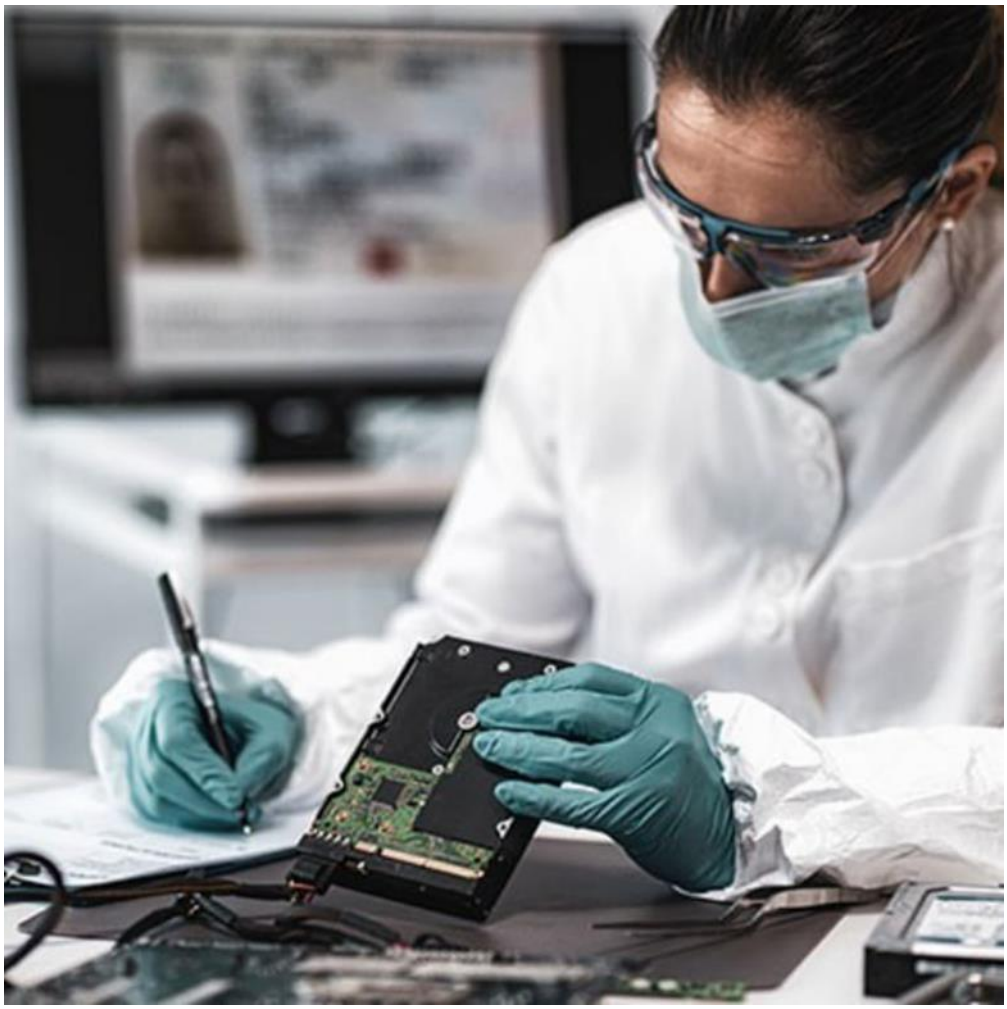
CURSO DE ESPECIALIACIÓN
CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

# Análisis Forense Informático

## Unidad 1. Metodología Forense



# Índice

# 1 Delito informático.

El exponencial progreso tecnológico que ha experimentado la sociedad en el último siglo ha supuesto una evolución en las formas de delinquir, dando lugar tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos.


Esta situación ha originado un debate en torno a la necesidad de distinguir o no los delitos informáticos del resto.

Un delito informático se puede definir de las siguientes maneras:

> *"Todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes"*
>
> **(Código Penal Español)**

> *"Los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos"*
>
> **(Convenio de Ciberdelincuencia del Consejo de Europa)**

# 2 Informática forense.

Se trata de la aplicación, en el ámbito IT, de técnicas científicas y analíticas especializadas para identificar, preservar, analizar y presentar datos que sean válidos en un proceso legal o investigación interna.

La "realización de un forense" se basa en la **investigación de un incidente de seguridad donde interviene información digital**.

Retos en Forense Digital

Los **principales retos** de esta investigación son:

- Las evidencias digitales son complejas.
- La densidad de los sistemas de almacenamiento cada vez es mayor y hay que tratar muchos más datos.

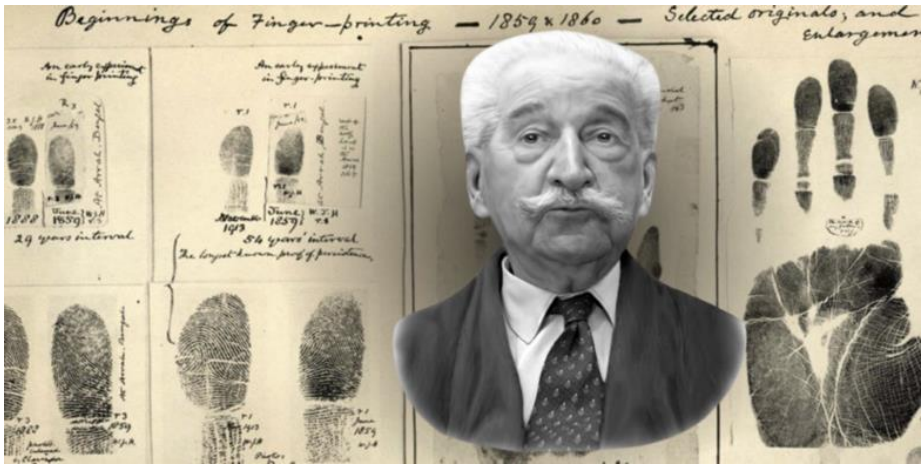
- La objetividad y conocimiento de los peritos y jueces.
- La inexistente estandarización de herramientas.
- El Cloud Computing dificulta el proceso forense, como veremos.
- Cada vez se utiliza más la encriptación, que dificulta o imposibilita la obtención de evidencias digitales.
- Uso de dispositivos SSD (Solid State Drive), que mueven la información y cambian el hash del dispositivo de forma autónoma. Los datos ya no residen siempre en el mismo espacio.
- ¿Es un arte o es una ciencia?
- Etc.

El video https://www.youtube.com/watch?v=2D5wTo1adbg explica muy bien las bases del forense digital

# 3 Principio de Locard

En 1910, un criminalista francés, el Doctor Edmun Locard (1877-1966), enunció lo que se convirtió en uno de los principios fundamentales sobre los que se ha basado la ciencia criminalística moderna, y el análisis forense digital por similitud.

"**Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto**" o, diciéndolo de una forma más sencilla, "**todo contacto deja un rastro**".




# 4 Incidente de seguridad.

Es un **evento adverso en el que algún aspecto de la seguridad** del ordenador puede estar amenazado. Pueden ser, por ejemplo:

- Pérdida de confidencialidad o integridad de los datos
- Interrupción del sistema.
- Interrupción o denegación de la disponibilidad de un servicio

**Ejemplos de incidentes de seguridad**:

1. Robo o fuga de información privada
2. instalación no autorizada de un programa espía que envíe información al exterior
3. Intrusión
4. Fraude
5. Ataque de malware
6. Spoofing de correo electrónico
7. Uso inapropiado de recursos
8. Accesos no autorizados a ordenadores corporativos
9. Violación de derechos de Propiedad intelectual

## 5 Análisis y/o proceso forense digital.

Como en los crímenes normales, también existen escenas del crimen y se llevan a cabo investigaciones en los crímenes digitales.

Por ello, es crítico realizar un análisis forense digital de los dispositivos relacionados con estos crímenes, con el fin de determinar la sucesión de eventos que han ocurrido en un sistema digital y que a su vez permitan formular hipótesis que se puedan validar o refutar, hasta resolver la investigación.

De forma simplificada, el proceso forense consta de las 5 fases siguientes, basadas en el principio de Locard, mencionado previamente:


Más detalladamente, la metodología utilizada en una investigación forense consta de las siguientes fases:


Fuente: https://www.hackingarticles.in/digital-forensics-an-introduction/

1. **Identificación del escenario**: Este es el primer paso que un investigador da en la escena del incidente. Hay que identificar el propósito de la investigación y reconocer las potenciales evidencias digitales.

   Una **evidencia digital** es una **pieza de información digital** guardada o transmitida entre uno o varios sistemas de información y que se puede utilizar como **prueba en un proceso judicial**.

2. **Preservación**: En este paso el investigador debe ir con cuidado, ya que debería asegurarse de que las pruebas no se han manipulado, lo que puede complicar la investigación.

   - **Asegurar la escena del incidente**: Se debe prohibir cualquier acceso a la prueba digital sospechosa, documentar todos los procesos y conexiones, desconectar las conexiones inalámbricas, etc. para mantener la evidencia segura.
   - **Limitar la interacción de la evidencia**: Hay que asegurarse de que la evidencia tiene una interacción limitada capturando la RAM o haciendo ataques "cold boot" sobre la evidencia.
   - **Mantener la cadena de Custodia**: La cadena de custodia es un registro de la secuencia en el que se recogieron las pruebas, fecha y marcas de tiempo en el momento de la extracción, el nombre del investigador que accedió a la evidencia y la manejó, etc.

3. **Adquisición ("collection")**: Este paso implica la adquisición de la evidencia de la forma más apropiada, intentando no causar ningún daño a la evidencia y empaquetarla en una bolsa de Faraday y/o antiestática. Metodologías básicas:

   - copia binaria
   - copia lógica
   - triaje...

4. **Examen ("examination")**: Este paso es un precursor para realizar cualquier análisis de la evidencia. Requiere una inspección esmerada de las pruebas para observar otros detalles secundarios. Por ejemplo, se filtran los ficheros sospechosos por:

   - Tipo
   - extensión o contenido
   - cadenas de caracteres que contiene, etc.

5. **Análisis**: En este paso, que se realiza en el laboratorio, el investigador lleva a cabo las tareas más cruciales como unir las partes y piezas de las pruebas, recuperar archivos eliminados, etc.

6. **Interpretación**: Este paso implica extraer conclusiones de la investigación tras la reconstrucción de la escena del incidente.

7. **Elaboración de un informe** Este paso normalmente implica preparar un informe detallado o un documento sobre toda la investigación. Es importante que durante todo el proceso se hayan tomado notas sistemáticamente.

8. **Presentación**: Se trata de un paso obligatorio sólo cuando se pide al investigador hacer una declaración. Esta debe hacerse en términos muy sencillos, para personas no técnicas, ya que muchas veces los jueces no entienden de tecnología.

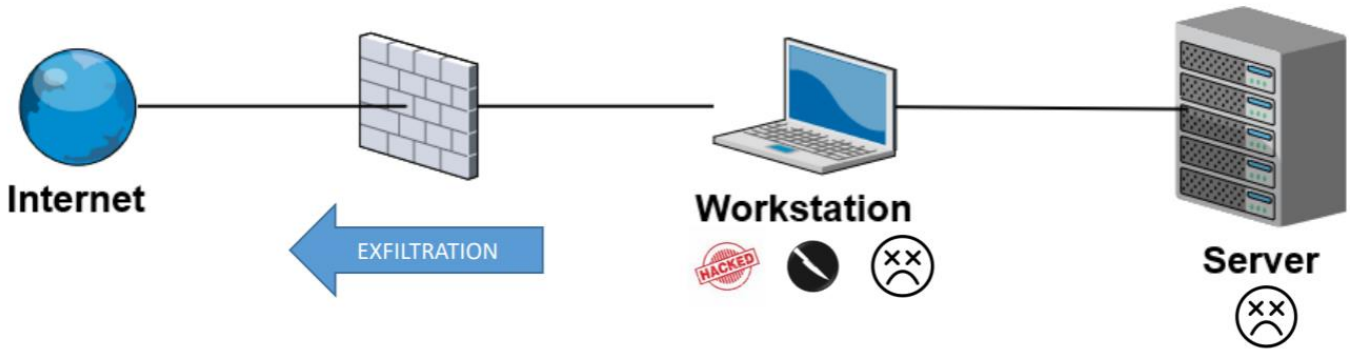
Tipos de investigaciones

De forma general, pueden diferenciarse dos tipos de investigaciones en este ámbito:

- **Investigaciones criminales:** aquellas que ocurren en el ámbito de un delito (civil o penal).
- **Investigaciones corporativas:** aquellas que persiguen una violación de la política
- corporativa (por ejemplo, acceso a contenidos no autorizados con recursos de la empresa). Algunas investigaciones corporativas pueden convertirse en investigaciones criminales.

La autoridad responsable de autorizar una investigación varía en función del tipo: para las investigaciones criminales suele ser necesaria una orden judicial, mientras que las investigaciones corporativas suelen estar reguladas por el departamento legal y el de recursos humanos de la empresa.

Finalmente, un aspecto importante que es necesario esclarecer en un incidente es el papel del equipo informático durante la fase de análisis, ya que puede ser la herramienta empleada para realizar el incidente o puede ser el objetivo del incidente. En otras palabras: ¿Es el arma del crimen o es el cadáver? ¿Y ambas?



# 6 Medios materiales para el forense.

Como forense digital, necesitaremos los siguientes medios materiales:

## 6.1 El laboratorio forense.

El puesto de trabajo principal de trabajo del forense informático. Las características del laboratorio forense incluyen:

- **Tamaño y ubicación** que irán en función del volumen de trabajo y el tipo de evidencias que se tratarán.
- **Lugar seguro** vigilancia continua y, a ser posible, con una única entrada.
- Se debe **registrar todos los accesos** en el laboratorio, en las evidencias, el material informático que entra y sale, etc.
- **Sistemas de seguridad**: cajas fuertes, alarmas, protección contra incendios y la falta de electricidad (UPS). Muy recomendable grabación de videovigilancia (sistema que usan los peritos informáticos como el Bruno Pérez Juncà).
- Áreas de trabajo **sin exposición en el exterior**, por ejemplo, sin ventanas. Aislado acústicamente.
- **Estaciones de trabajo offline para análisis de evidencias**: Son los equipos forenses. Estos equipos deben ser potentes (CPU, RAM, disco). Más información: https://www.ondata.es/recuperar/equipos-forensics.htm
- **Estaciones de trabajo online para consulta de documentación** por internet.

Ejemplo de laboratorio forense

## 6.2 Equipo forense para el laboratorio.

Orientativamente una estación de análisis forense debería tener las características (SUMURI TALINO KA-101, año 2022):

- Procesador Intel Core i9-10900X 3.7 GHz 10-Core LGA 2066
- Refrigeración líquida para la CPU que proporciona el máximo rendimiento de la CPU 32 GB de RAM DDR4 a 2666 MHz
- Un (1) SSD de 500 GB para el sistema operativo
- Un (1) SSD M.2 NVMe de 500 GB para archivos temporales y procesamiento Un (1) disco duro de clase NAS de 6 TB como evidencia
- Una (1) RTX 3050 con unidad de procesamiento de gráficos GDDR6 VRAM de 8 GB Una (1) bahía de intercambio en caliente de 2,5" con cuatro (4) bandejas extraíbles
- Una (1) bandeja de intercambio en caliente de 3.5" con cinco (5) bahías extraíbles Un (1) Blu-Ray 16x BD-R 4MB Cache SATA Blu-Ray Burner Lector de tarjetas forenses en el panel frontal
- Un (1) concentrador USB 3.0 de 4 puertos
- Un (1) concentrador USB 2.0 de 10 puertos Tableau T3iu Forensic Bridge
- Una (1) fuente de alimentación de 1200 vatios
- Ventiladores silenciosos de gama alta en todo el sistema (rodamiento de bolas de fluido hidráulico con una vida útil de 300,000 horas)
- Microsoft Windows 11 Pro de 64 bits


https://sumuri.com/product/talino-ka-review/

## 6.3 Equipo de respuesta (material portátil).

Cuando el perito tiene que salir, es necesario que lleve un conjunto de herramientas para hacer su trabajo. No hay un equipo único para todos los profesionales, y se hará según sus necesidades. El objetivo es tener lo necesario para recoger las evidencias digitales. La lista puede incluir:

- **Cámara digital**: Para tomar vídeo y fotos. Hay que desactivar el micrófono para no tomar audio que se podría llegar a usar en tu contra en caso de juicio si el lenguaje no es correcto.
- **Guantes de látex** para no dejar huellas dactilares y contaminar las pruebas.
- **Libretas de notas** donde podemos anotarlo todo y hacer un esquema o croquis de la escena de forma rápida.
- **Etiquetas** para sellar las evidencias y también para etiquetar todo correctamente.
- **Papel para embalar y bolsas antiestáticas**, para evitar la pérdida de datos en sistemas de almacenamiento magnéticos por culpa de la electricidad estática.


Bolsas antiestáticas

- **Medios de almacenamiento**, como SSD y pendrives USB.
    - Siempre se debe intentar NO apagar las máquinas y obtener datos como logs, volcado de RAM y datos de los usuarios.
    - Después se puede hacer la imagen forense y para ello se necesita aún más espacio de almacenamiento.
    - Los dispositivos deben estar "limpios" (reiniciados a 0 en todas sus posiciones de memoria).
- **Dispositivos para bloquear la escritura físicamente**
    - Se utiliza para poder leer los dispositivos sin escribir accidentalmente o por parte del sistema operativo (por ejemplo, lo hace automáticamente para actualizar la fecha de acceso a los archivos).
    - Por ejemplo Tableau TK8u USB 3.0 forensic bridge (https://www.guidancesoftware.com/tableau/hardware/t8u)


Placa USB 3.0 TK8u

- **"Distro" forense**
    - Se pueden utilizar como alternativa económica a los dispositivos hardware (clonadoras y bloqueadores de escritura).
    - Estas distros cargan todos los dispositivos en modo solo lectura (RO=Read Only).

- **Material para proteger de radiación electromagnética**, por ejemplo, hoja de aluminio, bolsas de Faraday, etc.
    - En particular para evitar que un usuario remoto pueda borrar su móvil o portátil vía radio. Además, hay que poner el dispositivo en modo avión si se tiene acceso a la configuración.


Bolsas de Faraday

- **Juego de destornilladores y herramientas de precisión** para desmontar dispositivos de almacenamiento y otros. Con diferentes formatos de cabeza de tornillo (estrella, plano, philips, hexagonal, etc.)
- **Otros materiales**, como cables de alimentación, cables de datos, hub USB, tornillos, teclado, ratón, un TAP (Test Access Point) si hacemos investigación de red, etc.


TAP de red

Más información sobre Network TAP - https://www.gigamon.com/products/access-traffic/network-taps.html

- **Portátil forense**, con todo el software actualizado. También con copias de todos los documentos que se utilizan en formato digital (formularios y referencia). También con las aplicaciones necesarias.


SUMURI TALINO KA-L Alpha https://sumuri.com/product/talino-ka-l-alpha/

- **Sistemas de Encriptación o cifrado**, para guardar las evidencias protegidas a nivel lógico.
- **Claves de seguridad** del software que sea comercial, tanto software como hardware (claves hardware).
- **Caja** para llevarlo todo (estilo "pelicano") y proteger de humedad y rotura, con relleno de espuma protectora.

https://fulcrum.net.au/product/pelican-cases

## 6.4 Material forense.

Dentro del laboratorio deberíamos disponer, aparte de las estaciones forenses:

**Hardware:**

- Cables y discos duros
- Tarjetas gráficas
- Adaptadores o docks, etc.
- Clonadoras de disco en hardware.
- Dispositivos de almacenamiento (pendrives, discos duros, discos SSD ...)

**Software:**

- Diferentes Sistemas operativos
- Software forense (Ver al siguiente punto)
- Software ofimático: editor por informes, hojas de cálculo, etc.

**Ejemplos de Software forense de código abierto**

Distribuciones de código abierto como, por ejemplo:

- **Tsurugi Linux** - proyecto DFIR open source. Soporta investigaciones DFIR, análisis de malware y actividades OSINT. Tiene una versión Live por adquisición. También tiene una sección de investigación de Visión por computador - https://tsurugi-linux.org/
- **SIFT Workstation**: Máquina virtual Ubuntu con múltiples herramientas forenses. Gratuito - https://www.sans.org/tools/sift-workstation
- **Suite forense de paladín**: distro Linux live basada en Ubuntu con algunas herramientas forenses open source en una interfaz llamada "Paladin toolbox". Gratuito - https://sumuri.com/software/paladin/
- **CAINE**: Computer Aided Investigative Environment (CAINE) proyecto de forense digital con una GUI y muchas herramientas forenses open source - https://www.caine-live.net
- **Kali Linux**: Distribución Linux basada en Debian creada para tareas de ciberseguridad. Dispone de una opción para arrancar en modo forense (sólo lectura) - https://www.kali.org
- Pequeño curso sobre las distros - https://academy.cyber5w.com/courses/take/introduction-to-linux-distributions/pdfs/23646112-introduction-to-linux-forensics-distros

Herramientas de código abierto:

- **Autopsy**: Conjunto de herramientas forenses gratuitas que permiten un examen forense completo - https://www.sleuthkit.org/autopsy/
- **Guymager** - Adquisición de imágenes dd, E01, AFF. Muy rápido (aprovecha multi cpu) - https://guymager.sourceforge.io/
- Más información: 15 herramientas forense - https://www.guru99.com/computer-forensics-tools.html

**Software forense con licencia propietaria**

Algunas herramientas de licencia propietaria (por Windows):

- **X-Ways Forensics**: https://www.x-ways.net/
- **EnCase**: https://www.guidancesoftware.com/encase-forensic
- **Forensic Toollkit (FTK)**: https://accessdata.com/products-services/forensic-toolkit-ftk
- **Forensic Explorer (FEX)**: http://www.forensicexplorer.com/
- **Belkasoft Evidence Center**: https://belkasoft.com/ec
- **Axiom**: https://www.magnetforensics.com/products/magnet-axiom/

## 6.5 Conceptos importantes.

**Las evidencias digitales**

Son los "rastros" a los que se hace mención en el principio de Locard. Algunas evidencias digitales que buscamos en la escena del incidente para nuestra investigación forense son:

- Ordenadores, portátiles
- e-mails
- Objetivos multimedia
- SIM
- HDD, SDD
- USB, discos flash
- PDA's, tablets
- Logs
- Historial del navegador web

Cualquier tipo de información puede representarse de forma digital en un conjunto de bytes atendiendo a distintos formatos y estructuras: texto, audio, vídeo, imágenes, aplicaciones, etc. La persistencia de dicha información en un conjunto de bytes se conoce como archivo o fichero.

Una **investigación digital** es el examen realizado sobre una evidencia digital, motivado por la relación existente entre el dispositivo del que se obtuvo dicha evidencia con el incidente objeto de estudio. La investigación se lleva a cabo desarrollando una serie de hipótesis de lo ocurrido y buscando evidencias que refuten dichas hipótesis.

Una **evidencia digital** es un objeto digital que contiene información fiable que apoya o refuta una hipótesis, de forma que pueda ser utilizada en una investigación. Desde el punto de vista legal, es cualquier información probatoria almacenada o transmitida en formato digital, que cualquiera de las partes presenta como prueba ante un tribunal.

Por tanto, una **investigación forense digital** es un **proceso que utiliza la ciencia y la tecnología para analizar los objetos digitales recopilados**, desarrollando hipótesis y comprobando teorías para ser llevadas ante un tribunal, pudiendo contestar a las preguntas referentes a lo ocurrido.

El **tratamiento** (obtención, proceso y almacenamiento) **de las evidencias digitales es de suma criticidad durante una investigación**. Se deben extremar las precauciones de modo que el investigador no cometa alguna acción que anule la validez de la evidencia ante un tribunal.

**Tipos de investigaciones forenses digitales**

- Forense de sistemas (Linux, Windows, etc.)
- Forense de memoria
- Forense de dispositivos móviles
- Forense de redes
- Forense de Internet y nube
- Forense de IoT
- Etc.

**Forense digital vs Antiforense**

- **Forense digital:** Se trata de descubrir información sobre actividades ilegales de un usuario
- **Anti Digital Forensics o ADF:** Se trata de conseguir que no se pueda obtener esta información sobre actividades ilegales de un usuario usando técnicas como:
    - Manipular, borrar, ofuscar datos digitales
    - Hacer difícil el estudio de las evidencias, que consuma mucho tiempo y sea virtualmente imposible

**Qué son los datos y metadatos**

Es muy importante diferenciarlas para nuestro forense digital. Sus definiciones son:

- **Datos**: Cualquier información almacenada en la memoria de un dispositivo, importante para los usuarios. Normalmente se encuentra en crudo (raw) y sin procesar por el sistema operativo. Ejemplo: El contenido de un documento escrito por el usuario.
- **Metadatos**: Describe y da información sobre los datos. Siempre es procesado por el sistema. Ejemplo: El tipo de un fichero, el tamaño, el nombre, extensión, etc.

**Buenas prácticas en forense digital**

- **Documentación exhaustiva:** Hay que tomar notas durante todo el proceso.
- **Preservación de las evidencias:** Hay que asegurar su integridad.
- **Formación continua:**
    - Realización de cursos sobre análisis forense
    - Estudio de nuevas técnicas y herramientas
    - Recursos web y revistas especializadas
    - European Network of Forensic Science Institutes
- **Conducta profesional:** Hay que mantener en todo momento
    - Integridad
    - Confidencialidad
    - Ética
    - Moral

# 7 DFIR vs peritaje forense.

Tanto el DFIR como el peritaje informático, comparten el **análisis forense como disciplina central**. El análisis forense permite determinar el origen y las causas de un incidente de seguridad.

- En el caso de tratarse del ámbito DFIR, se quiere **cortar de forma rápida el incidente** y tomar medidas para la ejecución de la investigación para **evitar que se repita** en el futuro.
- En el caso del peritaje informático, se quiere **convertir las evidencias analizadas en pruebas válidas** en un procedimiento judicial.

## 7.1 Definición de DFIR.

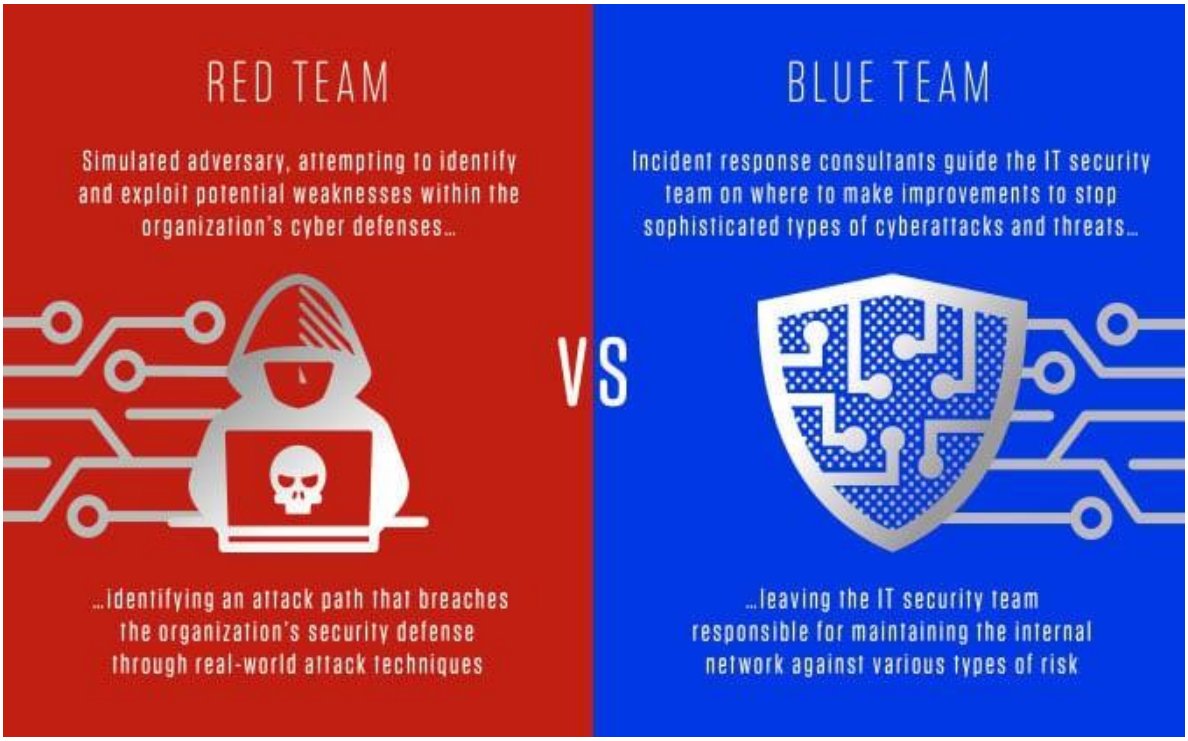
Las siglas DFIR corresponden a **Digital Forensics Incident Response**.

- La "respuesta ante incidentes", se define como aquella disciplina que pretende **detener rápidamente un incidente de seguridad, determinar su origen y alcance y establecer mejoras para evitar que el mismo vuelva a repetirse**.
- Un incidente de seguridad puede afectar gravemente a la organización e impactar en su política de protección de datos, pudiendo llegar incluso a ser sancionada.
- Se respetarán las directrices legalmente establecidas en la normativa de seguridad de la información:
    - **Reglamento General de Protección de Datos (RGPD)**, aprobada por el Parlamento Europeo y el Consejo de la Unión Europea
    - **Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD)**, transposición a la legislación española del RGPD (Ley orgánica 3/2018, de 5 de diciembre).

Cuando se descubre un incidente de seguridad, la organización, sobre la base de su política de seguridad, intentará:

- en primer lugar, detenerlo
- en segundo lugar y, normalmente, en paralelo, descubrir su origen y evitar que vuelva a producirse.

Para ello, lo más habitual es que se encargue al **"Blue Team"**, un equipo de especialistas en ciberseguridad de la organización, el análisis y resolución del incidente de seguridad. Se aplican técnicas de forense digital.




https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/

Este proceso de **análisis y resolución se produce "al vuelo"**, es decir, sobre las mismas evidencias afectadas por el incidente.

- Se produce, una **"contaminación" de las evidencias** por parte de los analistas de ciberseguridad, que impedirá, con una probabilidad muy alta, que estas evidencias puedan llegar a ser válidas en un procedimiento judicial.
- En el caso de un incidente de seguridad muy grave, con una importante afectación en la organización, especialmente si existen varias decenas o centenares de máquinas afectadas, lo **prioritario para la organización será la resolución del incidente** y no la judicialización de este.

En cualquier caso, una vez resuelto el incidente:

- Si se consigue determinar su origen y se desea presentar una denuncia contra los responsables (por ejemplo, una empresa de la competencia), seguramente las evidencias no podrán convertirse en pruebas.

- La parte denunciada, probablemente alegará, a través de su defensa y sobre la base del informe pericial de un perito informático, que las evidencias fueron contaminadas en el proceso de resolución del incidente.

## 7.2 Definición de Peritaje informático.

El peritaje informático, a diferencia de la "respuesta ante incidentes", no pretende, al menos de manera genérica, detener un incidente de seguridad.

El objetivo del peritaje informático es la **conversión de una evidencia informática en una prueba informática**.

- Cuando una organización, o un particular, advierten que determinada información que se encuentra en una evidencia informática (un disco duro, una memoria de almacenamiento masivo, un DVD, un terminal móvil, etc.), es vital para la resolución favorable de un conflicto, es fundamental que esta información entre, de alguna manera, en el procedimiento judicial como prueba.
- Para ello, deben contratarse los servicios de un **perito informático** que, mediante un procedimiento estandarizado de identificación, adquisición y análisis de la evidencia, la convertirá en una prueba, certificando que la información que contiene no ha sido alterada.

Para evitar que la evidencia sea contaminada:

- El primer paso deberá ser la realización de una **adquisición** de la misma **ante fedatario público (notario o secretario judicial)**, sin que la evidencia original sea accedida, en ningún momento, por el perito informático.
- El **fedatario público** anotará en su acta o diligencia, que el perito informático conecta la evidencia a una herramienta forense determinada para llevar a cabo el vuelco o clonación de la información, sin entrar a analizar la misma.
- Al final del proceso, el fedatario público anotará en el acta o diligencia la **huella digital (hash)** de la evidencia original.

Finalmente, para llegar a la constitución de la prueba, el perito informático, habitualmente (aunque no siempre, ya que dependerá de cada caso particular), realizará un análisis forense al volcado de la evidencia.

- Este **análisis forense podrá determinar el origen y las causas** del incidente de seguridad
- Se plasmará todo el procedimiento en un **informe pericial informático** que deberá ser ratificado ante la autoridad judicial.

## 7.3 Metodología del DFIR.

En la "respuesta ante incidentes" se trabaja:

- Sobre **sistemas o máquinas "vivas"**, es decir, en funcionamiento, necesitándose una respuesta, habitualmente, muy rápida, para encontrar el origen del problema y una solución.

- Es necesario utilizar programas informáticos capaces de realizar lo que se denomina como **"triaje"**, es decir, obtención rápida de información vital del sistema que, posteriormente, pueda ser analizada por el perito informático.

- Los **programas de triaje**, pueden ser ejecutados desde la memoria RAM de la máquina, con el fin de dejar el menor rastro posible.

- También se pueden llegar a realizar **capturas o volcados de la memoria RAM**, que podrán ser analizados posteriormente con herramientas como **Volatility**, con el fin de determinar los procesos en ejecución en el sistema, determinar la información que estuvieran obteniendo y enviando al exterior y/o las acciones que estuvieran ejecutando en perjuicio del sistema.

Existen **suites informáticas** muy útiles para técnicas **DFIR**:

- NirSoft
- BriMor Labs
- Programas de propósito específico como Bulk Extractor o MFTDump, entre otros.

La ejecución de cualquiera de estas herramientas deja **rastro en el equipo analizado**, por lo que el perito informático tendrá que ir con mucho cuidado.

Es muy importante señalar que:

- El **mantenimiento de la cadena de custodia es muy dificultoso** utilizando técnicas DFIR, ya que es necesario trabajar con las máquinas directamente
- El trabajar con equipos e instalar programas en las mismos, **contamina las evidencias e implica la pérdida de la cadena de custodia de las mismas**, por lo que judicializar el procedimiento será difícil o, más concretamente, será muy difícil que esta judicialización prospere, ya que siempre habrá enfrente un peritaje informático que señale que las evidencias fueron contaminadas durante el análisis forense.
- Si un perito informático utiliza técnicas DFIR para la realización de un análisis forense, podrá ser acusado por la parte contraria, de haber alterado las evidencias al trabajar directamente sobre las mismas, por lo que se hace necesaria la adopción de medidas de carácter técnico y legal para que el profesional quede cubierto, como la firma de un acuerdo de descarga de responsabilidades con la parte contratante.

Si no se puede detener el negocio y se desea acudir a los tribunales, lo más importante es que los analistas DFIR encargados de la detección y resolución del incidente, aíslen al paciente cero y seguidamente, el perito informático procederá a protocolizar la situación.

## 7.4 Metodología del Peritaje.

En el peritaje informático se trabaja:

- Habitualmente, **con sistemas "muertos"**, es decir, apagados.
- Se **extraen los dispositivos** y se procede en equipos externos.
- Las **evidencias deben ser adquiridas o clonadas ante un fedatario público** (habitualmente, un notario, aunque también podría ser un secretario judicial), que otorgue fe de la huella digital de las evidencias y garantice la preservación de la cadena de custodia en el marco del peritaje informático.
- **Nunca se puede trabajar directamente con las evidencias originales**.

La huella digital sólo garantiza la cadena de custodia de la evidencia desde el instante en que se calcula, no antes, por lo que un agente externo (de confianza, como un notario, aunque podría ser un aplicativo certificado), debe **certificar ese instante de tiempo**.

El perito informático no podrá ser acusado de haber manipulado la evidencia:

- Siempre que exista un **registro fechado mediante fe pública**, de la fecha en la que se calculó la huella digital.
- También es necesario que **la evidencia se demuestre no alterada al recalcular la huella digital** sobre la evidencia original.

En este caso, el perito informático realiza la clonación de las evidencias y trabaja con copias idénticas de las mismas para la realización del análisis forense y del posterior peritaje informático.

- Las herramientas utilizadas **no deben contaminar las evidencias**.
- Es **habitual "montar" los volúmenes**, obtenidos de los discos duros o pendrives originales, o de cualquier otra evidencia, en **modo de "sólo lectura"**.
- Posteriormente serán indexados en herramientas como **Autopsy, OsForensics, X-Ways o EnCase.**

Para la realización del peritaje informático, es aconsejable seguir **diversos estándares de realización de análisis forense e informes periciales informáticos**.

En sistemas Windows, es aconsejable analizar también artefactos como la MFT, el registro de Eventos, el Registro, las Shellbags, el Prefetch, las "Shadow Copies" o el timeline.

## 7.5 Resumen de diferencias.

| DFIR | Peritaje forense |
|---|---|
| **Objetivo: respuesta muy rápida, para encontrar el origen del problema y una solución** | **Objetivo: la conversión de una evidencia informática en una prueba informática** |
| **Se trabaja sobre sistemas o máquinas "vivas" o encendidas** | **Habitualmente, con sistemas "muertos" o apagados** |
| **Programas de "triaje" (obtención rápida de información vital del sistema)** | **Adquisición o clonación ante notario o secretario judicial** |
| **Difícil mantener cadena de custodia (recomendable hacerlo)** | **Obligatorio mantener cadena de custodia** |
| **Se contamina la evidencia en vivo, difícil de judicializar** | **No hay que contaminar las evidencias (montar en solo lectura)** |

# 8 Referencias.


- DFIR vs peritatge - https://peritoinformaticocolegiado.es/blog/diferencias-entre-la-respuesta-ante-incidentes-dfir-y-el-peritaje-informatico/
- Peritos judiciales informáticos - https://peritosinformaticos.es/carta-denuncia-de-la-bsa-peritacion-de-software-ilegal/
- introducción al forense digital
    - https://www.hackingarticles.in/digital-forensics-an-introduction/
    - https://www.hackingarticles.in/digital-forensics-an-introduction-part-2/
- https://github.com/mikeroyal/Digital-Forensics-Guide
- **RFC 3227** Directrices para recuperar evidencias - https://www.incibe.es/incibe-cert/blog/rfc3227
- 2024 mikeroyal/Digital-Forensics-Guide: Guía forense digital. Aprenda todo sobre análisis forense digital, análisis forense informático, análisis forense de dispositivos móviles, análisis forense de redes y análisis forense de bases de datos. https://github.com/mikeroyal/Digital-Forensics-Guide