ESPECIALIZACION EN CIBERSEGURIDAD

GUÍA INFOGRÁFICA PARA LA PREVENCIÓN DE LA SEGURIDAD DIGITAL Y RECONOCIMIENTO DE LOS PRINCIPALES CIBERDELITOS

JOSÉ FERNANDO GUTIÉRREZ RAMÍREZ

HERNÁN MAURICIO MÁRQUEZ MARULANDA

HAROLD ROMAÑA MACHADO

Universidad® Católica de Manizales
VIGILADA MINEDUCACIÓN
Obra de Iglesia de la Congregación
Hermanas de la Caridad Dominicas de La Presentación de la Santísima Virgen

GUÍA INFOGRÁFICA PARA LA PREVENCIÓN DE LA SEGURIDAD DIGITAL Y RECONOCIMIENTO DE LOS PRINCIPALES CIBERDELITOS

Trabajo de grado presentado como requisito para optar al título de Especialización en Ciberseguridad

Modalidad de grado: Artículo de investigación

Héctor Roberto Gordon Quinche

JOSÉ FERNANDO GUTIÉRREZ RAMÍREZ

HERNÁN MAURICIO MÁRQUEZ MARULANDA

HAROLD ROMAÑA MACHADO

UNIVERSIDAD CATÓLICA DE MANIZALES

FACULTAD DE INGENIERIA

ESPECIALIZACION EN CIBERSEGURIDAD

MANIZALES, CALDAS

2023

Nota de aceptación: 4.6

Dedicatoria: A nuestros padres e hijos que con su amor y apoyo incondicional son una fuerza fundamental para culminar este proceso.

Agradecimientos: A Dios, a la Universidad Católica de Manizales, a nuestros profesores por compartir con amor y paciencia todos sus conocimientos y a nosotros mismos por lograr finalizar este hermoso reto.

TABLA DE CONTENIDO

TABLA DE FIGURAS

RESUMEN

Este trabajo de investigación centra su atención en los ciberdelitos, tomando en cuenta que se trata de una problemática que ha presentado un auge especial durante la época de confinamiento atravesada por la sociedad mundial, dejando en evidencia la falta de conocimiento que tienen muchas personas en torno a las distintas modalidades de fraude y estafa que se pueden realizar mediante el uso de la tecnología y la conexión a internet. Para contribuir en la mitigación de este fenómeno, se propone la creación de una guía infográfica que ayude en la comprensión de los principales ciberdelitos, sus efectos y sus implicaciones,

En el marco de una metodología cualitativa, soportada en un enfoque propositivo, se formulan algunas estrategias de prevención para los ciberdelitos, que pueden ser adoptadas por cualquier ciudadano; además, se relacionan las rutas de atención, en caso de ser víctima de una acción de fraude o suplantación digital. Los resultados revelan cuáles son los ciberdelitos más comunes, presentando un análisis comparativo de la última década entre la ciudad y el resto del país,

Palabras Claves: Ciberdelitos, seguridad, guía infográfica

ABSTRACT

This research work focuses its attention on cybercrimes, taking into account that it is a problem that has presented a special boom during the time of confinement experienced by world society, revealing the lack of knowledge that many people have around to the different types of fraud and scam that can be carried out through the use of technology and the Internet connection. To contribute to the mitigation of this phenomenon, the creation of an infographic guide is proposed to help in understanding the main cybercrimes, their effects and their implications,

Within the framework of a qualitative methodology, supported by a proactive approach, some prevention strategies for cybercrimes are formulated, which can be adopted by any citizen; In addition, the service routes are listed, in case of being a victim of fraud or digital impersonation. The results reveal which are the most common cybercrimes, presenting a comparative analysis of the last decade between the city and the rest of the country,

Keywords: Cybercrime, security, infographic guide

INTRODUCCIÓN

La sociedad globalizada, inmersa en una era digital, había asumido el reto de dar el salto de una sociedad de la información a una sociedad del conocimiento; sin embargo, con la apertura masiva de plataformas y medios de comunicación digital, el tratamiento de los datos a través de múltiples softwares de código abierto y la necesidad de encontrar aprobación en las redes sociales, han hecho que esa idea de avanzar se convierta en un verdadero obstáculo.

Aunado a todo esto se encuentra la seguridad de la información. Múltiples casos de fraude, estafa, extorsión y suplantación se suman a la cadena de Ciberdelitos que acompañan ese mismo crecimiento de la sociedad digital, es decir, en la medida en la que se presentan los avances, también crecen las oportunidades para los delincuentes.

Los ciberdelitos se cometen con ayuda de las Tecnologías de la información y la Comunicación y constituyen una actividad ilegal tan diversa, que en muchos casos, ni siquiera se encuentra tipificada por la ley. Pese a esto, el uso de la tecnología es inevitable y en el mundo son cada vez más las personas que dependen de ella para realizar sus transacciones comerciales o personales, su actividad profesional o sus dinámicas de entretenimiento, lo que convierte la lucha contra los ciberdelitos y los ciberdelincuentes cada vez más difícil, toda vez que se trata de una actividad ilícita que se puede realizar desde cualquier parte del mundo.

Sin duda, son muchos las razones que motivan la aparición de los ciberdelitos: el lucro financiero, el espionaje, el fraude, el activismo e incluso la venganza, por esta razón la sociedad del futuro debe asumir posturas de seguridad cada vez más eficientes contra la amenaza que este fenómeno representa para la seguridad digital.

Este documento recopila algunos de los ciberdelitos más comunes, en un esquema de análisis que toma el panorama global, el contexto nacional y finaliza con un análisis de los casos que se presentan con mayor frecuencia en la ciudad de Manizales. El propósito del ejercicio investigativo es documentar los crímenes de naturaleza digital y explicar la manera en la que estos evolucionan de forma dinámica y constante, con el ánimo de prevenir a los usuarios de internet para que sean conscientes de las posibles amenazas y los riesgos en línea. De este modo, se pretende cumplir con el objetivo de informar a través del diseño de una guía infográfica que presente de forma ágil y en un lenguaje sencillo las implicaciones, las estrategias de prevención y las rutas de atención cuando se tenga sospecha o se presente un Ciberdelitos.

OBJETIVOS

OBJETIVO GENERAL

Diseñar una guía infográfica que permita la comprensión de los principales ciberdelitos, sus implicaciones, las estrategias de prevención y las rutas de atención.

OBJETIVOS ESPECÍFICOS

Identificar cuáles son los principales ciberdelitos en el contexto nacional y local a través de un ejercicio de revisión documental y de plataformas oficiales del Estado.

Describir y analizar los ciberdelitos en el contexto de la ciudad de Manizales, sus implicaciones y las estrategias de prevención que se han generado a través de la configuración de redes de apoyo.

Proponer estrategias para la prevención de los ciberdelitos que puedan ser adoptadas por la ciudadanía, las instituciones educativas, las autoridades judiciales de la región y el país.

DESCRIPCIÓN DEL PROBLEMA

La seguridad es un aspecto inherente a las necesidades humanas. Los cambios impuestos por los avances tecnológicos en el contexto sociocultural, implican que constantemente las personas deban preocuparse por su bienestar, no solo físico, también digital. Paradójicamente, un gran número de usuarios de plataformas, aplicaciones y redes digitales desconocen los riesgos que asumen al compartir información y las implicaciones que se pueden generar para la víctima y para aquel que comete el delito en el entorno virtual.

Según lo expresa Barrios (2012), en la actualidad el alcance de los equipos tecnológicos es bastante alto, teniendo en cuenta que la mayoría de las personas cuentan por lo menos con un equipo móvil o algún elemento tecnológico, donde la mayoría de esa población tiene conectividad a la red de internet. Es tal vez esta una de las ventanas que abre la posibilidad para cometer actividades delictivas, para las cuales no existen fronteras, ni restricciones de horarios, generando lo que se conoce como delitos transnacionales. Este panorama constituye una problemática que, en primera instancia debe ser atendida por todos los usuarios independientemente de su rol o de su cargo, para generar un estado de alerta permanente frente a los riesgos de sufrir un Ciberdelitos, así como las implicaciones judiciales y las consecuencias en caso de cometerlo.

PLANTEAMIENTO DEL PROBLEMA

La aparición y la evolución de los Ciberdelitos han hecho reaccionar a los Gobiernos de todo el mundo, no solo para fortalecer sus esquemas de seguridad informática, en caso de sufrir ataques cibernéticos que logren filtrar información que ponga en riesgo la seguridad de la nación, también en términos de regulación en el uso de plataformas y tipificación de algunos delitos electrónicos, informáticos o digitales que han generado vacíos legales, al no tener antecedentes históricos de este tipo de actividad.

Pese a que se trata de un fenómeno delictivo popular en todo el mundo, la categorización de los ciberdelitos varía de acuerdo con múltiples variables sociodemográficas como la condición socioeconómica, la educación, las dinámicas socioculturales y desde luego, el acceso a internet. Por ejemplo, en Latinoamérica los delitos informáticos que se presentían de forma más asidua son los siguientes:

Figura 1. *Principales Ciberdelitos en Latinoamérica*

Nota: información obtenida en (Acosta, Benavides, & García, 2020)

En Colombia, La Policía Nacional (2023) ha identificado varios tipos de delitos informáticos que se cometen en el país, jerarquizando aquellos más comunes o que se presentan

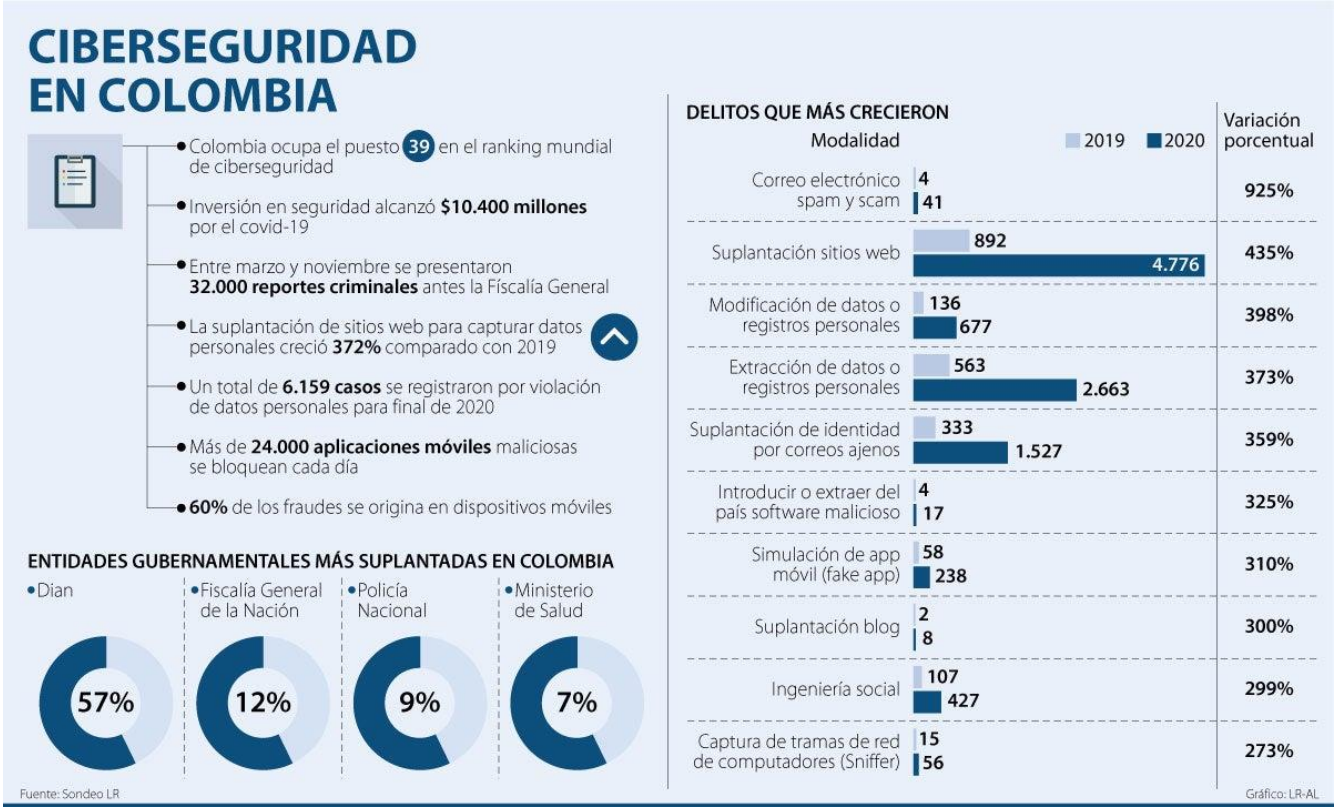
con mayor frecuencia como es el caso del Fraude electrónico, donde se usa la red de internet para realizar una estafa que permite obtener dinero de forma ilícita; la suplantación de identidad, que se refiere a la usurpación del nombre y los datos de una persona para realizar transacciones o enviar correos maliciosos; el robo de información, que implica la obtención ilegal de datos confidenciales, bancarios o personales para fines malintencionados; el acoso en línea, relacionado con el hostigamiento o la intimidación en redes sociales, y la distribución de contenidos ilegales, delito que implica la difusión de material como pornografía infantil o material terrorista.

Para combatir estos delitos, la Policía del país cuenta con una división especializada en ciberdelitos, que se encarga de investigar y prevenir esta serie de situaciones informáticas. Además, se han establecido medidas legales y reglamentarias para combatir estos delitos como la ley de delitos informáticos, que contempla penas severas para quienes los cometan. (Policia Nacional de Colombia, 2023). Pese a esto, los resultados no son óptimos, estimando que hace falta inversión, pero sobre todo un esquema de difusión para la prevención que logra un mayor alcance en el territorio nacional.

La época de confinamiento generada por la pandemia del Covid-19, se convirtió en un escenario ideal para la aparición de nuevas formas de vulnerar la seguridad informática para los ciberdelincuentes, logrando realizar grandes fraudes y múltiples casos de suplantación, aprovechando que la mayor parte de la sociedad se encontraba realizando sus actividades laborales, sociales, familiares o de ocio, a través de internet.

La Figura 2 muestra como la Ciberseguridad representó para el país un momento de crisis en el año 2020.

Figura 2. *Crecimiento de los ciberdelitos en el año 2020 en colombia*

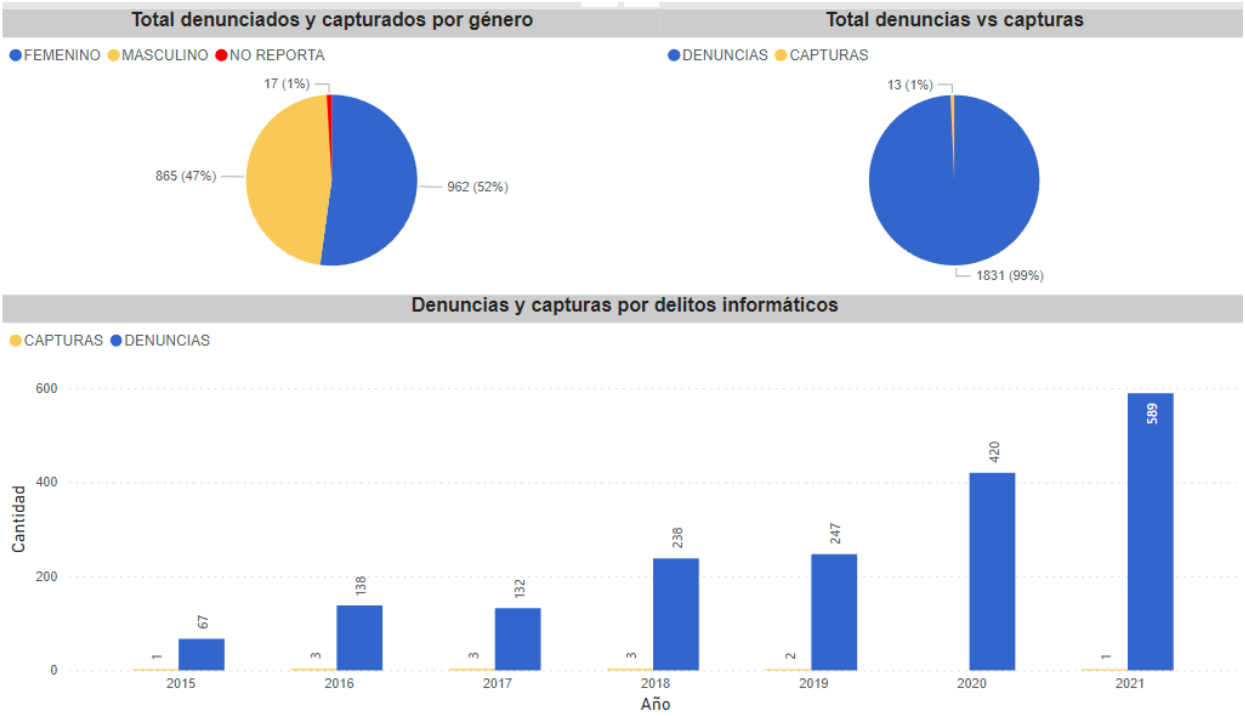


Nota. Información presentada por (Acosta Argote , 2021)

Es evidente cono los Ciberdelitos subieron en al menos un 37% durante el primer trimestre de 2020, considerados por las autoridades como los peores meses de la crisis y determinando que la suplantación de identidad fue el fraude más común, no solo en los entornos financieros, también educativos y sociales.

En este mismo orden de ideas, en la ciudad de Manizales se reconoce un aumento considerable en el sistema de denuncias por delitos informáticos durante los años 2019,2020 y 2021; sin embargo, también se corrobora que las autoridades no tienen la capacidad para resolver las situaciones denunciadas, dado el bajísimo número de capturas.

Figura 3. *Denuncias y capturas por ciberdelitos en la ciudad de Manizales*



Nota. Estadística anual de denuncias y capturas en la ciudad de Manizales. Policía Nacional de Colombia.

Es claro entonces que, en el caso de la ciudad de Manizales, la existencia de distintos delitos informáticos coincide con la mayoría de este tipo de delitos que se presentan en el país: acceso abusivo a un sistema informático; obstaculización ilegítima de sistema informático o red de telecomunicación; interceptación de datos informáticos; daño Informático; uso de software malicioso; violación de datos personales; suplantación de sitios web para capturar datos personales; hurto por medios informáticos y semejantes; Transferencia no consentida de activos.

Cada uno de estos actos encuentra tipificado en la normatividad sobre delitos informáticos Ley 1273 de 2009; sin embargo, hace falta pedagogía y difusión de la información, para que la sociedad, en términos de prevención, asuma posturas y tome medidas que protejan su identidad, su reputación y sus bienes en el marco de las operaciones y la exposición digital.

Este documento es pertinente porque presenta un aporte en la estrategia de prevención y difusión de los delitos informáticos describiendo y analizando su incidencia la ciudad de Manizales, tomando como referencia los informes presentados por la Policía Nacional de Colombia y los datos estadísticos de otras entidades del Estado, para diseñar una guía infográfica que sintetice los datos, permita una mayor comprensión de la problemática y entregue algunos consejos prácticos para evitar ser víctima de diferentes tipos de Ciberdelito.

JUSTIFICACIÓN

La actividad cotidiana se movilizada cada día con más intensidad hacia internet, razón por la cual el grado de exposición de las personas se hace más complejo y crítico. Es pertinente conocer el alcance de las acciones propias y ajenas en los entornos virtuales y en las plataformas de interacción social, prestando especial atención a la posible vulneración de la intimidad y de los datos que se pueden generar en todo momento.

Al hacer referencia a los ciberdelitos, ineludiblemente se debe hacer alusión a aspectos como seguridad, prevención, cultura digital y normatividad. No se trata de la reiteración de una conducta social o un hecho aislado, ajeno a la realidad del territorio colombiano, por el contrario, tal como lo afirma el portal Pantallas Amigas (2014), ser víctima de ciberdelitos o incluso competerlos por desconocimiento va más allá de la mala suerte, se trata de un riesgo asociado con la cultura en línea, situación para la cual cada ciudadano debería estar preparado.

Pese al cúmulo de información y a la difusión diaria de noticias relacionadas con toda clase de avisos y delitos cometidos a través de internet estafas, amenazas, difamaciones, acoso, entre otros, el control técnico y el control jurídico se quedan cortos. Por esta razón abordar el tema de los ciberdelitos resulta pertinente, no solo para el reconocimiento de los principales casos en el país, también para generar un análisis del contexto local, en este caso la ciudad de Manizales, y promover una contribución tangible a través de una guía infográfica, documento donde se condensen las situaciones, la normativa y las recomendaciones en torno a los ciberdelitos.

CONTEXTO GEOGRÁFICO

En Europa desde hace unos años se han tomado medidas contra la delincuencia informática, en atención al crecimiento de usuarios de internet y la difusión de plataformas y espacios virtuales de teletrabajo o enseñanza-aprendizaje. Precisamente, La –unión europea se ha encargado de promover la atención que se debe prestar a la ciberdelincuencia tomando desde el año 2001 la decisión de firmar el tratado de Budapest, ante el crecimiento, las fallas y los vacíos legales asociados con el auge de las nuevas tecnologías. No obstante, para ese momento, pocos países gozaban de una adecuada infraestructura tecnológica y por lo tanto minimizaron el impacto del acuerdo, además la regulación y la normatividad legal frente a aquello que se podía considerar un Ciberdelito era incipiente.

En Colombia, los delitos informáticos representan, especialmente durante la última década, un problema en constante crecimiento, producto del aumento de la penetración de las tecnologías de la información y la comunicación en la sociedad. El hacking, la ciberextorsión, el phishing, el fraude en línea y la pornografía infantil son tal vez los delitos más populares en el territorio nacional, que, ante la falta de leyes, la ausencia de recursos para la seguridad informática en el caso de muchas plataformas y la poca cultura de las personas para proteger sus datos o tomar precauciones antes de ingresar a los entornos virtuales, se multiplican hasta convertirse en fraudes o delitos de una mayor proporción.

En el país es común escuchar que se mencionen los hackers como los causantes de las fallas en seguridad y responsables de los delitos informáticos, haciendo uso de técnicas avanzadas que les impiden ser rastreados. Manizales, pese a ser una ciudad intermedia en el orden nacional, también registra un aumento anual de los delitos informáticos, lo que ha puesto en alerta a las autoridades locales y regionales, llevándolas a emprender acciones como la

estrategia Ciudadano Ciberseguro, que desde el año 2021 está enfocada en la preparación de estudiantes, familias y empresas frente a los riesgos que trae el uso de las nuevas tecnologías.

Cabe mencionar que en la ciudad se presentan múltiples hurtos por internet, siendo este uno de los delitos más frecuentes, por eso, la manera de contrarrestar esta problemática desde la administración local ha sido mediante la formación de ciudadanos ciberseguros, una apuesta que debe comenzar a dar rendimientos positivos durante los próximos años.

Figura 4. *Campaña Ciudadano Ciberseguro*

Nota. Imágenes de la campaña ciudadano Ciberseguro de la ciudad de Manizales, promovidas por la secretaria de Tic y Movilidad en el año 2021

MARCOS DE LA INVESTIGACIÓN

ANTECEDENTES

Para Prado (2022), según lo expresa en el documento de investigación “Los delitos informáticos y su soporte probatorio”, las teorías del delito que se aplican en el país, guardan una relación directa entre el delito y la acción ejercida, donde se deben establecer los elementos del dolo sobre el individuo, tales como el conocimiento previo de que se está incurriendo en un delito o en una falta a la ley, así como la voluntad para desarrollar dicha conducta.

En consecuencia, en el documento se establece una jerarquización de los delitos informáticos, aclarando que estos deben considerarse como trasnacionales, puesto que superan las fronteras de los países, además, se desarrollan de manera amplia en un campo amplio que va desde los delitos del patrimonio hasta los delitos sexuales. Finalmente, la recolección de la información digital para el seguimiento de un caso de orden penal, deberá siempre ser tratada por personal idóneo para evitar su adulteración.

En el documento “¿Qué diferencias en ciberdelitos existen entre Colombia y España?” Publicado por Ayala y Dique (2022), se persigue el cumplimiento de un objetivo asociado con la identificación de las diferencias de ciberdelitos entre dos países que hablan la misma lengua, detalle que también representa una relación entre los victimarios. Asimismo, se establece un análisis sobre el convenio de Budapest como norma pionera para combatir la problemática.

La metodología de revisión documental asume un estilo de literatura comparada, donde se analizan no solo los ciberdelitos más comunes, también la forma en la que han sido abordados a partir de la normatividad legal vigente de cada gobierno. Es así como se concluye que en Colombia se protege el bien jurídico de la información y los datos, mientras en España se ha

logrado avanzar un poco más en la protección de la intimidad, el derecho a la propia imagen y la violación del domicilio.

El documento presentado por ONU(2021), denominado “Recopilación de todas las conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros durante las reuniones del Grupo de Expertos encargado de realizar un estudio exhaustivo sobre el delito cibernético celebradas en 2018, 2019 y 2020”, es producto del trabajo de un grupo de expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético en la ciudad del Viena. En este informe se presenta unas recomendaciones y observaciones sobre la tipificación de los delitos informáticos que deben realizar los países, aspecto que lo convierte en un documento absolutamente relevante. Aclarando que Los Estados Miembros deberían tener en cuenta que muchas disposiciones sustantivas del derecho penal concebidas para los delitos no cometidos en línea también pueden ser aplicables a los delitos cometidos en línea.

Dentro de la tipificación se encuentran los delitos cibernéticos básicos que afectan a la confidencialidad, la integridad y la disponibilidad de las redes de computadoras y los datos informáticos; las formas de actividad cibernética delictiva nuevas y emergentes, como el uso indebido delictivo de criptomonedas, los delitos cometidos en la web oscura y la Internet de las cosas, el phishing, y la distribución de programas maliciosos y otros programas informáticos utilizados para cometer actos delictivos; la divulgación de información personal y la pornovenganza; el uso de Internet para cometer actos relacionados con el terrorismo, para incitar a cometer delitos motivados por prejuicios y al extremismo violento; la prestación de apoyo técnico o asistencia para la comisión de un acto cibernético delictivo; la creación de plataformas en línea ilícitas o la publicación de información para cometer delitos cibernéticos; la obtención de acceso por medios ilícitos a sistemas informáticos o la piratería de dichos sistemas; la

interceptación o el daño ilícitos de datos informáticos y el daño ilícito a sistemas informáticos; la interferencia ilícita en los datos y sistemas informáticos; el uso indebido de dispositivos; la falsificación y el fraude informáticos; el abuso y explotación sexuales de menores; la infracción de la propiedad intelectual; el abuso y explotación sexuales de menores, y la inducción de menores al suicidio; xv) la influencia ilícita sobre infraestructuras de información esenciales.

Acosta, et al. (2020), en el documento "Delitos informáticos: impunidad organizacional y su complejidad en los negocios", se refiere a la importancia de determinar y jerarquizar los diferentes tipos de delitos informáticos y a partir de allí, diseñar una herramienta de vanguardia en el ámbito de la seguridad para enfrentar de manera efectiva las consecuencias de cada delito y entender el funcionamiento desde el rol de víctima de este acto delictivo. El en documento se hace hincapié en que cada usuario debe asumir un cuidado especial con la información de primer nivel (personal, financiera, empresarial) y comprender el funcionamiento y las alertas de los sitios o aplicaciones que frecuenta, ya que estos pueden ser vulnerados por profesionales de oficios (hacker, cracker, phracker y piratas informáticos), pasando de ser usuarios, a víctimas.

La perspectiva metodológica de la investigación es exploratoria y toma los resultados de la búsqueda de leyes y documentos legales sobre normativa en torno a los ciberdelitos para triangularlas con las actuaciones jurídicas en algunos casos que se han presentado en el país, concluyendo que no solo se trata de la existencia de la ley, también del conocimiento y la difusión de la misma, acercando los fundamentos del derecho a los usuarios, porque paradójicamente quienes cometen el delito si permanecen al tanto de las actuaciones y las omisiones de la norma. Cabe mencionar que se trata de un estudio relevante porque aborda con mayor énfasis los casos de estafa y fraude financiero que en el territorio nacional y en el ámbito local se reconocen como uno de los delitos más frecuentes.

El informe de la Interpol (2020), denominado “Ciberdelincuencia: efectos de la Covid-19, presenta un panorama general y deductivo del impacto de los ciberdelitos en los diferentes continentes y posteriormente en las regiones”. El punto de partida para el estudio es la pandemia sin precedentes que afectó el panorama mundial de las ciberamenazas, intentando evidenciar la dificultad que representó para las autoridades enfrentar la crisis sanitaria y el aumento de la actividad delictiva e la red.

El documento explica que cada vez son más los particulares y pequeñas empresas, que se centran en construir una infraestructura se adecué no solo a las necesidades, también a los riesgos, generando un esquema de protección o alerta temprana sobre un posible ciberdelito. Precisamente, en vista de estos hechos, la Dirección de Ciberdelincuencia de Interpol ha aprovechado su exclusivo acceso a datos de los 194 países miembros y de sus socios privados para elaborar el Informe de evaluación global sobre los delitos cibernéticos relacionados con la COVID-19, ofreciendo una visión competa del panorama de la ciberdelincuencia.

La metodología del informe se basa en los datos recopilados de todos los países miembros en el marco de la encuesta mundial de INTERPOL sobre ciberdelincuencia realizada en el año 2020 y una posterior sistematización que permitió dentro de los resultados, emitir una serie de recomendaciones generales, aspecto similar al presente ejercicio investigativo, pero con la diferencia en el contexto geográfico y la elección de los tipos de ciberdelitos, que varían según el territorio.

En el documento “Los delitos informáticos en el ámbito de la protección del patrimonio personal según el Derecho Penal” presentado por Quesada (2016), se realiza un análisis desde la perspectiva del impacto de la globalización en el uso de las redes y los avances, a proyección y el desarrollo del sector financiero a través de este campo. El autor reflexiona acerca de todas las

operaciones que los usuarios han logrado simplificar mediante el uso de la tecnología, pero al mismo tiempo explica que esto comporta series riesgos asociados con la presencia de delitos informáticos. En el documento se aborda como pregunta de investigación si son suficientes los lineamientos de la legislación penal colombiana para la protección del bien jurídico de la información y de los datos en el caso de los delitos informáticos.

La metodología empleada para configurar el documento es descriptiva, acudiendo a la revisión documental de la norma y la doctrina relacionada con la ciberdelincuencia, tomando como categoría de análisis la afectación de los derechos para el uso de la red de internet que supone el uso de internet desde la óptica del Derecho Penal.

El autor concluye que los delitos informáticos representan uno de los casos penales que más se reconocen en redes, asociados con estafas, hurtos, injurias, acoso, entre otros y que pese a ser tan comunes no se pueden normalizar, ya que en teoría, las legislaciones han adoptado cambios e instrumentos normativos de carácter internacional para hacer frente a esta problemática. El texto finaliza afirmando que existe en el país un interés legítimo del legislador para la salvaguarda y reivindicación de los derechos de los ciudadanos.

Barrios (2012) es el autor de la investigación “El delito informático en la legislación colombiana”, documento que describe las conductas delictivas asociadas con el avance tecnológico y las implicaciones desde el punto de vista normativo. Bajo un enfoque de revisión documental con una perspectiva de análisis hermenéutico, el autor propone que se analice el momento actual del derecho penal colombiano frente a la conducta compleja de los delitos informáticos.

Este documento en particular, pese a tener una década de su publicación, representa un insumo bastante interesante, porque permite reconocer el inicio de los procesos de capacitación y preparación de toda la sociedad, no solo de las autoridades y entidades del estado, también del ciudadano común, frente a un flagelo que terminaría por convertirse en una amenaza permanente. En el documento también se hace referencia al ciberterrorismo como una amenaza catastrófica para la sociedad mundial, lo que conlleva a reforzar la seguridad y a tejer una red de apoyo internacional para la cooperación ante este tipo de problemáticas.

Ojeda, et al. (2010), en el documento "Delitos informáticos y entorno jurídico vigente en Colombia" describen y analizan la evolución de los delitos informáticos a la luz de la Ley 1273 del año 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. Esto indica que desde ese momento se equipara la legislación colombiana con la de otros países en términos de cibercrimen, toda vez que se trata de un fenómeno que para ese momento venía afectado las relaciones y las comunicaciones personales, empresariales e institucionales.

En el documento se asume el ciberdelito como una tendencia que incide no solo en el campo tecnológico también en el económico, político y social, por lo que se realiza un análisis detallado de la norma, su aporte y alcance, junto a otros elementos de juicio que permitan entender la realidad de la seguridad informática. El enfoque metodológico es analítico descriptivo y se basa en el análisis del marco jurídico para concluir que las comunicaciones y la informática representan un nuevo paradigma de las relaciones personales, que requiere con urgencia un complemento legal para combatir los delitos que se generan, toda vez que ponen en riesgo no solo a las personas, también a las organizaciones. Toda esta situación requiere un

apropiado conocimiento del contexto tecnológico, informático y de sus proyecciones delictivas, razón que refuerza la necesidad de configurar un documento como el que se presenta en el desarrollo de esta investigación.

MARCO NORMATIVO

El crecimiento de los entornos virtuales, las tecnologías de las telecomunicaciones y la administración de plataformas y sistemas informáticos es un asunto que involucra tanto a las personas como a las instituciones u organizaciones. El mundo actual permanece en línea, es decir, conectado, situación que genera un nuevo contexto para la convivencia ciudadana, la interacción y el ejercicio profesional. Por esta razón, durante las últimas dos décadas, los gobiernos de todo el mundo han depurado sus leyes, ampliando la capacidad y el alcance de sus herramientas jurídicas y sus competencias, intentando regular las problemáticas, que se configuran como delitos dentro el escenario virtual.

El Convenio de Budapest

Es un tratado internacional que tiene como objetivo combatir la cibercriminalidad y proteger los derechos y libertades fundamentales en línea. Fue adoptado en la ciudad de Budapest, Hungría, en el año 2001, entrando en vigencia desde el año 2004. El convenio establece medidas para prevenir y combatir delitos cibernéticos como el acceso ilegal a sistemas informáticos, el sabotaje informático, el fraude informático y la pornografía infantil en línea. En el Tratado también se establecen las normas para la protección de datos personales y la privacidad en línea, por este motivo, es considerado uno de los tratados más importantes en la lucha contra la cibercriminalidad a nivel internacional y ha sido ratificado por más de 60 países, incluyendo los Estados Unidos y los países de la Unión Europea. (Unión Europea, 2001)

Se debe mencionar que el convenio de Budapest se subdividió entre los artículos 2 y 6, como las conductas contra “la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos”, como son el acceso ilícito, la interceptación ilícita, ataque a la integridad del sistema, ataque a la integridad de los datos y abuso de los dispositivos. Y en los artículos 7 y 8, como conductas informáticas, en este caso la falsificación y el fraude informático.

En el territorio colombiano, los riesgos informáticos están relacionados principalmente con el robo de datos personales y empresariales, la violación de la privacidad, la propagación de malware y virus, y el fraude en línea. Para combatir el crimen informático, la ley en Colombia cuenta con instrumentos legales como la Ley 1273 de 2009, donde se tipifican como delitos las conductas relacionadas con la delincuencia informática, y la Ley 1581 de 2012 que regula la protección de datos personales.

Ley 1237 de 2009

Se trata de la normatividad sobre delitos informáticos, por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado, denominado De la protección de la información y de los datos, buscando preservar la integridad de los sistemas que utilicen tecnologías de la información y las comunicaciones. Dentro de la ley se hace énfasis en la descripción de los ciberdelitos a través de un articulado presentado de la siguiente manera:

> **Artículo 269A.** Acceso abusivo a un sistema informático.
>
> **Artículo 269B:** Obstaculización ilegítima de sistema informático o red de telecomunicación.
>
> **Artículo 269C**: Interceptación de datos informáticos.

Artículo 269D: Daño Informático.

Artículo 269E: Uso de software malicioso.

Artículo 269F: Violación de datos personales.

Artículo 269G: Suplantación de sitios web para capturar datos personales.

Artículo 269I: Hurto por medios informáticos y semejantes.

Artículo 269J: Transferencia no consentida de activos.

Ley 1581 de 2012

Esta ley estatutaria establece las disposiciones generales para la protección de datos personales, desarrollando el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que existan sobre ellas en bases de datos o archivos. Para lograr que se implemente la normativa, se establecen una serie de principios rectores para el tratamiento de datos: Principio de legalidad en materia de Tratamiento de datos, Principio de finalidad, Principio de libertad, Principio de veracidad o calidad, Principio de transparencia, Principio de acceso y circulación restringida, Principio de seguridad, Principio de confidencialidad.

Ley 599 de 2000

Se trata de la parte del articulado del código penal colombiano, donde se tipifican como delitos la pornografía y la explotación sexual de persona menores de edad a través de internet, estableciendo en el Artículo 218, la regulación para el material de carácter sexual que involucre a

menores de edad re persona menor de 18 años de edad y en el Artículo 219 A, la regulación para el uso de los medios de comunicación para difundir este tipo de información.

MARCO TEÓRICO - CONCEPTUAL

En el marco de la fundamentación conceptual, se debe establecer que dentro de la ley colombiana se ha planteado una normativa que no discrimina a profundidad entre los términos Delito Informático y Ciberdelito, que, pese a referirse a una actividad criminal que se realiza mediante el uso de la tecnología, si presentan algunas diferencia, pues los delitos informáticos son mucho más amplios y pueden incluir cualquier tipo de actividad criminal que involucre la tecnología, mientras los ciberdelitos son más específicos y hacen alusión a las actividades criminales que se hacen únicamente a través de internet.

Diferencia entre delitos informáticos y ciberdelitos

Pese a que se ha buscado un consenso como lo explican Acosta, Benavides y García (2020) en torno a la definición de los ciberdelitos para diferenciarlos de los delitos informáticos, esto lo que ha provocado es la aparición de nuevas nominaciones: delitos teletemáticos, crímenes virtuales, cibercrimen, ciberterrorismo, entre otros, optando más bien por hace énfasis en la protección y la forma de resguardar la los datos de forma legal mediante el uso de programas de seguridad.

El ritmo impetuoso con el que se desarrolla la tecnología, se diseña los aplicativos, se configuran los entornos virtuales para el trabajo y el aprendizaje y se modifican las plataformas de telecomunicación, hace que sea cada vez más estrecha la diferencia que en un determinado momento se estableció entre los delitos informáticos y los ciberdelitos. De acuerdo con Ayala y Duque (2022), “los delitos informáticos son un grupo de conductas genéricas, que adquieren

importancia por el surgimiento de nuevas tecnologías, las cuales buscan proteger la información de las personas que se pueden vulnerar a través de un medio digital" (p.7). Esto se complementa, mencionando que existe un grupo de delitos de esta naturaleza que se comenten con ayuda de la tecnología y a través de la red, pero no aplican directamente en el ciberespacio, como sucede con la estafa o la extorsión, que puede realizarse usando una red social, pero derivar en un resultado físico de constreñimiento de la voluntad de la persona. Según Ayala y Duque (2022): "estos delitos se caracterizan porque ponen en peligro algunos bienes jurídicos como el patrimonio, la fe pública, la intimidad personal, la libertad y formación sexual, el honor, los derechos morales y patrimoniales de autor" (p.8).

Por otro lado, los ciberdelitos, que son una extensión de los delitos informáticos, se entienden como los delitos que son realizados propiamente dentro de la web. Para Posada (2017), se debe considerar que la doctrina especializada ha dicho que "los ciberdelitos o cibercrímenes son aquellos comportamientos ilícitos que se dirigen a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación" (p.103).

En este caso, para la diferenciación de los ciberdelitos, se debe tener en cuenta que a diferencia del delito informático, donde se usan los sistemas como medio para este tipo de conductas, si se requiere una conexión y permanencia dentro de la red o plataforma de datos para realizar las conductas punibles. Tomando las palabras de Ayala y Duque (2022):

> Diferenciar entre ciberdelito y delito informático es de gran relevancia, ya que como se puede observar en la ley 1273 del 2009 (que sirvió para la creación de un nuevo bien jurídico en Colombia llamado, "de la protección de la información y de los datos") , ayudó a demostrar que es lo que se quiere proteger, mencionando de forma explícita la confidencialidad, la integridad y la disponibilidad de los

> datos y de los sistemas informáticos; no obstante, el 269I y 269J habla de los atentados informáticos y otras infracciones. Se puede evidenciar que se sanciona dos cosas diferentes, en el primer caso los datos y sistemas informáticos, y en el segundo caso son los atentados informáticos y otras inflaciones, demostrando que del artículo 269A al 269G son ciberdelitos porque son delitos que solo se pueden cometer a través de sistemas informáticos y los artículos 269I y 269J son delitos informáticos ya que utilizan los sistemas informáticos como medios para cometer otras infracciones. (p.12)

Delitos informáticos

Se considera como delito informático la actividad relacionada con el uso ilegal de sistemas informáticos, la distribución de malware, la interrupción de servicios de red o la explotación de vulnerabilidades en sistemas, Según lo explica Prado (2022), los delitos informáticos son una rama de conductas delictivas que están reconocidas en la norma, para proteger los bienes jurídicamente tutelados, por eso so contemplan delitos que atentan contra el patrimonio, contra la integridad moral, física y sexual.

Al tratarse de un campo de aplicación tan amplio “se deben mantener las condiciones básicas de los delitos, para que las conductas sean valoradas desde el juicio de tipicidad objetiva, es decir, que estas sean típicas, antijurídicas y culpables, excluyendo la responsabilidad objetiva como lo dice el estatuto penal” (p.10). Esto quiere decir que los delitos se pueden juzgar de igual forma, independientemente de haber sido cometidos en un escenario real o en un escenario virtual.

En definitiva, según Acosta, Benavides y García (2020) el delito informático es:

> Una forma de delinquir extrayendo información personal directamente del ciberespacio, el cual abarca el problema, amenazando entornos privados de la sociedad en general, además de adicionar posibles daños patrimoniales, personales o empresariales, producidos por el abuso de datos extraídos (p. 356).

Pese a la existencia en la normativa, es muy importante considerar que los delitos de esta naturaleza no cuentan con fronteras, por tanto, se consideran transnacionales, toda vez que se ejecutan por medios tecnológicos. En este caso, el recaudo probatorio, tal como lo explica Prado (2022):

> Requiere que se realice a través de expertos en informática, denominados peritos, situación y que se involucre de manera activa al juez de control de garantías, quien debe avalar el recaudo de los elementos de prueba en unos términos absolutamente perentorios, como en los casos de recuperación de información o la incautación o aprehensión de equipos. (p.12)

Ciberdelitos

Se trata de un término para referirse al tipo de actividad criminal que se lleva a cabo a través de la red, utilizando medios electrónicos, como Internet. Los ciberdelitos pueden incluir actividades como el robo de información personal, el fraude en línea, el robo de propiedad intelectual o el ciberespionaje.

Sin duda, tal como lo afirman Acosta, Benavides y García (2020): “el delito organizado se ha fortalecido a través de los años, debido a la misma evolución del sistema en general y, a la transnacionalización de sus redes delictivas” (p. 13). Desde esta perspectiva, la red de ciberdelitos ha logrado extenderse y focalizar sus objetivos en el mercado financiero y

empresarial, con mayor frecuencia. Según Torres, (2015): “la modernización ha traído consigo, que el manejo de la información se realice mediante procesadores informáticos que permiten almacenar una cantidad considerable de información y que, al mismo tiempo, se pueda acceder de manera rápida y efectiva a esos datos” (p.116). Se trata además de un esquema donde no se discrimina entre la información personal, institucional o empresarial.

El abanico de posibilidades para los ciberdelitos se abre para los delincuentes informáticos, quienes sacan provecho a través de estrategias como el chantaje, el desprestigio o el secuestro de información. Por eso, cuando se habla de un ciberdelito, Fuentes, Mazún y Cancino (2018) refieren que se trata de un conjunto de comportamientos que generan un delito penal y que debe ser tratado legalmente, ya que este tiene por objeto generar daño a terceros, derivando en algunos casos en la pérdida de bienes jurídicos. La Organización para la Cooperación y el Desarrollo Económico – OCDE- (2014) manifiesta que un ciberdelito viene dado por el comportamiento ilegal que es contrario a le ética y no es autorizado, por eso tiene restricciones de divulgación y transmisión de datos en la red.

Tipología de los delitos

Si bien, cada territorio presenta diversidad en el tipo de infracciones o delitos cometidos mediantes el uso de la tecnología y en los entornos virtuales, resulta conveniente asumir una postura de análisis que coincida con la tipificación que se propone en la presente investigación. Lara, Martínez y Viollier (2014) simplifica la clasificación de los delitos informáticos o ciberdelitos nominándolos de la siguiente forma: acceso No autorizado, daño a datos o programas informáticos, sabotaje informático, interceptación no autorizada, espionaje informático

Tabla 1. Infractores, recomendaciones y riesgos de delitos informáticos

DELITOS	INFRACTORES	RECOMENDACIONES	RIESGOS
Acceso no autorizado	Hacker/Cracker	▪ Utilizar contraseñas seguras. ▪ Mantener como política auditoría de accesos y niveles de seguridad en los usuarios.	Riesgo de acceso
El daño a los datos o programas informáticos	Phracker	▪ Poner especial atención en el tratamiento de correos electrónicos. ▪ Tener una política en cuanto a la inserción de dispositivos (flash, cd…). ▪ Disponer de un programa que respalda la data diariamente.	Riesgo en la infraestructura
El sabotaje informático	Piratas informáticos	▪ Navegar por páginas web seguras y confiables. ▪ Instalar Antivirus.	Riesgo de seguridad general
La intercepción no autorizada	Hacker	▪ Utilizar firewall. ▪ Instalar indicadores de usuarios no autorizados.	Riesgo de desaparición de los controles tradicionales
El espionaje informático	Cracker/Piratas informáticos	▪ Actualizar regularmente el sistema operativo. ▪ Ser cuidadoso al utilizar programas de acceso remoto. ▪ El manejo de la data debe estar custodiada por personal de confianza.	Riesgo de dependencia en el personal clave. Riesgo de utilidad.

Nota: información obtenida de Lara y Viollier (2014)

Tomando como base la clasificación propuesta en la Tabla 1, se puede hacer alusión también a los ataques más comunes que se presentan en el ciberespacio colombiano, tal como lo plantea González (2020), que no discriminan entre empresas, usuarios naturales o gobiernos. Se trata de una de las amenazas más significativas en la actualidad y exige que se priorice la seguridad en todo en el torno virtual, sobre todo cuando el flujo de información depende de la conexión a la red. La revista Portafolio (2018) determinó en un estudio acompañado por la compañía Microsoft, que Colombia estaba era el segundo país de América Latina más expuesto a riesgos de delitos informáticos, afirmando que “el 12% de los sistemas móviles habían sido atacados al menos una vez por un Software malicioso (Malware).

Algunos de los ciberdelitos comunes en el mundo, que se perciben con mayor frecuencia en Colombia son:

Los ataques bancarios. Acción que les permite a los delincuentes obtener beneficios lucrativos, obtener información privada y violentar los sistemas de seguridad de las empresas

El Cibercrimen. Se refiere a las conductas inadecuadas que constituyen un delito dentro del ciberespacio. Las más comunes son la suplantación de identidad, el robo de información, las estafas y los fraudes.

La Estafa Nigeriana. Es un tipo de engaño donde la víctima es persuadida a través de un correo electrónico que le indica que a obtenido un premio asociado con una solicitud de un depósito de dinero para hacer la entrega del beneficio.

Estafa electrónica. Se trata de un delito común en el país, puesto que se realiza a través de las redes sociales, donde las víctimas guardan silencio para no ser expuestas o ridiculizadas y la acción no alcanza trascendencia al no ser denunciada.

Forjacking. Es una nueva modalidad donde se introduce un código dañino en páginas web para realizar el robo de información. Suele estar enfocado en los proveedores y en las cadenas de abastecimiento de las entidades.

Malware: Se trata de un Software malicioso, cuyo fin es dañar dispositivos y robar datos con algún fin lucrativo. Los más comunes son los virus, los troyanos, el spyware, los gusanos u el secuestro de datos (ransomware)

Phishing: Se refiere a un método de engaño, solicitando a la víctima información confidencial como contraseñas, a través de correos electrónicos o páginas web falsas.

Ransomware: En este delito, los intrusos obtienen información para luego solicitar un rescate.

Vishing: Es un tipo de delito que se deriva del phishing, donde se engaña a las víctimas por medio de llamadas telefónicas y un delincuente informático puede suplantar la identidad de una entidad reconocida y solicitar datos confidenciales o la descarga de algún programa que puede ser un malware. Al combinar voz y phishing le hacen creer a la víctima que se comunican con personal de confianza.

Los delitos sexuales

Sin duda los delitos sexuales merecen una mención especial, considerando que existen plataformas y medios virtuales que han promovido la pornografía como una clase de entretenimiento para adultos; sin embargo, los riesgos de carácter sexual dentro de los delitos informáticos son el territorio colombiano una realidad que afecta a niños, niñas, adolescentes y adultos. Estos riesgos incluyen el ciberacoso, la sextorsión, el grooming y la explotación sexual en línea.

Ciberacoso. Es una forma de acoso en línea que puede incluir insultos, amenazas, humillaciones y difamaciones. Se realiza a través de una red social o un canal virtual de comunicación.

Sexting. Se refiere al envío y recepción de contenido sexual explícito a través de dispositivos móviles, lo que puede resultar en la explotación sexual de menores.

Sextorsión. Se trata de una forma de chantaje que consiste en amenazar a una persona con publicar imágenes o videos íntimos si no accede a las demandas del chantajista.

Grooming. Estrategia utilizada por los agresores sexuales para ganarse la confianza de menores de edad con el fin de conseguir imágenes íntimas o establecer encuentros sexuales.

Explotación sexual en línea. Es la producción, distribución y consumo de material sexual explícito que involucra a menores de edad, independientemente de su consentimiento.

Frente a los delitos sexuales se debe añadir que la ley en Colombia cuenta con instrumentos legales para enfrentar estos riesgos, como la Ley 1336 de 2009 que penaliza el acoso sexual y la Ley 1979 de 2019 que regula la protección integral de la infancia y adolescencia contra la violencia. Sin embargo, la aplicación de la ley es un tanto complicada, debido a la dificultad para identificar a los agresores y la complejidad de las pruebas digitales.

Es importante también que los ciudadanos estén informados sobre los riesgos de carácter sexual en delitos informáticos y tomen medidas preventivas para evitar ser víctimas, asumiendo un uso responsable las redes sociales y adoptando estrategias de seguridad en línea. Claro está, que la recomendación más importante es la denuncia de cualquier conducta sospechosa o delito de este tipo a las autoridades competentes.

Los delitos informáticos / ciberdelitos en Colombia

De acuerdo con la fiscalía general de la Nación de Colombia, se reportaron 16,748 casos de delitos informáticos en el año 2020. Esta cifra representa un aumento del 38% en comparación con el año anterior, donde se reportaron 12,131 casos.

Los delitos informáticos más comunes reportados en el país incluyen la suplantación de identidad, el acceso abusivo a sistemas informáticos, la estafa y el fraude electrónico, el hurto informático y la pornografía infantil.

Según un informe de la Policía Nacional, durante los primeros meses del año 2021 se registró un aumento del 41% en los delitos informáticos en comparación con el mismo periodo del año anterior. Es importante destacar que estas cifras pueden no reflejar la totalidad de los delitos informáticos en el país, dado que muchos de estos delitos no son denunciados o reportados a las autoridades correspondientes.

Un dato que resulta relevante lo presenta un estudio realizado por la firma de seguridad informática Kaspersky (2021), donde se afirma que Colombia es uno de los países de Latinoamérica con mayor cantidad de ataques de phishing, una técnica utilizada por los ciberdelincuentes para obtener información confidencial de manera fraudulenta, a través de correos electrónicos falsos que parecen provenir de empresas o instituciones confiables. El estudio revela que, durante el segundo trimestre de 2021, Colombia ocupó el tercer lugar en Latinoamérica con mayor cantidad de ataques de phishing, con una tasa del 17,5%. Además, el sector más afectado por este tipo de ataques en Colombia fue el financiero, seguido por el sector gubernamental y el de los servicios de internet.

Esto pone de manifiesto la importancia de que los usuarios de internet en Colombia estén cada vez más informados y capacitados para identificar y evitar este tipo de ataques, así como la necesidad de que las empresas y organismos públicos implementen medidas de seguridad efectivas para proteger la información de sus clientes y usuarios.

METODOLOGÍA

El estudio sobre los delitos informáticos y los ciberdelitos es de naturaleza cualitativa con un enfoque descriptivo, que desde la perspectiva de Hernández, Fernández y Baptista (2010) permite describir, comprender e interpretar un fenómeno a través de las percepciones la indagación y la experiencia. En este caso se acude a la revisión de la lit4eratura, pero también a las bases de datos especializadas en los asuntos relacionados con los delitos informáticos o cibernéticos, que principalmente son aportados por la Policía Nacional de Colombia.

La naturaleza de la investigación garantiza un acercamiento a la cotidianidad de la problemática en el país, visibilizando los tipos de ciberdelitos más comunes. Este enfoque permite además comprender la conducta social, sus actuaciones en términos de omisión o denuncia y la forma en la que se expanden este tipo de delitos para alcanzar nuevas dimensiones a nivel social, económico o cultural.

Es importante aclarar que este estudio no se basa en métodos de recolección de datos estandarizados, porque no se pretende una jerarquización, ni una revisión cuantificada de los resultados, por el contrario, se plantea la comprensión de una problemática para determinar alternativas de solución y establecer una serie de conclusiones.

El producto u objeto de diseño de esta investigación es una Guía Infográfica (https://issuu.com/mauriciomarquez79/docs/infografia_final1), donde se organicen de forma amigable y dinámica los principales delitos informáticos y ciberdelitos y se presenten estrategias, consejos o recomendaciones para que las personas dimensionen el impacto de las acciones ilegales a través de los medios virtuales y tomen conciencia sobre el uso responsable de la tecnología.

La guía infográfica como instrumento, presenta una colección de imágenes y datos en un texto simpe que sintetiza una información específica que puede ser fácilmente decodificada. Asimismo, se debe resaltar el valor de una infografía como material didáctico, toda vez que representa la base de un proceso formativo. De acuerdo con Paredes (2018):

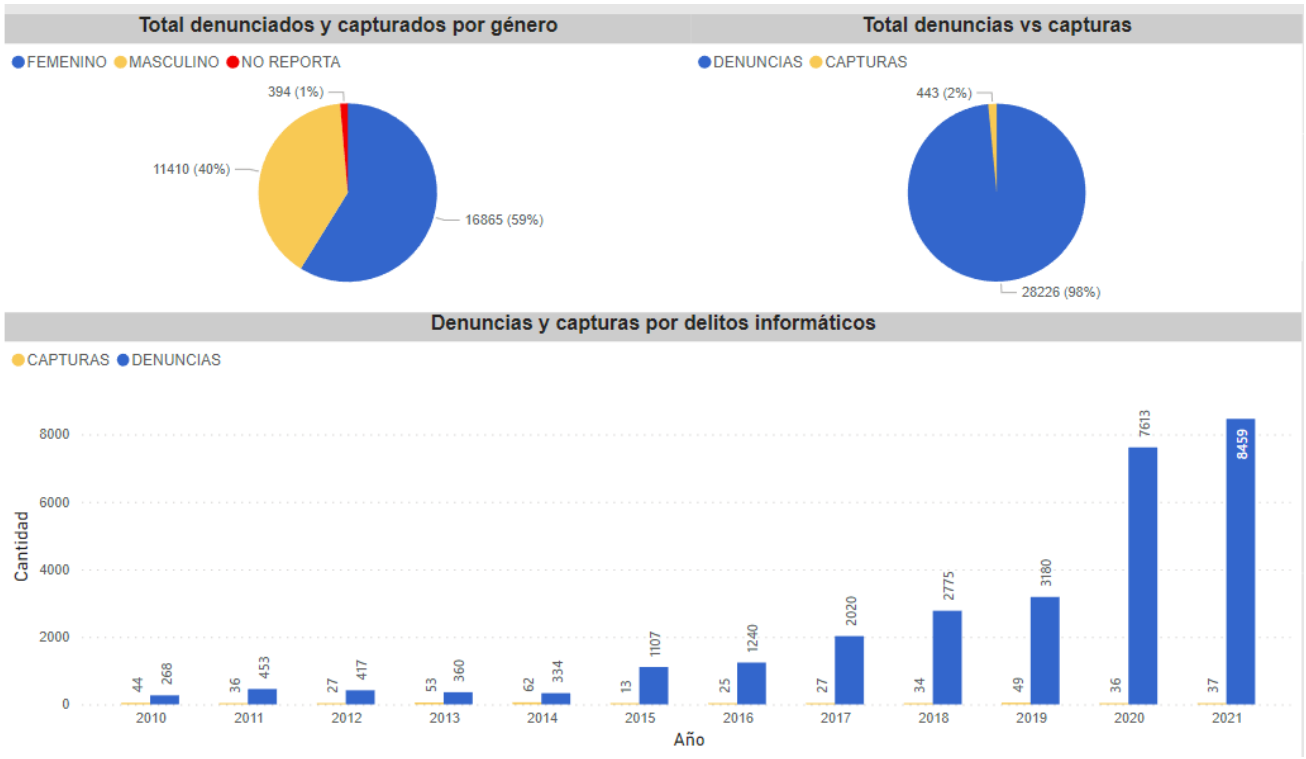
> La infografía ha estado presente siempre de forma habitual en los libros para completar los contenidos curriculares y presentarlos de una manera más atractiva o en forma de láminas ilustrativas que se colocan de manera estratégica en distintos espacios. Su potencial es claro y es una herramienta didáctica muy apreciada (…) Es una herramienta eficaz que favorece y facilita la comprensión y retención de conocimientos complejos y un recurso didáctico para presentar ciertas temáticas de forma comprensible y amena a la sociedad. (p.16)

RESULTADOS

La Policía Nacional de Colombia es la entidad encargada de realizar la recopilación de los datos estadísticos consolidados de todo el territorio nacional sobre delitos informáticos y ciberdelitos (la Institución no establece una diferencia y hace uso indiscriminado de ambos términos). Es así como en el informe presentado en el año 2022, expone una serie de datos y cifras donde se discrimina la variable de género de la persona que incurre en el delito, así como el reporte estadístico del total de capturas y denuncias, junto a un panorama global que deja en evidencia la evolución del tipo de delito desde el año 2010 hasta el año 2021. A continuación, se presenta cada una de las figuras, junto a un análisis descriptivo de los resultados de las variables y una asociación desde la perspectiva legal con la norma y sus posibles implicaciones. Cabe mencionar que se trata de la tipificación de los delitos más comunes en el país.

Una particularidad que se puede identificar en todos los informes y datos aportados por la entidad, es el crecimiento abrupto de cada uno de los ciberdelitos durante los años 2020 y 2021, hecho que encuentra explicación en la época de confinamiento a la que se vio sometido el mundo, incluyendo a la sociedad colombiana, haciendo que las personas se vieran abocadas hacia el uso de la tecnología para continuar realizando sus labores profesionales, sociales, culturales, financieras, educativas, artísticas, entre otras, sumando además sus interacciones familiares. Este auge en el uso de las plataformas de comunicación trajo evidentes consecuencias negativas, debido a la poca previsión de las personas sobre la protección de sus datos en el ciberespacio y la especial atención que los ciberdelincuentes le han brindado a estas circunstancias.

Figura 5. *Acceso Abusivo al Sistema Informático*

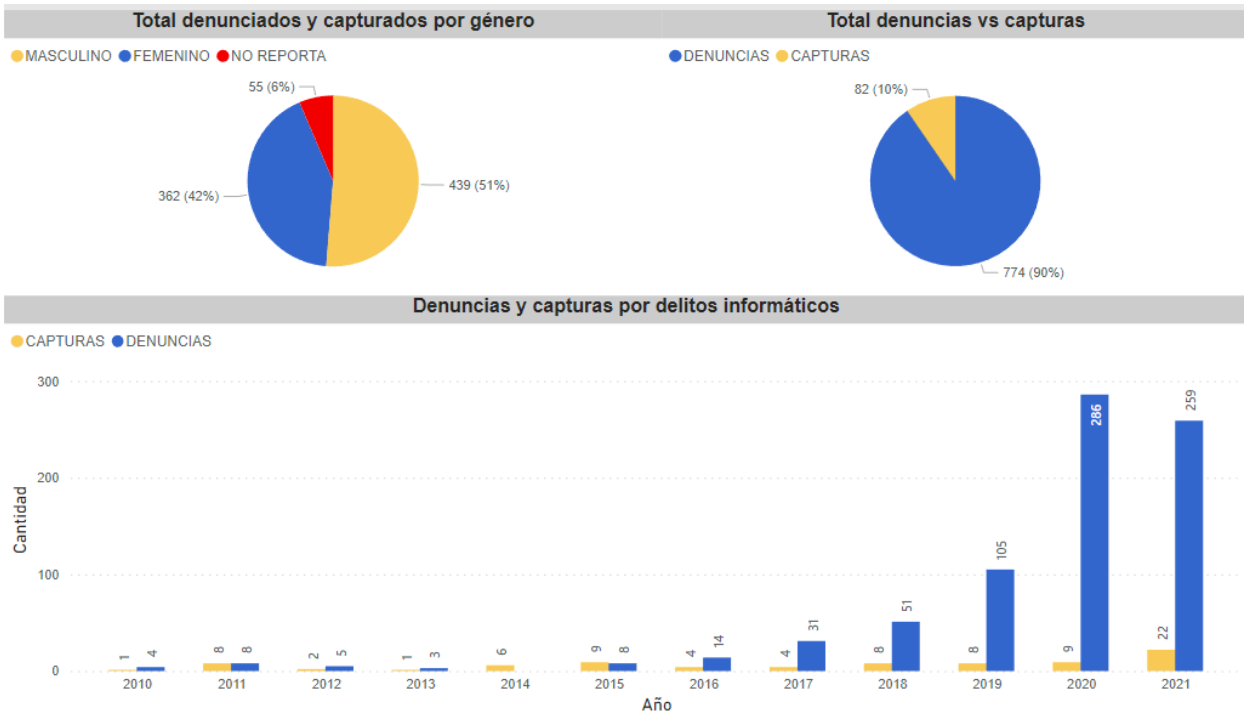


Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

La Figura sobre el Acceso abusivo a un sistema informático se encuentra tipificada dentro de la ley en el Artículo 269A, donde se establece una pena de prisión una multa para aquella persona que, sin consentimiento alguno se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo.

Se trata de un delito que en el país, tal como lo revela la gráfica es cometido principalmente por personas del género femenino, con una brecha enorme entre el número de denuncias y el número de capturas. Tal como se ha mencionado, un crecimiento de más del 100% se evidencia entre los años 2019 y 2021 en el país.

Figura 6. *Obstaculización ilegítima de sistema informático o red de telecomunicación*

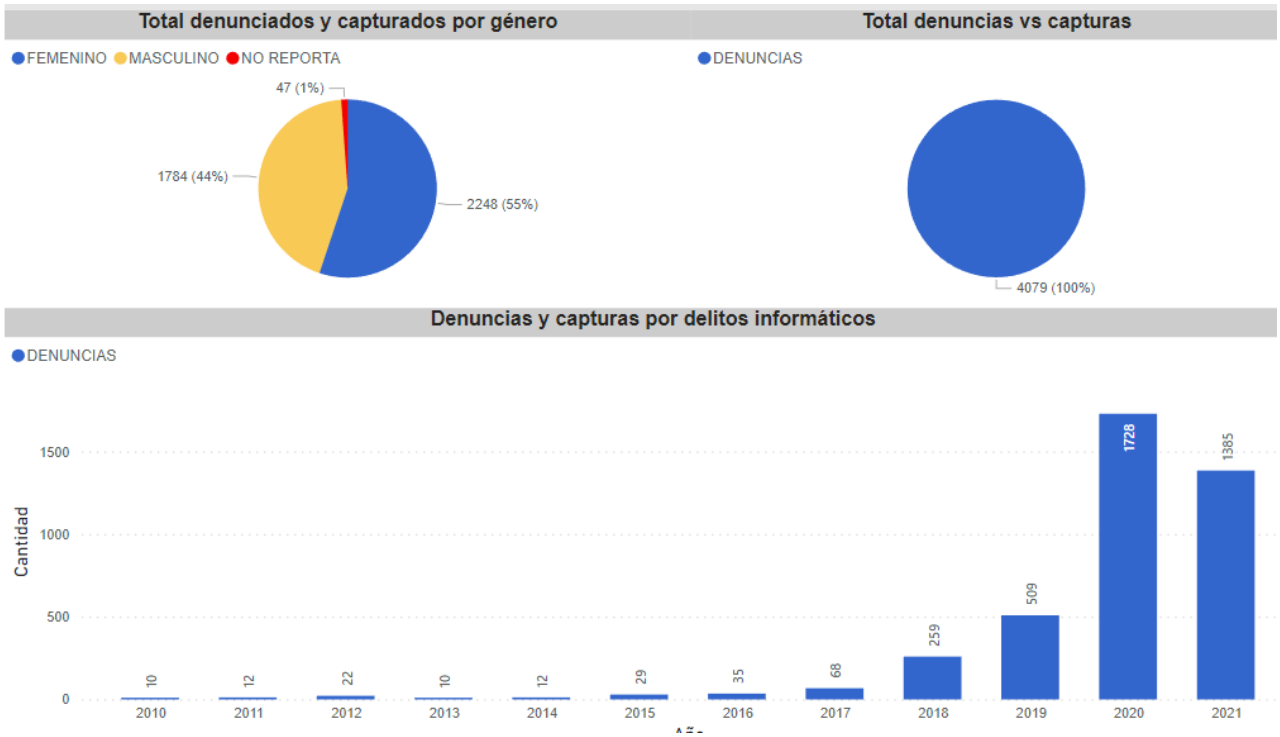


Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

De acuerdo con el Artículo 269B incluido en la normatividad sobre delitos informáticos del país, esa trata de un delito donde una persona que no está facultada para hacerlo, impide el funcionamiento o el acceso a un sistema informático o a los datos dentro de una red de telecomunicaciones. Para este delito se establecen penas de prisión y multas. Se trata de un delito que se considera permanente, porque su ejecución en un entorno informático depende de la voluntad del atacante.

Se trata de una acción delictiva tipificada que se presenta en un porcentaje cercano entre hombres y mujeres desde hace una década, pero que solo reporta un 10% de capturas, pese a lo complejo que resulta la obstaculización de un sistema, que en el caso de una empresa puede representar la pérdida de grandes rubros económicos.

Figura 7. *Interceptación de datos informáticos*

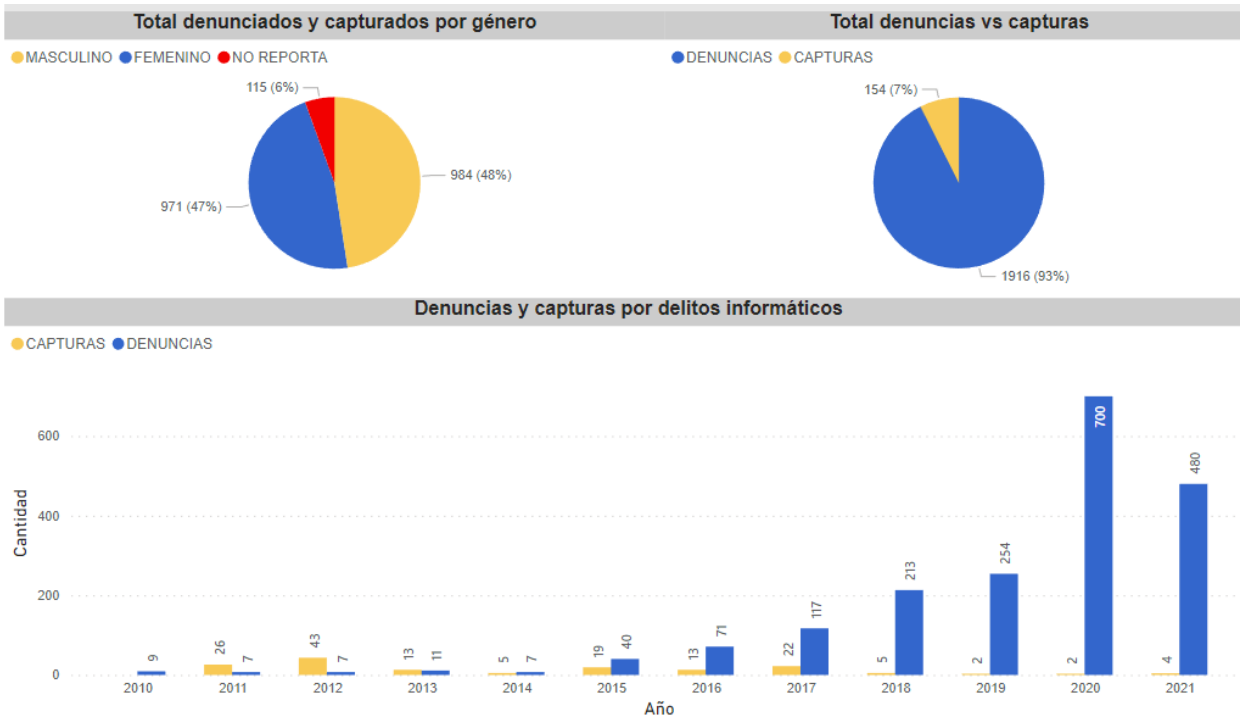


Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

En el caso de la interceptación de datos informáticos, tipificado como delito en el artículo 269C de la normativa, se reconoce la incidencia que tiene esa acción delictiva, que se relaciona directamente con el artículo 15 de la Constitución, donde se establecer el derecho que tienen todas las personas a su intimidad personal y familiar, entendiendo que al interceptar su información o sus comunicaciones se está violentando su libre albedrío.

Resulta muy particular que, de los 4,079 casos reportados durante la última década, no exista ni una sola captura, aunque podría explicarse en términos de la ausencia de denuncias, porque en la mayor parte de las cosas la víctima ni siquiera se entera de que está siendo interceptado ilegalmente a través de un medio informático o una plataforma digital.

Figura 8. *Daño Informático*



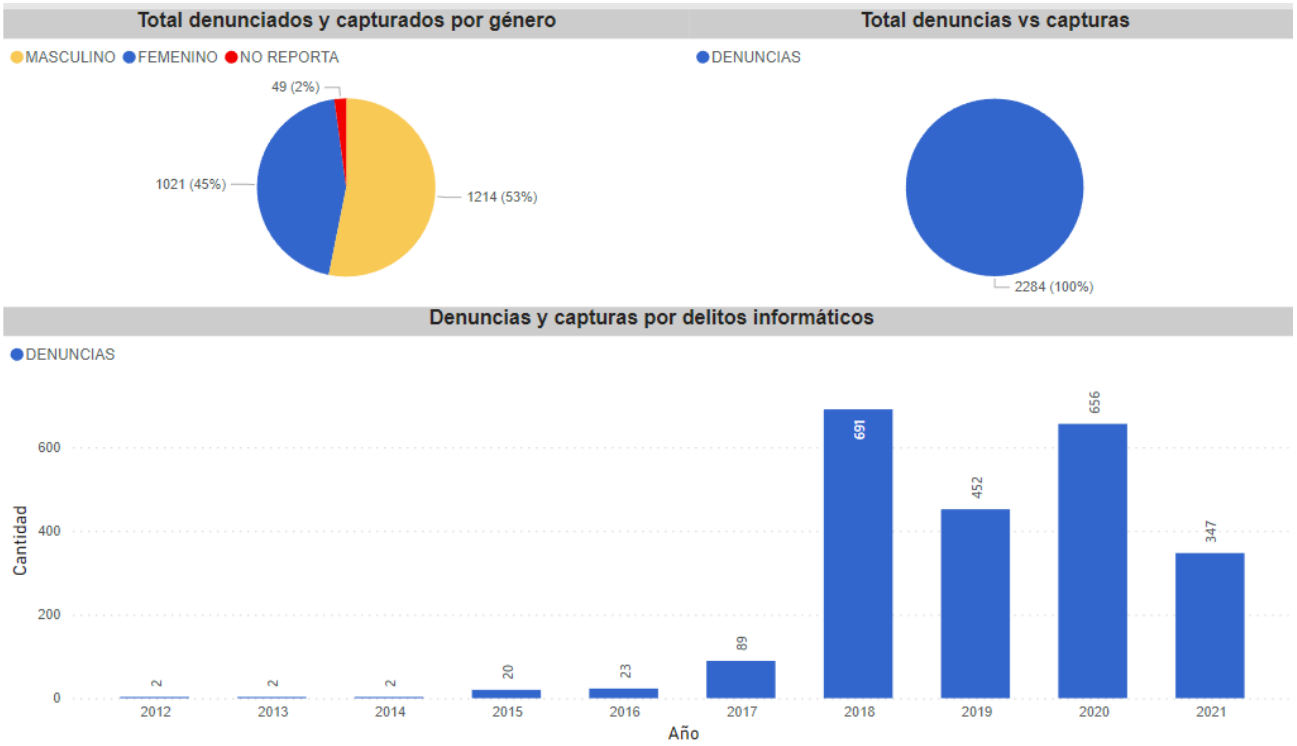
Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

El daño informático, tipificado dentro de los delitos informáticos en el artículo 269D, hace referencia a los casos donde una persona que no tiene facultades para manipular información, elimina, sustituye, altera o modifica datos. Se trata de un delito que atenta contra de la privacidad en distintos formatos, ya que la información se puede almacenar en variedad de dispositivos y formatos. En el caso del almacenamiento de la información en línea o en la nube, se trata de una de las maneras más utilizadas por las personas, sin embargo, los códigos de acceso o permisos son fácilmente vulnerables, aspecto al que el convenio sobre Ciberdelincuencia de Budapest se refiere como atentados a la integridad de los datos,

En Colombia, se reconoce una un aumento de este delito entre los años 2019 y 2020, pero particularmente se produce un descenso en el año 2021, que se relaciona con el tiempo de confinamiento, que le otorgó a las personas un mayor espacio y tiempo para prestar atención a

las medidas de protección de sus datos y de su información personal. Pese a esto, el porcentaje de capturas en la sumatoria de años es únicamente del 7%.

Figura 9. *Uso de software malicioso*



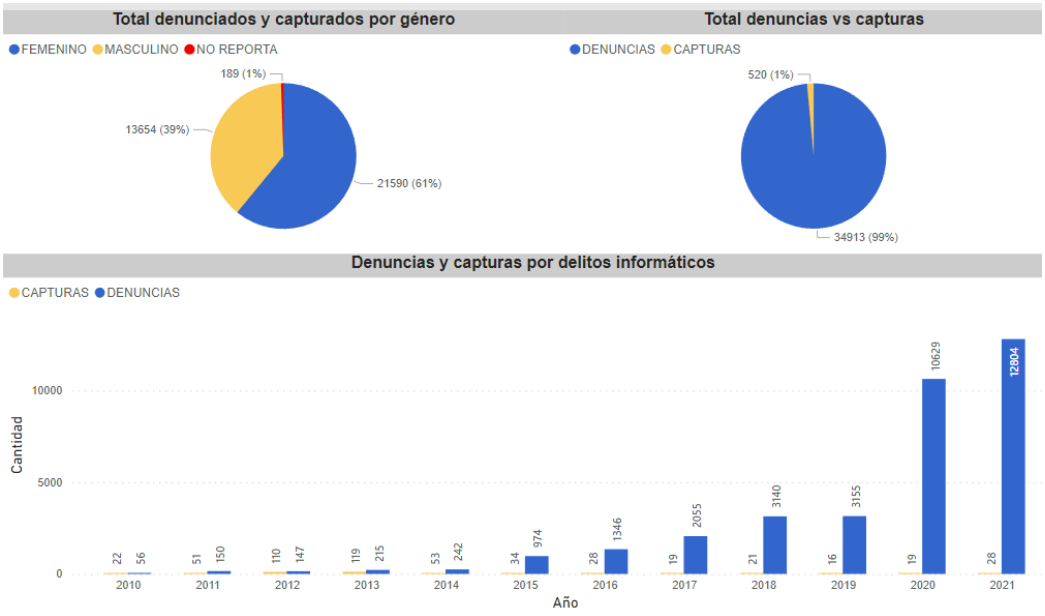
Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

El uso de Software malicioso hace referencia a lo que una persona realiza al distribuir, enviar, extraer o introducir programas que sean dañinos para el funcionamiento de los equipos que garantizan el alojamiento de datos, la navegación y las telecomunicaciones.

Se trata de un delito tipificado en el Artículo 269E, que se puede clasificar en tres grupos: Software de sistema, que permite explotar todos los beneficios de un equipo físico, software de programación; programas orientados con el fin de crear nuevas herramientas informáticas como java, y finalmente el software de aplicación, diseñado para cumplir alguna tarea específica.

Este es un delito bastante común, pero que las personas no asumen como tal, toda vez que al ser víctimas lo que buscan es asesoría para fortalecer su seguridad informática y la protección de sus redes y equipos. En el año 2018 se presentó en Colombia el pico más alto de este delito, que las autoridades asocian generalmente con el intento de manipulación o destrucción de información que se presenta de forma masiva producto de la popularidad que adquieren algunos de estos softwares maliciosos en redes sociales.

Figura 10. *Violación de datos personales*



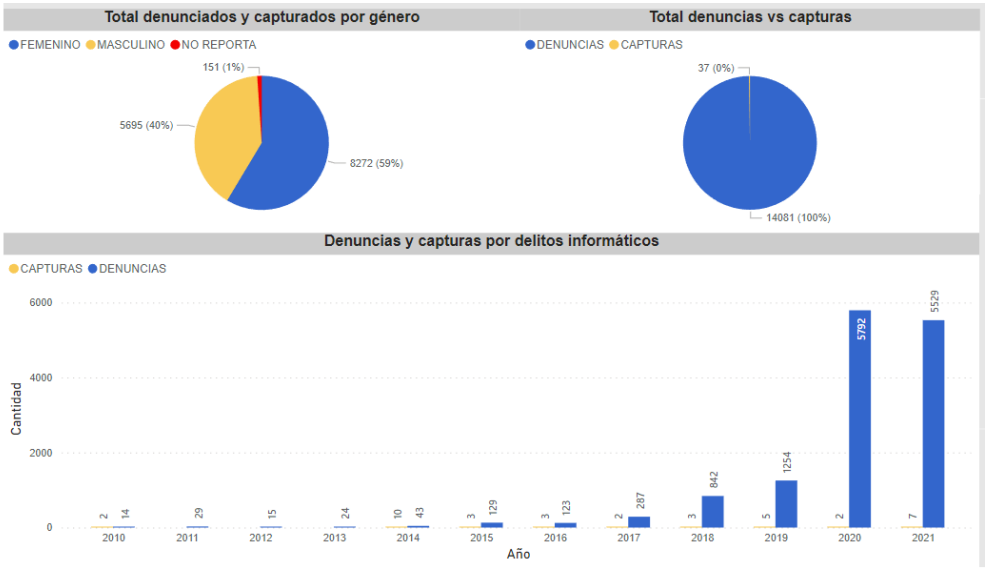
Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

La Violación de los datos personales, tipificada en el Artículo 269F, es uno de los ciberdelitos con mayor impacto y crecimiento en el país, alcanzando en el año 2021 un total de 12904 casos, donde el género femenino tiene un mayor protagonismo o facilidad para extraer información, códigos, contraseñas o archivos de terceros.

Pese a que se reconocen 520 capturas, este número solo representa el 1% sobre las más de 34 mil denuncias que se han realizado durante la última década en el país, entendiendo que los

ciberdelincuentes casi siempre utilizan perfiles falsos para cometer este tipo de actos y luego saben eliminar sus pasos en la red para que sea muy complejo rastrearlos.

Figura 11. *Suplantación de sitios web para capturar datos personales*



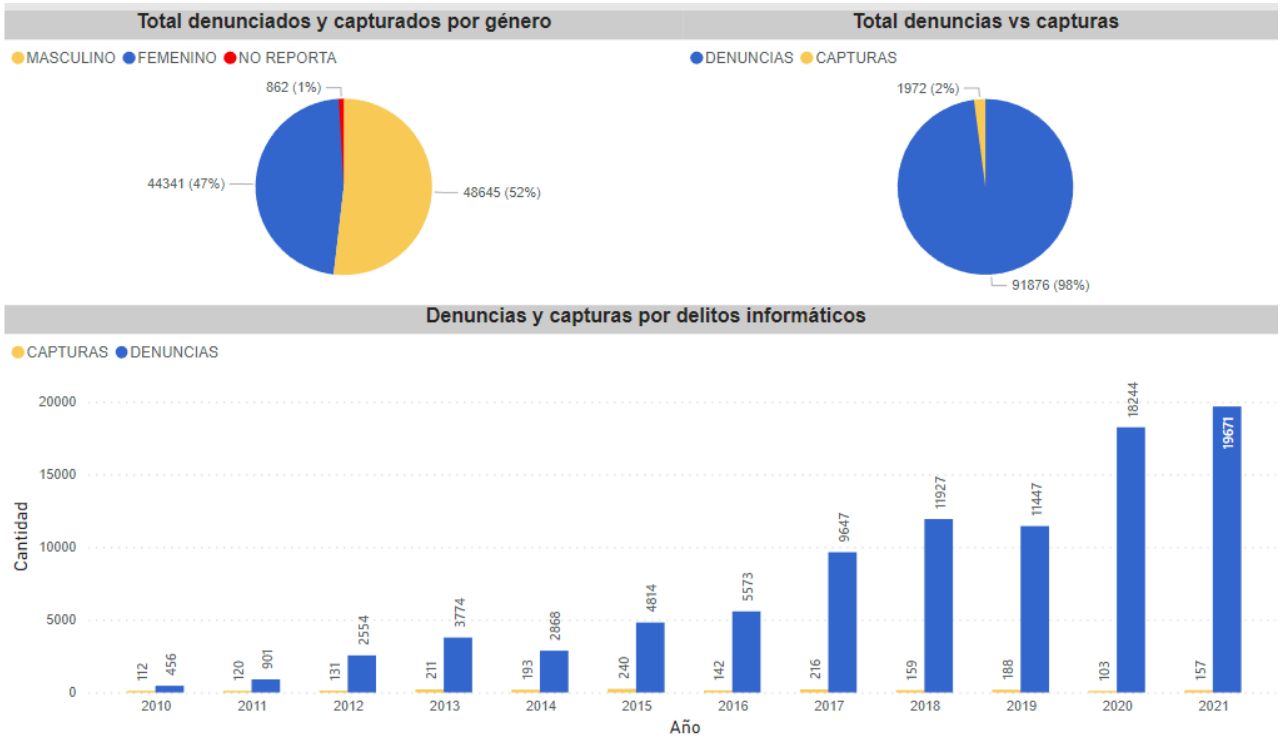
Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

En el artículo 269G se tipifica la suplantación de sitios Web para capturar datos personales, situación que permite, con intenciones ilícitas desarrollar o ejecutar acciones electrónicas que involucren el uso de ventanas emergentes o enlaces. Esta es una de las estrategias que los estafadores informáticos emplean para introducir publicidad engañosa, información falsa o pornografía en portales que tienen reputación virtual y la confianza de los usuarios de los canales digitales o plataformas de información.

Claramente, durante los años 2020 y 2021 se aumentaros los casos, que en general no se materializan en denuncias porque las personas sienten que ha sido por voluntad propia que han

ingresado a los enlaces y que en parte es culpa de su curiosidad terminar involucrados en un fraude o engaño cibernético.

Figura 12. *Hurto por medios informáticos*

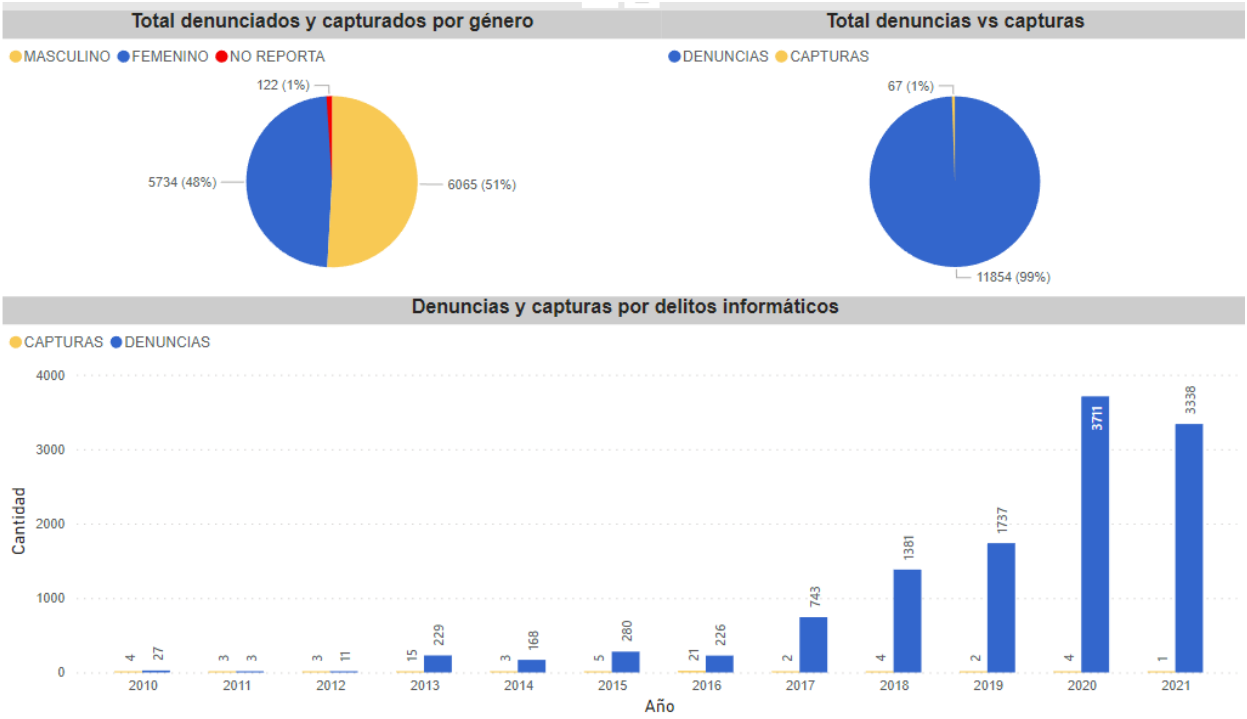


Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

El hurto informático es el delito con mayor crecimiento exponencial dentro del consolidado estadístico que entrega la Policía Nacional, evidenciando que, en la medida en la que se desarrolla la tecnología, crecen las plataformas y aumenta el uso de las redes sociales, también crece la capacidad de fraude y robo a través del ciberespacio.

En el artículo 269I se establece que es un delito donde se superan las medidas de seguridad y se manipula un sistema informático para suplantar un usuario, autenticar información y generar permisos que vulneran la seguridad de un tercero.

Figura 13. *Transferencia no consentida de activos*

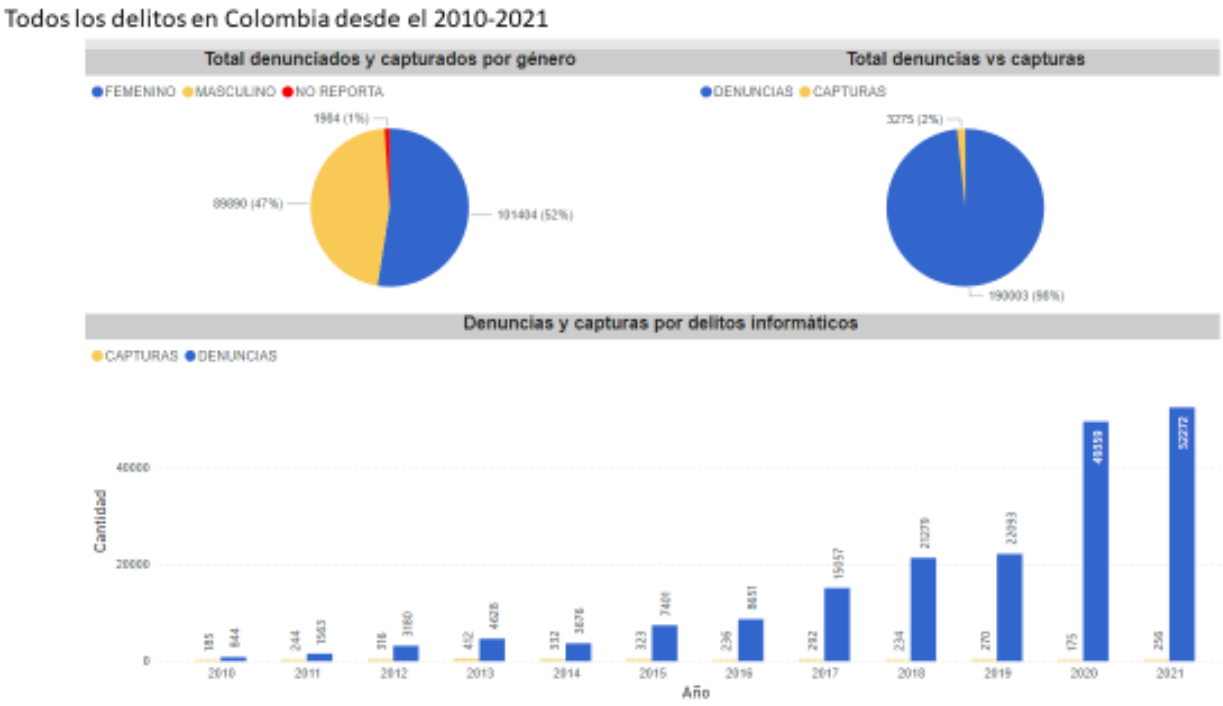


Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

La transferencia no consentida de activos, tipificada en la ley en el Artículo 269J, hace referencia a las intenciones lucrativas con la que una persona manipula un sistema informático para obtener beneficios. Este delito es duramente castigado en la ley, sin embargo es muy bajo el índice de capturas, pese a la gran cantidad de denuncias, hecho que hace que todavía muchas personas prefieran no hacer sus operaciones financieras a través de plataformas digitales.

Finalmente, la Figura 14 muestra el consolidado de los delitos informáticos y ciberdelitos en Colombia desde el año 2010 hasta el año 2021, dejando en evidencia el crecimiento abrupto en la época de confinamiento y al mismo tiempo la baja cantidad de capturas frente a la enorme cantidad de denuncias. Se puede afirmar también que la variable género no tiene una significativa incidencia en los resultados, porque los porcentajes son muy equilibrados.

Figura 14. *Consolidado de los delitos informáticos y los ciberdelitos en Colombia 2010-2021*



Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

ANÁLISIS Y DISCUSIÓN

Un total de 5 mil manizaleños se certificaron desde año 2021 como ciudadanos ciberseguros, situación que les permitió convertirse en un eslabón importante dentro en una cadena para contrarrestar los delitos que tienen como escenario las plataformas virtuales.

La puesta en marcha del programa Ciudadano Ciberseguro, coordinado por la Secretaría de TIC y Competitividad de Manizales, en convenio con la Fundación Universidad Empresa Estado Eje Cafetero (FUEEEC), estableció la estrategia como un paso para acercar a la ciudad hacia la meta de convertirse en ciudad inteligente.

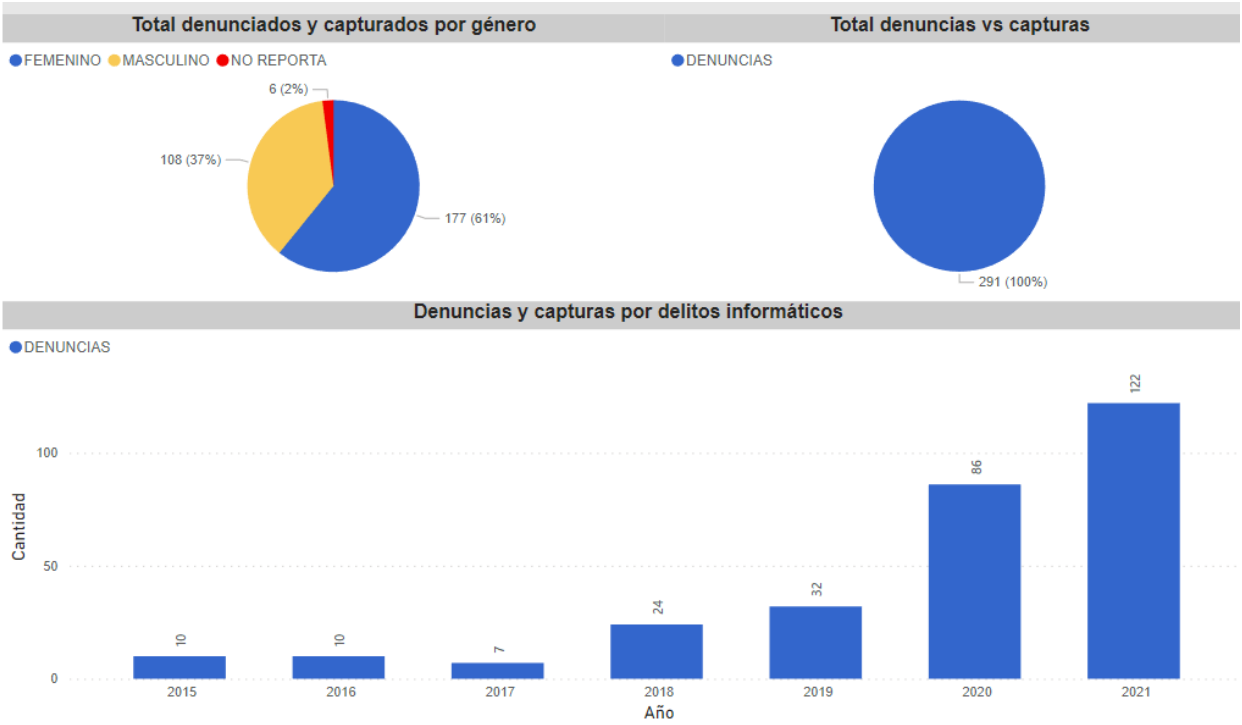
Todas estas alternativas fueron creadas por la creciente ola de Ciberdelitos que se generó durante la época de confinamiento dentro de la pandemia. Es posible afirmar que los Ciberdelitos entre el año 2020 y 2021 a nivel nacional y local crecieron alrededor de un 60%.

Se deber tener muy en cuenta que se trata de una suma de esfuerzos para impulsar la competitividad y la conectividad que fortalecen la ciencia la tecnología y la innovación en la ciudad. En el año 2023, aún se sigue teniendo acceso a la plataforma y se puede generar el certificado como ciudadano Ciberseguro

Es así como, en la ciudad de Manizales se reconocen delitos tipificados en la ley, que según el informe de la Policía Nacional (2021) donde se focalizan los territorios, desde el año 2015 hasta el año 2021 se han presentado de la siguiente manera:

:

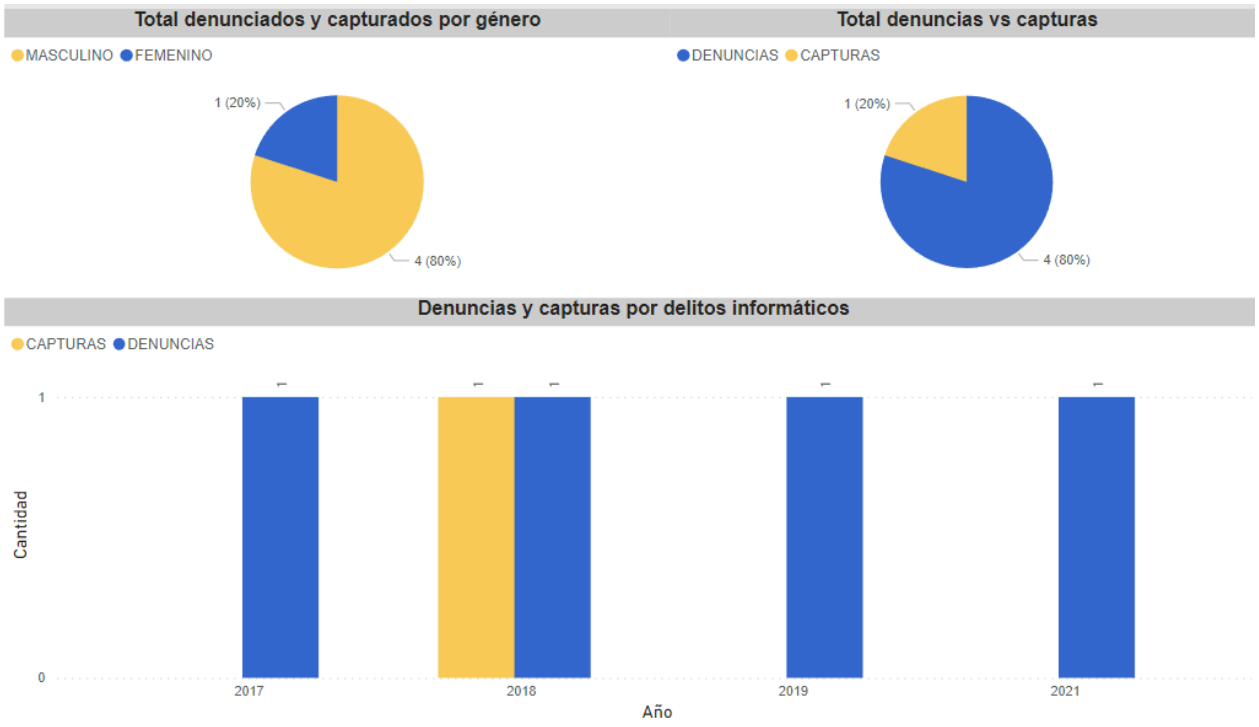
Figura 15. *Acceso abusivo a un sistema informático*



Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

En el caso del acceso abusivo a un sistema informático, se evidencia en el informe que el mayor crecimiento se presentó durante la época de confinamiento. Al igual que en el resto del país, de un total de 291 denuncias no se ha logrado dar con ninguna captura, entendiendo que se trata de un delito que generalmente es detectado fuera del rango de tiempo en el que se está presentando. Adicionalmente, los casos que se presentan en este tipo de delito en ocasiones son realizados por personas cercanas, en una especie de espionaje o control sobre la información.

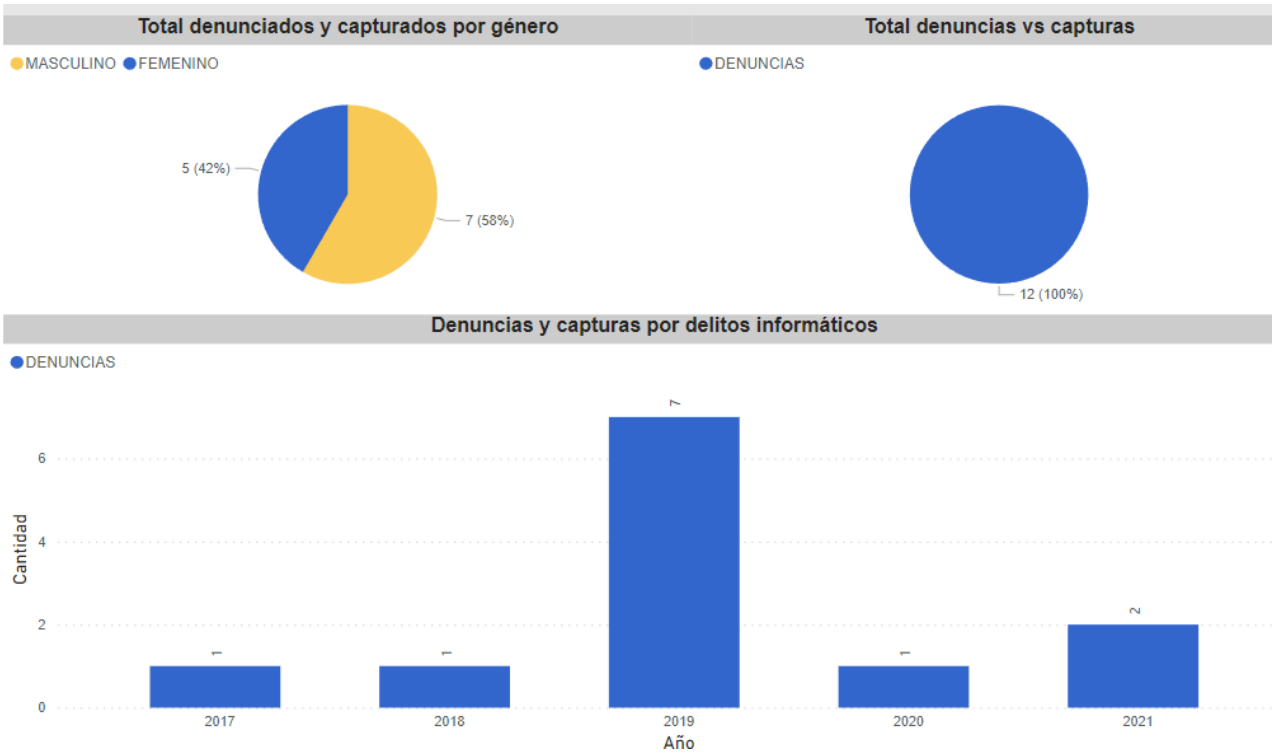
Figura 16. *Obstaculización ilegítima de sistema informático o red de telecomunicación*



Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

La obstaculización de un sistema informático o cibernético tiene una particularidad y es la participación del género femenino, generalmente porque son las mujeres quienes tienen mayor facilidad de contacto y confianza con aquel que terminará siendo la víctima en el proceso de configuración del delito. En este delito solo se reconocen 5 casos denunciados y una sola captura, haciendo énfasis en que se trata de un modelo de delito que puede ser operado desde una zona lejana, convirtiéndolo en transfronterizo

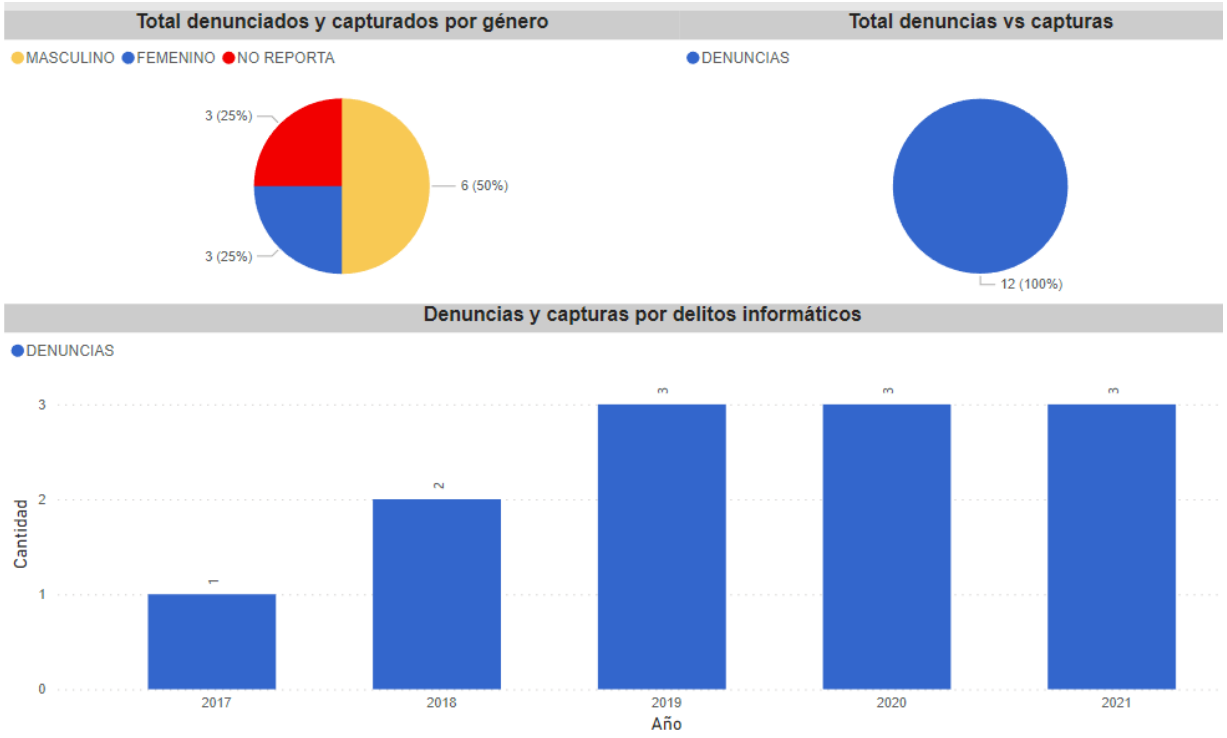
Figura 17. *Interceptación de datos informáticos*



Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

La interceptación de datos, a diferencia de los demás ciberdelitos, tuvo un mayor número de casos reportados en el año 2019, lo que indica que se trata de una acción que no está directamente asociada con la época de confinamiento, sino con un modelo de seguimiento con fines extorsivos o de manipulación de información para beneficios de terceros sobre un total de 12 denuncias, no se notifica ninguna captura.

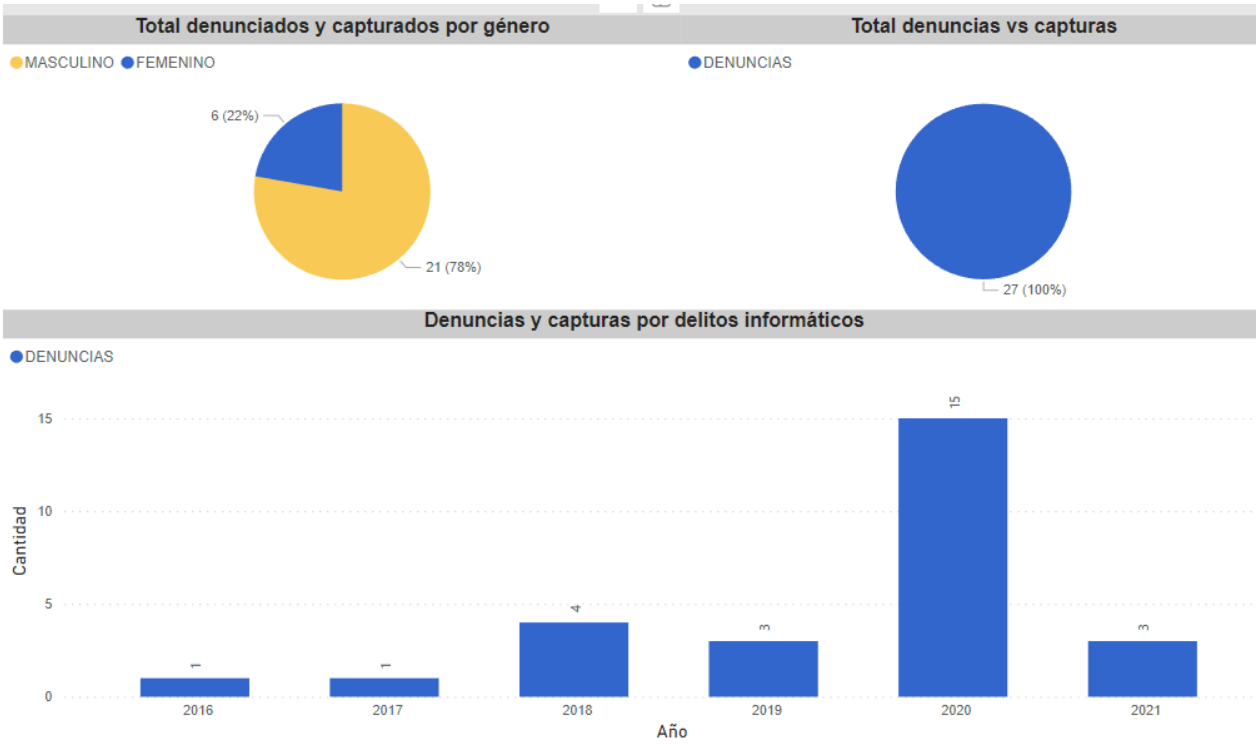
Figura 18. *Daño Informático*



Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

Los nueve casos de daño informático que han sido denunciados en la ciudad en un lapso de cinco años, representan una condición de la sociedad que está relacionada con la venganza o la acción malintencionada. En muchas ocasiones, este delito se configura porque las personas simplemente desean estropear el trabajo, la reputación o el éxito de otra persona y toman medidas que atentan contra el funcionamiento de su red de tecnología o su plataforma, en el caso de los escenarios virtuales

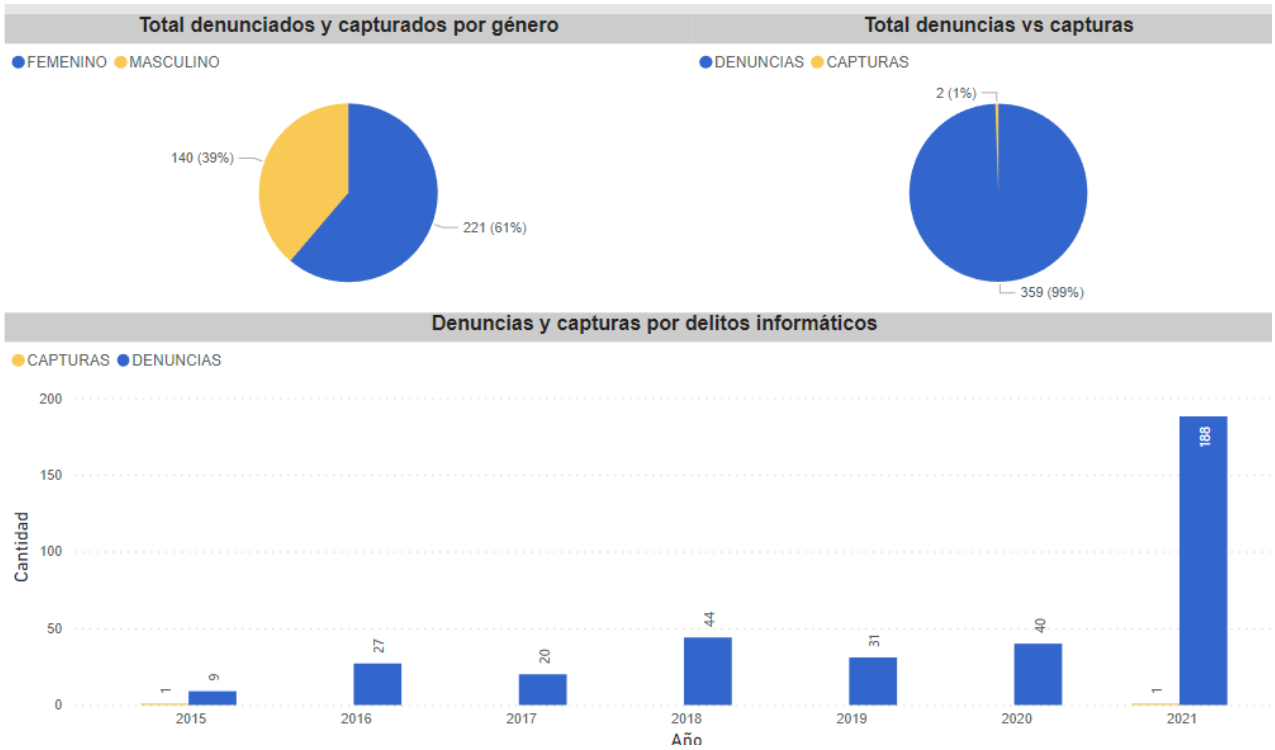
Figura 19. *Uso de software malicioso*



Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

El uso del software malicioso es frecuente y no generalmente porque las personas tengan la intención de hacer un daño, sino porque se genera una oportunidad de engañar, asi no se obtengan beneficios. No obstante, durante la época de confinamiento, este tipo de delito, pese a estar tipificado en la ley, se incrementó, aprovechando el ingreso permanente de las personas a portales y plataformas de información y entretenimiento, dejando de lado la precaución al momento de compartir datos solicitados para su acceso. Resulta muy importante generar conciencia sobre este punto y acudir siempre a portales oficiales que tengan elementos de validación e identidad.

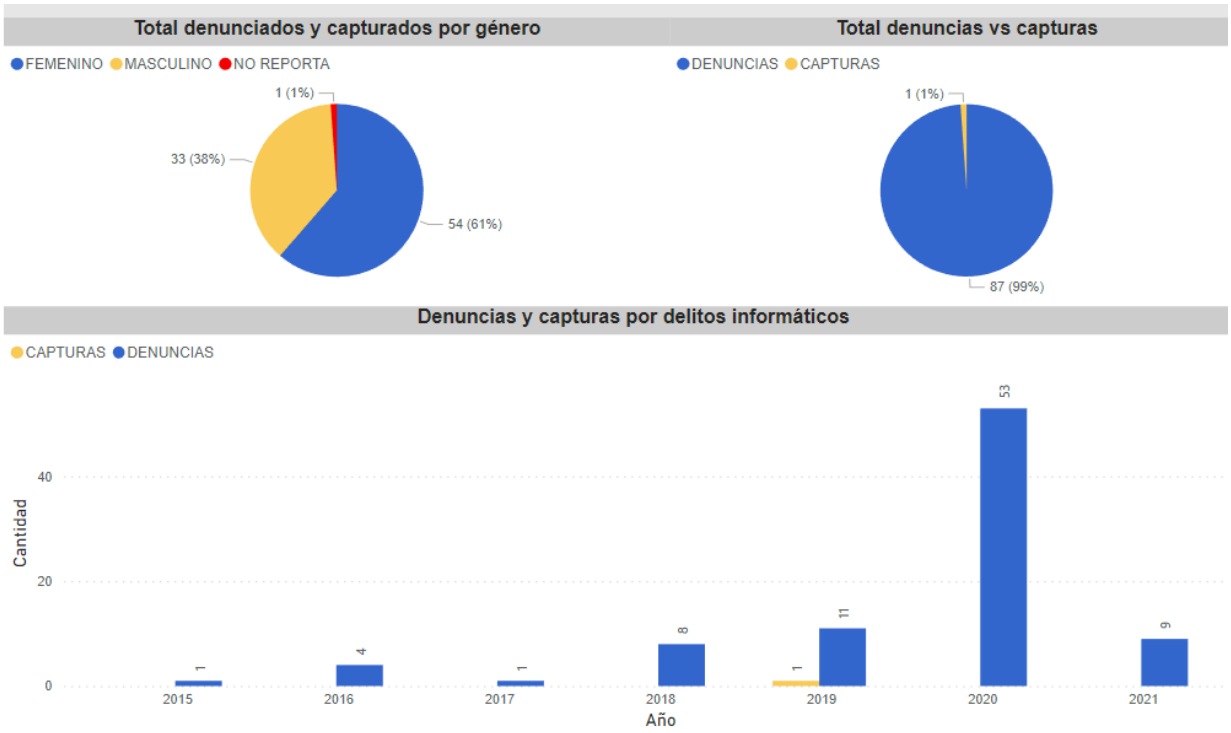
Figura 20. *Violación de datos personales*



Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

Este delito es el primer paso para la suplantación. La captación de los datos se hace de múltiples maneras, especialmente a través de campañas engañosas que prometen beneficios para quienes se suscriban. En Manizales es un delito que creció significativamente durante la pandemia, por cuenta de la ilusión de muchas personas que intentaron buscar empleos u oportunidades de negocio a través de las redes y plataformas que al final no eran seguros

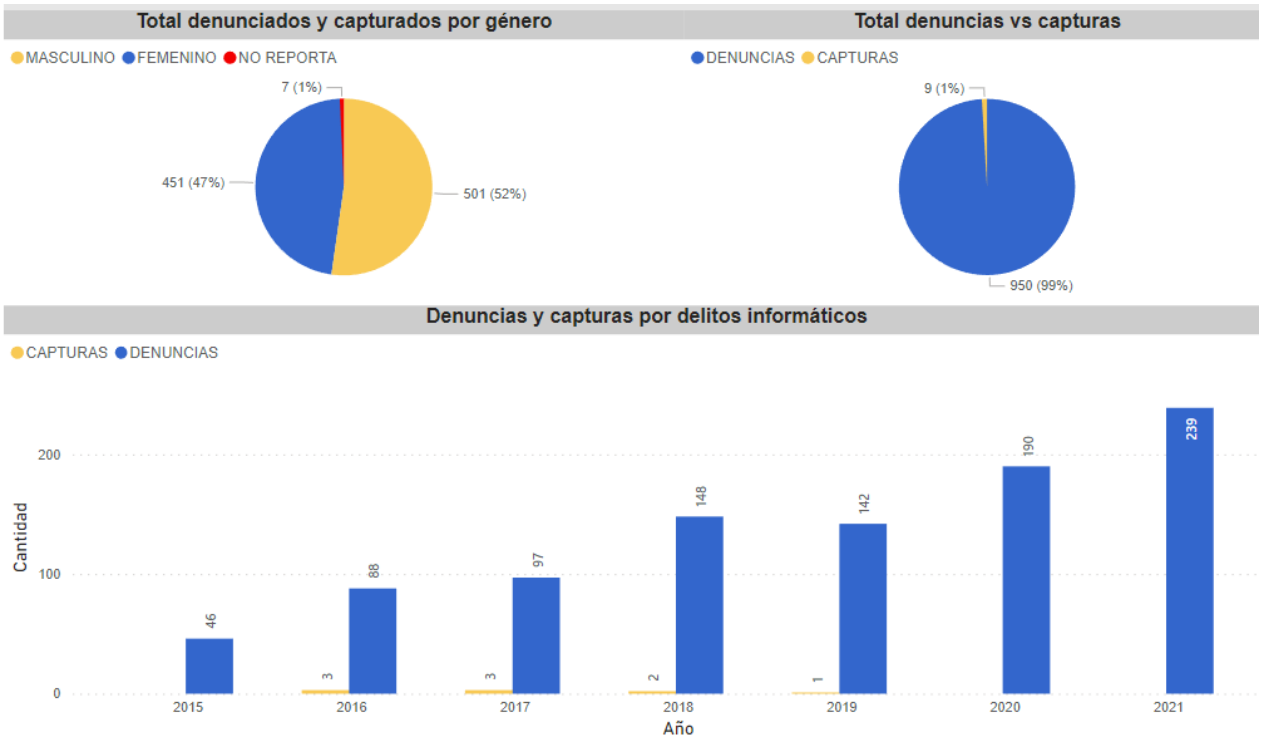
Figura 21. *Suplantación de sitios web para capturar datos personales*



Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

Este es un delito con muchos casos reportados en la ciudad de Manizales. Se trata generalmente de un proceso de suplantación, que se ha hecho popular debido a la facilidad que prestan en la actualidad las entidades financieras, almacenes, cooperativas o empresas para otorgar créditos, préstamos o bienes materiales. La obtención de los datos, claves o contraseñas les permite a los cibercriminales obtener beneficios que luego perjudican a quien ha sido suplantado.

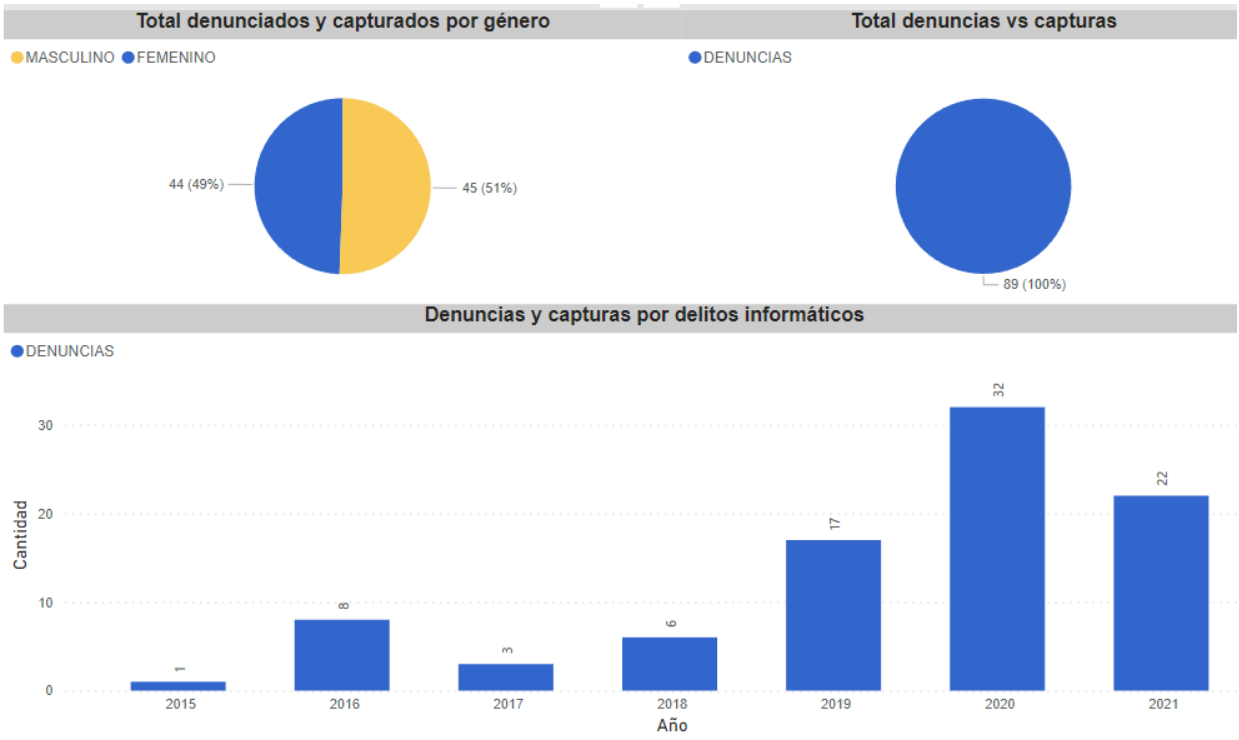
Figura 22. *Hurto por medios informáticos y semejantes*



Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

El hurto por medios informáticos es más común de lo que parece, sobre todo porque una vez se comparten datos en la red, estos quedan girando en un entorno donde pueden ser fácilmente extraídos y manipulados. Una de las modalidades conocidas es la telefónica, sin embargo, en la actualidad, la mayoría de las plataformas tienen canales de comunicación independientes a los que los usuarios accedes para compartir sus datos personales y las claves de sus cuentas sin ningún tipo de certeza ni verificación.

Figura 23. *Transferencia no consentida de activos*

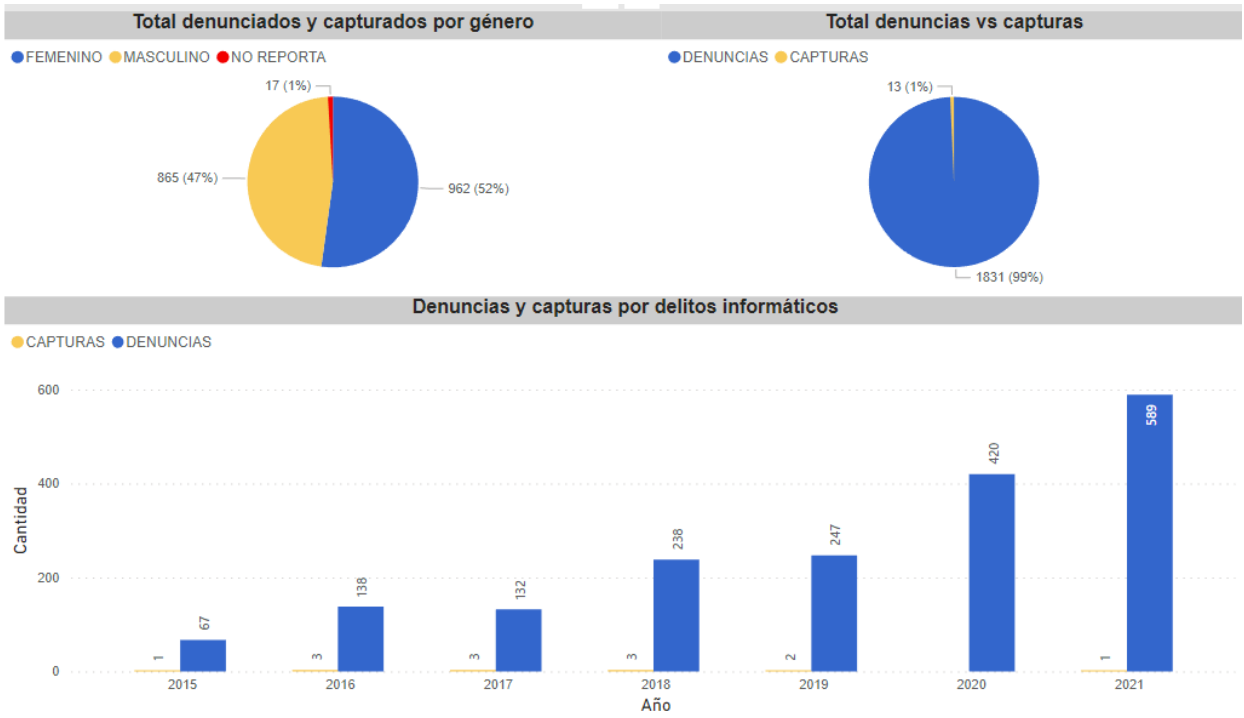


Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

La transferencia no consentida de activos es una consecuencia lógica de la violación de los datos y del hurto por medios informáticos. De acuerdo con la figura se han reportado 80 delitos durante los últimos años en la ciudad, en una tendencia irregular, que evidencia que los delitos tienen temporadas, es decir, están asociados con los momentos de mayor uso de dispositivos, redes y plataformas como es el caso de la época de navidad, los días de pago o las vacaciones.

La grafica de consolidado final entregada por la policía en el informe territorial sobre la ciudad de Manizales, evidencia un total de 1831 delitos denunciados y solamente 13 personas capturadas, lo que permite establecer que más allá de la existencia de la normatividad, hacen falta mejores esquemas de seguridad y estrategias para que la prevención ayude a reducir los casos y la comunidad coopere en el reconocimiento de los ciberdelincuentes.

Figura 24. *Consolidado Manizales 2015-2021 Ciberdelitos y delitos informáticos*



Nota. Información obtenida del informe anual sobre delitos informáticos (2021)

CONCLUSIONES

Existen distintas razones por las que la ley no actúa de manera efectiva en algunos casos de riesgos informáticos en Colombia. Una de ellas es la falta de recursos y personal capacitado en las entidades encargadas de hacer cumplir la ley, lo que dificulta la investigación y el procesamiento de los casos. Otra razón es la complejidad de algunos casos de riesgos informáticos, que requieren de conocimientos especializados en informática y tecnología para su investigación y resolución. En muchos casos, los delitos informáticos son cometidos por personas ubicadas fuera de Colombia, lo que dificulta la aplicación de la ley por parte de las autoridades locales. Además, se deben considerar todos los casos de riesgos informáticos que no son denunciados por las víctimas, en ocasiones por desconocimiento de la existencia de leyes que los protegen o por miedo a represalias. Esto dificulta la acción de las autoridades para perseguir y sancionar a los responsables.

Es preciso que dentro del imaginario sobre las tecnologías de la información de las personas de la ciudad de Manizales y de todo el territorio colombiano, las personas contemplen no solo las riesgos, también las consecuencias de los delitos informáticos y de los ciberdelitos, comprendiendo que los primeros se pueden configurar fuera de línea con el apoyo de un dispositivo electrónico y que los segundos se producen dentro de la red en un escenario virtual de intercambio de información en tiempo real; no obstante, por desconocimiento en ambos casos, no solo se puede ser víctima, también una mala decisión o un mal consejo puede convertir a alguien en victimario.

Se reconocen dentro de la ley colombiana normas e instrumentos para enfrentar los riesgos informáticos y combatir el ciberdelito, pero la aplicación de la ley o al menos su

efectividad sigue siendo limitada. Hacen falta campañas y una mayor conciencia ciudadana frente a los riesgos que se generan en los entornos virtuales y mediante el uso de plataformas digitales, sobre todo cuándo le solicitan al usuario datos personales o información financiera.

En la ciudad de Manizales se reconoce la existencia de la mayoría de delitos tipificados en la normativa, pero al igual que en el resto del país, existe mucha omisión y ausencia de denuncias, junto a un bajo índice de capturas. No obstante, se reconoce que las campañas emprendidas por las administraciones locales para formar ciudadanos digitales, giran en torno a la comprensión general del funcionamiento de los sistemas informáticos y de los entornos web, así como frente al uso de contraseñas seguras, la actualización permanente de los datos, el uso de cauteloso de plataformas y correos electrónicos, el análisis crítico de mensajes e invitaciones de personas extrañas, el uso de redes seguras y sobre todo la educación familiar ante los riesgos a los que se expone la privacidad personal con los el desarrollo de las tecnologías de la información.

REFERENCIAS

Acosta Argote , C. (2021). *La suplantación de sitios web y robo de datos están entre los delitos más frecuentes y denunciados.* Obtenido de https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, vol. 25, núm. 89*.

Ayala Martínez, J. P., & Duque Martínez, D. A. (2022). *¿Que diferencias en Ciberdelitos existen entre Colombia y España?* Obtenido de https://repository.ces.edu.co/bitstream/handle/10946/6025/Trabajo%20de%20grado.pdf?sequence=6&isAllowed=y

Bariios, S. (2012). *El delito informatico en la legislación colombiana* . Obtenido de https://repositorio.cuc.edu.co/bitstream/handle/11323/905/EL_DELITO_INFORMATICO_EN_LA_LEGISLACION_INFORMATICA.pdf?isAllowed=y&sequence=1

Código Penal, LEY 599 DE 2000 (Senado de la republica 2000).

Código Penal, LEY 1273 DE 2009 (Congreso de la republica 2009).

Interpol. (2020). *COVID-19 Cybercrime Analysis Report-Design.* Obtenido de https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf?inLanguage=esl-ES

Naciones Unidas . (2021). *Recopilación de todas las conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros durante las reuniones del Grupo de Expertos encargado de realizar un estudio exhaustivo sobre el delito cibernético celebrada en 2018, 2019 y 2020.* Obtenido de https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/CRP/V2101015.pdf

Ojeda, J. E., Rincon, F., Arias, M. E., & Daza, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de contabilidad, 11 (28)* , 41-61.

Pantallas Amigas. (2014). *Seis recomendaciones para la prevención del Ciberbullying.* Obtenido de https://www.pantallasamigas.net/ciberdelitos/?utm_term=&utm_campaign=&utm_source=adwords&utm_medium=ppc&hsa_acc=2066832176&hsa_cam=2062991670&hsa_grp=111119908974&hsa_ad=476087932288&hsa_src=g&hsa_tgt=dsa-19959388920&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ve

Policia Nacional de Colombia. (2023). *Ciberdelitos.* Obtenido de https://www.minjusticia.gov.co/programas-co/politica-criminal/Paginas/SIPC-Ciberdelitos.aspx

Prado Cortazar , I. A. (2022). *Los delitos informáticos y su soporte probatorio.* Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/22811/Art%C3%ADculo%20Final.pdf?sequence=1&isAllowed=y

Quesada Varona, J. (2016). *Los delitos informáticos en el ámbito de la protección del patrimonio personal según el Derecho Penal.* Obtenido de

https://repository.unimilitar.edu.co/bitstream/handle/10654/15909/quitianmorerasilkyyojanna.pdf?sequence=1&isAllowed=y

Unión Europea. (2001). *Convenios sobre ciberdelincuencia.* Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Universidad®
Católica
de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia
de la Congregación

Hermanas de la Caridad
Dominicas de La Presentación
de la Santísima Virgen

Universidad Católica de Manizales
Carrera 23 # 60-63 Av. Santander / Manizales - Colombia
PBX (6)8 93 30 50 - www.ucm.edu.co

ANEXOS

Anexo 1: se anexa los pantallazos de guía infográfica

CIBERDELITOS LA REALIDAD DIGITAL EN COLOMBIA


JOSÉ FERNANDO GUTIÉRREZ RAMÍREZ
HERNÁN MAURICIO MÁRQUEZ MARULANDA
HAROLD ROMAÑA MACHADO

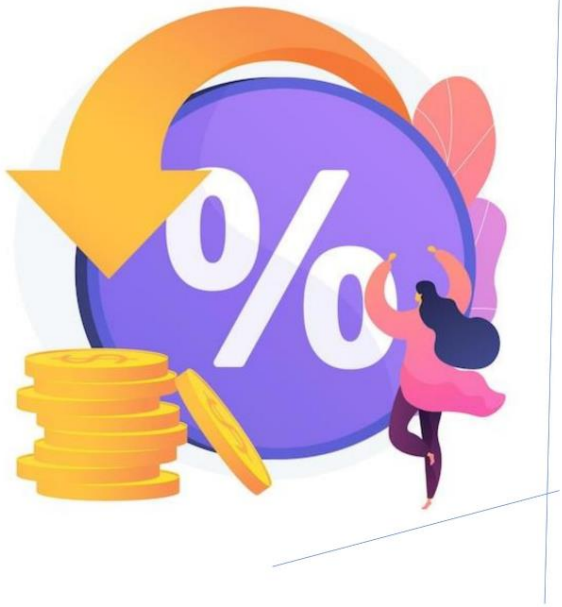
Introducción a los ciberdelitos en Colombia

Con el aumento en el acceso a internet y el desarrollo de la tecnología también se ha presentado un aumento en los delitos que se cometen en línea. Estos delitos pueden incluir fraude, robo de identidad, acoso, entre otro.

Estos delitos pueden incluir fraude, robo de identidad, acoso, entre otro.

El impacto de los ciberdelitos en la economía

Los ciberdelitos pueden tener un impacto en la reputación de las empresas y su capacidad para hacer negocios. Los consumidores pueden perder la confianza si sus datos personales son robados o si sufren una violación de seguridad en línea.



Las autoridades colombiana están tomando medidas para combatir los ciberdelitos. La Policía Nacional tiene una unidad especializada en delitos informáticos que trabaja para investigar y prevenir los ciberdelitos. También se han implementado leyes y regulaciones para proteger a los ciudadanos y las empresas en línea.

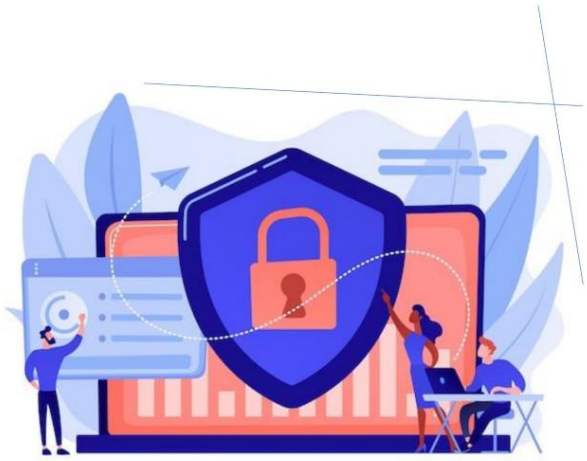
El futuro de los ciberdelitos

Es importante que los ciudadanos estén informados y preparados para protegerse contra los ciberdelitos. Esto puede incluir la educación sobre las últimas tendencias y técnicas de ataque, así como la implementación de medidas de seguridad en línea efectivas.

¿POR QUÉ ES IMPORTANTE ESTAR ACTUALIZADOS?

1. Estar actualizados permite tomar medidas preventivas para proteger su seguridad en línea y evitar ser víctima.
2. El conocimiento actualizado ayuda a salvaguardar su información personal y financiera.
3. Estar informados permite reconocer las señales de advertencia y los métodos utilizados por los ciberdelincuentes.
4. Estar al tanto ayuda a las personas a evitar estafas en línea y proteger sus cuentas bancarias, tarjetas de crédito y otros activos financieros.
5. Conocer los riesgos y las prácticas de seguridad en línea ayuda a mantener la privacidad y evitar la divulgación no deseada de información personal.

En resumen, estar actualizados sobre los ciberdelitos proporciona a las personas las herramientas necesarias para protegerse, tomar decisiones más seguras en línea y salvaguardar su seguridad, privacidad y datos personales.



Los ciberdelitos y la ley colombiana

La Ley Colombiana establece varios tipos de delitos informáticos y cibernéticos, que se encuentran tipificados en el Código Penal en el marco de la Ley 1273 de 2009 y en otras leyes y regulaciones relacionadas.

1. Acceso abusivo a un sistema informático: artículos (269A -269C)
2. Fraude informático: artículos (269F-269I)
3. Sabotaje informático: artículos (269B-269D-269E)
4. Suplantación de identidad: artículos (269G 269J)
5. Pornografía infantil
6. Amenazas o extorsión en línea
7. Acoso en línea

1. Acceso abusivo a un sistema informático:

Este delito se comete cuando una persona ingresa sin autorización a un sistema informático con la intención de obtener información confidencial, dañar el sistema o realizar cualquier otro tipo de actividad ilícita.

Para prevenir este delito:

- Uso de contraseñas seguras
- Uso de cifrado de datos y sistemas de autenticación de dos factores.

2. Fraude informático

Este delito se comete cuando una persona utiliza un sistema informático para realizar un fraude, como, por ejemplo, falsificar documentos o realizar transacciones financieras ilegales.

Para prevenir este delito:

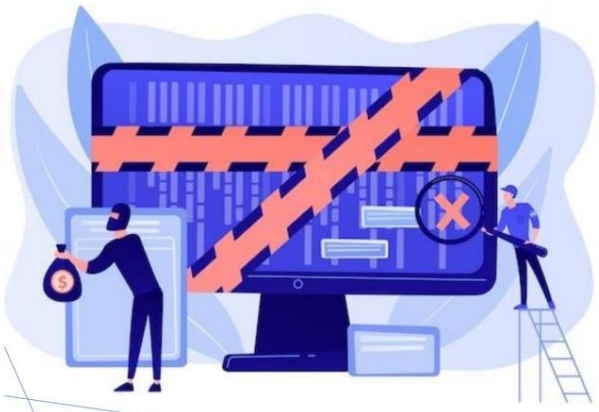
- Contar con sistemas de monitoreo y detección de fraude
- Establecer políticas claras de seguridad en la gestión de información

3. Sabotaje informático

Este delito se comete cuando una persona realiza una acción malintencionada para interferir con el funcionamiento de un sistema informático, con el fin de causar daño o pérdida de información

Para prevenir este delito:

- Implementación de sistemas de detección de intrusos
- Generación de copias de seguridad periódicas.



4. Suplantación de identidad

Este delito se comete cuando una persona se hace pasar por otra persona en línea, con el fin de obtener información o cometer algún tipo de fraude.

Para prevenir este delito:

- Establecer políticas claras de seguridad en la gestión de información confidencial.
- Establecer contraseñas seguras que no corresponden con los datos personales básicos.

5. Pornografía infantil

Este delito se comete cuando una persona produce, distribuye o posee material pornográfico que involucra a menores de edad.

PARA PREVENIR ESTE DELITO

- Instalar filtros de contenido inapropiado.
- Acceder únicamente a sitios seguros y de confianza.

6. Amenazas o extorsión en línea

Este delito se comete cuando una persona utiliza un medio electrónico para amenazar o extorsionar a otra persona, con el fin de obtener algún beneficio.

Para prevenir este delito:

- Implementar sistemas de monitoreo de comunicaciones.
- Realizar copias de seguridad periódicas.
- Conocer la ruta de atención y denuncia ante este tipo de hechos

7. Acoso en línea

Este delito se comete cuando una persona hostiga, intimida o molesta a otra persona a través de medios electrónicos.

Para prevenir este delito:

- Instalar filtros de contenido inapropiado.
- Evitar interactuar en plataformas con personas desconocidas.
- No compartir datos personales.

¿y qué otros ciberdelitos enfrentamos hoy?

- Grooming: adulto se gana la confianza de un menor en línea para explotarlo sexualmente. Prevención: Supervisar el uso de internet de los niños y fomentar la comunicación abierta.
- Ransomware: malware que bloquea archivos y exige un rescate. Prevención: Mantener el software actualizado, utilizar antivirus y hacer copias de seguridad.

- Phishing: engaño para obtener información personal haciéndose pasar por entidades legítimas. Prevención: No hacer clic en enlaces sospechosos, verificar la autenticidad de los sitios y no proporcionar información confidencial.
- Smishing: estafa mediante mensajes de texto para obtener información personal. Prevención: No responder a mensajes sospechosos y no proporcionar información por mensaje de texto.
- Vishing: estafa telefónica para obtener información personal o financiera. Prevención: Tener precaución al proporcionar información por teléfono y no compartir datos con desconocidos.

En general, para prevenir los delitos cibernéticos, es importante establecer políticas claras de seguridad en la gestión de información y educar sobre las prácticas seguras de uso de internet y sistemas informáticos. También se deben implementar medidas de seguridad adecuadas como la instalación de software de seguridad, la realización de copias de seguridad periódicas y la implementación de sistemas de monitoreo y detección de actividades sospechosas, alternativas que se puede generar desde el mismo hogar.

Alternativas locales para combatir los ciberdelitos

Un total de 5 mil manizaleños se certificaron desde año 2021 como ciudadanos ciberseguros, situación que les permitió convertirse en un eslabón importante dentro en una cadena para contrarrestar los delitos que tienen como escenario las plataformas virtuales.

La puesta en marcha del programa Ciudadano Ciberseguro, coordinado por la Secretaría de TIC y Competitividad de Manizales, en convenio con la Fundación Universidad Empresa Estado Eje Cafetero (FUEEEC), estableció la estrategia como un paso para acercar a la ciudad hacia la meta de convertirse en ciudad inteligente.

Todas estas alternativas fueron creadas por la creciente ola de Ciberdelitos que se generó durante la época de confinamiento dentro de la pandemia. Es posible afirmar que los Ciberdelitos entre el año 2020 y 2021 a nivel nacional y local crecieron alrededor de un 60%.

Se deber tener muy en cuenta que se trata de una suma de esfuerzos para impulsar la competitividad y la conectividad que fortalecen la ciencia la tecnología y la innovación en la ciudad. En el año 2023, aún se sigue teniendo acceso a la plataforma y se puede generar el certificado como ciudadano Ciberseguro

https://www.ciudadanociberseguro.com/

Ejemplo de un caso legal

A continuación, se presenta un caso publicado por el portal Ámbito Jurídico en el segmento de noticias penales, bajo una circunstancia específica de un delito configurado por medio de una herramienta tecnológica, pero donde su sustento jurídico y establecido en la ley se configura por medio de un delito establecido en el código penal aparatado del los delitos informáticos.

Condenan a profesor que cometió delitos sexuales a través de 'grooming'

29 de Marzo de 2023

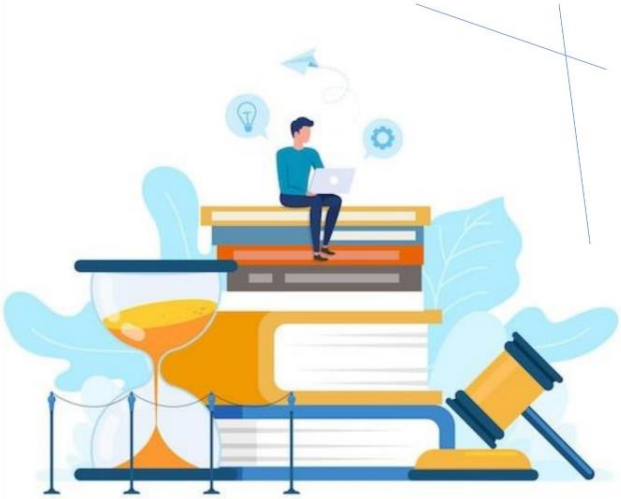
La Corte Suprema de Justicia ratificó la condena a nueve años de prisión contra el formador musical de la banda marcial de un colegio que a través de un proceso de "*online child grooming*" o "propuesta sexual telemática a menores" consiguió cometer delitos sexuales contra una estudiante de 11 años de edad.

https://www.ambitojuridico.com/noticias/penal/condenan-profesor-que-cometio-delitos-sexuales-traves-de-grooming

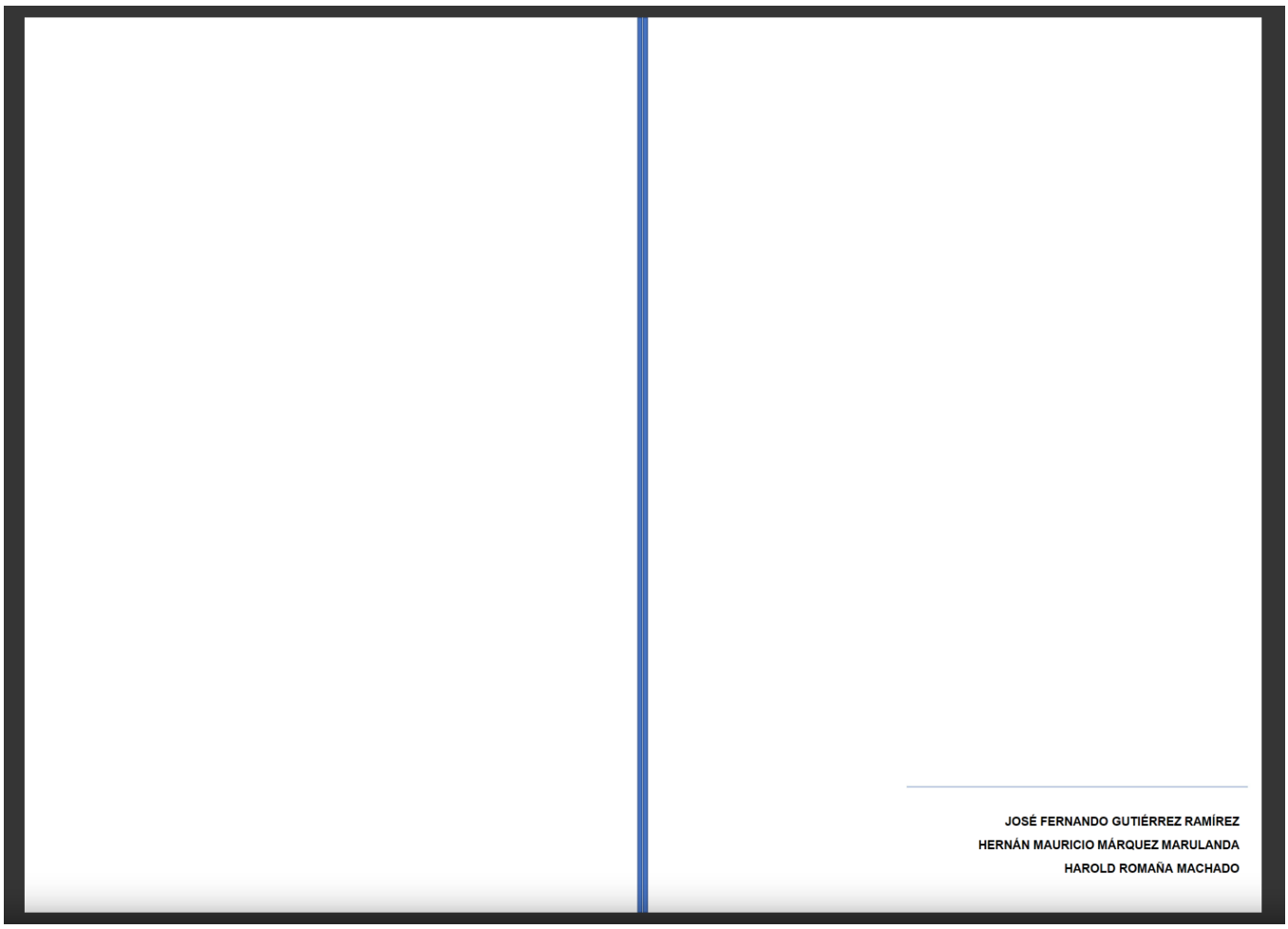
Explicación por parte de la redacción del portal:

¿Está tipificado el 'grooming' en Colombia?

A diferencia de otros países, la Sala dejó en claro que **en Colombia el *grooming* no está tipificado como un delito por si solo, únicamente puede ser objeto de reproche penal cuando se relaciona y tiene una correspondencia con los actos sexuales contra los menores**, es decir, cuando esa inducción a través del uso de las TIC o enlace virtual con el menor tiene como objetivo el contacto sexual, como sucedió en este caso (**M. P. Hugo Quintero Bernate**).



Queda en evidencia la fragilidad de la ley colombiana con respecto a los Ciberdelitos, ya que muchos de estos en realidad no se configuran como delitos, por esta razón, los delitos mencionados en este mismo texto como: pornografía infantil, amenazas o extorsión en línea y acoso en línea; no son delitos por sí solos, simplemente que en la configuración del caso se encuentran factores que están establecidos y configurados bajo otros artículos penales.


JOSÉ FERNANDO GUTIÉRREZ RAMÍREZ
HERNÁN MAURICIO MÁRQUEZ MARULANDA
HAROLD ROMAÑA MACHADO