Guardia Civil

Mando de Apoyo

Jefatura de Servicios Técnicos

Seguridad en las Tecnologías de la Información y la comunicación

SEMINARIO: CIBERDELINCUENCIA, EVIDENCIAS DIGITALES Y CADENA DE CUSTODIA

ACADEMIA DE INGENIEROS

Cap. Jesús Cano Carrillo

Estado de alarma, 18 de junio de 2020


53407

Qué veremos hoy?

- Algo sobre delitos informáticos
- Introducción a la informática forense
- La cadena de custodia
- …Y Lo que queráis

Delito informático

- Definición clásica de **delito** “**como la acción típica, antijurídica, culpable y punible**”
- Código Penal **“son delitos las acciones y omisiones dolosas o imprudentes penadas por la ley.”**
- Delito informático **“conjunto de conductas antijurídicas relacionadas con el tratamiento automático de la información por medio de ordenadores**”.

- Ámbito anglosajón: “**Computer Crime**” (genéricamente conductas inapropiadas). Otros términos: **Cybercrime**, **computer-oriented crime**
- Ámbito europeo: Señalar convenio del Consejo de Europa sobre Ciberdelicuencia, conocido como Convenio Budapest, primer tratado internacional para la armonización de leyes nacionales

Convenio Budapest -- ciberdelincuencia

- Establecer una **política penal común**
- **Cooperación entre los Estados** y el sector privado
- **Proteger los legítimos intereses de TI**
- Prevenir los actos dirigidos contra la **confidencialidad, la integridad** y la **disponibilidad, mediante la tipificación** de esos actos
- Lucha efectiva: para **detección/investigación y cooperación internacional rápida/fiable.**

DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL ESPAÑOLA

- **Delitos "comunes"**
  - ***Fraude informático*, Artículos 255 y 256**
  - ***Falsificación informática.*** Artículos 248 y 249
- **Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.** Artículo 270
- **Delitos relacionados con el contenido**
  - **Difusión de pornografía infantil**. Artículo 189
  - **Provocación sexual y prostitución**. Artículo 186 y 187
  - **Amenazas (169), injurias (208) y calumnias**. Artículo 205
  - **Apología racismo y xenofobia.** Artículo 607

DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL ESPAÑOLA

- **Delitos contra la confidencialidad, la integridad y la disponibilidad**
  - ***Delito de intrusión informática.*** *Artículo 197 bis apartado primero.*
  - ***Interceptación de datos informáticos.*** *Artículo 197 bis apartado segundo*
  - ***Producción o adquirir, o facilitar a terceros para facilitar la comisión de los delitos artículo anterior.*** *Artículo 197 ter*
  - ***Actuar en organización o grupo criminal.*** *Artículo 197 quater.*
  - ***Responsabilidad de la persona jurídica.*** *Artículo 197 quinquies*
  - ***Delitos de daños Informáticos****. Artículo 264*

Fenomenología

- El ciberespacio
  - un entorno propicio
  - No legislación propia
  - Facilita el anonimato y la ocultación
- La investigación de estos delitos: **compleja**
  - **Múltiples localizaciones**
  - **Multiplicidad de víctimas**
  - Heterogeneidad de delitos y modus operandi

- **Transnacionalidad.**
- **Investigación rápida.**
- **Distancia física.**
- **Competencia territorial y ubicuidad.**
- **Complejidad.**

Fenomenología

Competencia territorial y ubicuidad II

- LECrim **Articulo 14 y 15:** reglas por la que se determina las competencias de Jueces y Tribunales
- Para resolver los problemas de competencia, el Pleno no Jurisdiccional de la Sala II del Tribunal Supremo en reunión fecha 3/02/2005 tomó el acuerdo de que :

> **"El delito se comete en todas las jurisdicciones territoriales en las que se haya realizado algún elemento del tipo, en consecuencia, el juez de cualquiera de ellas que primero haya iniciado las actuaciones, será, en principio competente para la instrucción de la causa".**

PROCESO DE INVESTIGACIÓN

Se caracteriza por

- Ser un proceso **continuo.**
- **Organizado** = pasos ordenados y lógicos.
- Encontrar a los **autores:** con el tiempo → más **complejo**.
- **Previsorio**, esto es, requiere un planteamiento.
- Es una **actividad analítica-sintética.**
- Explica las causas, quién, cómo, cuándo, por qué y para qué.

FASES DE UNA INVESTIGACIÓN

Fase inicial

- **Asegurar las pruebas del delito.**
- **Identificar al presunto autor.**

- ✓ Proteger el lugar de los hechos.
- ✓ Inspección Ocular.
- ✓ Técnica de aislamiento.
- ✓ Finalmente antes de proceder al levantamiento de pruebas, realizar la fijación de evidencias, tomando copias de seguridad y almacenando toda la información.

FASES DE UNA INVESTIGACIÓN

Fase intermedia

- **Analizar y clasificar las posibles evidencias**

- ✓ **Registro e incautación.**
- ✓ **Análisis forense de sistema y soportes intervenidos.**
- ✓ **Informe policial incriminatorio**

FASES DE UNA INVESTIGACIÓN

Fase final

- Instrucción judicial

✓ Todo el trabajo realizado se presenta ante la Autoridad Judicial

Ejemplo (Phishing)

- **INCIBE, definición:**

"El phishing es una forma de ataque basada en técnicas de ingeniería social, utilización de código malicioso o la combinación de ambas, en la que el delincuente, haciéndose pasar por alguna empresa o institución de confianza, y utilizando las TIC, trata de embaucar al atacado para que le proporcione información confidencial, que posteriormente es utilizada para la realización de algún tipo de fraude".

Modus

- ✓ **Se envían email falso**
- ✓ Estafadores **obtienen claves, entran en las cuentas de las víctimas**
  - **Enmascarando su identidad**
  - **Ut**ilizan Proxys, VPN u ordenadores Zombis (botnets)
- ✓ Se **transfieren los fondos** a un **"mulero"**, que actúa con o sin conocimiento en un hecho delictivo.
- ✓ El **mulero** pone cuenta bancaria y transferencias bancarias, Western Union o similar, u otras (ejm casinos virtuales). El mulero gana 5-10% de las transferencias.

Ejemplo (Troyano bancario)

- **Malware** que persigue el **robo de datos de cuentas bancarias electrónicas**.
- Existen varias corrientes de diseño de malware bancaria, según el país de origen de los diseñadores (Ejm. Rusa o Brasileña).
- Vías de Infección por ingeniería social
  - Spam con archivo adjunto
  - Spam con enlace a paginas con descarga: solicita la instalación de algo
  - Spam con enlaces a portales web infectados (servidor malicioso)

Otras técnicas

- **Keylogging:** Registran pulsaciones y capturas de pantallas.
- **Paginas falsas:** Web falsa que imita a la original.
- **Formularios falsos:** Superpone una ventana que contiene un formulario.
- **Campos extras en formularios:** inyecta código HTML en los formularios de las páginas web para solicitar más información.
- **Pharming:** modificar el sistema de resolución de nombres de dominio (DNS) para conducir al usuario a una página web falsa.
- **Ataque MITM "Man-in-the-middle".** Leer y modificar mensaje entre el cliente y el sitio legítimo (ejm. Banco)

ANÁLISIS FORENSE

- Órdenes penal, civil, mercantil. Terminología habitual: Análisis Forense o Pericial
- Definición:

Consiste en la aplicación de técnicas científicas, técnicas y analíticas especializadas en una rama del conocimiento o destreza especial que permite identificar, analizar y presentar una serie de conclusiones que aporte información útil para el esclarecimiento de la realización de un ilícito en un proceso legal

Evidencias

- Estudio inicial de unos ***vestigios***
- Se identifican como ***indicios***
- ***Se constituyen en evidencias***
- ***Alcanzarán si procede*** la categoría de ***prueba*** en juicio

Principios de la evidencia

- Relevante, esto es, pertinente a la situación que se analiza.
- Confiable, debe ser auditable y repetible su estudio.
- Suficiente para sustentar los hallazgos y verificar las afirmaciones.

Clasificación de las evidencias

- **Evidencia física:** hace referencia al material informático como por ejemplo: discos duros, pendrives, etc.
- **Evidencia digital:** corresponde a la información almacenada en las evidencias electrónicas.

Recopilación de las evidencias

Estándar RFC 3227: directrices para la recopilación de evidencias y su almacenamiento. Es un estándar de facto.

- Como capturar una imagen.
- Realizar notas detalladas.
- ¿Dilema entre recolección y análisis? primero recolección y después análisis.
- **Recoger la información según el orden de volatilidad (de mayor a menor**).
- Por cada dispositivo la recogida de información puede ser de distinta manera.

Orden de volatilidad

1) Registros y contenido de la caché del S.O.

2) Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria.

3) Información temporal del sistema.

4) Disco.

5) Logs del sistema.

6) Configuración física y topología de la red.

7) Documentos.

Precauciones

- **No apagar el ordenado**r hasta que se haya recopilado toda la información volátil.
- **No confiar en la información proporcionada por los programas del sistema** ya que pueden haberse visto comprometidos. Se debe recopilar la información mediante programas desde un medio protegido.
- **No ejecutar programas que modifiquen la fecha y hora** de acceso de todos los ficheros del sistema.
- **Privacidad: marco legal establecido** (Observar que los ficheros log incluidos ya que pueden *almacenar patrones de comportamiento del usuario* del equipo)

Herramientas de análisis

- **Ajenas al sistema** ya que éstas pueden haberse visto comprometidas.
- **Que alteren lo menos posible el escenario**
- Adecuadas a los sistemas operativos con los que se trabaje
- Kit de análisis elemental:
  - Listado y examen de procesos.
  - Examen del estado del sistema.
  - Programas para realizar copias bit a bit (clonar) + Huella digital (Hash)

Cadena de Custodia

- ***Conjunto de actividades*** para ***preservar y garantizar la integridad y permanencia de las muestras*** del delito, garantizando su validez procesal en juicio.
- Se ha de documentar todo el tratamiento de las evidencias desde su recogida, traslado, custodia, análisis y presentación.
- Esto es para dotar de fuerza o cualidad probatoria y consiste en probar que el indicio presentado en el juicio es realmente el mismo que fue recuperado en el lugar de comisión del hecho delictivo.

Cadena de Custodia

Documentada y detallada:

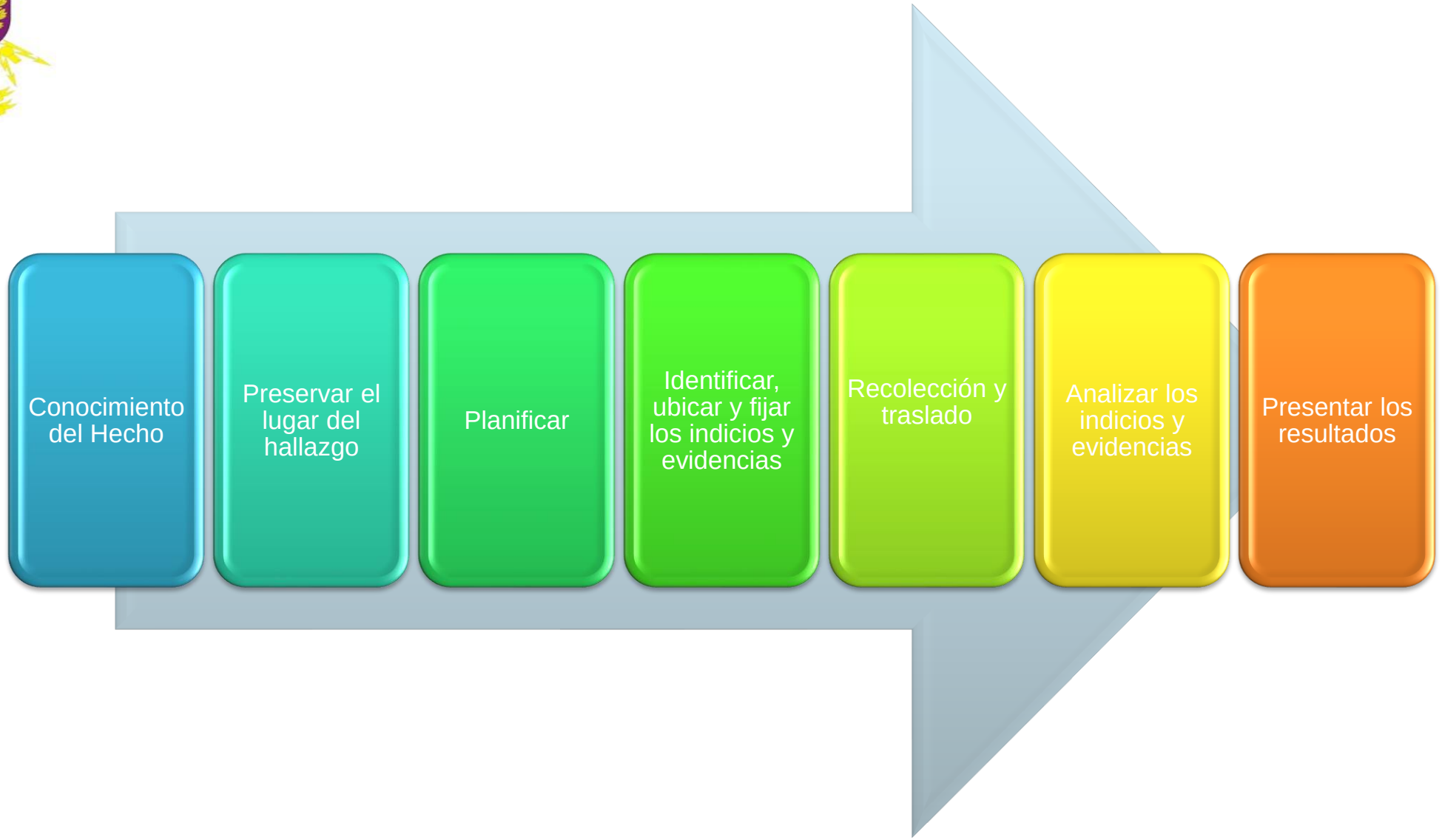
- Dónde, cuándo y quién **descubrió** y **recolectó** la evidencia.
- Dónde, cuándo y ¿quién **manejó** la evidencia.
- Quién ha **custodiado** la evidencia, cuánto **tiempo** y cómo la ha **almacenado**
- En el caso de que la evidencia cambie de custodia indicar cuándo y cómo se realizó el **intercambio**, incluyendo número de identificación, etc.

Secuencia según la LECRIM

- Artículo 297 LECrim: Obtención de manera legítima de las evidencias.
- Artículo 456 LECrim: Necesidad de personas formadas.
- Artículo 336 LECrim: Orden de reconocimiento por peritos (para obtener relación con el delito).
- Artículo 460 LECrim: Nombramiento de los peritos (por medio de oficio
- Artículo 475 LECrim: El objeto del Informe Pericial.
- Artículo 477 LeCrim: Estricto cumplimiento de las Garantías Legales (Secretario).
- Artículo 478 LeCrim: Aspectos que deben existir en los informes periciales (Descripción, Relación detallada de las operaciones y Conclusiones).

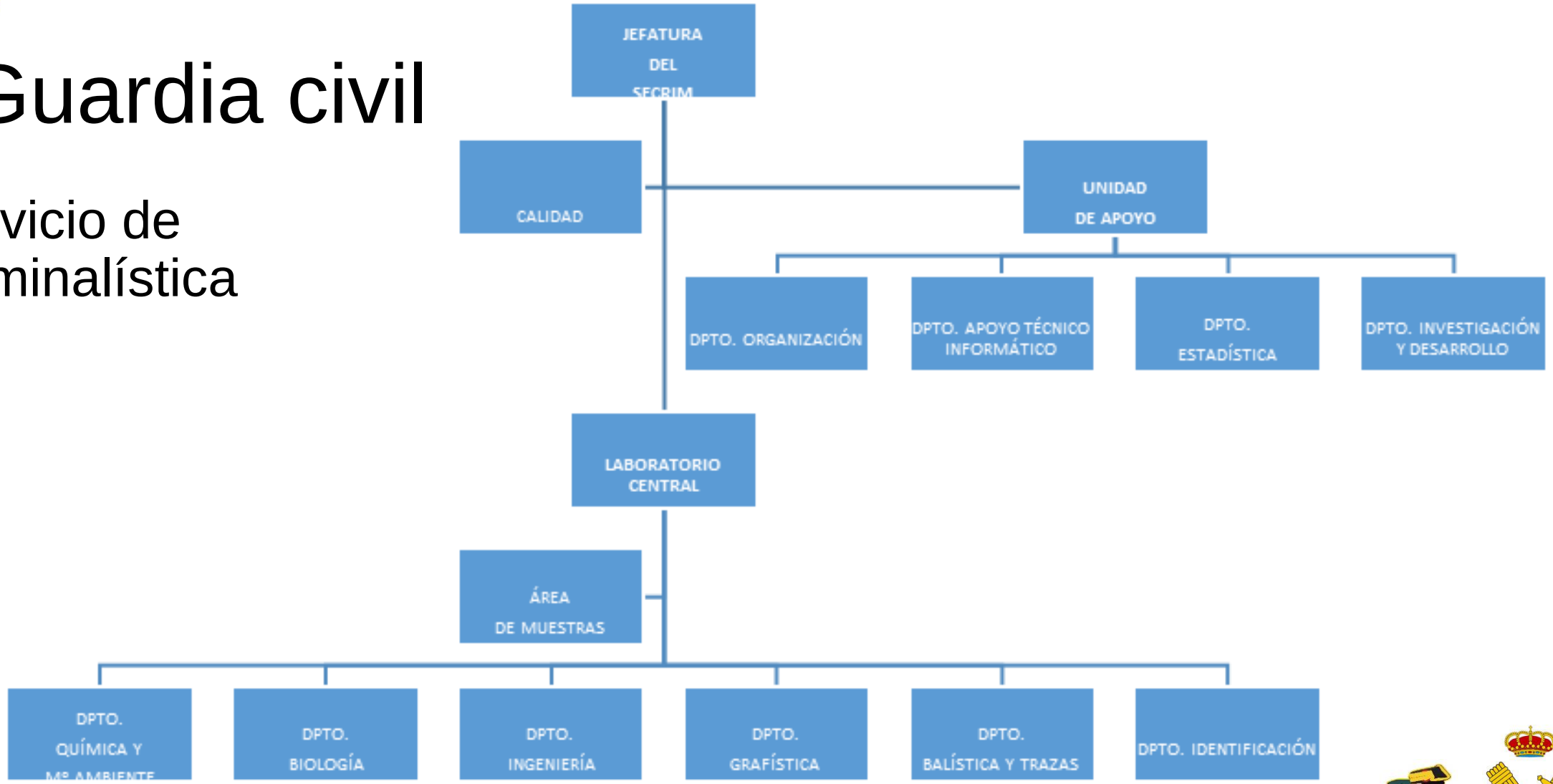
“Principio de Privacidad”

Sin un mandato Judicial no se podrá realizar el estudio de ninguna muestra recogida


Conocimiento del Hecho
Preservar el lugar del hallazgo
Planificar
Identificar, ubicar y fijar los indicios y evidencias
Recolección y traslado
Analizar los indicios y evidencias
Presentar los resultados

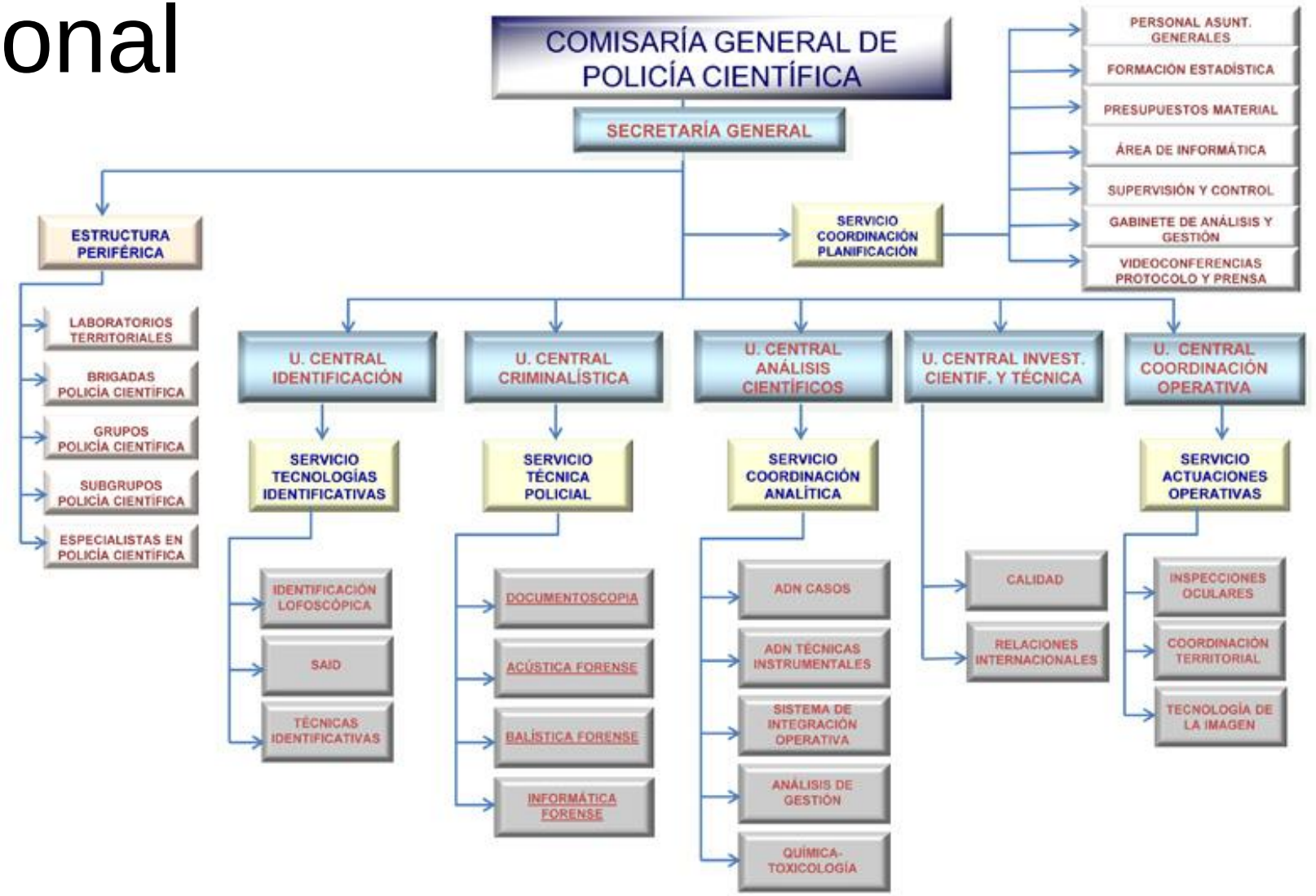
Guardia civil

- Servicio de Criminalística



Policía Nacional

COMISARÍA GENERAL DE POLICÍA CIENTÍFICA




HOY, EN LA TIRA DE LINUXHISPANO:
CHISTES DE INFORMÁTICOS
ESTO ES UN PUNTERO QUE LLEGA A UN RESTAURANTE Y LE DICE EL CAMARERO: "ME TEMO QUE SIN RESERVA NO VOY A PODER DARLE MESA"
JA JA JA
¿QUÉ LE DICE UN ORDENADOR GRANDE A UN ORDENADOR PEQUEÑO? - TAN PEQUEÑO Y YA COMPUTAS
JA JA JA
tira de linuxhispano.net
by danigm
POWERED BY TBO

ACADEMIA DE INGENIEROS

Seminario sobre ciberdelincuencia y evidencias digitales