CARTILLA METODOLÓGICA DE ATENCIÓN DE DELITOS INFORMÁTICOS

REPÚBLICA DE COLOMBIA
POLICÍA NACIONAL
DIOS Y PATRIA

FISCALÍA
GENERAL DE LA NACIÓN


CENTRO CIBER
POLICIA
DELL
POLICÍA

Contenido

1. PROBLEMÁTICA

Aumento en las denuncias ciudadanas por la afectación a la información y a los datos, como consecuencia del necesario aumento en el uso de las tecnologías de la información y las comunicaciones en la vida cotidiana.

2. OBJETIVO

Unificar conceptos sobre los delitos informáticos contenidos en la Ley 1273 de 2009, sus modalidades y caracterización, con el fin de servir de orientación a los servidores de la Fiscalía General de la Nación y a los funcionarios de policía judicial de la Policía Nacional de Colombia, para la correcta recepción de denuncias en materia de delitos informáticos y diseñar la ruta de atención sobre el tratamiento del cibercrimen.

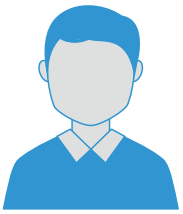
3. ALCANCE

Está dirigida a los servidores de la Fiscalía General de la Nación y funcionarios de policía judicial de las unidades de la Policía Nacional de Colombia, encargados del ingreso, registro y análisis de las noticias criminales e información administrativa sobre delitos informáticos, caracterizaciones y sus modalidades.

4. ACTORES Y ROLES

USUARIO

Persona natural o jurídica que requiere un servicio de la justicia, el usuario no necesariamente es una víctima.



VÍCTIMA

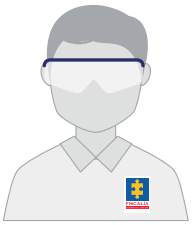
Se trata de la persona a la cual se le afecta el bien jurídico tutelado "de la protección de la información y de los datos".

FISCAL

Director de la investigación, le corresponde la dirección, coordinación, control jurídico y verificación técnico-científica de las actividades que desarrolle la policía judicial. (Ley 906 de 2004 Art. 200).

POLICÍA JUDICIAL

Funcionarios que apoyan la investigación penal, bien sea de forma permanente (art. 201 CPP), supletoria (páragrafo art. 201 CPP) permanente especial (art. 202 CPP) o transitoria (art. 203 CPP), en todo el territorio nacional.



PERITOS

Son expertos en informática forense encargados de descubrir, recolectar, recuperar, analizar y custodiar la evidencia de tipo digital obtenida.

PROGRAMA METODOLÓGICO

Herramienta que surge de la reunión entre Fiscalía General de la Nación y los miembros de Policía judicial, donde se determinan los objetivos en relación con la naturaleza de la hipótesis delictiva y el plan de trabajo investigativo a desarrollar.

5. DEFINICIONES Y SIGLAS

Ataques a DNS: Los ciberdelicuentes buscan vulnerabilidades en el protocolo IP para alterarlo y dirigir al usuario a otro sitio web con fines malintencionados. Los usuarios son víctimas cuando un ciberdelincuente redirige todo el tráfico entrante a un servidor de su elección. Esto les permite lanzar ataques adicionales, o recoger los registros de tráfico que contienen información sensible.

Ataque de Denegación de Servicios DoS (Denial of Services) y Ataque Distribuido de Denegación de Servicios DDoS (Distributed Denial of Services): Método utilizado en donde el atacante busca bloquear un servidor o servicio mediante la sobrecarga de éste o simplemente aprovechando un fallo que cause el bloqueo, y posteriormente el cierre del proceso o servicio del software afectado. Los atacantes sobrecargan el ancho de banda de una red o un servidor, congestionando los recursos del sistema y con ello, pueden explotar posibles vulnerabilidades en el software y en los sistemas de seguridad, todo ello, desde un mismo dispositivo. El ataque DDoS funciona de la misma manera, pero articulado desde varias fuentes de ataque o diversos dispositivos.

Atacante Interno - Insider: Es el ataque realizado por una o varias personas que pertenecen a la organización afectada. Se presenta en fraudes, robos, sabotajes o accidentes relacionados con los sistemas informáticos.

Banker: Programa de malware que se dirige a sitios web de instituciones financieras con el fin de captar información.

BEC (Bussines Email Compromise - compromiso de cuentas de correo empresariales): Esta modalidad consiste en que un estafador usa el correo electrónico para engañar a alguien para que envíe dinero o divulgue información confidencial. El atacante se hace pasar por una figura confiable, luego pide que se pague una factura falsa o datos confidenciales que pueden usar en otra estafa.

Botnet: Conjunto o red de robots informáticos o bots que pueden controlar todos los ordenadores/servidores infectados de forma remota. El objetivo que se persigue es generalmente un ataque informático masivo para la destrucción de sistemas, para dificultar las operaciones o para el robo de información.

Buffer Overflow: Ataque mediante un software que busca desbordar la capacidad de memoria asignada por el sistema operativo haciendo que el sistema falle y le permita al atacante tomar el control.

Cambiazo: Tipo de fraude que sucede cuando la víctima se encuentra realizando una transacción con su tarjeta y permite la ayuda de terceras personas, que logran mediante engaños cambiar la tarjeta por otra con características similares y ver la clave personal, para posteriormente realizar transacciones fraudulentas.

Código Fuente: Conjunto de líneas de texto, escritas en un lenguaje de programación, con los pasos que debe seguir la computadora para ejecutar un programa.

Carding: Término que describe el tráfico y el uso no autorizado de los datos de tarjetas de crédito.

Criptografía: Es un método de protección de la información y de los datos, mediante la utilización de códigos que garantizan que, solo el remitente y destinatario puedan leer y procesar el mensaje.

Criptomonedas: Activo digital que utiliza criptografía fuerte para asegurar las transacciones, controlar la creación de unidades adicionales y verificar la transferencia de activos usando tecnologías de registro distribuido (DLT). Las criptomonedas son un tipo de divisa alternativa o moneda digital comúnmente utilizado como medio de intercambio virtual.

CSRF "Cross-site request forgery": Es un programa informático malicioso utilizado comúnmente para robar información personal; este ataque fuerza al navegador web de su víctima, el cual está conscientemente validado en algún servicio (correo electrónico, aplicación o sitio web de alguna entidad financiera, entre otros) a enviar una petición a una aplicación web vulnerable

Datáfono falso - Datáfono payaso: Modalidad delictiva en la cual el atacante desliza, acerca o inserta la tarjeta de la víctima por un datáfono que tiene la misma apariencia de uno original pero que está programado para capturar la información de la tarjeta; posteriormente, cuando la tarjeta aparentemente no pudo ser leída para realizar la transacción requerida, presentan otro datafono, que es el que realmente sirve, y con éste nuevo datáfono se realiza efectivamente la transacción. En ese momento, y con el datáfono inicial, el atacante ya tiene la información de la tarjeta de crédito.

Defacement - Desfiguración: Tipo de ataque que se realiza contra un sitio web, en el que se modifica la apariencia de alguna de sus páginas, para llevar a cabo algún tipo de acción fraudulenta o de vandalismo. Los motivos detrás de estos ataques varían, suelen ser por razones políticas, ideológicas o con propósito puramente malicioso.

DLT (Distributed Ledger Technology) Tecnología de Registro Distribuido: Sistema de seguridad digital utilizado principalmente en el tráfico de activos digitales, permitiendo a los usuarios y sistemas realizar el registro de las transacciones de manera descentralizada en diferentes lugares al mismo tiempo.

DNS: Sistema de Nombres de Dominio, es un protocolo que traduce o convierte los caracteres numéricos que conforman las direcciones IP a nombres legibles para la lectura humana.

Explotación de vulnerabilidades: Aprovecharse de un fallo en el sistema informático o en un equipo terminal para que el ciberdelincuente logre tener acceso parcial o total.

Fake App - Simulación de aplicación móvil: Se trata de aplicaciones que son falsas, y realmente están pensadas como malware para apropiarse de datos personales o tomar poder de dispositivos móviles.

Gusano informático: Software tipo malware diseñado para que, de manera oculta y autosuficiente, pueda mantenerse dentro de un dispositivo, auto ejecutarse y propagarse a otros por me-

dio de la red. Dentro de las finalidades de este tipo de malware se encuentran las de identificar vulnerabilidades en los sistemas, ralentizarlos, obstaculizar su funcionamiento y en otros casos, son usados como mecanismo de propagación para otros tipos de malware.

Identidad Virtual: Es la identidad online o reivindicada en el ciberespacio por un individuo, organización o dispositivo electrónico.

Ingeniería Social: Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

Keylogger (Capturadores de teclado): Software o dispositivo hardware diseñado para registrar y/o memorizar las pulsaciones que se realizan en el teclado poniendo en riesgo la seguridad de los datos al develar nombres de usuario y contraseñas.

Malware - Software Malicioso: Cualquier tipo de software diseñado o utilizado para infiltrarse en un dispositivo y generar un daño o capturar de manera fraudulenta la información contenida en él.

Man in the Browser -Hombre en el navegador: Ataque para interceptar datos transmitidos por el navegador. Método en el cual, una persona, aprovechándose de las vulnerabilidades del navegador del sistema o del equipo de la víctima, intercepta las comunicaciones. El método para ver toda la información que viaja por la red se despliega a través de programas que se llaman sniffers, herramientas que permiten poner la placa o tarjeta de red en modo monitor, logrando así analizar la información de la red.

Man in the middle - Hombre en el medio: Ataque mediante el cual se interceptan las comunicaciones no públicas de la víctima, asumiendo el atacante, un rol de intermediario entre ésta y su interlocutor, sin ser notado, pudiendo suplantar la identidad de uno u otro según lo requiera para ver la información y modificarla a su antojo, de tal forma que las respuestas recibidas en los extremos pueden estar dadas por el atacante y no por el interlocutor legítimo.

Manipulación de código fuente: Alteración que se realiza sobre el lenguaje en el que está escrito determinado programa para afectar su funcionamiento o el del sistema de información que lo contiene.

Phishing - Suplantación de sitios web: Es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas. Mediante correos electrónicos que contienen enlaces, se enruta la conexión de una víctima a través de una página falsa hacia otras páginas WEB con el objetivo de obtener información (páginas web vistas, información de formularios, contraseñas etc.). Comúnmente utilizada para robar información personal.

Protocolo IP: Conjunto de reglas que rigen el formato y transporte de los datos enviados a través de Internet o una red local.

Ransomware: Es una clase de Malware que se caracteriza porque luego de comprometer o infiltrarse en un dispositivo o sistema como cualquier otro Malware, bloquea el equipo o cifra los archivos y exige "rescate" para "liberar" la información. Modalidad de ciberdelincuencia empleada para extorsionar digitalmente a víctimas a cambio de un pago.

SCAM: Es una variante del Phishing en la cual engañan a las personas por medio de correos electrónicos, chats o páginas web, haciéndoles ofrecimientos que solo los llevan a ser estafados.

Shimmer: Robo de información del chip de tarjetas de crédito/débito utilizado en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su posterior uso fraudulento.

Sim Swap: El fraude de SIM Swapping se produce cuando una persona se hace con el control del número de teléfono de alguien, luego de ponerse en contacto con un operador de telecomunicaciones y convencerlo para que transfiera el número de teléfono de la víctima a una nueva tarjeta SIM.

Skimming: Consiste en el copiado de la banda magnética de una tarjeta (crédito, débito, etc.). Robo de información de tarjetas de crédito, utilizado en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su posterior uso fraudulento.

Smishing - Fraudes por mensaje de texto: Modalidad consistente en el uso del phishing-métodos de engaño para obtener información personal confidencial o estafar a alguien- pero a través de SMS (mensajes cortos de celular) en lugar de correos electrónicos.

Sniffer: Es una herramienta de software o hardware que permite al ciberdelincuente supervisar todo el tráfico de un equipo en internet en tiempo real y capturar la información que por allí se transmite. Su uso es implementado para fines maliciosos, como robar contraseñas, interceptar correos electrónicos, espiar conversaciones de chat, etc.

SPAM: Correo electrónico NO SOLICITADO que se distribuye masivamente con fines comerciales. También es utilizado para engañar al usuario haciéndolo descargar o ejecutar un archivo en el equipo la máquina y quede infectada para tomar control de esta.

Spoofing: Suplantación de identidad del remitente del mensaje de correo electrónico, IP o cualquier otra app con la finalidad de obtener información sensible.

SQL Injection - Inyección de código SQL: Es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

Vishing: El vishing corresponde a llamadas que hacen para engañar a las personas con la promesa de falsos premios, oferta u ofrecimientos bancarios y de esta manera obtener información sensible.

6. MARCO LEGAL O NORMATIVO

- Constitución Política de Colombia Art. 15
- Ley 599 de 2000 – Código Penal Colombiano
- Ley 906 de 2005 – Código de Procedimiento Penal
- Ley 1273 de 2009 – Ley de Delitos Informáticos
- Convenio de Budapest de 2001 – Convenio Contra la Cibercriminalidad
- Ley 1928 de 2018 – Aprobación del Convenio de Budapest en Colombia

7. DESARROLLO

CRITERIOS

Para el registro de la información en los sistemas tecnológicos, se tendrán en cuenta los siguientes criterios:

- **Modalidad.** Manera o método utilizado por una persona o un grupo de personas, para cometer el delito, que involucra la relación entre el entorno, la víctima y el victimario. Se discrimina para cada tipo o clase de delito informático.

- **Modo.** Herramienta, elemento o mecanismo utilizado por el delincuente para cometer el delito.

8. MODALIDADES Y MODOS

De acuerdo con el Convenio sobre la ciberdelincuencia de 2001 (Convenio Budapest), el cibercrimen se podría definir como las infracciones contra la confidencialidad, la integridad y la disponibilidad de la información, de los datos y de los sistemas informáticos; por tal motivo, en Colombia se expidió la Ley 1273 de 2009, donde se crea el bien jurídicamente tutelado de la información, los datos y los sistemas de información, tipificando conductas asociadas a la afectación de este bien, bajo 9 delitos.

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

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.

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.

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.

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

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

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

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.

Artículo	Tipificación	Modalidad	Modo
269 J	**Transferencia no Consentida de Activos** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá...	Transferencias **NO** consentidas	1. Ingeniería Social. 2. Software Malicioso. 3. Phishing. 4. Vishing. 5. Smishing. 6. SIM SWAP. 7. Explotación de Vulnerabilidades. 8. Insider. 9. Carding.

9. RUTA PARA LA ATENCIÓN DEL DELITO

Víctima: Persona a la cual se le afecta el bien jurídico tutelado *"de la protección de la información y de los datos".*

Denuncia Virtual: El denunciante podrá realizarla personalmente o de manera virtual, mediante la plataforma *¡Adenunciar!, ¡Denuncia fácil!*

Denuncia Telefónica: En este canal se incluye el Centro de contacto y las líneas telefónicas de la Fiscalía General de la Nación.

Receptor de la Denuncia: Persona encargada de la atención ciudadana con el fin de recepcionar el hecho denunciado.

Identificar los procedimientos realizados en cada etapa del proceso:

- Recepcionar denuncia.
- Programa metodológico.
- Interceptación de comunicaciones Artículo 235 CP.
- Búsqueda selectiva en base de datos.
- Conservación y preservación de información en internet.
- Medidas de Cooperación Internacional.
- Evidencia digital.
- Operaciones encubiertas virtuales.

10. ACTORES INTERVINIENTES

Receptor de la denuncia: Persona encargada de la atención ciudadana para acoger y recibir el problema jurídico denunciado.

Canales de denuncia Presencial:

1. Centros de Atención de la Fiscalía –CAF y Puntos de Atención de la Fiscalía –PAF.
2. Casas de Justicia del Ministerio de Justicia y del Derecho donde hace presencia la Fiscalía General de la Nación.
3. Grupos de Acción Unificada por la Libertad Personal – GAULA, en caso de secuestro y extorsión.
4. Jornadas de atención a víctimas y ferias de servicio., en las que se habilite el servicio de recepción de denuncia
5. Grupos de Flagrancias (Anteriormente conocidos como Unidades de Reacción Inmediata-URI).
6. Estaciones de la Policía Nacional.
7. Inspecciones de policía

Canal de denuncia Virtual

1. Sistema Nacional de Denuncia Virtual ¡ADenunciar! o ¡Denuncia fácil!
2. www.fiscalia.gov.co
3. Correo electrónico (ges.documentalpqrs@fiscalia.gov.co)
4. Botón clic to call y videollamada en lengua de señas colombiana, disponibles en la página web de la Fiscalía General de la Nación.

Canal de denuncia vía telefónica: En este canal se incluye el Centro de contacto y las líneas telefónicas de la Fiscalía General de la Nación.

Centro de contacto: Es el medio no presencial por el cual la ciudadanía puede acceder a información relevante y orientación sobre los servicios.

Desde celular **122**

Línea gratuita nacional **018000919748**

Denuncia escrita: En este canal se encuentran los documentos físicos entregados en la Ventanilla Única de Correspondencia de cada dependencia y demás medios escritos.

11. INICIATIVA INVESTIGATIVA

Se realizará análisis de la información allegada a la Fiscalía General de la Nación por anónimos (escritos y/o correos electrónicos), con el fin de verificar si los hechos denunciados corresponden a la variable de delitos informáticos.

Actores Intervinientes

FISCAL

Encargado de dirigir y coordinar las funciones de policía Judicial que en forma permanente cumple la Policía Nacional y los demás organismos que señale la ley.

Director de la investigación, le corresponde la dirección, coordinación, control jurídico y verificación técnico-científica de las actividades que desarrolle la policía judicial.

La articulación entre despachos fiscales y la Policía Judicial de la Fiscalía General de la Nación y de la Policía Nacional, actualmente se desarrolla esta labor con las siguientes unidades:

- Delegada contra la Criminalidad Organizada.
- Dirección Especializada contra los Delitos Informáticos.
- Dirección Especializada Contra las Organizaciones Criminales.
- Delegada para las Finanzas Criminales.
- Dirección de apoyo a la Investigación y Análisis contra la Criminalidad Organizada.
- Fiscalías de Investigaciones Priorizadas de la Dirección del Cuerpo Técnico de Investigación.
- Unidad de Fiscalía para la Protección de Datos Personales.
- Fiscalía de Estructura de Apoyo.

POLICÍA JUDICIAL

Servidores públicos que, en ejercicio de sus funciones de Policía Judicial, reciban denuncias, querellas o informes de otra clase, de los cuales se infiera la posible comisión de un delito, realizarán de inmediato todos los actos urgentes, tales como inspección en el lugar del hecho, inspección de cadáver, entrevistas e interrogatorios. Además, identificarán, recogerán, embalarán técnicamente los elementos materiales probatorios y evidencia física y registrarán por escrito, grabación magnetofónica o fonóptica las entrevistas e interrogatorios y se someterán a cadena de custodia.

En la actualidad la función de investigación de cibercrímenes se encuentra distribuido en las dos entidades de la siguiente forma:

- *Grupos investigativos en contra de los delitos informáticos,* de la delegada para la seguridad territorial.
- *Grupos Investigativos Contra los Delitos Informáticos* de la dirección del cuerpo técnico de investigación.
- *Funcionarios de Policía Judicial SIJIN.*
- *Funcionarios de Policía Judicial de la DIJIN.*
- *Funcionarios de Policía Nacional,* destacados en las estructuras de apoyo.
- *Funcionarios del CTI,* destacados en las estructuras de apoyo.

PERITOS

Expertos en informática forense encargados de descubrir, recolectar, recuperar, analizar y custodiar la evidencia de tipo digital obtenida. Entre sus funciones están:

1. Identificar contenedores de evidencia digital.
2. Obtener información de sistemas de información de manera técnica.
3. Realizar imágenes forenses.
4. Extracción de información a equipos terminales con almacenamiento de datos.
5. Extracción de información a equipos terminales móviles.
6. Tratamiento y estudio Técnico de la evidencia digital.
7. Recolectar y estudiar datos volátiles.

12. PROCEDIMIENTOS REALIZADOS EN CADA ETAPA DEL PROCESO

RECEPCIÓN DE DENUNCIA

Este procedimiento es el primer contacto con la comunidad para iniciar un trámite directo con la Fiscalía General de la Nación y generarse una noticia criminal para resolver el pedido ciudadano a través de una investigación judicial.

PROGRAMA METODOLÓGICO

Es una herramienta de trabajo que surge de la reunión entre el fiscal y los miembros de Policía Judicial, donde se determinan los objetivos en relación con la naturaleza de la hipótesis delictiva y el plan de trabajo investigativo a desarrollar. Se utiliza con el fin de:

- *Organizar y explicar la investigación,* con el fin de identificar y asegurar los medios cognoscitivos necesarios que le permitan a la Fiscalía diseñar su teoría del caso.
- *Contener los objetivos,* criterios para evaluar la información, delimitación de tareas, procedimientos de control y recursos.
- *Establecer lineamientos* para el programa metodológico e indicaciones para la conformación de grupos de tareas especiales.

ACTOS URGENTES

Los servidores públicos que, en ejercicio de sus funciones de policía judicial, reciban denuncias, querellas o informes de otra clase, de los cuales se infiera la posible comisión de un delito, realizarán de inmediato todos los actos urgentes, tales como inspección en el lugar del hecho, inspección de cadáver, entrevistas e interrogatorios. Además, identificarán, recogerán, embalarán técnicamente los elementos materiales probatorios y evidencia física y registrarán por escrito, grabación magnetofónica o fonóptica las entrevistas e interrogatorios y se someterán a cadena de custodia.
Sobre esos actos urgentes y sus resultados la policía judicial deberá presentar, dentro de las treinta y seis (36) horas siguientes, un informe ejecutivo al fiscal competente para que asuma la dirección, coordinación y control de la investigación.

INTERCEPTACIÓN DE COMUNICACIONES

El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. En este sentido, se desplegarán las actividades investigativas necesarias, (vigilancias, entrevistas, seguimientos), así como el procesamiento de la información recolectada.

BÚSQUEDA SELECTIVA EN BASES DE DATOS

Es la recopilación de información referida en una investigación, que reposa en bases de datos en entidades públicas o privadas y que no son de libre acceso, sino a través de autorización previa del juez de control de garantías.

Para el caso de plataformas de correos, redes sociales, aplicaciones de mensajería y páginas web, se debe solicitar: nombres, correos, celulares, direcciones IPs con horas y fechas exactas de conexión, fechas de creación y cualquier dato que aporte al desarrollo de la investigación.

CONSERVACIÓN Y PRESERVACIÓN DE INFORMACIÓN EN INTERNET

Es necesario conservar y preservar los datos que se encuentren en la nube con la mayor rigurosidad posible, dentro de varios métodos existentes, se sugieren aplicar las siguientes técnicas:

- Fijación inicial horaria o estampa de tiempo.
- Grabación de la información obtenida.
- Fijación final horaria o estampa de tiempo.
- Cálculo de algoritmos.
- Captura y almacenamiento de información utilizando técnicas (Capturas de pantalla, grabación de video, grabación de acciones del usuario, impresión PDF, almacenamiento de código fuente, descarga de contenidos, utilización de software especializado)

COTEJOS

Estudios técnico-científicos comparativos de diferentes áreas de la criminalística que permitan confrontación entre elementos materiales probatorios a fin de identificar semejanzas o diferencias.

MEDIDAS DE COOPERACIÓN INTERNACIONAL

Solicitudes de cooperación judicial a las autoridades extranjeras. Los jueces, fiscales y jefes de unidades de Policía Judicial podrán solicitar a autoridades extranjeras y organismos internacionales, directamente o por los conductos establecidos, cualquier tipo de elemento material probatorio o la práctica de diligencias que resulten necesarias, dentro del ámbito de sus competencias, para un caso que esté siendo investigado o juzgado en Colombia. Las autoridades concernidas podrán comunicarse directamente a fin de determinar la procedencia de las actuaciones relacionadas en la solicitud.

Actualmente el Centro Cibernético Policial de la Dirección de Investigación Criminal e INTERPOL, mantiene un acuerdo de cooperación con la Agencia de la Unión Europea para la Cooperación Policial EUROPOL, facilitando de esta manera la coordinación, instrumentos de cooperación y alianzas.

> Colombia sostiene desde el año 2012, un acuerdo de Cooperación Operativa y Estratégica en materia judicial con EUROPOL, siendo el único país en Latinoamérica en lograr un acuerdo con dicha agencia, contando con un oficial de enlace en el J-CAT.

Este acuerdo ha permitido el acceso a importantes herramientas de intercambio de información en materia operacional, actualmente el C4 cuenta con acceso a SIENA (Canal de comunicación segura con los más de 28 estados miembros).

La integración de Colombia con los países de la región a través de AMERIPOL, ha permitido articular esfuerzos para la lucha contra el cibercrimen a nivel regional.

CARTA ROGATORIA

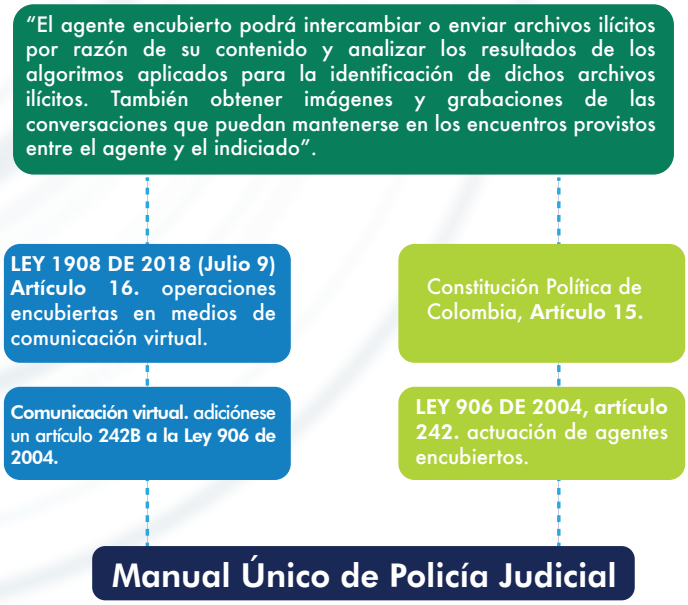
Es la solicitud que libra una autoridad judicial colombiana o extranjera en el marco de un proceso judicial, dirigida a la autoridad homóloga en otro país o en Colombia, respectivamente, con el ruego de que lleve a cabo una determinada diligencia judicial, la práctica de pruebas o brinde información.

TRATADO DE ASISTENCIA JUDICIAL MUTUA (MLAT)

Compromiso establecido entre Estados, con el fin de asistir de la mejor manera a la otra parte, en materia penal en cualquier investigación o procedimiento, respecto a conductas delictivas.

EVIDENCIA DIGITAL

OPERACIONES ENCUBIERTAS VIRTUALES



Es el registro de información guardada o difundida a través de un sistema informático que puede utilizarse como prueba en un estrado judicial.

LÍNEAS DE ATENCIÓN 24/7

Canales de comunicación para la cooperación con otras agencias gubernamentales nacionales e internacionales, los cuales hayan suscrito convenios de cooperación.

CIBERPATRULLAJE

Concepto: El ciberpatrullaje se define como la actividad que adelantan los funcionarios de Policía Judicial de la Policía Nacional, con el fin de recolectar información de fuentes públicas en Internet, que permita orientar procesos judiciales y disciplinarios por parte de las autoridades de control competentes.

Esta actividad, será desarrollada en la web desde el enfoque judicial, a través de la cual se busca identificar conductas contrarias a los estamentos jurídicos colombianos y que repercutan directamente en la convivencia y seguridad ciudadana, los elementos materiales probatorios y/o evidencia física recolectada en esta actividad, será puesta a disposición de las autoridades de control disciplinario y judicial.

13. NORMATIVIDAD QUE LO FUNDAMENTA

DE ACUERDO AL CÓDIGO DE PROCEDIMIENTO PENAL:

Funciones de Policía Judicial:

Artículo 314. Labores previas de verificación.

Ley 906 de 2004

Artículo 205. Actos Urgentes.
Artículo 213. Inspección del lugar del hecho.
Artículo 242. Actuación de agentes encubiertos.
Artículo 556. Actos de investigación.

Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

Artículo 12. Conservación de los mensajes de datos y documentos.

Operaciones encubiertas en medios de comunicación virtual

LEY 1908 DE 2018 (Julio 9)

Artículo 16. Operaciones encubiertas en medios de comunicación virtual. Adiciónese un artículo 242B a la Ley 906 de 2004: Artículo 242B.

MANUAL DE POLICÍA JUDICIAL

18.3 Aspectos relevantes.

2.4.1. Actos urgentes.

RESOLUCIÓN NRO. 0260 DEL 25 DE ENERO DE 2023, "Por la cual se define la estructura orgánica de la Dirección de Investigación Criminal e INTERPOL, se determinan las funciones de sus dependencias internas".

14. ANEXOS

REFERENCIAS BIBLIOGRAFICAS.

Plan de Contingencia y Continuidad de Negocio. Obtenido de: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

Departamento Nacional de Planeación. (14 de Julio de 2011). Obtenido de CONPES 3701 https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeación. (1 de julio de 2020). Obtenido de CONPES 3995: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Departamento Nacional de Planeación. (11 de abril de 2016). Obtenido de CONPES 3854: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

OAS. (23 de 11 de 2001). Organización de estados americanos. Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

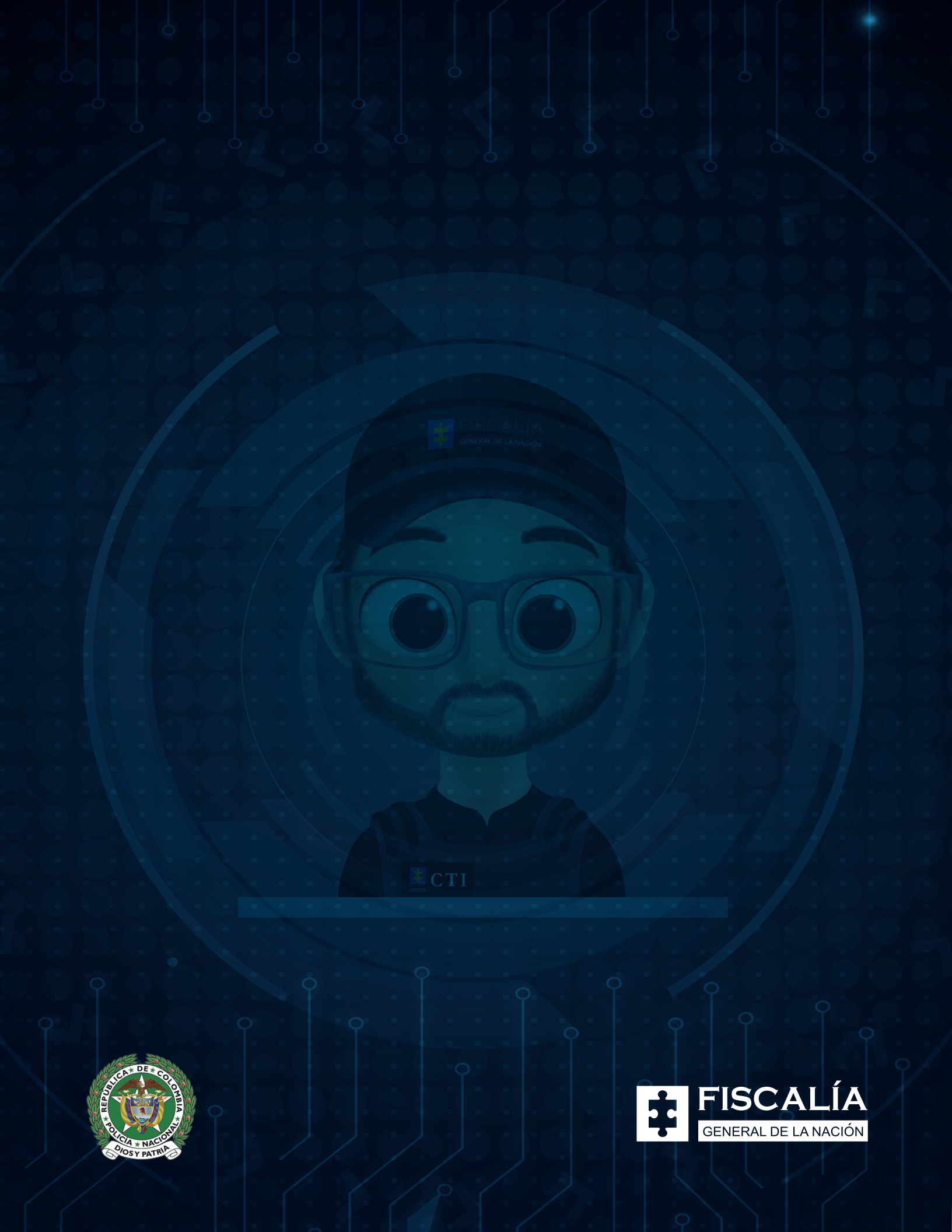
Senado. (1 de Enero de 2009). Obtenido de secretariasenado: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Senado (2018), Ley 1928 de 2018, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, recuperado de https://www.senado.gov.co/.

Nir (2021), Ingeniería social, claves y precauciones desde la seguridad informática, https://www.unir.net/ingenieria/revista/ingenieria-social/

INCIBE (2020), El ataque del "Man in the middle" en la empresa, riesgos y formas de evitarlo recuperado de https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo.

Posada Maya, Ricardo. "Los cibercrímenes: Un nuevo paradigma de criminalidad". Bogotá, Grupo Editorial Ibañez, 2017.



REPÚBLICA DE COLOMBIA
POLICÍA NACIONAL
DIOS Y PATRIA

FISCALÍA
GENERAL DE LA NACIÓN