transfieran o dispongan de los activos de otra persona sin su consentimiento y con el propósito de obtener un beneficio económico ilícito, serán castigados con penas de prisión y multas.

Código Penal colombiano Ley 599 de 2000, capitulo séptimo del libro segundo, titulo III: de la violación a la intimidad, reserva e interceptación de comunicaciones. Artículo 192: El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de dieciséis (16) a cincuenta y cuatro (54) meses, siempre que la conducta no constituya delito sancionado con pena mayor. El que en provecho propio o ajeno o con perjuicio de otro divulgue o emplee el contenido de un documento que deba permanecer en reserva, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor.

Este delito se considera una violación al derecho constitucional de la intimidad y a la privacidad de las personas y es castigado con penas severas; a destacar respecto a este delito es el hecho de sancionar no solo a la persona que comete la intercepción o sustracción, sino que en el mismo sentido sanciona a todos aquellos que colaboren o faciliten su comisión. Teniendo en cuenta que este delito se agrava si la persona que comete la violación ilícita de comunicaciones lo realiza con el fin de obtener un beneficio económico o causar un perjuicio a la víctima.

Artículo 193: El que, sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor. El artículo en cuestión permite y tiene como objeto

prevenir y sancionar la compra y venta en especialidad, de todos aquellos dispositivos con la disposición y utilización de interceptar comunicaciones privadas entre personas sin su consentimiento independientemente de la finalidad con la cual sea de necesidad las comunicaciones. Este artículo tiene una importancia especial en la era digital, ya que los dispositivos tecnológicos cada vez más sofisticados y accesibles al público general pueden facilitar la interceptación ilegal de las comunicaciones privadas, atentando contra la privacidad de las personas y la protección de sus derechos fundamentales. En ese sentido, este artículo busca proteger la privacidad de las personas y prevenir posibles abusos en este ámbito.

Artículo 194: El que en provecho propio o ajeno o con perjuicio de otro divulgue o emplee el contenido de un documento que deba permanecer en reserva, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor. Hace referencia a la divulgación o uso no autorizado de documentos que están clasificados como reservados, es decir, que contienen información que se ha mantenido en secreto debido a su importancia y que ésta protegida por la Ley. Dicho delito también se puede extender a la obtención de información clasificada como reservada de manera ilegal.

Artículo 196: El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida comunicación o correspondencia de carácter oficial, incurrirá en prisión de cuarenta y ocho (48) a ciento ocho (108) meses. La pena descrita en el inciso anterior se aumentará hasta en una tercera parte cuando la comunicación o la correspondencia esté destinada o remitida a la Rama Judicial o a los organismos de control o de seguridad del Estado. ‘Se enmarca y refiere a la sustracción, destrucción, control o impedimento de una comunicación o correspondencia de carácter oficial sin la debida autorización o en contra de la Ley. En adición, la norma establece que si el objeto de la violación ilícita de las comunicaciones o correspondencia es causar daño o perjuicio, la pena se aumentará de manera proporcional y en ningún caso será inferior a la mitad de la pena máxima prevista y es importante destacar, que este delito no solo se refiere

a la violación ilícita de comunicaciones o correspondencia emitida por autoridades públicas sino que también a todo tipo de información que la ley califique como oficial y sea objeto de protección especial.

Artículo 197: El que con fines ilícitos posea o haga uso de equipos terminales de redes de comunicaciones o de cualquier medio electrónico diseñado o adaptado para emitir o recibir señales, incurrirá, por esta sola conducta, en prisión de cuatro (4) a ocho (8) años. La pena se duplicará cuando la conducta descrita en el inciso anterior se realice con fines terroristas. (Código Penal Colombiano, Ley 5000 – 2000. Pg. 98 – 100). Este artículo tiene como objetivo prevenir y sancionar el uso ilegal de los equipos y redes de comunicaciones para realizar actividades ilegales, como el acceso no autorizado a datos, la distribución de contenido ilegal, la difusión de virus informáticos entre otros, logrando así proteger la seguridad de la información y la privacidad en el uso de las redes sociales y equipos de comunicaciones

Ley 679 de 2001, prohibiciones para los proveedores, servidores, usuarios o administradores que promuevan la explotación a menores en cuanto a actitudes sexuales (sanciones administrativas).

CAPITULO II. - DEL USO DE REDES GLOBALES DE INFORMACIÓN EN RELACIÓN CON MENORES.

ARTÍCULO 04. COMISIÓN DE EXPERTOS. Dentro del mes siguiente a la vigencia de la presente ley, el Instituto Colombiano de Bienestar Familiar conformará una Comisión integrada por peritos jurídicos y técnicos, y expertos en redes globales de información y telecomunicaciones, con el propósito de elaborar un catálogo de actos abusivos en el uso y aprovechamiento de tales redes en lo relacionado con menores de edad. La Comisión propondrá iniciativas técnicas como sistemas de detección, filtro, clasificación, eliminación y bloqueo de contenidos perjudiciales para menores de edad en las redes globales, que serán transmitidas al Gobierno nacional con el propósito de dictar medidas en desarrollo de esta ley.

> Los miembros de la Comisión serán funcionarios de la planta de personal ya existente en las entidades públicas cuya función sea la protección del menor y el área de comunicaciones, y su designación corresponderá al representante legal de las mismas. En todo caso, formarán parte de la Comisión, el director del Instituto Colombiano de Bienestar Familiar, el Defensor del Pueblo, un experto en delitos informáticos del DAS, el fiscal general de la Nación, y a sus reuniones será invitado el delegado para Colombia de la Unicef. La Comisión a la que se refiere el presente artículo, presentará un informe escrito al Gobierno Nacional dentro de los cuatro meses siguientes a su conformación, en el cual consten las conclusiones de su estudio, así como las recomendaciones propuestas.” (Ley 679 de 2001).

Conforme a la Ley 1273 de 2009 se tipificaron delitos informáticos en Colombia según algunos términos: obstaculización ilegítima del sistema informático o re de telecomunicación; interceptación de datos por medios informáticos; uso de software malicioso; acceso abusivo a un sistema informático; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios web para capturar datos personales y transferencia no consentida de activos.

Se presentan algunas jurisprudencias relevantes sobre ciberdelito en Colombia:

Sentencia SP 592 de 2022: La sentencia SP 592 de 2022 proferida por el Magistrado Diego Eugenio Corredor marca un hito en la jurisprudencia colombiana en donde la Corte Suprema de Justicia (2022) analiza y enlista los elementos constitutivos para el delito de acceso abusivo a un sistema informático, en el ordenamiento jurídico colombiano. Este escrito presenta una breve reseña de sus consideraciones y toma postura crítica frente a las pautas que ella sienta para la aplicación de este tipo penal.

El 2 de marzo de 2022 la Corte Suprema de Justicia decidió sobre la demanda de casación y doble conformidad formulada contra la sentencia proferida por la Sala Penal del Tribunal Superior de Medellín, que confirmó la condena por el delito de concierto para delinquir y revocó las absoluciones que se habían proferido en primera instancia por los delitos de acceso abusivo a sistema informático.

Debido a que el demandado fungía como empleado de una entidad financiera, este tenía la posibilidad de acceder a las cuentas bancarias de los clientes y decidió permanecer en ellas con el fin de cometer los ilícitos que tenía pactados con la banda delincuencial con la cual operaba.

Adicionalmente, la Corte Suprema de Justicia resaltó, en esta sentencia, que, para la doctrina, el acceso abusivo a un sistema informático también se configura mediante un mero intrusismo informático, es decir, “cobija a aquellas conductas de meros accesos o permanencias perpetradas cuyo único fin es el de vulnerar una base de datos, una contraseña o una configuración lógica”, que permita acceder a algún tipo de redes de comunicación electrónica.

Así las cosas, la Corte señaló que los elementos para la configuración del delito son los siguientes:

- Sujeto activo no calificado, por no necesitar de una condición especial para quien accede a un sistema informático “sin autorización”, o que, teniéndola, decide conscientemente mantenerse conectado.
- Sujeto pasivo, persona natural o jurídica titular del sistema informático.
- Lesionar varios bienes jurídicos tutelados, entre ellos, la información, los datos y la intimidad. En ese sentido, ha sido reconocido como un tipo penal pluriofensivo
- Solo admite el dolo en el actuar del ciberdelincuente.
- Es un delito de mera conducta, por cuanto, la sola intromisión en una red informática, en las condiciones establecidas en el tipo penal, afecta el bien jurídico tutelado.
- Contempla dos verbos rectores, acceder o mantener.
- Como ingrediente normativo, exige que el sujeto activo de la acción a) acceda en el sistema informático sin autorización, o, b) aun cuando, teniendo el permiso del titular legítimo del derecho, se mantiene dentro del mismo, excediendo las facultades otorgadas.

Finalmente, respecto al término insider, la Corte se refirió a que este se utiliza cuando la persona que comete el ilícito, aun teniendo permiso, se excede o se aparta de

él. En cambio, el término outsider es usado para determinar a aquellas personas que, no siendo autorizadas, penetran a determinada plataforma o base de datos de información.

Sentencia C-224/19: La Sentencia C-224/19 de la Corte Constitucional (2019) de Colombia fue emitida en mayo de 2019 por la Magistrada Cristina Pardo Schlesinger y se refiere a la constitucionalidad del Decreto 1377 de 2013, el cual regula el manejo de datos personales en Colombia. A continuación, se presenta un análisis de los puntos más importantes de esta sentencia:

La Corte Constitucional señala que el derecho fundamental a la protección de datos personales es un derecho autónomo y autónomo, que deriva del derecho a la intimidad personal y familiar, y se encuentra protegido por la Constitución Política de Colombia y por diversos instrumentos internacionales.

- La Corte establece que la regulación del manejo de datos personales debe ser adecuada, necesaria y proporcional, es decir, que debe estar orientada a proteger la privacidad y otros derechos fundamentales, pero sin limitar excesivamente la libertad y el desarrollo de las personas.
- La Corte Constitucional declara la constitucionalidad condicionada del Decreto 1377 de 2013, y señala que varias de sus disposiciones deben ser interpretadas y aplicadas de manera restrictiva para garantizar la protección efectiva de los derechos fundamentales de los titulares de los datos personales.
- La Corte establece que, en el contexto del manejo de datos personales, es necesario garantizar el principio de consentimiento informado, es decir, que los titulares de los datos deben ser informados de manera clara y precisa sobre el uso que se les dará a sus datos y deben otorgar su consentimiento expreso y libre para dicho uso.
- La Corte Constitucional señala que los titulares de los datos personales tienen derecho a conocer, actualizar, rectificar y suprimir sus datos personales, y que los responsables del manejo de datos deben adoptar medidas adecuadas para garantizar la seguridad y confidencialidad de dichos datos.

La Sentencia C-224/19 de la Corte Constitucional de Colombia destaca la importancia de la protección de los datos personales como un derecho fundamental autónomo y

establece una serie de principios y medidas que deben ser adoptados por los responsables del manejo de dichos datos para garantizar su adecuada protección y respeto a los derechos fundamentales de los titulares de estos.

La ley establece penas para las personas que cometan delitos informáticos, que pueden incluir multas y prisión, dependiendo de la gravedad del delito. Además, los proveedores de servicios de internet son responsables por los delitos informáticos que se cometan a través de sus redes, y deben tomar medidas para prevenirlos y conservar los registros de actividad de sus usuarios por un período mínimo de cinco años.

La fiscalía general de la Nación es la encargada de investigar y procesar los delitos informáticos en Colombia, y se creó la Unidad de Delitos Informáticos para coordinar y llevar a cabo estas investigaciones. Colombia también puede cooperar con otros países para investigar y procesar delitos informáticos que afecten a más de un país, y puede solicitar la extradición de personas que hayan cometido delitos informáticos en Colombia y se encuentren en otro país. Además, el Código Penal colombiano establece penas para ciertos delitos informáticos, como el acceso abusivo a un sistema informático o la interceptación de datos sin autorización, y las autoridades locales de Bogotá pueden hacer cumplir estas leyes.

Es importante tener en cuenta que la tecnología y las amenazas asociadas están en constante evolución, por lo que es posible que en el futuro se establezcan leyes y regulaciones específicas en Bogotá y otras ciudades para abordar los ciberdelitos.

METODOLOGÍA

TIPO DE INVESTIGACIÓN

La investigación es teórica, ya que en este tipo de investigación el énfasis del estudio está en generar conocimiento sin colocarlo en práctica. Por consiguiente, se realiza la recopilación de datos y así se generan nuevos conceptos generales.

ENFOQUE

Esta investigación presenta un enfoque de análisis Cualitativo, en donde utilizamos la recolección de datos para finar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación. El enfoque cualitativo suele partir de una pregunta de investigación, que deberá formularse en concordancia con la metodología que se pretende utilizar. Allá es donde se pretende ir; tratar de analizar los datos estadísticos que nos presenten las fuentes para así trazar los objetivos anteriormente expuestos.

DISEÑO

En este tipo de investigación se trabaja el diseño de investigación diagnóstica, ya que se inclina hacia la evaluación de la causa raíz de un tema específico. Aquí se evalúan los elementos que contribuyen a una situación problemática. Hay tres partes en el diseño de la investigación diagnóstica, el inicio del problema, el diagnóstico y la solución.

PARADIGMA

En esta investigación se desarrolla el paradigma crítico, el cual permite que el lector pueda establecer un análisis sobre el tema expuesto, es decir el Ciberdelito. En este orden de ideas y teniendo en cuenta que la investigación trata el tema de un comportamiento ilícito, el lector puede tomar una posición crítica ante el tema y adoptar una postura conveniente que permita estar informado y a la expectativa de la realidad de las víctimas de este delito, teniendo presente que todos los individuos se hallan expuestos a las amenazas de la inseguridad de este medio.

MÉTODO

En la investigación en curso se desarrolló un enfoque mixto, quiere decir la combinación del enfoque cuantitativo y cualitativo, que genera planteamientos acostados, midiendo los fenómenos sobre los ciberdelitos, de igual manera analizando múltiples realidades, pero entendiendo la amplitud de esta.

El autor Christ (2007) argumenta que la investigación mediante métodos mixtos se ha fortalecido en los últimos veinte años, y los estudios exploratorios cualitativos, seguidos de estudios confirmatorios, han sido comunes y concurrentes. En esa misma

línea, Dellinger y Leech (2007) analizan, también, la validez de los métodos mixtos en la investigación. Tal como lo señalan los autores, durante los años 90, las investigaciones con diseños mixtos se hicieron muy útiles en campos como: Educación, Enfermería, Medicina, Psicología y Comunicación, en el entendido de que el uso de más de un método potenciaba la posibilidad de comprensión de los fenómenos en estudio, especialmente, si estos se refieren a campos complejos en donde está involucrado el ser humano y su diversidad.

Denzin y Lincoln (2002) plantean una revisión profunda acerca de los procesos de triangulación, lo cual aportó a la comunidad científica, en especial en el ámbito cualitativo, importantes elementos que también impactaron de manera positiva las propuestas de investigación denominadas como mixtas. Seguidamente el enfoque de investigación.

TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Se realizará una encuesta que permitirá recopilar la información en la muestra de estudio, se formulará un cuestionario, para cuantificar las variables de estudio, utilizando una serie sistematizadas de preguntas que se llevará a un grupo predeterminado de personas que tengan la información que interesa a la presente investigación.

POBLACIÓN Y MUESTRA

Se optó por hacer uso y de acuerdo con la revisión de la literatura de la investigación descriptiva con enfoque cualitativo que se limita a tomar como referencia las cifras y valorarlas, pero sin ningún fin de atribuirles estandarización de estos datos, la investigación descriptiva permite realizar una descripción de una situación y del fenómeno logrando obtener información acerca del qué, cómo, cuándo y dónde, relativo al objeto de estudio.

REFERENCIAS BIBLIOGRÁFICAS

Acuña, L., y Villa, S. (2018). *Estado actual del cibercrimen en Colombia con respecto a Latinoamérica.* [Monografía de Especialización, Universidad Nacional Abierta y A Distancia, Colombia].

Anónimo. (26 de agosto de 2013). Diez millones de colombianos, víctimas de delitos informáticos en el último año. *El Espectador.*

https://www.elespectador.com/tecnologia/diez-millones-de-colombianos-victimas-de-delitos-informaticos-en-el-ultimo-ano-article-442538/

Arias, M., Ojeda, J., Rincón, F., y Daza, L. (2010) *Delitos informáticos y entorno jurídico vigente en Colombia.* http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Bujato, J., y Alvarado, J. (2022). *El ciberdelito en el derecho penal Colombiano.* [Archivo PDF]. https://bonga.unisimon.edu.co/bitstream/handle/20.500.12442/10933/El_Ciberdelito_Derecho_Penal_Colombiano_Resumen.pdf?sequence=1&isAllowed=y

Brenner, S. (2009) Cibercrimen: amenazas criminales desde el ciberespacio*. Revista chilena de Derecho y Tecnología.* https://rchdt.uchile.cl/index.php/RCHDT/article/view/24030

Choi, K., Toro, M. (2017). *Cibercriminología. Guía para la investigación del cibercrimen y mejores prácticas en seguridad digital*. Universidad Antonio Nariño, Bogotá.

Christ, T. (2007). A recursive approach to mixed methods research in a longitudinal study of postsecondary education disability support services. *Journal of Mixed Methods Research*, 226-241.

Corte Constitucional. (2019). Sentencia C-214 de 2019 del 22 de mayo de 2019. M.P. Cristina Pardo Schlesinger.
https://www.corteconstitucional.gov.co/relatoria/2019/C-224-19.htm

Corte Suprema de Justicia. (2022). Sentencia SP592 de 2022 del 2 de Marzo de 2019. M.P. Eugenio Corredor Beltrán. https://cortesuprema.gov.co/corte/index.php/2022/04/01/acceso-abusivo-a-un-sistema-informatico-concepto/

Davara, M. (2002). *Delitos Informáticos: Generalidades*. [Archivo PDF]. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Dellinger, A.B., & Leech, N.L. (2007). Toward A UNIFIED VALIDATION FRAMEWORK IN MIXED METHODS RESEARCH. *Journal of Mixed Methods Research*, 309–332. https://doi.org/10.1177/1558689807306147

Denzin, N. y Lincoln, Y. (2002). The Qualitative Inquiry Reader. *Forum: Qualitative Social Research*, 3(4), Art. 35.

Diaz, A. (2010) *El Delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio De Budapest.* [Tesis doctoral, Universidad de la Rioja]. https://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf

Diálogos Punitivos. (Junio 10 de 2022). *La Corte Suprema de Justicia aclaró elementos normativos del acceso abusivo a un sistema informático.* https://dialogospunitivos.com/la-corte-suprema-de-justicia-aclaro-elementos-normativos-del-acceso-abusivo-a-un-sistema-informatico/

Gorostidi, J. (2020). La pluralidad de víctimas derivada de la elevada lesividad en los ciberdelitos: una respuesta penal proporcional. *Revista de Derecho Público* https://revista-estudios.revistas.deusto.es/article/view/1822/2246

Guerrero, B., y Castillo, D. (s.f.). *Desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano*. [Archivo PDF] https://repository.unad.edu.co/handle/10596/13387

Ley 5000 de 2000. Por medio de la cual se expide el Código Penal. 24 de Julio de 2000. D.O. No. 44097. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

Ley 679 de 2001. Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. 03 de agosto de 2001. D.O. No. 44509. www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=18309

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. 5 de enero de 2009. D.O. No. 47223. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Llanos, R. (17 de octubre 2009) Hackers borran contenido de nuevo periódico digital. *Periódico El Tiempo*. https://www.eltiempo.com/archivo/documento/MAM-3672589

Maldonado, A. (2022). Ciberdelincuencia. [Archivo PDF]. https://www.academia.edu/8947347/Ciberdelincuencia

Martínez, C. (2016). *Los desarrollos tecnológicos y su influencia en el crecimiento de los ciberdelitos en Colombia*. [Especialización en Seguridad Informática, Universidad Piloto de Colombia]. http://repository.unipiloto.edu.co/handle/20.500.12277/8577

Martínez, G. (2022). *Ciberdelitos. Instrucción y prueba. Ediciones Experiencias*. [PDF] https://www.perlego.com/es/book/3804395/ciberdelitos-instruccin-y-prueba-pdf

Montañez, A. (2017). Análisis de los delitos informáticos en el actual sistema penal colombiano. Bogotá-DC, 10. https://repository.unilibre.edu.co/bitstream/handle/10901/11041/AN%C3%81LISIS%20DE%20LOS%20DELITOS%20INFORM%C3%81TICOS%20EN%20EL%20ACTUAL%20SISTEMA%20PENAL%20COLOMBIANO%20revisado%20NHJ%20OK.pdf?sequence=3

Nogales, J. (2012). Tecnologías de Internet. Naturaleza y evolución de Internet. https://aulaglobal2.uc3m.es/file.php/39339/html/doc/ti/ti-01.html

Recio, J. (2012). De la seguridad informática a la seguridad de la información. asociación española para la calidad*. Revista mensual de la Asociación Española para la Calidad* 14-19. https://dialnet.unirioja.es/servlet/articulo?codigo=4867991

Ramirez, J., y Campo, A. (2021). Uncovering cybercrimes in social media through natural language processing. *Journals complexy* https://www.hindawi.com/journals/complexity/2021/7955637/

Rayón, M., & Gómez, J. (2014). Cibercrimen: Particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense estoy *Revista Dialnet* 47, 209 – 234. https://dialnet.unirioja.es/servlet/revista?codigo=5135

Rivera, A. (1995). *Dimensiones de la informática en el derecho.* Editorial Jurídica Radar, Santa fe de Bogotá, 89.

Restrepo, M. (2016). Formulación de un paradigma para la investigación judicial. [Archivo PDF]. file:///C:/Users/Hogar/Downloads/Dialnet-FormulacionDeUnParadigmaParaLaInvestigacionJudicia-5823644%20(1).pdf

Rodríguez., et al. (1996). *Metodología de la investigación cualitativa*. [PDF] https://www.researchgate.net/publication/44376485_Metodologia_de_la_investigacion_cualitativa_Gregorio_Rodriguez_Gomez_Javier_Gil_Flores_Eduardo_Garcia_Jimenez

Rodriguez, R. (15 de Julio de 2018). Historia de un cracker" barranquillero. *Periódico El Heraldo.* https://www.elheraldo.co/noticias/tecnologia/un-barranquillero-entre-los-hackers-mas-destacados-del-mundo-74831

Suárez, A. (2009). *La estafa informática.* Bogotá: Grupo Ibáñez.

Sneyers, A. (1990). *El fraude y otros delitos informáticos. Tecnologías de Gerencia y producción*. Ediciones T.G.P. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Tanque de Análisis y Creatividad de las TIC. (2019). Tendencias cibercrimen Colombia. [Archivo PDF]. https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Tirado, M., y Cáceres, V. (2021). La política criminal frente al ciberdelito sexual contra niños, niñas y adolescentes en Colombia. *Revista Científica General José María Córdova*, *19*(36), 1011-1033. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1900-65862021000401011

Universidad Militar Nueva Granada. (s.f.). *Protección de datos personales*. https://repository.unimilitar.edu.co/bitstream/handle/10654/7650/PROTECCION%20DE%20DATOS%20PERSONALES(1).pdf?sequence=1&isAllowed=yfr

Villar, L., y Pérez, C. (2016). *Coyuntura TIC: Informe de las Tecnologías de la Información y las Telecomunicaciones TIC*. https://www.repository.fedesarrollo.org.co/handle/11445/15

Wall, D. (2007). Cybercrime: The transformation of crime in the information age. https://www.wiley.com/en-us/Cybercrime%3A+The+Transformation+of+Crime+in+the+Information+Age-p-9780745627359