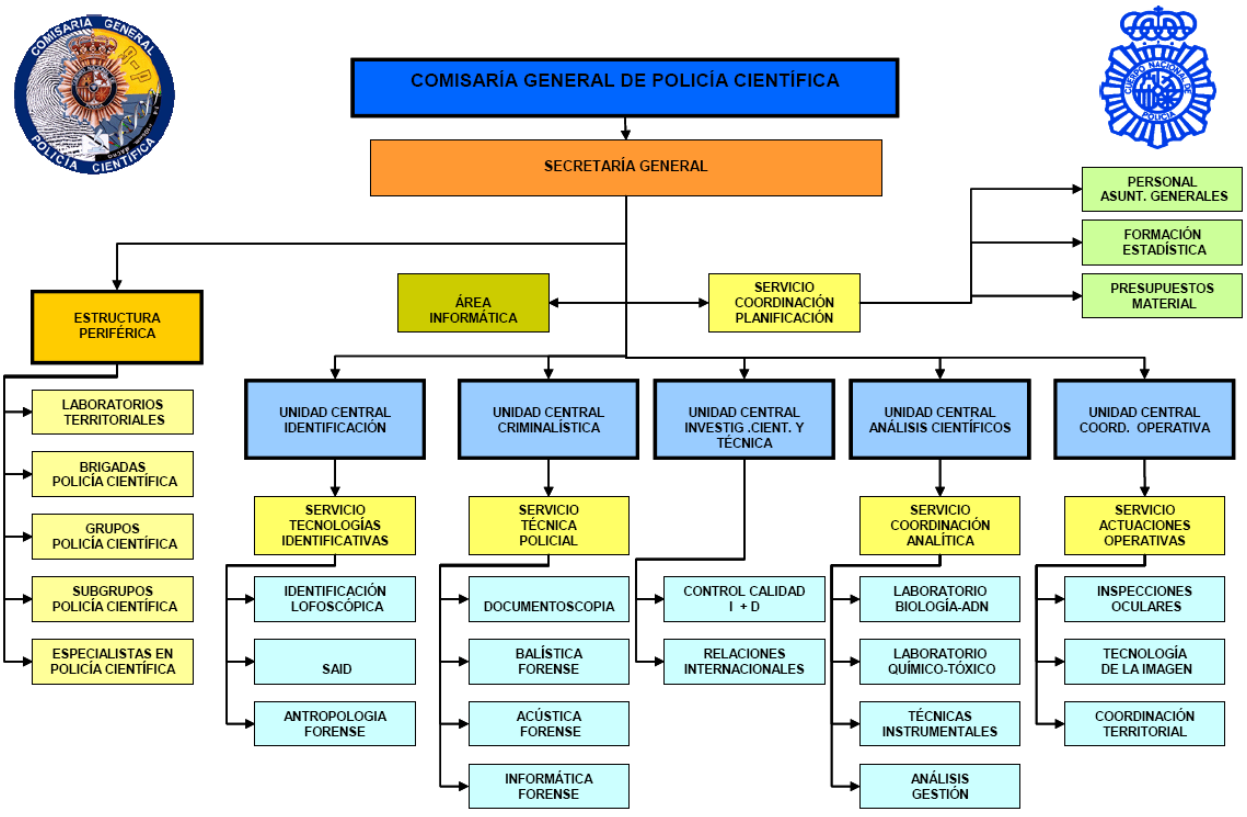
COMISARIA GENERAL DE POLICIA CIENTIFICA

La Orden INT/2103/2005, de 1 de julio, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía y el Real Decreto 1181/2008, de 11 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, establece que, en el ámbito del Cuerpo Nacional de Policía, bajo la coordinación de la Dirección Adjunta Operativa, la Comisaría General de Policía Científica tiene como misión la **"prestación de los servicios de criminalística, identificación, analítica, e investigación científica y técnica, así como la elaboración de los informes periciales y documentales que le sean encomendados"**.

Las funciones de la policía científica se extienden en la teoría y en la práctica habitual, a la inspección ocular en el lugar de los hechos, fuente de alimentación de la actividad probatoria; a la recogida de efectos, documentos, armas e instrumentos para su estudio y puesta a disposición judicial; al embalaje, transporte y recepción de las muestras biológicas o físicas con las debidas garantías de custodia; a la identificación del imputado y de las huellas, vestigios o rastros que el mismo deja en el lugar del crimen; al estudio y tratamiento de las muestras, de los elementos balísticos, efectos y documentos, registros fónicos, fonográficos y fotográficos; a la elaboración de los informes documentales y periciales sobre estas materias realizados a requerimiento de los Tribunales de Justicia, y la defensa de los mismos en la vista oral, donde culmina toda actividad probatoria.

ESTRUCTURA COMISARÍA GENERAL DE POLICÍA CIENTÍFICA

Al amparo de la Orden INT/2103/2005, de 1 de julio, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía y el Real Decreto 1181/2008, de 11 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, establece que, en el ámbito del Cuerpo Nacional de Policía, la Comisaría General de Policía Científica tiene la siguiente estructura:



☐ UNIDAD CENTRAL DE IDENTIFICACIÓN.

Asume las funciones relacionadas con la reseña dactilar y fotográfica, el servicio automático de identificación dactilar y antropología, así como la elaboración de los informes periciales, de interés policial y judicial, relacionados con la materia de su competencia.

☐ UNIDAD CENTRAL DE CRIMINALÍSTICA.

Asume las funciones de estudiar y realizar informes periciales de interés policial y judicial, en materia de falsificación documental, grafoscopia, balística forense, identificativa y operativa, trazas instrumentales, acústica forense e informática forense.

☐ UNIDAD CENTRAL DE INVESTIGACIÓN CIENTÍFICA Y TÉCNICA.

Asume las funciones relacionadas con la investigación científica y técnica y el control de calidad, así como las relaciones con otros organismos e instituciones, tanto nacionales como internacionales, en materia de policía científica y coordinación en materia de cooperación internacional de las diferentes Unidades Centrales de la Comisaría General.

☐ **UNIDAD CENTRAL DE ANÁLISIS CIENTÍFICOS**.

Asume las funciones de gestionar los laboratorios de Policía Científica en las áreas de Biología-ADN, Química y Toxicología, así como la realización de analíticas especializadas y la elaboración de los informes periciales, de interés policial y judicial, relacionados con las materias de su competencia. Igualmente, ejerce funciones en el Análisis de Gestión Operativa.

☐ **UNIDAD CENTRAL DE COORDINACIÓN OPERATIVA.**

Asume las funciones de coordinación de los Servicios Operativos a nivel nacional y las relacionadas con la tecnología de la imagen, así como la inspección ocular; tanto en su faceta operativa como en la elaboración de métodos y procedimientos técnicos para su realización y práctica.

UNIDAD CENTRAL DE CRIMINALISTICA

Dentro de la Comisaría General de Policía Científica, en la Unidad Central de Criminalística y a su vez dentro del Servicio de Técnica Policial se encuentra la **SECCIÓN DE INFORMÁTICA FORENSE.**

Las primeras pericias en esta área se empiezan a hacer en 1999, con el tiempo pasa a formarse un Grupo de Pericias Informáticas y ya en el año 2008 pasa a tener el nivel de Sección.

La Sección de Informáticas Forense está organizada en dos grupos:

1. GRUPO DE ANALISIS DE SOFTWARE

Se encarga de extraer la información de soportes digitales, discos duros, disquetes, discos CD o DVD, soportes de memoria del tipo compact flash, memory stick, SD card, XD card y sus variantes del tipo micro o dúo y dispositivos USB del tipo pendrive , mp3, mp4 , ipod o discos duros externos; o firewire.

2. GRUPO DE ELECTRONICA

Extrae la información de dispositivos electrónicos y telefonía móvil. Incluyendo tanto la memoria interna del teléfono como la tarjeta SIM. Las tarjetas de memoria adicional que incorporan algunos de teléfonos se podrían clasificar como un soporte informático portátil.

DISTRIBUCIÓN TERRITORIAL

Se tiende a la descentralización, para poder dar respuesta a todas las peticiones de los distintos juzgados de España.

Actualmente existen grupos de Informática Forense en: Comisaría General de Policía Científica (sede en Madrid, con competencia a nivel nacional), Barcelona, Valencia, Sevilla, La Coruña, Murcia, Las Palmas de Gran Canaria. Granada, Málaga, Oviedo, Cantabria, Palma de Mallorca, Vigo, Madrid Jefatura, Zaragoza.

INFORMÁTICA FORENSE

Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio electrónico, teniendo su fundamento en las leyes de la física, de la electricidad y el magnetismo. (Evidencia Digital).

Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada.

La criminalidad organizada en materia de nuevas tecnologías viene creciendo de manera exponencial. La pericia informática es uno de los medios probatorios con más auge en los procesos civiles, mercantiles y penales.

Este es el marco de competencias de los Laboratorios de Informática Forense.

COMETIDO DE LA SECCION DE INFORMATICA FORENSE

Analizar el contenido de soportes digitales, dispositivos electrónicos o terminales de telefonía móvil, intervenidos con ocasión de la comisión de un acto delictivo, extraer las evidencias que sirvan de prueba judicial, (ficheros, imágenes) que estén relacionadas con el asunto investigado y presentarla de forma clara y ordenada en el Informe Pericial, respondiendo a los puntos de pericia solicitados por el juez en cada caso.

Posteriormente defender el IP en el Juicio Oral.

Los investigadores de informática forense usan gran cantidad de técnicas para descubrir las evidencias, incluyendo herramientas de software que automatizan y aceleran el análisis

Las evidencias electrónicas pueden recogerse en diferentes lugares y de diferentes fuentes, y podrán encontrarse en cualquier elemento o sistema que se esté utilizando para transmitir o almacenar los datos.

En una investigación forense digital se presta una especial atención al cuidado en la manipulación de los soportes a analizar, para mantener la integridad de la evidencia. Los peligros para las evidencias digitales son muchos y graves, y van de la mano de los virus informáticos, del deterioro electromagnético o mecánico del soporte, e incluso con la presencia de trampas dejadas por el atacante.

Las reglas básicas que ayudan a asegurar que la evidencia no se destruya o quede alterada durante la investigación son:

1. Utilizar solo herramientas y métodos que hayan sido probados y evaluados previamente para determinar su precisión y sensibilidad reales;
2. Manipular lo menos posible la evidencia original para evitar cambiar los datos;
3. Establecer y mantener una cadena de custodia;
4. Documentar todo lo que se ha hecho.

Para evitar está alteración de la evidencia original se ha redactado un **Manual de Normas de Procedimient**o, en el que se concretan todas las operaciones de cada proceso, unifica y sistematiza el tratamiento de las evidencias, además es de obligado cumplimiento a todos los niveles de competencia.

ACTIVIDADES ILEGALES

Entre los delitos más habituales investigados se encuentran:

☐ Amenazas, injurias, calumnias, por medio de correo electrónico, SMS, tablones de anuncios, foros, chat.
☐ **P**rotección al menor: producción, distribución y posesión de pornografía infantil

☐ Falsificación de moneda y estafas bancarias:

Carding: uso de tarjetas de crédito ajenas o fraudulentas

Phising: redirección mediante correo electrónico a falsas páginas simuladas trucadas (común en las mafias rusas)

Cartas nigerianas (segunda fuente de ingresos del país, según el FBI; después del petróleo)

☐ Falsedad documental

☐ Inmigración Ilegal

☐ Manipulación de cajeros

☐ Agresiones sexuales

☐ También puede ser cualquier tipo delictivo: Homicidios, Tráfico de Estupefacientes, secuestros, extorsiones, etc..

A parte de estas descritas, cualquier tipo delictivo que pueda dejar rastros en un soporte digital y hoy en día pueden ser todos.

EVIDENCIAS DIGITALES

Debemos entender como evidencia digital cualquier soporte que sea capaz de contener información susceptible de ser extraída y reproducida en un informe pericial. Se considerarán evidencias informáticas de interés aquellas que contengan información del usuario del dispositivo a analizar, y no meramente información destinada a tareas o funciones necesarias para la máquina.

TIPOS DE EVIDENCIAS

Podemos establecer pues tres tipos de soportes:

☐ **Soportes Informáticos**

1.- Soportes portátiles: aquellos que disponen de una carcasa que permite su traslado garantizando la integridad de la información en ellos contenida, por lo tanto hablamos de disquetes, discos CD o DVD, soportes de memoria del tipo compact flash, memory stick, SD card, XD card y sus variantes del tipo micro o dúo y dispositivos USB (del tipo pendrive , MP3, MP4 , ipod o discos duros externos) o firewire.

2.- Soportes contenidos en equipos portátiles o sobremesa: incluye principalmente discos duros ubicados en el interior de equipos informáticos, discos duros de tipo IDE, SCSI o SATA en sus distintos tamaños de 3,5 pulgadas, 2.5 pulgadas y 1,8 pulgadas o microdrive. En este tipo también podrían incluirse dispositivos del tipo PDA o PALM.

☐ **Terminales de telefonía móvil**. Incluyendo tanto la memoria interna del teléfono como la tarjeta SIM. Las tarjetas de memoria adicional que incorporan algunos de teléfonos se podrían clasificar como un soporte informático portátil.

☐ **Dispositivos electrónicos**. En este grupo incluiríamos cualquier dispositivo electrónico capaz de almacenar información, tales como los skimmers usados en la falsificación de tarjetas, tarjetas de televisión de pago, etc.

ANÁLISIS FORENSE DE UN SOPORTE DIGITAL

El objetivo es encontrar toda la información relacionada con el asunto investigado que se encuentre almacenada en el soporte analizado. En primer lugar hay que plantearse el tipo de soporte a analizar, estado físico del mismo, sistema operativo, etc.

Las fases de un análisis forense son:

1. **Duplicar**
2. **Analizar**
3. **Presentar**: Redactar el Informe Pericial

Duplicar quiere decir, realizar una copia exacta de la evidencia para analizarla. Existen dos formas:

- Volcado: Traspaso de datos originales en un formato apto para ser tratado por la herramienta de análisis que se vaya a utilizar.
- Clonado: Copia exacta del original, realizada bit-a-bit.

Duplicar la evidencia (IMAGING) presenta una serie de inconvenientes como son, el tiempo requerido y la necesidad de un soporte para el volcado; a su vez presenta muchas ventajas como son, mantener la integridad de la evidencia y la posibilidad de repetir el análisis las veces que sea necesario.

A la hora de analizar la información nos encontramos con una serie de dificultades:

☐ Tamaño de la muestra.

☐ Ficheros de tipo desconocido.

☐ Desconocimiento del funcionamiento de las aplicaciones informáticas, motivo por el cual se debe estar en constante formación.

☐ Cambios en la apariencia de la información (extensiones de ficheros/signaturas).

☐ Ficheros borrados.

☐ Ficheros protegidos.

☐ Ficheros cifrados.

☐ Esteganografia.

INFORME PERICIAL

Es el medio de prueba consistente en la declaración de conocimiento que emite una persona, que no sea objeto necesario del proceso, acerca de los hechos, circunstancias o condiciones personales inherentes al hecho punible, conocidos dentro del proceso y dirigidos al fin de la prueba, para lo que es necesario poseer determinados conocimientos científicos, artísticos o prácticos.

Las características que debe presentar: Debe ser ordenado, sistemático, preciso y lógico.

Se realiza en dos partes:

1ª.-Estudio en laboratorio que se plasma por escrito.

2ª.- Exposición hablada ante la Autoridad Judicial en el Juicio Oral.

Fundamentación legal: Capitulo VII: Del Informe Pericial

Art.456 LECr. El Juez acordará el Informe Pericial cuando, para conocer o apreciar algún hecho o circunstancia importante en el Sumario, fuesen necesarios o convenientes conocimientos científicos o artísticos.

Artº 478 LECr: El Informe Pericial comprenderá:

a) Descripción de la persona o cosa que sea objeto del mismo en el estado o del modo en que se halle...

b) Relación detallada de todas las operaciones practicadas por los peritos y de su resultado, extendida y autorizada en la misma forma que la anterior.

c) Las conclusiones que de tales datos formulen los peritos conforme a los principios y reglas de su ciencia o arte.

La estructura básica del Informe Pericial:

1) ANTECEDENTES.- Donde consta el órgano solicitante, el objeto del informe y el material examinado.

2) ESTUDIO REALIZADO.- Constan los datos de la persona que realiza el informe y análisis del material.

3) CONCLUSIONES: Explicación de las implicaciones, descripción de los elementos que componen el informe, fecha y firma de los peritos actuantes.

CLONADO TARJETAS DE BANDAS MAGNETICAS – SKIMMING

Un tipo de estudio que hace el Grupo de Electrónica de la Sección de Informática Forense es el estudio de lectores de banda magnetica y teclados bancarios, utilizados para el clonado de tarjetas bancarias.

Como miembros del Instituto Universitario de Investigación en Ciencias Policiales (IUICP) se ha desarrollado junto con la Universidad de Alcalá de Henares y colaboración de la Guardia Civil, un software (programa) y un hardware (parte física del sistema) que permita recuperar y leer la información que almacenan los skimmers MP3 (un tipo de falsos lectores de bandas magnéticas que se adaptan en las bocas de inserción de las tarjetas en los cajeros para grabar las lecturas de las bandas magnéticas) y así poder saber la numeración de las tarjetas que han sido copiadas.

El *Grupo de Electrónica de esta Sección* es capaz de poder obtener la información total de los dispositivos MP3 acoplados a los cajeros, y que es grabada en forma de archivo de sonido

La información que contienen las tarjetas magnéticas o tarjetas de crédito/debito son leídas a través de un cabezal lector de bandas que lee la pista DOS de las tarjetas (pista que contiene la numeración de la tarjeta) y grabado en el MP3 de forma analógica por el conector de entrada al micro, quedando así los datos grabados en un archivo de sonido.

La importancia de este desarrollo para la recuperación de los datos de los skimmers MP3, viene dada por ser los *pioneros en Europa* en poder desarrollar un programa, acceder a los datos y ser capaces de descodificarlos para obtener la información de las bandas magnéticas.

TELEFONIA

Lo más interesante, desde el punto de vista forense, es su capacidad para almacenar información. Un teléfono inteligente está compuesto habitualmente de los siguientes componentes con capacidad para almacenar información:

1. Un terminal
2. Una o varias tarjetas SIM
3. Una o varias tarjetas de memoria adicional

Un **terminal de telefonía móvil** contiene dos tipos de memoria: memoria volátil y memoria no volátil. La memoria volátil es similar a la que todos conocemos como memoria RAM en los ordenadores personales. Es aquella cuya información se pierde al interrumpirse el flujo de corriente eléctrica. La no volátil es aquella cuyo contenido no se pierde al interrumpirse el flujo eléctrico que la alimenta. Esta última es la memoria que nosotros vamos a tener en consideración.

En la memoria no volátil de teléfono móvil es donde se almacenan todos los datos relativos a sistema operativo y programas, pero también los datos de usuario como pueden ser:

- ☐ Archivos de texto, imagen, sonido, vídeo.
- ☐ Agenda telefónica, registros de llamadas, mensajes SMS o multimedia
- ☐ Correos electrónicos, registros de visitas a páginas Web.
- ☐ Agenda personal, notas, citas, etc.

Las estructuras de estas memorias también varían entre fabricantes y entre los distintos modelos y versiones de terminales de cada fabricante. Este es el mayor problema con el que nos encontramos para poder acceder a los datos en ellas contenidos

La **tarjeta SIM** es un componente removible que contiene información esencial sobre el abonado. La función principal de la Tarjeta SIM es la autenticación del usuario del teléfono móvil a la red para obtener acceso a los servicios que tiene contratados.

Las tarjetas SIM están protegidas de acceso mediante un código de identificación personal (PIN). Este código PIN (número de 4 cifras) puede ser modificado por el abonado, de tal forma que sea la única persona que tenga conocimiento del mismo

El código de desbloqueo se denomina código PUK y es proporcionado por las compañías telefónicas que gestionan la tarjeta SIM bloqueada.

Datos contenidos en una SIM:

1. Información relativa al servicio prestado por la compañía telefónica.
2. Agenda de teléfonos e información sobre llamadas, realizadas, recibidas y perdidas
3. Información relativa a mensajes de texto, tanto SMS (mensajes de texto), como EMS (SMS, mejorado con animaciones, melodías, sonidos,…) y mensajes multimedia
4. Información de localización.