Apoyo Jurídico en la Fase de Investigación en los Procesos Penales tratados en la Dirección Especializada Contra los Delitos Informáticos de la Fiscalía General de la Nación en la ciudad de Bucaramanga

María Gabriela Pedraza Gómez

Trabajo de grado presentado como requisito para optar al título de Abogada

Directora

Yuli Andrea López Velasco

Abogada y Candidata a Magíster en DDHH

Tutora

Luz Dary Navas Gamboa

Especialista en Derecho Penal

Universidad Industrial de Santander

Facultad de Ciencias Humanas

Escuela de Derecho y Ciencia Política

Bucaramanga

2024

Dedicatoria

A mi mamá quien siempre ha estado apoyándome y creyendo en mí, por recordarme de lo que soy capaz y de dónde vengo, este triunfo te lo dedico a ti, te amo.

A Camilo Pilonieta por acompañarme en este camino y ser una voz de aliento y ternura en todo momento.

Agradecimientos

Agradecimientos muy especiales a la Universidad Industrial de Santander quien forjó mi crecimiento académico y el genuino interés por ejercer un derecho en pro de los intereses sociales y populares.

Contenido

Pág.

Lista de Tablas

Pág.

Lista de Figuras

Pág.

Resumen

Título: Apoyo jurídico en la fase de investigación en los procesos penales tratados en la Dirección Especializada Contra los Delitos Informáticos de la Fiscalía General de la Nación en la ciudad de Bucaramanga[*].

Autora: María Gabriela Pedraza Gómez[**].

Palabras Claves: Sujeto activo, sujeto pasivo, ciberdelito, Phishing, Malware, SIM SWAP, ransomware de bloqueo, Ataque DoS, DNS, Trojan, MITB, Carding, Insider, cambiazo, ingeniería social, modalidad.

Descripción: Este trabajo es el fruto del desarrollo de la práctica jurídica en la fiscalía seccional 07 de hurtos y delitos informáticos con la finalidad de identificar los desafíos prácticos y conceptuales que se presentan en el proceso de investigación a partir de los delitos enunciados en la ley 1273 del 2009, que corresponden a esta seccional.

Es así como en este escrito se presenta un breve contexto sobre conceptos relevantes para la comprensión de modalidades bajo las cuales se cometen estos delitos; así como las normas jurídicas aplicables sobre casos puntuales trabajados durante la práctica, se estudian además las causales de archivo a la par que se identifican las dificultades en la indagación que llevan a esta decisión, se identifican las limitaciones y obstáculos que se observaron y se realizan algunas recomendaciones a fin que la seccional 07 de delitos informáticos las tenga en consideración si desean mejorar en la celeridad y efectividad con la que se llevan los procesos en la etapa de investigación.

[*] Trabajo de Grado

[**] Facultad de Ciencias Humanas. Escuela de Derecho y Ciencia Política. Directora: Yuli Andrea López Velasco. Tutora: Luz Dary Navas Gamboa

Abstract

Title: Legal Support in the Investigation Phase of Criminal Proceedings Handled by the Specialized Directorate Against Cybercrime of the Office of the Attorney General in the City of Bucaramanga.[*]

Author: María Gabriela Pedraza Gómez.[**]

Keywords: Active subject, passive subject, cybercrime, phishing, malware, SIM swap, locker ransomware, DoS attack, DNS, Trojan, MITB, carding, insider, card swap, social engineering, method.

Description: This work is the result of the development of legal practice at the Sectional Prosecutor's Office 07 for Theft and Cybercrime, with the aim of identifying the practical and conceptual challenges that arise in the investigation process based on the crimes outlined in Law 1273 of 2009, which pertain to this section.

This document presents a brief context on relevant concepts for understanding the methods under which these crimes are committed and the applicable legal norms concerning specific cases handled during the practice. It also examines the reasons for case closures, identifying the investigative challenges that lead to this decision, along with the limitations and obstacles encountered. The findings are discussed, and some recommendations are provided for Sectional Prosecutor's Office 07 for Cybercrime to consider if they wish to improve the speed and effectiveness of the investigative process.

[*] Bachelor Thesis

[**] Faculty of Human Sciences. School of Law and Political Science. Director: Yuli Andrea López Velasco. Tutor: Luz Dary Navas Gamboa

Introducción

El avance continuo en el campo de las telecomunicaciones ha sido fundamental para el progreso de la sociedad moderna, brindando innumerables beneficios en términos de acceso a información y conocimiento. En este sentido, se puede afirmar que, gracias a la expansión de las tecnologías de información y comunicación, las personas en todo el mundo pueden conectarse instantáneamente, acceder a vastos recursos de información y participar en la economía digital de manera más eficiente. De esta forma, la virtualidad representa en el mundo actual un mecanismo de aprendizaje, innovación y desarrollo económico.

Ahora bien, este crecimiento también ha traído consigo vulneraciones a la seguridad informática, lo que representa desafíos significativos para el Derecho Penal a la hora de abordar estas nuevas conductas típicas, antijurídicas y culpables. Estos actos, que van desde el fraude electrónico hasta la invasión de la privacidad en línea, desafían los cimientos tradicionales del sistema legal. Colombia, como muchos otros países, se ve inmersa en este complejo tejido de desafíos jurídicos que emergen con la misma velocidad con la que la tecnología avanza.

En respuesta a esta situación, el gobierno colombiano ha implementado acciones para combatir los delitos cibernéticos, incluyendo la promulgación y ejecución de normativas específicas, así como la creación de delegaturas especializadas dedicadas a investigar y sancionar actividades ilegales en el ámbito digital.

No obstante, los desafíos sobre este tipo de conductas delictivas continúan debido a que las acciones que vulneran la protección de la información y de los datos cibernéticos son cada vez más recurrentes y evolucionan junto con la tecnología. Lo anterior, se ve reflejado en los índices de criminalidad de los últimos años, debido a que Colombia presenta un auge en las conductas

delictivas digitales. Al respecto, según los datos recolectados por la periodista Lina Muñoz Medina (2023) en su artículo *Fiscalía reportó avance contra delitos informáticos,* durante el año 2022 se registraron 65.794 denuncias por delitos cibernéticos, mientras que, para el 21 de mayo de 2023 ya se habían reportado 23. 640 casos.

Adicionalmente, la investigación de los delitos cibernéticos plantea un desafío especial debido a factores como el anonimato, la falta de conciencia de los usuarios para implementar medidas de seguridad preventivas, la naturaleza transnacional de algunas conductas delictivas y la dificultad que representa probar los elementos del tipo penal en conductas que están en constante cambio y que provocan diferentes daños a las víctimas.

Es justo aquí donde tiene lugar el presente trabajo, el cual pretende desarrollar un documento que aporte una comprensión más profunda de los obstáculos enfrentados por el sistema legal colombiano en la persecución efectiva del delito digital. Para lograr dicho objetivo, en el desarrollo de la práctica jurídico social propuesta se llevarán a cabo las siguientes actividades: en primer lugar, se realizará una compilación normativa y jurisprudencial de delitos informáticos contenidos en la Ley 1273 de 2009, haciendo énfasis en sus modalidades y caracterización; seguidamente, se plantea examinar casos concretos tratados en la jurisdicción de la Fiscalía Siete (07) Especializada Contra Delitos Informáticos, con el fin de identificar las dificultades prácticas que impiden la correcta investigación de los hechos delictivos; y, finalmente, se propone crear un listado de soluciones prácticas que faciliten la persecución de los delitos informáticos y el cumplimiento de los objetivos de proceso.

1. Planteamiento problema

Los delitos cibernéticos representan una creciente amenaza para la seguridad digital en la sociedad contemporánea. A medida que la tecnología avanza y se integra más en nuestras vidas cotidianas, también aumentan las oportunidades para la perpetración de delitos en línea. Sin embargo, la efectividad de la investigación y persecución de estos delitos se ve obstaculizada por una serie de desafíos prácticos y conceptuales. Estas dificultades incluyen, entre otras cosas, el anonimato en línea, la falta de colaboración entre jurisdicciones, la evolución constante de las técnicas criminales, y las limitaciones tecnológicas y legales en la recopilación de pruebas digitales.

Teniendo en cuenta lo antedicho, el presente trabajo se propone como un medio para profundizar en la comprensión de estos obstáculos. Para ello, se llevará a cabo un análisis exhaustivo de diversas dimensiones que influyen en la efectividad de la persecución del delito digital en Colombia. Esto incluirá la evaluación de la legislación actual, los recursos disponibles para las autoridades encargadas de hacer cumplir la ley, los desafíos técnicos y jurídicos asociados con la naturaleza transnacional de muchos delitos cibernéticos, así como las posibles lagunas en la coordinación entre diferentes entidades gubernamentales y sectores privados.

Así pues, se espera que este documento no solo contribuya a una comprensión más profunda de los obstáculos enfrentados por el sistema legal colombiano en la persecución del delito digital, sino que también sirva como punto de partida para el diseño e implementación de medidas más efectivas en este ámbito crucial para el correcto desarrollo del sistema penal acusatorio.

2. Alcance del trabajo

Con el presente trabajo se espera recolectar información práctica sobre las dificultades que se presentan en la investigación de los delitos cibernéticos, según los casos adelantados por la Fiscalía Siete (07) Especializada Contra Delitos Informáticos en el tiempo de duración de la práctica jurídico social planteada. Lo anterior, con el fin de lograr un material de apoyo que facilite la persecución penal y oriente al lector en los retos que enfrenta el operador investigativo y acusador a la hora de enfrentar el ciberdelito.

3. Objetivos

3.1 Objetivo general

Apoyar jurídicamente en la fase de indagación e investigación en los procesos penales en conocimiento de la Dirección Especializada Contra los Delitos Informáticos de la Fiscalía General de la Nación en la ciudad de Bucaramanga mediante la proyección de un documento que profundice en la comprensión de los obstáculos enfrentados por el sistema legal colombiano en la persecución efectiva del delito digital.

3.2 Objetivos específicos

Contextualizar sobre el marco legal del ciberdelito en Colombia utilizando la normativa vigente y la jurisprudencia relacionada.

Analizar casos específicos abordados en la jurisdicción de la Fiscalía Siete (07) Especializada Contra Delitos Informáticos para detectar las dificultades prácticas que obstaculizan la adecuada investigación de los delitos informáticos.

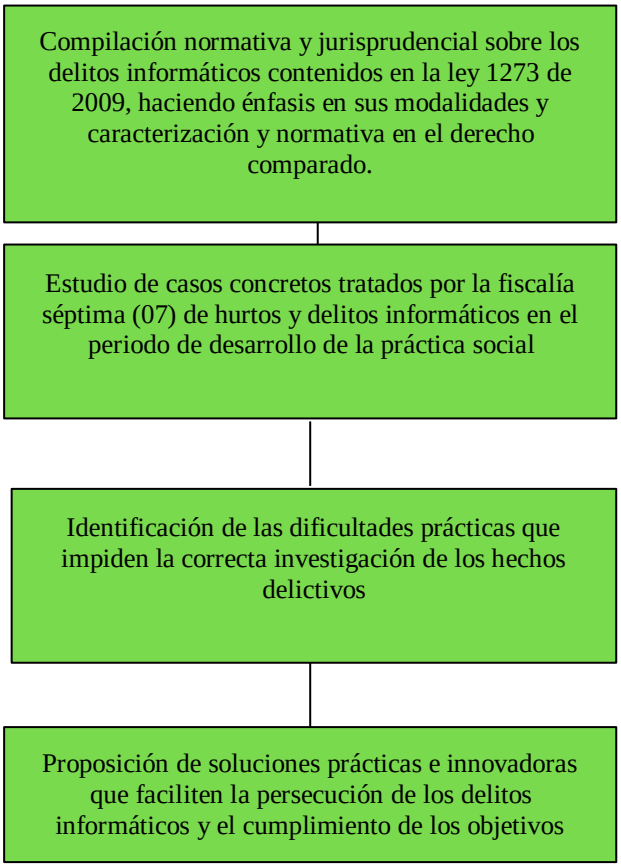
Elaborar soluciones concretas que agilicen la persecución de los delitos informáticos y promuevan el cumplimiento de los objetivos procesales.

4. Metodología

La metodología elegida para el desarrollo de la práctica jurídico social se divide en cinco etapas esquematizadas en la siguiente figura:

Figura 1.

Metodología



La metodología propuesta para alcanzar el objetivo planteado en el desarrollo de la práctica jurídico-social se fundamenta en una serie de actividades secuenciales y bien definidas. En primer lugar, se realizará una exhaustiva compilación normativa y jurisprudencial de los delitos informáticos contemplados en la Ley 1273 de 2009. Este proceso incluirá un apartado para el

análisis de un derecho comparado con panoramas de otros países, así como también una presentación y estudio detallado de las diversas modalidades delictivas y su caracterización legal, lo que permitirá una comprensión profunda de la legislación vigente en esta materia.

Posteriormente, se procederá a examinar casos concretos que hayan sido tratados en la jurisdicción de la Fiscalía Siete Especializada Contra Delitos Informáticos. Seguidamente, se realizará un análisis de los datos recolectados para identificar las dificultades prácticas que enfrentan los operadores judiciales en la correcta investigación y persecución de los delitos informáticos. Mediante el estudio de casos reales, se podrán identificar patrones, obstáculos y deficiencias en el proceso investigativo, lo que proporcionará una visión clara de las necesidades y desafíos presentes en la práctica judicial.

Finalmente, basándose en los hallazgos obtenidos en las etapas anteriores, se propondrá la creación de un listado de soluciones prácticas destinadas a mejorar la eficacia de la persecución de los delitos informáticos y garantizar el cumplimiento de los objetivos del proceso judicial. El objetivo final es proporcionar herramientas concretas y viables que contribuyan a fortalecer la etapa de investigación en el proceso penal en la lucha contra los delitos informáticos y asegurar la protección de los derechos de las víctimas y la sociedad en su conjunto.

5. Marcos

5.1 Marco de antecedentes jurídicos

Es imprescindible considerar que, debido a la novedad de los fenómenos tecnológicos y virtuales, no existen precedentes jurídicos o normativos específicos que aborden de manera explícita los delitos cibernéticos. Por consiguiente, estas conductas punibles carecían de una

regulación específica hasta la promulgación de la Ley 1273 de 2009, conocida como "la ley de los delitos informáticos". Así pues, debido a la necesidad de la regulación y a la influencia de la comunidad internacional, el Congreso dio vida a esta nueva ley que, en sus palabras:

> Se trata, de que el ordenamiento penal colombiano se sume a las políticas penales globalizadoras en materia del combate frontal contra la llamada criminalidad del ciberespacio y le brinde herramientas a la comunidad para la persecución de estos flagelos; al mismo tiempo, se busca brindar una adecuada tutela jurídica a un bien jurídico de tanta trascendencia en el mundo de hoy como lo es el atinente a la Protección de la Información y de los Datos (Gaceta del Congreso No 528 de 2007, p. 2.).

Esta normativa es actualmente reconocida como el punto de partida en la legislación sobre delitos cibernéticos, ya que introdujo modificaciones específicas en el Código Penal colombiano para proteger un nuevo bien jurídico: la información y los datos. La Ley 1273 se estructura en dos capítulos, el primero de los cuales aborda las medidas para proteger la confidencialidad, integridad y disponibilidad de la información, mientras que el segundo hace referencia a otras infracciones y ataques informáticos. “con ello el legislador penal colombiano confirmó su deseo de garantizar la seguridad de las funciones informáticas propiamente dichas, en contra de ataques cibercriminales, como figuras autónomas frente a los tipos penales tradicionales” (Posada, 2017, p.4)

No obstante, en la legislación previa se observa una tendencia a incluir referencias a los medios digitales en otros tipos penales, como aquellos que protegen los derechos de autor y la intimidad.

En ese sentido, se puede tener como antecedente normativo el Decreto 1360 de 1989. Esto, por introducir la regulación de la tecnología digital al establecer la inscripción del software en el

Registro Nacional de Derecho de Autor, brindando protección a las creaciones de software y otras soluciones informáticas.

Así mismo, para adaptar la legislación a las tendencias y prácticas contemporáneas, se incorporó en la Ley 599 del año 2000 la primera penalización para quienes comprometen sistemas informáticos. En esta ley, específicamente en el artículo 195 del libro II, título III, se tipifica el delito de "Acceso Abusivo a un Sistema Informático". Sin embargo, esta disposición tuvo una aplicación limitada en su duración de nueve años, ya que la gravedad de la conducta no justificaba la privación de la libertad y se consideraba inicialmente una simple multa como sanción.

Adicionalmente, la Ley 679 de 2001 constituye un antecedente relevante al establecer un estatuto para prevenir y contrarrestar la explotación, pornografía y turismo sexual con menores. Aunque esta normativa impuso restricciones a los proveedores de internet relacionados con contenido sexual de menores, no consideró estas acciones como delitos informáticos, limitándose a sanciones administrativas.

Por último, es importante mencionar la Ley 1928 de 2018 (budapesgt) en donde se retoma el "Convenio sobre la Ciberdelincuencia" ya que se trata de una de las medidas más recientes tomadas por el gobierno colombiano para tratar de disminuir los casos de delitos informáticos.

5.2 Marco de antecedentes académicos.

Dado que la Ley 1273 de 2009 incorpora nuevos delitos en un contexto delictivo que está en constante cambio y evolución, es esencial considerar la literatura especializada en delitos informáticos. Esto permite una comprensión más completa del tema al aprovechar los análisis y enfoques que diversos autores han ofrecido.

Uno de los textos más relevantes para los propósitos del presente trabajo es el del doctor en derecho Orlando Riascos Gómez (2010) quien planteó en su ensayo titulado *el delito*

informático contra la intimidad y los datos un análisis detallado de la tipificación penal del delito informático. Esto, comparando lo contemplado en el Código Penal Colombiano antes de la promulgación de la Ley 1273 y lo contemplado en la legislación de otros países, con el fin de cuestionar la estructuración de los delitos cibernéticos en la nueva normativa y la efectiva protección del bien jurídico. Al final de este escrito, cuestiona la elaboración de nuevo título desde distintos puntos académicos.

Ahora bien, en un estudio más reciente Jesús Arles Gamba Velandia (2019) en su investigación para obtener el título de maestro en justicia y tutela de los derechos con énfasis en ciencias penales y criminológicas realizó un estudio sobre el delito informático en el marco jurídico colombiano y el derecho comparado. En este escrito, titulado *El delito informático en el marco jurídico colombiano y el derecho comparado: caso de la transferencia no consentida de activos* estableció que, aunque Colombia ha avanzado significativamente en torno al fortalecimiento de la normatividad frente al ciberdelito, aún dista con respecto a la comunidad internacional, para identificar, colaborar y definir criterios comunes persecución y penalización de los diferentes delitos tipificados, lo que afecta la persecución de dichas conductas que se realizan cada vez más en el ámbito trasnacional.

Por otra parte, la ingeniera de sistemas Zulay Nayiv Sanchez Castillo (2017) en su Monografía de investigación para optar el título de especialista en seguridad informática titulada *Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia* plantea que la Ley 1273 de 2009 esta desactualizada por no contemplar las necesidades actuales en materia de ciberdelincuencia. Lo anterior, en razón a que los sistemas informáticos han evolucionado a tal punto que lo estructurado en la legislación penal no cubre las nuevas actuaciones delictivas ni los bienes jurídicos que están siendo vulnerados.

Premisa similar a la planteada por los estudiantes de la carrera de derecho Bechara, Alan Mosquera y Edwar Ledezma en su escrito *Análisis jurídico de la ley 1273 del 2009 y el surgimiento y expansión del delito de hurto y semejantes por medios informáticos*. Esto, en razón a que argumenta que la naturaleza misma de los delitos informáticos implica una evolución normativa constante, lo que representa un problema interminable no solo para el legislador colombiano, sino para toda la comunidad internacional.

5.3 Marco conceptual

Ahora bien, es menester tener en cuenta ciertos conceptos derivados del tema de estudio para facilitar el entendimiento del mismo. Con este fin, se traen a colación los conceptos más relevantes recopilados por la Fiscalía General de la Nación en la "*Cartilla metodológica de atención de delitos informáticos"* junto con anotaciones propias que complementan la contextualización de los términos.

Es importante mencionar que los conceptos aquí contenidos representan una mínima muestra de los términos utilizados para describir las técnicas y los medios de los ciberdelincuentes. Lo anterior, en razón a la vasta terminología que se tiene a nivel nacional e internacional.

Tabla 1.

Agrupación de términos sobre ataques cibernéticos

Ataques realizados mediante la manipulación de las víctimas	**Ataques realizados por medio de la manipulación de plataformas digitales (vulneraciones a los sistemas)**
SCAM	Ataques DNS
El Compromiso de Cuentas de Correo Empresarial (BEC)	Buffer Overflow
Phishing	Sniffer
Sim Swap	Ransomware
	Skimming

Ataques realizados mediante la manipulación de las víctimas	**Ataques realizados por medio de la manipulación de plataformas digitales (vulneraciones a los sistemas)**
Smishing	***MITB***
Revenge porn	***Software malicioso o Malware***
Cambiazo	***Explotación de vulnerabilidades***
	Ataque DoS (Denial of Service)
	Trojan (BANKER)
	Revenge porn
	Carding
	Insider

Así pues, los conceptos presentados en la anterior figura tratan sobre las actividades delictivas más comunes en el mundo cibernético agrupadas en dos categorías: en la primera, el atacante busca emplear medios informáticos para engañar a la víctima; en la segunda, busca vulnerar los sistemas informáticos en sí para lograr la extracción de información o el daño a la plataforma digital. Para una mejor comprensión del texto se hará una breve descripción de los diferentes modos:

5.3.1 Modos

5.3.1.1 Phishing. Es un ataque realizado por medio de ingeniería social que manipula psicológicamente a las personas para obtener información financiera o de datos personales. Los estafadores emplean correos electrónicos, mensajes de texto o llamadas telefónicas que aparentan ser de entidades o individuos confiables, como bancos o empresas conocidas.

Su objetivo es que las víctimas proporcionen datos sensibles, como contraseñas, números de cuenta o información personal. Este tipo de fraude puede resultar en la descarga de malware,

transferencia de fondos, suplantación de identidad y otros delitos que afectan negativamente el patrimonio económico de las víctimas y en algunas ocasiones también de sus conocidos.

5.3.1.2 Software malicioso o Malware. Es un tipo de programa diseñado para dañar, interrumpir o comprometer sistemas informáticos y redes, usualmente ingresan a los equipos y sistemas informáticos a partir de correos o links engaños en el cual los usuarios dan acceso sin saberlo a esta clase de ataque. Se clasifican en: virus, troyanos, ransomware, spyware y adware.

5.3.1.3 SIM SWAP o intercambio de SIM. Es un tipo de fraude en el que un delincuente cambia el número de teléfono de una víctima a una nueva tarjeta SIM controlada por el atacante. Esto permite al estafador recibir llamadas y mensajes destinados a la víctima, así como acceder a servicios que usan autenticación de dos factores (2FA). Este es un modo que también podríamos encontrar como modalidad en el 269i hurto por medios informáticos y semejantes ya que usualmente de este modo es que vulneran la seguridad de las cuentas de banca móvil las cuales cuentan con esta autentificación.

El proceso generalmente sigue estos pasos:

- Recolección de Información: El atacante obtiene detalles personales de la víctima mediante técnicas como phishing o la exploración de redes sociales.
- Contacto con el Proveedor de Telefonía: El delincuente se comunica con la compañía de telefonía móvil de la víctima y se hace pasar por ella para solicitar el cambio del número a una nueva SIM.
- Cambio de Número: Una vez aprobado el cambio por el proveedor, el número de teléfono de la víctima se transfiere a la SIM del atacante.

5.3.1.4 Explotación de vulnerabilidades. Se refiere al proceso de aprovechar fallos o debilidades en un sistema informático, software o red para obtener acceso no autorizado, causar daño, o ejecutar acciones maliciosas. Estas vulnerabilidades pueden ser errores de programación, configuraciones incorrectas, o fallos de seguridad que no han sido corregidos.

5.3.1.5 Ransomware de bloqueo. Es un tipo de malware que bloquea el acceso al sistema o los datos.

5.3.1.6 Ataque DoS (Denial of Service). Es un tipo de ataque que tiene por objetivo interrumpir el funcionamiento normal de un servidor, servicio o red, al sobrecargarlo con tráfico o solicitudes que excedan su capacidad de manejo. El objetivo es hacer que el sistema sea inaccesible para los usuarios, provocando una interrupción del servicio. También existe el Ataque DDoS (Distributed Denial of Service) el cual utiliza múltiples sistemas comprometidos (bots o una red de bots) (botnet) para lanzar un ataque coordinado, amplificando el impacto al generar un volumen masivo de tráfico.

5.3.1.7 Un ataque DNS (Domain Name System). Es una forma de ataque cibernético que explota vulnerabilidades en el sistema de nombres de dominio (DNS) para interrumpir la resolución de nombres de dominio a direcciones IP, desviar el tráfico a sitios fraudulentos, o afectar la disponibilidad y funcionalidad de servicios en línea.

Los usuarios pueden ser engañados para que ingresen datos sensibles en sitios falsos, un ejemplo de la ejecución de este ataque es el redireccionamiento de pago a una supuesta página que aparenta ser de la entidad bancaria y al ingresar tus datos realmente estas ingresándolos en una página fraudulenta.

5.3.1.8 Trojan (BANKER). Que son malwares que están dirigidos a obtener acceso a información de entidades financieras, a fin de robar los datos de las cuentas bancarias o de los sistemas de pago online de los usuarios.

5.3.1.9 Ataque Man In The Browser (MITB). Este ataque consiste en que se interceptan las comunicaciones de red utilizando programas llamados sniffers, que permiten que el atacante pueda ver toda tu navegación en la red, si bien no puede ver la información de sitios de pago online o la que se encuentra cifrada, si puede ver a qué sitios accediste, manipulando la red en tiempo real y con esta información, luego interferir las conexiones de red y duplicar el sitio web creando uno falso donde al poner la información permitirá el robo de credenciales.

5.3.1.10 Revenge porn. Que es conocido también como violencia digital o violencia de género digital dependiendo del contexto propio de cada situación, este hace referencia a cuando alguien comparte contenido íntimo de otra persona sin su autorización, generalmente imágenes o videos de naturaleza sexual o íntima, con la intención de humillar, avergonzar o dañar a la persona afectada.

5.3.1.11 Carding. Hace referencia a obtener, vender o usar de manera fraudulenta la información de tarjetas de crédito o débito. Los criminales que se dedican al carding obtienen los datos de las tarjetas de diversas maneras, como a través de ataques de phishing, malware, brechas de seguridad en bases de datos, o comprándolos en mercados ilegales (dark web).

5.3.1.12 Insider. El término "insider" hace referencia a una persona que tiene acceso autorizado a la información, sistemas o recursos dentro de una empresa, organización o entidad bancaria y que puede utilizar ese acceso para llevar a cabo actividades que van en contra de los intereses de la organización.

5.3.1.13 Cambiazo. Se refiere a una situación en que la víctima se encuentra realizando una transacción en un cajero con su tarjeta y permite la ayuda de terceras personas, que mediante engaños le cambian su tarjeta por otra logrando a partir de la confusión de la víctima que ésta exponga su clave, para luego hacer transacciones fraudulentas. esta modalidad es generalmente de crimen organizado, constituyendo bandas con división de roles tales como:

1. Inhabilitador de cajero o obstaculizador: quien inhabilita los cajeros para que no lean el chip de la tarjeta y así facilitar el acercamiento del cambiador a la víctima.

2. Cambiador: quien se acerca a la víctima simulando ser un usuario del cajero y mediante estrategias de ingeniería social logra tomar la tarjeta de la víctima e intercambiarla por una de iguales características y apoderándose de la clave.

3. Distractor u operador: finge ser un usuario del cajero para abrir el camino al cambiador dando la impresión de que el cajero está en funcionamiento.

6. Información de la organización

6.1 Definición de la organización

La Fiscalía General de la Nación es una entidad de la rama judicial del poder público con plena autonomía administrativa y presupuestal, cuya función está orientada a brindar a los ciudadanos una cumplida y eficaz administración de justicia.

6.2 Misión

La Fiscalía General de la Nación garantiza el derecho al acceso a la justicia de los habitantes del territorio nacional, por medio de la investigación de las conductas punibles, el ejercicio de la acción penal y de la acción de extinción del derecho de dominio, en el marco del

debido proceso. Así mismo, protege los derechos a la verdad y a la reparación de las víctimas de los delitos y participa activamente en el diseño y la ejecución de la política criminal del Estado.

6.3 Visión

En 2024, la Fiscalía General de la Nación será reconocida como una organización confiable, transparente y eficiente, que hace presencia oportuna en todo el territorio a partir de la innovación de las metodologías de investigación, con lo que habremos contribuido a una sociedad libre de violencia. Con el trabajo realizado, la entidad será un lugar en donde los funcionarios se inspiren cada vez más a dar lo mejor de sí.

6.4 Organigrama

Figura 2.

Organigrama: estructura orgánica de la Fiscalía General de la Nación

Nota: Adaptado *De Estructura Orgánica De La Fiscalía General De La Nación,* 2022, fiscalia.gov.co (https://www.fiscalia.gov.co/colombia/la-entidad/organigrama/). CC BY 2.0

6.5 Detalles específicos relacionados con la práctica

La labor ejercida en calidad de practicante se realizará de forma presencial en la ciudad de Bucaramanga, en la Dirección Especializada Contra los Delitos Informáticos de la Fiscalía General

de la Nación. El apoyo jurídico se brindará específicamente a Fiscalía Siete (07) Especializada Contra Delitos Informáticos, realizando las siguientes funciones:

- Proyectar escritos de acusación, órdenes a policía judicial, órdenes de archivo.
- Brindar atención y direccionamiento a los usuarios, con el fin de suministrar la información necesaria y recopilar los documentos que se requieran para avanzar en las investigaciones.
- Proyectar respuestas a derechos de petición y solicitudes elevadas por las víctimas en los procesos penales.
- Colaborar y apoyar el desarrollo de las actividades relacionadas con la naturaleza de su cargo, cuando por necesidades del servicio, su superior lo requiera.
- Brindar apoyo en las jornadas de descongestión.
- Recolectar y clasificar oportunamente y de acuerdo con las instrucciones del superior inmediato la correspondencia que ingresa al Despacho.
- Recibir y efectuar llamadas telefónicas, tomar nota de ellas y establecer los contactos requeridos por el fiscal para convocar a las partes a diligencias de toda naturaleza.
- Apoyar en recepción de entrevistas a testigos.

7. Cronograma de actividades

Tabla 2.

Cronograma de actividades

Actividad	Mayo				Junio				Julio				Agosto			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Actividad 1. Realizar una compilación de normativa y jurisprudencia sobre los delitos informáticos contenidos en la Ley 1273 de 2009.																
Actividad 2. Estudiar casos concretos tratados por la Fiscalía Siete Especializada Contra Delitos Informáticos que sirvan a desarrollo del trabajo.																
Actividad 3. Identificar las dificultades prácticas que impiden la correcta investigación de los hechos delictivos.																
Actividad 4. Proponer soluciones prácticas e ideas innovadoras que faciliten la persecución de los delitos informáticos y el cumplimiento de los objetivos del proceso.																

8. Desarrollo de la práctica jurídico social.

8.1 Primer informe: Contextualización sobre el marco legal del ciberdelito en Colombia utilizando la normativa vigente y la jurisprudencia relacionada.

8.1.1 Marco legal del ciberdelito nacional - internacional

8.1.1.1 Tratados y Convenios Internacionales. Esta regulación se ha ampliado con normativa internacional como lo es el *convenio de Budapest* el cual se aprobó mediante la Ley 1928 de 2018, este tratado contra la ciberdelincuencia reforzó los mecanismos contra los ciberdelitos y abordó los retos delictivos relacionados con el uso de la información y los datos informáticos, incorporando desde definiciones frente a la terminología informática hasta direccionamientos para la tipificación y medidas legislativas de los delitos informáticos o ciberdelitos. La corte constitucional en la Sentencia C-224/19 de Revisión oficiosa de la Ley 1928 de 2018 señala que "El Convenio sobre la Ciberdelincuencia se presenta como un instrumento internacional cuyo objetivo es intensificar la cooperación entre los Estados Parte del mismo, mediante la materialización de una política criminal común en contra de la comisión de delitos cibernéticos.

Lo anterior, como una respuesta a los profundos cambios provocados por la digitalización, convergencia y globalización de datos y sistemas informáticos. De esta manera, al establecer las condiciones para prevenir la comisión de ilícitos en las redes informáticas, compromete a los países signatarios a adoptar su legislación interna para combatir posibles amenazas a bienes jurídicos tutelados como la confidencialidad, la integridad y la disponibilidad de datos y de los sistemas informáticos, protegiendo en general los intereses vinculados al desarrollo de las tecnologías de la información.

La totalidad de las disposiciones contenidas en el Convenio conservan como base la cooperación entre las Partes, lo cual es un desarrollo del tratamiento igualitario y los efectos recíprocos del Convenio. Destaca la Corte que lo contenido en este instrumento efectiviza los fines esenciales de la Constitución, atiende la soberanía e independencia del Estado colombiano en materia penal, y observa los mandatos constitucionales que se concretan con la adquisición de compromisos internacionales regidos por principios de conveniencia, soberanía nacional, reciprocidad y equidad."

8.1.1.2 Normativa y jurisprudencia en Colombia. El avance continuo en el campo de las telecomunicaciones ha sido fundamental para el progreso de la sociedad moderna, brindando innumerables beneficios en términos de acceso a información y conocimiento. En este sentido, se puede afirmar que, gracias a la expansión de las tecnologías de información y comunicación, las personas en todo el mundo pueden conectarse instantáneamente, acceder a vastos recursos de información y participar en la economía digital de manera más eficiente. De esta forma, la virtualidad representa en el mundo actual un mecanismo de aprendizaje, innovación y desarrollo económico.

Ahora bien, este crecimiento también ha traído consigo vulneraciones a la seguridad informática, lo que representa desafíos significativos para el Derecho Penal a la hora de abordar estas nuevas conductas típicas, antijurídicas y culpables. Estos actos, que van desde el fraude electrónico hasta la invasión de la privacidad en línea, desafían los cimientos tradicionales del sistema legal. Colombia, como muchos otros países, se ve inmersa en este complejo tejido de desafíos jurídicos que emergen con la misma velocidad con la que la tecnología avanza.

En respuesta a esta situación, el gobierno colombiano ha implementado acciones para combatir los delitos cibernéticos, incluyendo la promulgación y ejecución de normativas

específicas, la realización de convenios internacionales, así como la creación de delegaturas especializadas dedicadas a investigar y sancionar actividades ilegales en el ámbito digital.

Hasta el año 2009 no existía una regulación en colombia frente a los delitos informáticos, en este año se expide la ***Ley 1273 de 2009*** que incorporó un nuevo bien jurídico tutelado en el código penal colombiano denominado **"de la protección de la información y de los datos"** y por consecuencia una compilación de delitos con la que se buscó sancionar y regular las conductas relacionadas con el mal uso de las redes informáticas, acceso a la información y protección de datos, tipificando delitos que van desde acceso abusivo a un sistema informático hasta transferencia no consentida de activos.

Así mismo se han realizado importantes aportes desde la jurisprudencia de la corte constitucional y la corte suprema de justicia que han dado mayor claridad sobre este naciente panorama jurídico de los delitos informáticos y la protección de la información:

Tabla 3.

Jurisprudencia relevante

Jurisprudencia Relevante en Delitos Informáticos		
Sentencia	**Jurisdicción**	**Importancia**
C-1011 de 2008	Corte Constitucional	– Declara exequible el Proyecto de Ley Estatutaria No. 27/06 Senado – 221/07 Cámara (Acum. 05/06 Senado) y se resalta la importancia de proteger la información y los datos en la era digital en un contexto donde los ataques cibernéticos y los fraudes digitales son cada vez más sofisticados – Establece los criterios para la indemnización cuando se violen los procedimientos y principios del habeas data. – Determina los principios y obligaciones que orientan la administración de datos personales de contenido financiero y

Jurisprudencia Relevante en Delitos Informáticos

Sentencia	Jurisdicción	Importancia
		dando claridad a las nociones necesarias para el desarrollo de la misma, desarrollando el concepto de *titular de la información, operadores de información, fuente de información, usuario y demás.* – Establece la competencia de la superintendencia de industria y comercio financiera frente a la protección de las garantías de los derechos del titular y la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto a la actividad de administración de datos personales y la facultad de imponer sanciones sobre los mismos.
SP 903-2024	Corte Suprema de Justicia Sala de Casación Penal	– La corte ofrece un análisis respecto de la naturaleza del tipo penal correspondiente al 269I y esclarece que, con este, el legislador buscó darle un énfasis al delito por medio informativo más no creó un nuevo tipo penal pues este ya estaba calificado dentro de las circunstancias de agravación del hurto simple. – Aclaro frente al hurto por medios informáticos y semejantes y la prerrogativa de reparación integral consagrada en el artículo 269 de la Ley 599 de 2000 donde se establece la aplicabilidad taxativa a *los capítulos I al VIII del Título VII del Código Penal, los capítulos I al VIII del Título VII del Código Penal,* que mediante una interpretación integral y

Jurisprudencia Relevante en Delitos Informáticos

Sentencia	Jurisdicción	Importancia
		sistemática de la norma, el hecho de que sea aplicable a los delitos contra el patrimonio económico, siendo el hurto por medios informáticos uno de estos, implica que esta prerrogativa será aplicable al indiciado por este tipo de delito informático
SP 1508-2017	Corte Suprema de Justicia	– Esta decisión es relevante porque trata sobre el **acceso abusivo a un sistema informático**. En este caso, una persona fue condenada por ingresar sin autorización a una plataforma informática con el fin de alterar información. La Corte Suprema ratificó que dicho comportamiento constituye un delito según la Ley 1273 de 2009. – Reforzó la idea de que el acceso no autorizado a sistemas informáticos sin importar cual sea la finalidad u intención es punible
SP-16533-2018	Corte Suprema de Justicia	– Esta sentencia es importante ya que versa sobre un caso de estafas realizadas por un grupo de personas las cuales utilizarán medios informáticos para la comisión de las mismas. Estas personas realizaban transacciones fraudulentas. Al hacer el análisis de la tipificación del delito la corte establece, que cuando se hiciere uso de un sistema informático o red para la comisión de estos delitos el marco de persecución legal puede extenderse al convertirse en delitos informáticos.

8.1.1.3 Normativa en el derecho comparado. Frente a la normatividad y contexto internacional he realizado el análisis de los siguientes países a fin de establecer y enumerar en el siguiente informe los retos y aproximaciones necesarias para construir un contexto legislativo frente a los ciberdelitos desde un panorama global que se hace necesario frente a la naturaleza sin fronteras de esta clase de delitos.

8.1.1.3.1 Alemania. En Alemania, los delitos informáticos están regulados principalmente en el Código Penal Alemán (Strafgesetzbuch, StGB), y en 1986 se se adoptó la Segunda Ley contra la Criminalidad Económica o Ley de Delitos Informáticos que específicamente busco regular los ciberdelitos relacionados contra el patrimonio y la seguridad de los datos. Las secciones del StGB más relevantes para ciberdelitos van desde acceso ilegal a datos protegidos (Sección 202a), intercepción ilegal de datos (Sección 202b), fraude informático (Sección 263a), hasta daño a datos (Sección 303a).

Además, incluye dentro de su normatividad a El Reglamento General de Protección de Datos de la Unión Europea (GDPR), imponiendo estrictas reglas sobre la protección de datos personales y la privacidad. Estableciendo una sólida infraestructura para combatir los ciberdelitos, incluyendo la Oficina Federal de Policía Criminal (BKA) y el Centro de Ciberseguridad (Deutschland ,2023).

En una comparativa con el derecho colombiano podríamos decir que, si bien la tipificación de los delitos podría ser similar en varias de sus secciones, la normatividad alemana frente al ciberdelito es un poco más amplia debido a su especificidad frente a las reglas que rigen la protección de datos y sus avances tecnológicos propios, esto sumado a la creación del centro de ciberseguridad el cual tiene un enfoque directo para combatir este tipo de delitos.

En tanto a modelo comparativo se podría usar como referencia para la creación de instituciones para la protección de los datos y la ciberseguridad, sin embargo se hace necesario la contextualización de un panorama jurídico y que atienda a las realidades materiales y las modalidades propias de sus contextos, que están supeditadas también a los desarrollos tecnológicos de cada país, sin embargo no se debe olvidar que en el ciberespacio las fronteras territoriales se vuelven indivisibles hasta el punto en que cualquiera con acceso a una red informática o sujeto a bases de datos podría ser víctima de ciberataques desde cualquier parte del mundo, razón por la cual la legislación colombiana ha tenido que adaptarse a estos retos que impone el desarrollo de nuevas tecnologías y modalidades de fraudes informáticos, buscando integrar a partir del convenio de budapest una normatividad internacional a fin de lograr consolidar contextos legales y tecnológicos más allá de las particularidades de cada país.

8.1.1.3.2 Brasil. En Brasil la regulación de los delitos informáticos se encuentra focalizada en dos leyes principales que son la Ley 12737 del 2017 (La ley Carolina Dieckmann) y la ley 12965 del 2014 que determina el Marco Civil de internet. Para comprender el alcance de la figura de los delitos informáticos en Brasil, debemos entonces entender estas dos leyes para lo cual se debe referirse a la ley 12737 del 2017 denominada la ley del Cibercrimen establece delitos relacionados con el uso delictivo de sistemas informáticos.

Así mismo, la ley 12965 del 2014 plantea un alcance más amplio sobre la regulación del uso del internet, y determinó unos lineamientos tanto en términos de protección de derechos como el establecimiento de los deberes en cabeza de usuarios y proveedores en relación con las herramientas informáticas.

De esta ley se desprenden ciertos principios deberes y garantías como lo son: la neutralidad de la red, la protección de datos personales y la responsabilidad de los intermediarios. Por último,

el código penal de Brasil contempla sanciones para los delitos informáticos relacionadas con los tipos penales como lo serían la extorsión, el fraude y otros delitos de esta naturaleza; en ese sentido, hay ciertas similitudes entre la legislación colombiana en este aspecto, iniciando porque en ambas regulaciones existe una protección de la privacidad y los datos personales de los individuos en la red, haciendo evidente que para ambas legislaciones es una prioridad la protección de los derechos de los usuarios de medios informáticos.

Sin embargo, pese a tener ciertas similitudes la frente a los delitos que se persiguen, estos se abordan desde perspectivas diferentes, por ejemplo para Brasil se persiguen delitos como la difusión no autorizada de datos personales, mientras que en Colombia se persigue este delito como la violación de datos personales, la cual no solo está limitada a la difusión si no también se configura con otros verbos como la divulgación, venta, compra y otros más que abarcan otros posibles escenarios para la comisión del delito lo que permite ver una diferencia clara en relación con los derechos que pretenden proteger y el alcance normativo.

Finalmente, una diferencia fundamental es el desarrollo de la normatividad frente a la responsabilidad de los intermediarios y proveedores de las redes informáticas, si bien para ambas legislaciones existe responsabilidad no solo para los usuarios que hacen uso indebido sino también para los proveedores de estos servicios debido a que deben asegurar una prestación transparente del servicio que garantice la seguridad de los usuarios.

En Colombia aun cuando esta responsabilidad se ha desarrollado a nivel jurisprudencial, no se ha consolidado con tanta precisión el alcance de la misma, como si lo hace Brasil en su ley 12965 del 2014 con garantías como la neutralidad de red.

8.2 Segundo informe

Análisis de casos específicos abordados en la jurisdicción de la Fiscalía Siete (07) Especializada Contra Delitos Informáticos e identificación de las dificultades prácticas que obstaculizan la adecuada investigación de los delitos informáticos.

Para dar cumplimiento a mi segundo objetivo el cual consiste en el análisis de casos específicos abordados durante la práctica jurídica, se hace necesario esclarecer las modalidades y modos bajo las cuales se da las conductas tipificadas en la ley 1273 del 2009, para esto tuve como apoyo la Cartilla metodológica de atención de delitos informáticos realizada por la fiscalía general de la nación donde nos ilustra acerca de los modos en los que se materializan estos delitos:

Para fines de la comprensión de los siguientes enunciados nos referiremos a modalidad como las circunstancias de lugar, tiempo, modo u ocasión que califican la conducta del sujeto activo y a modo como el concepto definido para una modalidad específica mediante la cual se logra la comisión del delito.

8.2.1 Delitos presentes en la ley 1273 de 2009, modalidades y modos.

Estos son solo algunos de los medios y modalidades a través de los cuales se llevan a cabo las conductas tipificadas en la ley 1273 del 2009, en las siguientes tablas realizadas por la fiscalía para la orientación a funcionarios se cualifican estos modos de actuar para la comisión de los delitos informáticos determinando modo, modalidad y delito.

Esta información será relevante al momento de comprender el análisis de casos específicos que se presentarán más adelante. Para la contextualización de estos modos previamente se realizó la caracterización en el marco conceptual donde se puede encontrar las definiciones y particularidades de cada uno.

Tabla 4.

Fiscalía General de la Nación, 2024.

Artículo	Tipificación	Modalidad	Modo
269 A	**Acceso abusivo a un sistema informático** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá…	**Acceso Físico** (desde el equipo o terminal directamente afectado) **Acceso Remoto**	1. Ingeniería Social. 2. Software Malicioso. 3. Phishing. 4. Vishing. 5. Smishing. 6. SIM SWAP. 7. Explotación de Vulnerabilidades

Nota: Información tomada de la Cartilla Metodológica de Atención de Delitos Informáticos, P.11, Fiscalía General de la Nación, 2024.

Tabla 5.

Fiscalía General de la Nación, 2024.

Artículo	Tipificación	Modalidad	Modo
269 B	**Obstaculización ilegítima de sistema informático o red de telecomunicación** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá…	**Impedir** (Supone la inutilización **absoluta** del sistema, los datos o la red de telecomunicaciones) **Obstaculizar** (Supone la inutilización **parcial** del sistema, los datos o la red de telecomunicaciones)	1. Ransomware de bloqueo o de cifrado 2. Ataque DoS. 3. Ataque DDoS. 4. Botnet. 5. Ataque DNS 6. Buffer Overflow.

Nota: Información tomada de la Cartilla Metodológica de Atención de Delitos Informáticos, P.12, Fiscalía General de la Nación, 2024.

Tabla 6.

Fiscalía General de la Nación, 2024.

Artículo	Tipificación	Modalidad	Modo
269 C	**Interceptación de datos informáticos** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá...	**Interceptación** de datos **personales** (sensibles, privados o semiprivados) o **impersonales** (aquellos no referidos a personas pero que no resultan anónimos)	1. Se realiza por medios electrónicos, informáticos, ópticos, magnéticos. 2. Trojanos (Banker). 3. Ataque MitB Man in the browser. 4. Ataque MitM Man in the middle.

Nota: Información tomada de la Cartilla Metodológica de Atención de Delitos Informáticos, P.11, Fiscalía General de la Nación, 2024.

Tabla 7.

Fiscalía General de la Nación, 2024.

Artículo	Tipificación	Modalidad	Modo
269 D	**Daño Informático** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá...	**Daño** informático o lógico propiamente dicho sobre **datos, sistemas de tratamiento de información o componentes o soportes lógicos del sistema** **Daño** físico sobre **infraestructura informática (Hardware)**	1. Defacement. 2. Software Malicioso. 3. Inyección de código. 4. Daño físico de equipos, partes o componentes de un sistema de información. 5. Alteración, borrado o destrucción de Información.

Nota: Información tomada de la Cartilla Metodológica de Atención de Delitos Informáticos, P.12, Fiscalía General de la Nación, 2024.

Tabla 8.

Fiscalía General de la Nación, 2024.

Artículo	Tipificación	Modalidad	Modo
269 E	**Uso de software malicioso** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá...	**Desarrollo de software malicioso** **Uso de software malicioso** **Distribución de software malicioso**	1. Software Malicioso

Nota: Información tomada de la Cartilla Metodológica de Atención de Delitos Informáticos, P.12, Fiscalía General de la Nación, 2024.

Tabla 9.

Fiscalía General de la Nación, 2024.

Artículo	Tipificación	Modalidad	Modo
269 F	**Violación de datos personales** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos, o medios semejantes, incurrirá...	**Vulneración de la Confidencialidad, Integridad** y/o **Disponibilidad** de datos personales contenidos en cualquier medio informático.	1. Ingeniería Social. 2. Software Malicioso. 3. Phishing. 4. Vishing. 5. Smishing. 6. Explotación de Vulnerabilidades

Nota: Información tomada de la Cartilla Metodológica de Atención de Delitos Informáticos, P.12, Fiscalía General de la Nación, 2024.

Tabla 10.

Fiscalía General de la Nación, 2024.

Artículo	Tipificación	Modalidad	Modo
269 G	**Suplantación de sitios web para capturar datos personales** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventana emergentes, incurrirá... En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave...	**Desarrollo, Implementación, Comercialización o Utilización de sitios web**	1. Falsedad de identidad Virtual. 2. Phishing. 3. Vishing. 4. Smishing. 5. Explotación de Vulnerabilidades 6. Ingeniería Social

Nota: Información tomada de la Cartilla Metodológica de Atención de Delitos Informáticos, P.12, Fiscalía General de la Nación, 2024.

Tabla 11.

Fiscalía General de la Nación, 2024.

Artículo	Tipificación	Modalidad	Modo
269 I	**Hurto por medios informáticos y semejantes** El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá...	Apropiarse de un bien **superando medidas de seguridad** informáticas Apropiarse de un bien **suplantando a un usuario** ante los sistemas de autenticación	1. Ingeniería Social. 2. Software Malicioso. 3. Phishing. 4. Vishing. 5. Smishing. 6. SIM SWAP. 7. Explotación de Vulnerabilidades. 8. Insider. 9. Carding.

Nota: Información tomada de la Cartilla Metodológica de Atención de Delitos Informáticos, P.12, Fiscalía General de la Nación, 2024.

Teniendo una perspectiva más amplia de los diferentes modus operandi mediante los cuales se llega a las actuaciones delictivas dentro y fuera del ciberespacio que afectan la seguridad y protección de los datos, así como los sistemas informáticos y las comunicaciones a través de

tecnologías digitales, los cuales dan inicio a las indagaciones, es preciso para el estudio de los casos puntuales tener la claridad frente a las causales por las cuales se dan cierre a estos procesos penales en etapa de indagación.

8.2.2 Archivo de los procesos penales

El archivo de las diligencias es una prerrogativa del ente acusador cuando, en un caso, se determina que no se cumplen los requisitos mínimos necesarios para proceder con la acción penal. Esto ocurre cuando los elementos probatorios y la evidencia física obtenida son insuficientes para formular una imputación y continuar con el proceso penal, ya que no son lo bastante claros para ilustrar y cumplir con los requisitos del tipo penal en relación con los hechos. Sin embargo, esta decisión no impide la posibilidad de reanudar la indagación si surgen nuevos elementos de prueba que permitan caracterizar el hecho como delito y/o identificar el sujeto activo. En ambos escenarios, la decisión debe ser informada a las víctimas involucradas en el proceso. De conformidad con el código de procedimiento penal ley 906 del 2004 y las importantes interpretaciones dadas por la corte constitucional y la corte suprema de justicia, las causales por las cuales le está permitido al ente fiscal la determinación de la orden de archivo son las siguientes:

8.2.2.1 Archivo por atipicidad de la conducta. Este tipo de archivo se da cuando se determina que el hecho investigado no se ajusta a la descripción de un delito en la ley penal. En otras palabras, se concluye que la conducta en cuestión no encaja en ninguno de los tipos penales previstos por el Código Penal o las leyes especiales. Este tipo de archivo encuentra sustento en el artículo 79 de la ley 906 del 2004 y en la sentencia de la corte constitucional C-1154 del 15 de noviembre del 2005 con ponencia del magistrado Manuel Jose Cepeda Espinosa.

8.2.2.2 Archivo por imposibilidad de ubicar el sujeto activo. Este tipo de archivo se da "Cuando luego de adelantadas las averiguaciones resultan imposible encontrar el sujeto activo de la acción." interpretación brindada por la sentencia de la Sala Plena calendada del 5 de Julio de 2007 de la Corte Suprema de Justicia con ponencia del magistrado Yesid Ramírez Bastidas, al realizar un estudio al concepto de atipicidad objetiva ilustrado por la Corte Constitucional en la sentencia C-591 de 2005.

8.2.2.3 Archivo por imposibilidad de ubicar el sujeto pasivo. Este tipo de archivo se da cuando a pesar de citar a la víctima o intentar establecer comunicación con el denunciante los intentos son fallidos reduciendo las pocas probabilidades de lograr un resultado positivo dentro de la investigación y de identificar al sujeto activo.

8.2.2.4 Desistimiento de la víctima (causal no jurídica). El desistimiento de la víctima es una figura jurídica que permite al sujeto pasivo (la víctima) renunciar a la acción penal que ha iniciado, sin embargo, este solo tiene lugar en las querellas, por tanto para la unidad de delitos informáticos cuando la víctima desea desistir y los elementos recolectados durante la investigación no son suficientes para establecer el sujeto activo, al no ser esta una causal reconocida para los delitos dolosos y debido a que no se encuentra dentro de las causales permitidas para el archivo de procesos del Sistema Penal Oral Acusatorio SPOA, este desistimiento, sin que existan motivos y circunstancias fácticas que permitan determinar la existencia del delito, conlleva a un archivo que se registra como una conducta atípica o imposibilidad de encontrar al sujeto activo.

Considerando los anteriores fundamentos, podemos analizar casos puntuales con los cuales tuve contacto, desarrolle alguna labor o formule la causal de archivo.

Considerando todo lo mencionado, es posible proceder a realizar una tabulación de las denuncias, modalidad con la que se logra el actuar delictivo y a su vez las causales que llevaron a

la terminación o cierre de la investigación. La información relacionada fue recolectada en el periodo de tiempo en el que realicé mi práctica jurídica (2 de mayo - 2 septiembre), así mismo la participación en los diversos procesos me permitió expandir el conocimiento en torno a las consultas y casos que se desarrollaron durante este periodo.

8.2.3. Tabla de archivos realizados durante el periodo de inicio a finalización de mi práctica.

Nota: Como ya se mencionó el desistimiento no es una causal de archivo que se encuentre dentro de la jurisprudencia o normatividad, en este tipo de delitos sin embargo le tendremos en cuenta como circunstancia, ya que a pesar de no ser jurídicamente posible establecerla como causal, en la realidad material a menudo dificulta la continuidad de la investigación, llevando a una consecuencia de archivo por cualquiera de las causales según la consideración del fiscal.

primer causal: Imposibilidad de ubicar el sujeto activo: (13)

Segunda causal: Atipicidad: (10)

tercer causal: Imposibilidad de ubicar al sujeto pasivo: (0)

Archivos donde la víctima desiste y es imposible continuar con la investigación: (7)

Tabla 12.

Archivos realizados en la práctica jurídica en Fiscalía 07 hurto y delitos informáticos.

Proceso N° de Rad.	Causal de Arch.	Delito	Modo
680016000160202263261	Imposibilidad de ubicar al sujeto activo	Hurto por medios informáticos y semejantes ART. 269	PSE - Transacciones fraudulentas
680016000160202262349	Imposibilidad de ubicar al sujeto activo	Hurto por medios informáticos y Semejantes	Vishing

Proceso N° de Rad.	Causal de Arch.	Delito	Modo
		Art. 269i	
6800160002582018 00636	Imposibilidad de ubicar al sujeto activo	Hurto por medios informáticos y semejantes agravado	Phishing
680016000160202263261	Atipicidad	Hurto por medios informáticos y semejantes Art. 269i	Ingeniería Social - Cambiazo
680016000160202263731	Imposibilidad de ubicar al sujeto activo	Hurto por medios informáticos y semejantes Art. 269i	Ingeniería Social - Cambiazo
6800160002582018 00636	Atipicidad	Acceso abusivo a un sistema informático	Scam - Correo electrónico y redes sociales SPAM
680016000160202268401	Atipicidad	Hurto por medios informáticos y semejantes art. 269i	Ingeniería Social - Cambiazo
680016000160202263731	Imposibilidad de ubicar al sujeto activo	Hurto por medios informáticos y semejantes art. 269i	Ingeniería Social - Cambiazo
680016000160202257000	Atipicidad	Acceso abusivo a un sistema informático	Scam - Correo electrónico y redes sociales SPAM
680016000160202000730	Archivos donde la victima – Atipicidad	Hurto por medios informáticos y semejantes	Ingeniería Social - Cambiazo

Proceso N° de Rad.	Causal de Arch.	Delito	Modo
		art. 269i	
680016000160201802681	Archivos donde la victima desiste - Imposibilidad de ubicar al sujeto activo	Hurto por medios informáticos y semejantes art. 269i	Ingeniería Social - Cambiazo
680016000160202254635	Archivos donde la victima desiste – Atipicidad	Hurto por medios informáticos y semejantes art. 269i	Ingeniería Social - Banca móvil
680016000160202315422	Imposibilidad de ubicar al sujeto activo	Hurto por medios informáticos y semejantes art. 269i	Explotación de una vulnerabilidad en el software de los servidores DNS (Pharming)
680016106051202204840	Imposibilidad de ubicar al sujeto activo	Hurto por medios informáticos y semejantes art. 269i	Ingeniería Social - Cambiazo
680016000160202266375	Archivos donde la victima desiste – Atipicidad	Hurto por medios informáticos y semejantes art. 269i	PSE - Transacciones fraudulentas
680016008828201600140	Archivos donde la victima desiste - Atipicidad	Transferencia no consentida de activos valiéndose de alguna manipulación informática o artificio semejante art. 269j ley 1273 de 2009	Sin establecer

Proceso N° de Rad.	Causal de Arch.	Delito	Modo
680016000160202266375	Archivos donde la victima desiste - Atipicidad	Hurto por medios informáticos y semejantes art. 269i	PSE - Transacciones fraudulentas
680016106051202203840	Imposibilidad de ubicar al sujeto activo	Hurto por medios informáticos y semejantes art. 269i	Ingeniería Social - Cambiazo
680016000160202253810	Imposibilidad de ubicar al sujeto activo	Hurto por medios informáticos y semejantes art.	PSE - Transacciones fraudulentas
680016008828201501923	Imposibilidad de ubicar al sujeto activo	Suplantación de sitios web para capturar datos personales art 269g ley 1273 de 2009, agravado por realizarse sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros art. 269h n1	Phishing
680016000160202313331	Archivos donde la victima desiste – Atipicidad	Hurto por medios informáticos y semejantes art. 269i	PSE - Transacciones fraudulentas

Proceso N° de Rad.	Causal de Arch.	Delito	Modo
680016000160201603685	Imposibilidad de ubicar al sujeto activo	Acceso abusivo a un sistema informático art 269ª	Sin establecer
680016000160201700205	Imposibilidad de ubicar al sujeto activo	Acceso abusivo a un sistema informático art 269ª	Sin establecer
680016000160202266375	Archivos donde la victima desiste - Atipicidad	Hurto por medios informáticos y semejantes art. 269i	PSE - Transacciones fraudulentas

En conclusión, la imposibilidad de encontrar el sujeto activo es una de las mayores dificultades para la fiscalía a la hora de llevar a cabo la investigación de estos delitos, ya que incluso cuando la segunda causal más común es la atipicidad, está en muchas ocasiones es dada por la imposibilidad de ubicar el sujeto activo y establecer los elementos esenciales del tipo penal. En estos archivos se presentaron dos patrones, el primero, cuando a pesar de que la fiscalía realizó las averiguaciones pertinentes, no le fue posible establecer la identificación del sujeto activo y el segundo donde la víctima desiste sin haber aportado los elementos necesarios para continuar con la investigación.

La predominancia de esta primera causal también tiene su génesis en que esta clase de conductas delictivas pueden realizarse desde el anonimato por medio de transacciones móviles a través del robo de credenciales, suplantación de sitios web, vulneración de seguridad y acceso a bases de datos, suplantación de identidad y otras más los cuales son clasificados como ciberdelitos por la posibilidad de cometerlos remotamente dificultando la persecución del sujeto activo de la conducta.

La segunda causal de archivo se determina cuando no existen suficientes elementos materiales probatorios o circunstancias fácticas que indiquen la existencia efectiva de los hechos que dieron lugar a la denuncia. Esto puede ser debido a la existencia de la primera causal es decir no se logra identificar al sujeto activo y más allá de esto no hay rastro alguno de la existencia de los hechos denunciados que pueda dar inicio a la indagación, además es posible un patrón particular frente a los hurtos por medios informáticos cuando se trata de transacciones fraudulentas y es que cuando las entidades bancarias no logran comprobar o establecer que el hurto se cometió por falta o imprudencia del propietario de la cuenta bancaria frente a sus credenciales de ingreso a la banca móvil y tampoco que no fue una vulneración a su seguridad bancaria, suelen restituir los dineros al tarjetahabiente, situación que no se presenta con la modalidad de cambiazo ya que en estos la responsabilidad del cuidado de la tarjeta está en manos del propietario, al ser restituido el dinero hurtado a las víctimas o denunciantes, la afectación al patrimonio económico, elemento esencial determinante para la adecuación típica del delito de hurto por medios informáticos, deja de existir por ende la vulneración al bien jurídico tutelado y por lo tanto no se configuran los elementos esenciales del tipo y esto termina en una atipicidad de la conducta. Dejando la posibilidad al banco quién sería ahora la víctima o afectado de poder realizar una nueva denuncia frente a los mismos hechos.

Frente a la atipicidad y la imposibilidad de establecer el sujeto activo hay un patrón que se encuentra en el medio de ambas el cual se presenta en uno de los delitos más comunes y con mayor vocación de éxito, los hurtos que se dan por medio de la modalidad de cambiazos e ingeniería social, donde al existir contacto directo con la víctima para mediante engaños robar su tarjeta de cuenta bancaria y su clave al usuario del cajero, son captados por las cámaras del cajero logrando una mayor posibilidad de identificar a los indiciados, sin embargo frente a esto persiste otra

dificultad y es el tiempo de conservación de estos videos y la demora en el inicio de la investigación por parte de la fiscalía desde la ocurrencia de los hechos, dado que la cantidad de denuncias recepcionadas supera los 50 casos diarios entre denuncias virtuales y presenciales, dilatando los tiempos en los que se da revisión a cada uno de los procesos y por consiguiente a la ejecución de órdenes de policía judicial para obtener los registros fílmicos de cajeros, generando que en ocasiones la solicitud de estos registros llegue tardíamente y se obtenga una respuesta negativa por parte de los bancos o empresas de seguridad los cuales los conservan un tiempo máximo de ocho meses y en ocasiones puede llegar a ser inferior. De los ocho procesos archivados con esta modalidad cinco de ellos fueron archivados por la inexistencia de registros fílmicos debido en su mayoría a que el tiempo de conservación se había cumplido antes de que llegara la solicitud de los videos de las cámaras de los cajeros al banco o empresa de seguridad, uno de ellos debido al mal funcionamiento de las cámaras presentes en el cajero y finalmente dos por el desistimiento de las víctimas, lo cual dificulta la posibilidad de realizar una plena identificación del sujeto activo. Por ende, este patrón descrito puede llevar tanto a un archivo por tipicidad al no poder establecer con certeza la existencia de los hechos o a archivo por imposibilidad de establecer el sujeto activo, los cuales están directamente relacionados.

Si bien la cantidad de archivos por imposibilidad de establecer el sujeto pasivo presentes en la tabla en referencia, fue un total de cero, durante el desarrollo de la práctica tuve conocimiento de procesos archivados por imposibilidad de encontrar al sujeto pasivo, donde el patrón determinante es la no comunicación o desinterés por parte de la víctima, sumado a inasistencia o falta de respuesta a previas citaciones, llamadas, correos electrónicos o entrevistas programadas por parte de los funcionarios de fiscalía. Esto en muchas ocasiones atiende a desinterés por parte

de la víctima en continuar con el proceso, ya sea por la reparación o restitución del bien o dineros hurtados, o por el simple agotamiento de las instancias y tiempos que pueda conllevar el proceso.

Finalmente, el desistimiento, aunque no constituye formalmente un motivo de archivo, es una situación fáctica adecuable y presente en cada una de las causales de cierre de la investigación. En otras palabras, el papel que desempeñan las víctimas dentro de la investigación como fuente de información y en la vinculación de material probatorio, es determinante, ya que en muchas ocasiones se requieren documentos y aportes que sólo se pueden obtener con autorización de la persona afectada.

Por esta razón, el desistimiento de la víctima se convierte en una circunstancia relevante a considerar, puesto que, al retirarse del proceso o dejar de colaborar activamente, se dificulta o incluso imposibilita la obtención de pruebas necesarias para continuar o iniciar la investigación. Esto puede llevar, en la práctica, al archivo del caso, especialmente cuando la Fiscalía no logra reunir los elementos probatorios suficientes por sí misma.

8.2.4 Análisis de casos específicos y actuaciones realizadas

Para este objetivo daré un breve resumen general del caso, sin datos específicos como nombres de personas, empresas o direcciones a fin de mantener la información confidencial, ya que estos datos no deben ser expuestos, asimismo el análisis de vocación de éxito de la investigación y labores de apoyo realizadas:

Los nombres referenciados son netamente para la fluidez del texto estos no corresponden a los datos reales de las víctimas o indiciados, así como los datos alusivos a la edad se tomarán sólo como referencias cuando sea necesario más no serán exactos.

Caso número 1: 68796000153202100303 hurto por medios informáticos y semejante agravado numeral 1 sobre redes informáticos o sistemas informáticos del sector financiero.

Modalidad: en este caso no se logra establecer una modalidad ya que deviene de circunstancias muy específicas.

Tras la muerte del señor MARTÍN PÉREZ a los 57 años de edad, quien decía ser su compañera permanente la señora LUNA GÓMEZ de 27 años se apoderó de las cuentas de banco y tarjetas débito, haciendo compras superiores a los 150.000.000 millones de pesos, el señor MARTIN PEREZ era ciudadano colombiano con residencia estadounidense con familia de un hijo y su esposa residentes en estados unidos, sin embargo MARTIN PEREZ residía en un pueblo de Santander hacía más de 3 años en el país, en época de pandemia tuvo un problema de salud que le ocasionaron su muerte, tras estar en la clínica la señora LUNA fue a visitarlo en varias ocasiones y manifestó ser su pareja, sin embargo el señor MARTÍN PÉREZ lo negó a su médico y a una enfermera, tras su muerte la esposa e hijos se enteraron del estado de la cuenta del señor MARTÍN y de que LUNA se encontraba viviendo en la casa y usando el carro que era de MARTÍN, una vez enterados radican la denuncia.

para el desarrollo de investigación de esta denuncia fueron necesarios las siguientes OPJ(órdenes de policía judicial y oficios: se realizó un oficio al banco en el cual tenía la cuenta de ahorros el señor MARTIN, solicitando la verificación de la existencia de la cuenta, extractos bancarios, log transaccional, esto permitió evidenciar la existencia de la cuenta y los retiros que se hicieron tras su muerte, una vez se tienen los datos exactos a partir del log transaccional del cajero en el cual se realizaron los retiros, hora y fecha exactas se procede con la solicitud de registros fílmicos al banco y ATH de las fechas y horas en las que se realizaron los retiros tras la muerte del señor MARTÍN, una vez verificadas las imágenes se identifica que evidentemente la señora LUNA realizó retiros con las tarjetas del señor MARTIN tras su muerte sin autorización, sin embargo la indiciada manifestaba ser la compañera permanente del señor MARTIN, así que inició un proceso

de reconocimiento de unión marital de hecho, debido a esto se debió dar espera a la decisión de este proceso civil, la cual fue desfavorable para la señora LUNA ya que no se logró establecer la existencia de la UMH, esta decisión refuerza la acusación ya que la señora LUNA no tenía ningún derecho a disponer de los bienes del señor MARTIN siendo así, también se tomaron las entrevistas por medio de informe fpj realizado por investigador del CTI al médico que le vio durante su estancia en la clínica ya que el dejo anotación en la revisión que realizó al paciente de la manifestación del señor MARTÍN frente al parentesco con LUNA, el cual manifestó que ella no era su esposa y que su cónyuge se encontraba en estados unidos, con estos elementos y los de la identificación y plena identidad de la señora LUNA, se realizó el escrito de acusación al proceso en referencia.

Actividad: apoyo con la elaboración del escrito de acusación.

Análisis: En este tipo de hurtos por medios informáticos, donde se suplanta la identidad del tarjetahabiente en cajeros electrónicos uno de los elementos más importantes a fin de establecer la identificación del sujeto activo es el registro fílmico de los cajeros, en este caso la orden de policía judicial se realizó pocos meses después de la denuncia y el banco aún conservaba los registros videográficos pudiendo establecer junto con el LOG Transaccional, que en la hora y fecha indicada de los retiros no autorizados la señora LINA aparece manipulando el cajero electrónico para apoderarse de los dineros de la cuenta de ahorros del señor MARTÍN.

Caso número 2: 680016000160201901418 hurto por medios informáticos y semejante agravado numeral 1 sobre redes informáticos o sistemas informáticos del sector financiero.

Modalidad: Ingeniería Social – Cambiazo: La víctima se da cuenta de que su tarjeta no estaba siendo leída por el cajero por lo que se acerca a las instalaciones de la entidad bancaria donde le informan que la que trae consigo no es su tarjeta, al revisar el saldo de su cuenta bancaria

se da cuenta que han realizado retiros por el valor de 1.874.000 de pesos, trae consigo las fotografías entregadas por el banco seleccionadas y sustraídas de las cámaras del cajero en el cual se realizaron los retiros, donde se logra ver con claridad la cara de la persona que realiza los retiros, en resultado investigativo con sevicol (Seguridad y vigilancia colombiana) se logra determinar la identidad del indiciado, ya que a esta ser una modalidad tan común y de crimen organizado, sevicol tiene una base de datos de personas identificadas y sin identificar (bajo apodo) que se dedican a cometer hurto por medio de esta modalidad.

Actividad: apoyo en redacción de oficio para solicitar información sobre la ubicación de residencia del indiciado a entidad pública.

Análisis: En la modalidad de cambiazos las cámaras de los cajeros son fundamentales, así como las listas que manejan las empresas de seguridad de los cajeros. donde ubican a las personas que cometen de manera organizada este delito, buscando tener una base de datos para facilitar la identificación de los indiciados en este tipo de denuncias. con la revisión de estos registros filmográficos en muchas ocasiones se puede esclarecer la identidad de él o los indiciados, identificando además el rol que cumplen en la banda u organización. A pesar de que la calidad del video en ocasiones no es muy buena, al ser un crimen organizado con perdurabilidad en el tiempo, en ocasiones se logra identificar a los sujetos activos por sus características físicas o por los demás participantes los cuales de manera reiterativa han realizado cambiazos.

Caso número 3: 680016000160202266375 hurto por medios informáticos y semejante agravado numeral 1 sobre redes informáticos o sistemas informáticos del sector financiero.

Modalidad: Ingeniería Social - Cambiazo

La víctima le realiza cambiazo al aceptar ayuda de una persona que le dice que ha dejado su sesión abierta y que ahora debe volver a ingresar la tarjeta, cuando se da cuenta han realizados

una serie de retiros de su cuenta de banco y presenta la reclamación, al llamarlo para obtener mayor información y elementos de prueba, la víctima manifestó haber llegado a un acuerdo con la entidad bancaria y que quería que se realizará archivo del proceso.

Actividad: Apoyo en realización de constancia de archivo y redacción de causal de archivo del proceso.

Análisis: En este caso si la autorización o consentimiento firmado de la víctima de la víctima, la fiscalía no puede solicitar o tener acceso a información necesaria para la investigación, como la certificación de la cuenta bancaria, extractos de la cuenta de ahorros, log transaccional con lo cual poder solicitar los registros fílmicos e identificar al indiciado por lo cual la investigación debe concluir con un archivo por atipicidad de la conducta o imposibilidad de establecer al sujeto activo dependiendo del concepto del fiscal.

Caso número 4: 680016008828201900481 hurto por medios informáticos y semejante agravado numeral 1 sobre redes informáticos o sistemas informáticos del sector financiero.

Modalidad Ingeniería Social - Cambiazo

el banco aporta un cd con una carpeta vacía donde no se encuentran los registros fílmicos por tanto se sugiere realización de opj solicitando nuevamente los registros fílmicos y aclarando que el cd antes enviado se encontraba vacío.

Actividad: Revisión de expediente y se deja por escrito en expediente físico la nota de sugerencia de realización de OPJ solicitando nuevamente los registros fílmicos y aclarando que el cd antes enviado se encontraba vacío.

Análisis: Esta es una de las posibles consecuencias de que se realice la orden policía judicial después de que haya pasado el tiempo de conservación de los registros fílmicos de los cajeros o de que las cámaras de los cajeros hayan sido intervenidas o inhabilitadas, en estos casos

donde no existe una trazabilidad del movimiento del dinero y no tenemos registros fílmicos el resultado de la actividad investigativa tiene baja probabilidad de éxito.

Caso número 5: 680016000160202313331 hurto por medios informáticos y semejantes art 269 i ley 1273 del 2009.

Modalidad: PSE - Transacciones fraudulentas: la víctima manifiesta que en las horas de la madrugada se realizaron unas transferencias pagos por pse por el valor de 63.000.000 millones, fue a la entidad bancaria y puso el derecho de petición para que se investigara, al establecer comunicación a fin de solicitar un relato más amplio de los hechos y que aportará los elementos materiales probatorios que tuviera en su poder, la víctima manifestó que deseaba desistir de la investigación ya que había llegado a un acuerdo con el banco para la reintegración de una parte del dinero y no quería perder más el tiempo ya que no tenía más información sobre quién pudo haber realizado el hecho.

Actividad: Apoyo en realización de constancia de archivo y redacción de causal de archivo del proceso.

Análisis: sin la disposición de la víctima de continuar con el proceso y aportar elementos materiales probatorios en esta modalidad la probabilidad de éxito de la investigación es baja por lo que se procede a la realización de archivo por imposibilidad de encontrar el sujeto activo.

Caso número 6 :680016008828201802907 violación de datos personales.

Modalidad: no establecida, circunstancias particulares.

Un trabajador de una empresa reconocida de la ciudad de Bucaramanga de compra y venta de vehículos Motocicletas, denuncia a un trabajador técnico mecánico por estar contactando a clientes por medio de WhatsApp ofreciendo sus servicios en taller personal, valiéndose del acceso a la información de contacto de los clientes a la que tenía acceso por su empleo en la empresa. Sin

embargo, al citar a la víctima a fin de que aporte nuevos elementos probatorios para continuar con la investigación, dado su no asistencia e imposibilidad de contactar con el sujeto pasivo se procede a realizar el archivo del proceso.

Actividad: Apoyo en realización de constancia de archivo y redacción de causal de archivo del proceso.

Análisis: en muchos de las denuncias realizadas la víctima deja de asistir a las citaciones realizadas por fiscalía o se vuelve no localizable en estos casos se procede al archivo del proceso a fin de que la víctima se acerque a brindar la información necesaria para continuar con la investigación, si los elementos previamente existentes no son suficientes para establecer la existencia de los hechos denunciados.

Caso número 7: 680016008828201501923 suplantación de sitios web para capturar datos personales art 269g ley 1273 de 2009 agravado por realizarse sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero nacionales.

Modo: falsedad de identidad virtual.

El representante legal del acueducto denuncia la creación de un perfil de Facebook del acueducto metropolitano de Bucaramanga el cual recibe incluso peticiones y quejas, sin ser este un perfil oficial. Al investigador realizar la búsqueda de la dirección ip desde la cual se ingresaba a esta página, en informe IPJ se comunica la imposibilidad de ubicar la ip, se cita a la víctima en repetidas ocasiones para recolectar mayores elementos, sin embargo, no asiste así que se procede a realizar archivo por imposibilidad de establecer el sujeto activo.

Actividad: Apoyo en realización de constancia de archivo y redacción de causal de archivo del proceso.

Análisis: frente al delito de suplantación de sitio web una de las formas de ubicar al sujeto activo es lograr su localización a partir de la IP y a partir de esto se busca ubicar con la información del servidor de internet, sin embargo, cuando el resultado de esta búsqueda es negativo, existe poca vocación de éxito en la investigación.

Caso número 8: 680016008828202105964 acceso abusivo a un sistema informático art 269a ley 1273 de 2009.

Modalidad: malware.

A la víctima le robaron sus credenciales de ingreso a la cuenta de Instagram y la suplantaron, pidiendo dinero a sus familiares y conocidos, los cuales 4 de ellos realizaron transferencias a cuentas de banco.

Actividad: Apoyo en llamadas a testigos para solicitar extractos y certificación bancaria a fin de obtener un rastro de las transacciones.

Análisis: En casos como este es necesaria no sólo la participación activa de la denunciante sino también de las personas que se vieron afectadas con el hurto de los dineros por medio de la suplantación de la denunciante, esto quiere decir que sin el aporte de los afectados económicamente de la certificación de la cuenta de banco, extractos y log transaccional no sería posible identificar al sujeto activo, por tanto se cita a rendir entrevista a las personas afectadas a fin de solicitar su consentimiento y documentos necesarios para el desarrollo de la investigación.

Caso número 9: 680016008828201905146 hurto por medios informáticos y semejantes art 269 i ley 1273 del 2009.

Modalidad: Malware. Mediante operación electrónica se sustrae de la cuenta empresarial de consorcio va*** la suma de 17.725.110 millones de pesos para realizar un pago a una empresa de servicios públicos, la respuesta de la entidad bancaria a la cual le vulneran su seguridad es que

el computador desde el que se hizo el pago debió estar comprometido con un virus informático denominado malware (troyanos bancarios de manipulación remota) y por ende no responde por la suma, en informe se le solicita a la empresa de servicios públicos que aporte datos biográficos de la persona a la cual pertenece la cuenta de la factura la cual se pagó la suma de 17.725.110 millones de pesos, la empresa prestadora de servicios responde que no recibió ningún pago de ese número de factura o cuenta y el banco no da los datos de la persona a la cual le pertenecía la factura cancelada, debido a que las empresas prestadoras de servicios no suministran esta información a las entidades bancarias. Se procede a realizar oficio reiterando a la empresa prestadora de servicios que suministre los datos biográficos de la persona a la que pertenecía la factura saldada, con anexo del oficio del banco donde administra la información de la empresa prestadora de servicios como receptora del pago.

Actuaciones: Se realiza revisión del expediente físico a fin de ubicar los elementos probatorios existentes y apoyo en la realización de oficio en respuesta a la comunicación aportada por la empresa prestadora de servicio, debido a que la entidad bancaria refiere que la empresa prestadora de servicios si recibió el pago a la cuenta que tienen habilitada para la recepción de dineros provenientes de facturación, con copia de la comunicación del banco.

Análisis: en este caso al parecer los computadores de la empresa tenían instalado un malware lo cual permitió que la transacción se realizara incluso desde el mismo equipo de sus oficinas y con la ip del lugar, dejando como única posibilidad de ubicar al sujeto activo, el obtener los datos biográficos de la persona a la que pertenecía la cuenta pagada a la empresa prestadora de servicios.

Caso número 10: 680016008828201501711 Acceso abusivo a un sistema informático, agravado por aprovecharse de la confianza depositada del poseedor de la información o por quien tuviere un vínculo contractual con este.

Modalidad: Insider: la víctima, una empresa de telecomunicaciones presenta denuncia frente a uno de sus empleados, un consultor de servicio personalizado a clientes, el cual desbloquea IMEIS de celulares reportados como robados con su usuario de red asignado por la empresa, en informe de la empresa se verificó el número con el que los IMEIS fueron desbloqueados y este pertenecía al indiciado. Sin embargo, al ser un caso denunciado en el 2015, se intentó comunicación y se realizó citación por parte de la fiscalía a los demandantes para saber si deseaban continuar con el proceso.

Actuación: al ser un caso que tiene más de nueve años de la presentación de su denuncia se brindó apoyo en la realización de oficio de citación a la empresa víctima para saber si desean continuar con el proceso y aportar los soportes actualizados de la información brindada en la denuncia.

Análisis: Este es un caso que tiene elementos materiales probatorios muy concretos que permiten la verificación de los hechos y establecer al sujeto activo, sin embargo, debido a la congestión procesal existente en el sistema penal colombiano, hasta casi 9 años después, no se le ha dado celeridad a la investigación.

8.3 Tercer informe: Dificultades prácticas que impiden la correcta investigación de los hechos.

Uno de los obstáculos más frecuentes que la Fiscalía 07 unidad de hurtos y delitos informáticos enfrenta, es la identificación del sujeto activo debido a la naturaleza anónima y transaccional y la complejidad técnica de estos delitos, estas características inherentes a los delitos

cibernéticos crean un entorno donde la identificación del sujeto activo se vuelve un reto, intensificando los desafíos que enfrenta la Fiscalía en su labor.

Siendo esta imposibilidad una de las consecuencias más graves de un conjunto de dificultades interrelacionadas. La complejidad para establecer quién es el responsable de estos delitos es, en gran medida, resultado de varios factores que entorpecen el proceso investigativo desde sus primeras etapas. En muchos casos la naturaleza anónima que tienen este tipo de delitos, junto con el uso de herramientas avanzadas para ocultar la identidad de los autores, la falta de desarrollo en tecnologías y estrategias innovadoras de investigación, dificulta en gran medida el trabajo de los investigadores. Las modalidades de ataques en los delitos informáticos son cada vez más sofisticadas y la tecnología para contrarrestarlos no siempre está a la par, lo que coloca a la Fiscalía en una posición desventajosa. Sin herramientas avanzadas y métodos innovadores, el alcance de las investigaciones del Cuerpo Técnico de Investigación (CTI) y la Seccional de Investigación Judicial y Criminal (SIJIN) es limitado, lo que se traduce directamente en una mayor dificultad para identificar al sujeto activo.

Otro factor determinante corresponde a la congestión procesal que caracteriza al sistema penal colombiano, la cual retrasa la revisión y seguimiento de los delitos informáticos. Esta sobrecarga de casos impide que los funcionarios de fiscalía y el cuerpo técnico de investigadores de los que dispone, actúen con la prontitud que se requiere en cada una de las denuncias que son recepcionadas, retrasando la revisión y el inicio de las investigaciones, lo que permite que en ocasiones la evidencia se degrade o que se pierda la oportunidad de capturar datos esenciales para identificar al responsable algo crucial para preservar la evidencia y dar inicio efectivo a la investigación. La demora en la emisión de Órdenes de Policía Judicial (OPJ) y en la realización de otras diligencias esenciales significa que, para cuando se inicia formalmente la investigación, el

rastro del sujeto activo puede haberse perdido, haciendo casi imposible su identificación. Esto debido a que el deber de realización de OPJ corresponde al fiscal y secundariamente al asistente fiscal los cuales cuentan con innumerables procesos del año actual y de años anteriores que deben estar en constante revisión para objetivamente establecer si ya existen los elementos probatorios suficientes para identificar al sujeto activo o si es necesario continuar con una orden a policía judicial para continuar con la investigación, sumado a esto está la revisión de los informes entregados por los investigadores, todo esta multitud de denuncias para la gestión de dos funcionarios, lo cual hace que algunas denuncias no sean revisadas con la prontitud necesaria.

El desistimiento o falta de interés por parte de la víctima es un factor determinante debido a que sin su cooperación el proceso de investigación carece del impulso que puede llegar a brindar el sujeto pasivo ya que son fuentes directas de información y de elementos probatorios iniciales que permiten establecer un rastro para el inicio y continuidad de las indagaciones. La falta de contacto continuo y la ausencia de datos relevantes dejan a los investigadores con poco material con el cual trabajar, lo que muchas veces conduce al estancamiento del caso, esto sumado a que para la mayoría de solicitudes de información realizadas por los investigadores a entidades bancarias, estatales o empresariales es necesario el consentimiento de la víctima el cual cuando la víctima o denunciante desiste de la investigación ya no será válido y por tanto la Fiscalía se enfrenta a un vacío en la investigación que complica aún más la identificación del sujeto activo.

Así mismo un factor no aplicable a todos los delitos, pero si a uno de los más frecuentes en la unidad que es el hurto por modalidad de cambiazo e ingeniería social, es el de la falta de diligencia por parte de las entidades bancarias, especialmente en lo que respecta a la instalación y mantenimiento de cámaras de seguridad en cajeros electrónicos. En los casos que implican retiros no autorizados, la ausencia de imágenes claras o la inexistencia de grabaciones adecuadas dificulta

enormemente la identificación del delincuente. Sin esta evidencia crucial, la posibilidad de encontrar al sujeto activo se reduce drásticamente, afectando la capacidad de la Fiscalía para llevar adelante una investigación efectiva.

En resumen, la imposibilidad de identificar al sujeto activo en los delitos informáticos no es un problema aislado, sino la consecuencia directa de una serie de dificultades sistémicas y operativas que afectan el proceso investigativo desde sus cimientos. Superar estas barreras es esencial para mejorar la capacidad de la Fiscalía de responder a estos delitos de manera efectiva y garantizar que los responsables sean identificados y llevados ante la justicia.

8.4 Cuarto informe: Propuestas y recomendaciones.

Para mejorar la actividad investigativa de los delitos informáticos por parte de la Fiscalía, es fundamental implementar una serie de acciones que optimicen el proceso, desde la estructuración de los casos hasta el fortalecimiento del personal y los recursos tecnológicos disponibles.

Una estrategia clave sería desarrollar modelos predefinidos de Órdenes de Policía Judicial (OPJ) y oficios basados en las modalidades delictivas más comunes. Al tratarse de delitos recurrentes en condiciones similares, como el "cambiazo", se puede estandarizar la creación de estos documentos, asegurando que se recojan los elementos de prueba adecuados y se solicite la información pertinente desde el inicio de la investigación. Este enfoque permitiría ganar eficiencia y reducir los tiempos de reacción ante estos delitos, ya que el trabajo de estructuración se realizaría una sola vez y se ajustaría a las particularidades del caso en curso. Además, se facilitaría la recopilación de evidencia crítica desde las primeras etapas de la investigación, lo que es vital en los delitos cibernéticos, donde el rastro de los delincuentes tiende a desvanecerse rápidamente.

La contratación de personal capacitado para la revisión e impulso de procesos sería otra medida esencial. La congestión procesal afecta significativamente la prontitud con la que se pueden atender los casos, y la acumulación de denuncias tanto del presente año como de años anteriores retrasa las investigaciones. Ampliar el personal de la unidad, tanto en el área jurídica como en la técnica, permitiría reducir la carga sobre fiscales y asistentes, quienes podrían enfocarse en los casos activos de manera más eficaz. Este refuerzo permitiría también una atención más oportuna a los informes presentados por los investigadores, lo que evitaría la pérdida de evidencia o la expiración de oportunidades críticas.

Otro aspecto a considerar son las capacitaciones continuas a los investigadores ya que son de vital importancia en un campo tan dinámico como los delitos cibernéticos. La tecnología evoluciona rápidamente, tanto en las herramientas que los delincuentes usan para perpetrar estos delitos, como en las soluciones para combatirlos. Proporcionar a los investigadores formación regular sobre las nuevas tecnologías y herramientas forenses digitales avanzadas, ayudaría en la mejora de las capacidades para investigativas. Capacitaciones de los desarrollos tecnológicos con un enfoque en las herramientas de combate de los delitos informáticos a nivel global.

Dada la naturaleza transfronteriza de los delitos informáticos, es imprescindible establecer acuerdos de cooperación internacional, ya que las investigaciones de estos delitos con frecuencia implican múltiples jurisdicciones, por lo que es esencial trabajar con agentes internacionales, tanto en un nivel técnico como legal, para ubicar a los delincuentes. Este tipo de cooperación permitiría acceder a datos alojados en otros países, facilitaría el intercambio de información crítica y reforzaría los esfuerzos para capturar a los responsables, algo esencial en un entorno digital sin fronteras.

En resumen, mejorar la actividad investigativa de la Fiscalía 07 de hurtos y delitos informáticos requiere la implementación de modelos procesales más ágiles y estructurados para lograr la celeridad necesaria en la fase investigativa, el incremento de su personal a fin de lograr abarcar una mayor cantidad de revisiones e impulso a los procesos y recursos tecnológicos que permitan la adopción de tecnologías innovadoras, así como la consolidación de acuerdos internacionales que faciliten el combate a estos delitos sin fronteras.

Referencias

Bechara, Y. Mosquera, A. y Ledezma, E. (2020). *Análisis jurídico de la ley 1273 del 2009 y el surgimiento y expansión del delito de hurto y semejantes por medios informáticos*. [Tesis de pregrado, Universidad Cooperativa De Colombia]. Repositorio institucional - Universidad Cooperativa de Colombia.

Camargo Cardona, L. (2019). *Regulación en Colombia de los delitos informáticos*. Universidad piloto de Colombia.

Congreso de Colombia. (2004). *Ley 906 de 2004.* Secretaría del Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004_pr001.html

Corte Constitucional, (2018). *Sentencia C-224/19, Revisión oficiosa de la Ley 1928 de 2018 "Por medio de la cual se aprueba el convenio sobre la ciberdelincuencia,* adoptado el 23 de noviembre de 2001, en Budapest".

Corte Constitucional. (2005). *Sentencia C-1154/05 sobre demanda de inconstitucionalidad contra los artículos 15 (parcial), 16 (parcial), 79, 177 (parcial), 274, 284, 285, 288 (parcial), 290 (parcial), 291, 306 (parcial), 308 (parcial), 327 (parcial), 337, 383 (parcial), 435, 436 y 455 de la Ley 906 de 2004 "por la cual se expide el Código de Procedimiento Penal*."

Corte Suprema de Justicia. (2007). *Auto 2007-0019 de 5 de julio de 2007: Archivo de las diligencias por la fiscalía - Casos en que procede y diferencias con la preclusión de la investigación.*

Deutschland.de. (2023). *Ciberpolicía en Alemania: jornada de reclutamiento en la Oficina Federal de Investigación.* https://www.deutschland.de/es/topic/economia/ciberpolicia-en-alemania-jornada-de-reclutamiento-oficina-federal-de-investigacion

ESET. (2014, julio 11). *Man-in-the-browser: ¿Cómo pueden interceptar tu navegador?* WeLiveSecurity. https://www.welivesecurity.com/la-es/2014/07/11/man-in-the-browser-como-pueden-interceptar-navegador/

Fiscalía General de la Nación. (s.f.). *Cartilla metodológica de atención de delitos informáticos*. https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf

Función Pública. (2009). Ley 1273 de 2009. *La cual modifica el Código Penal, creando el bien jurídico 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.* Diario Oficial. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35103

Función Pública. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Gamba, J. (2019*). El delito informático en el marco jurídico colombiano y el derecho comparado: caso de la transferencia no consentida de activos*. [Tesis de maestría, Universidad Externado de Colombia]. Repositorio institucional - Universidad Externado de Colombia.

Gandini, I. (2016). *Ley de los delitos informáticos en Colombia.* http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

Germany. (2023). *Strafgesetzbuch (StGB).* https://www.gesetze-im-internet.de/stgb/.

Gonzales Guzmán, D.A. (2017). *La protección de información y los datos en el marco de la ley 1273 de 2009: Un estudio del dato y la información como objeto material en el tipo penal hurto por medios informáticos.*

Guerra, B. J. (sf). *Consideraciones para la regulación penal del delito informático*. Sexta Ponencia: Delitos Informáticos - Abogacia e Informática (p. 3). Colegio de Abogados

IBM. (n.d.). *Ingeniería social*. IBM. https://www.ibm.com/es-es/topics/social-engineering

Johnson, L. (2023, March 15). *What is malware? Understanding the different types. Cybersecurity Insights.* https://www.cybersecurityinsights.com/what-is-malware

LEGIS Xperta. (s/f). *Auto 2007-0019 de julio 5 de 2007* https://xperta.legis.co/visor/jurcol/jurcol_75992042374df034e0430a010151f034

Manjarrés, I & Jiménez, F. (2012). *Caracterización de los delitos informáticos en Colombia*. Pensamiento Americano, pp 71-82.

Muñoz, L. (2023). *Fiscalía reportó avance contra delitos informáticos.* https://www.infobae.com/colombia/2023/12/16/fiscalia-reporto-avance-contra-delitos-informaticos-con-69-capturas-y-45-imputaciones-en-2023/

Planalto. (2012). *Lei Nº 12.737, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, para tipificar criminalmente a invasão de dispositivo informático alheio para obtenção de vantagem ilícita*. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Planalto. (2014). *Lei Nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil*. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Posada Maya, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. *Revista Nuevo Foro Penal* Vo. 13. No. 88. pp 72-112.

Riascos, O. (2010). El delito informático contra la intimidad y los datos de la persona en el derecho colombiano. *Revista Electrónica De Derecho Público Mínimo* 1(20), 1-20. https://www.researchgate.net/publication/297324290_El_delito_Informatico_contra_la_Intimidad_y_los_datos_personales

Sánchez Castillo, Z. N. (2017). *Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia.* Universidad Nacional Abierta y a distancia. [Tesis de especialización, Universidad Nacional Abierta y a Distancia -UNAD]. Repositorio Institucional – Universidad UNAD.

Secretaría del Senado. (2009). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*. 5 de enero de 2009. Diario Oficial, núm. 47223.

Suarez Sánchez, A. (2017). *Manual del delito informático en Colombia. Análisis Dogmático de todos los Tipos Penales de los Delitos Informáticos descritos en la Ley 1273 de 2009* Universidad Externado de Colombia.

Unión Europea. (2016). *Reglamento (UE)*. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679