

Introducción al Análisis Forense Informático

Mariano Sánchez Martín (a partir de
un original de Rafael López García)



GOBIERNO
DE ESPAÑA

MINISTERIO
DE EDUCACIÓN
Y FORMACIÓN PROFESIONAL



Unión Europea-
NextGenerationEU



XUNTA
DE GALICIA

INSTITUTO EDUCACIÓN
SECUNDARIA
SAN CLEMENTE

Orígenes de la disciplina forense

- Avanza y se hace más científica desde la Ilustración hasta madurar en el s. XX ([ver](#))
 - [Traumatología](#), [toxicología](#), [antropometría](#), [huellas dactilares](#), [test de Uhlenhuth](#), [ADN](#), etc.
- [Edmond Locard](#) (1877-1966)
 - Criminólogo francés que fundó el primer laboratorio policial en Lyon, Francia, en 1910
 - Autor del libro “*Manual de Técnica Policiaca*”

Principio de intercambio de Locard

*Todo contacto
deja un rastro*

Si hay contacto entre dos elementos, habrá un intercambio



Fuente de la imagen: <https://www.facebook.com/CapacitacionCienciasForenses>

Parte I: Definición de Análisis Forense Informático

Definición de Análisis Forense Informático (I)

- *“La informática forense es el proceso de identificar, preservar, analizar y presentar las evidencias digitales de una forma legalmente aceptable”*
 - Rodney McKemmish, 1999. [[ver](#)]



Definición de Análisis Forense Informático (II)

- Aplicación de técnicas y procedimientos científicos y analíticos especializados a **infraestructura tecnológica**
 - O bien porque dicha infraestructura ha sufrido un **incidente de seguridad informática**
 - P. ej.: Hackean un servidor y roban datos empresariales
 - O bien es un **delito cuya resolución depende de la tecnología empleada por sus actores**
 - P. ej.: Verificar una coartada a través de un móvil

Tipos de infraestructura (I)

- PC
 - Windows
 - GNU/Linux
 - MacOS
- Dispositivos móviles
 - Android
 - iOS
- Dispositivos de Red
 - Redes Ethernet
 - Redes Wifi
- Dispositivos IoT
 - Wearables
 - Videoconsolas
 - SmartTV
- Sistemas Cloud
 - AWS
 - Azure
 - Google Cloud
- Disp. almacenamiento

Tipos de infraestructura (II)

- Impresoras
- Dispositivos industriales (OT)
 - Scada
 - Human-Machine Interface (HMI)
 - PLC
 - Sistemas de telecomunicaciones
- Software
 - SO
 - Apps
- Datos:
 - Documentos
 - Multimedia
 - BD

Dos enfoques del Análisis Forense Informático

- En muchas ocasiones su misión es **presentar evidencia ante un Tribunal** de Justicia
 - Casos de competencia desleal, fuga de información, incumplimiento de contrato, plagio, acoso, fraude financiero, investigación de seguros, homicidios, secuestros, pornografía infantil, ciberterrorismo...
- En otras ocasiones trata de **analizar un incidente**
 - En este módulo **no se trata de responder al incidente**
 - No trata de contenerlo, solucionarlo y recuperar el sistema
 - DFIR (Digital Forensics Incident Response)

Objetivos

- Investigación de incidente de seguridad
 - ¿Quién nos ha atacado?
 - ¿Cuándo se ha producido el ataque?
 - ¿Cómo se ha producido?
 - ¿Qué vulnerabilidad se explotó?
 - ¿Qué hizo dentro del sistema?
 - ¿Dónde?
- En caso de delitos
 - ¿Existe información relevante en el dispositivo?
 - ¿Dónde estaba en el momento del delito?
 - ¿Qué conversaciones mantuvo?
 - ¿Qué archivos descargó / visualizó / creó?
 - ¿Qué programas usó?
 - ¿Qué periféricos usó?

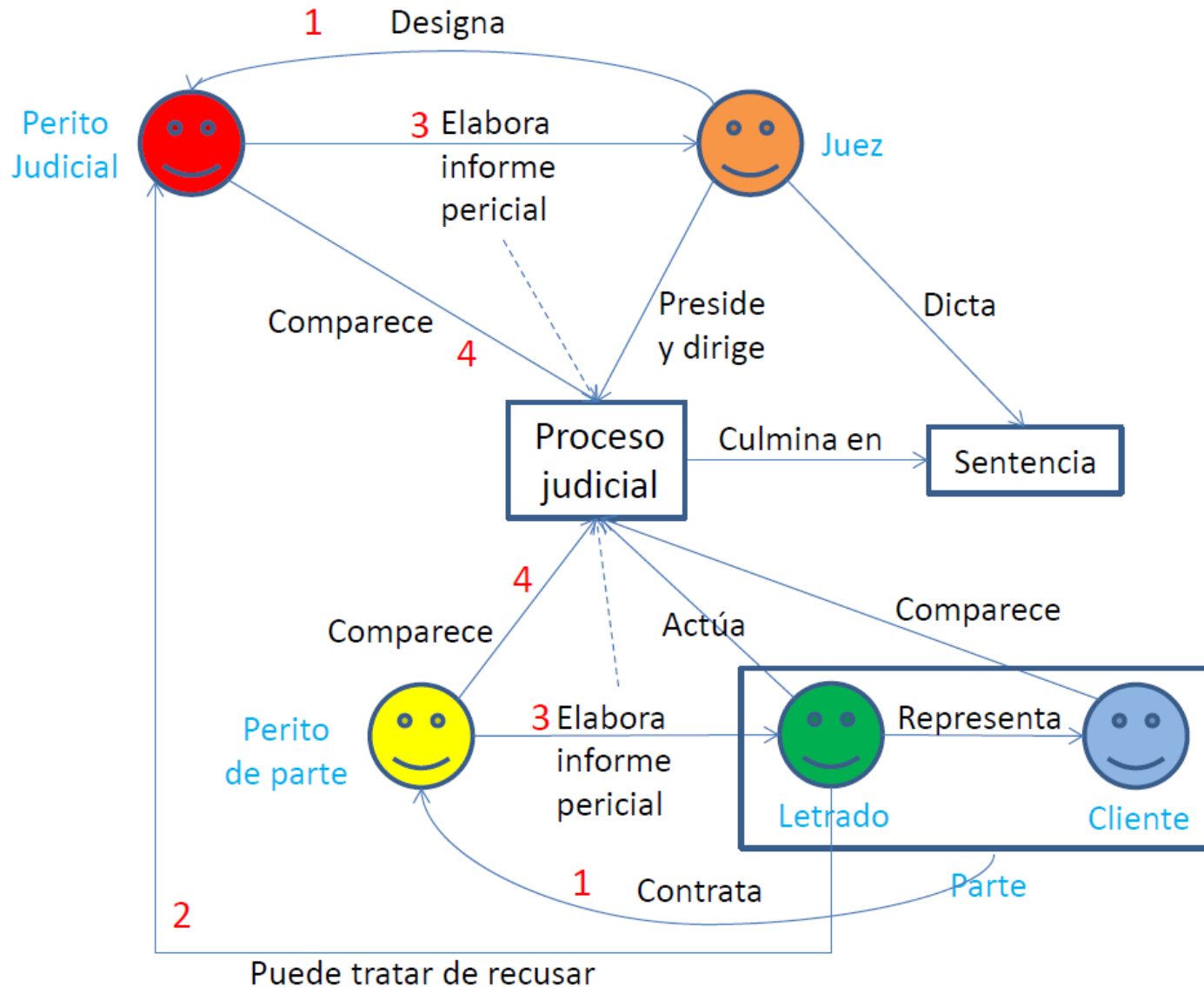
Parte II: El Perito Judicial

Función principal del perito

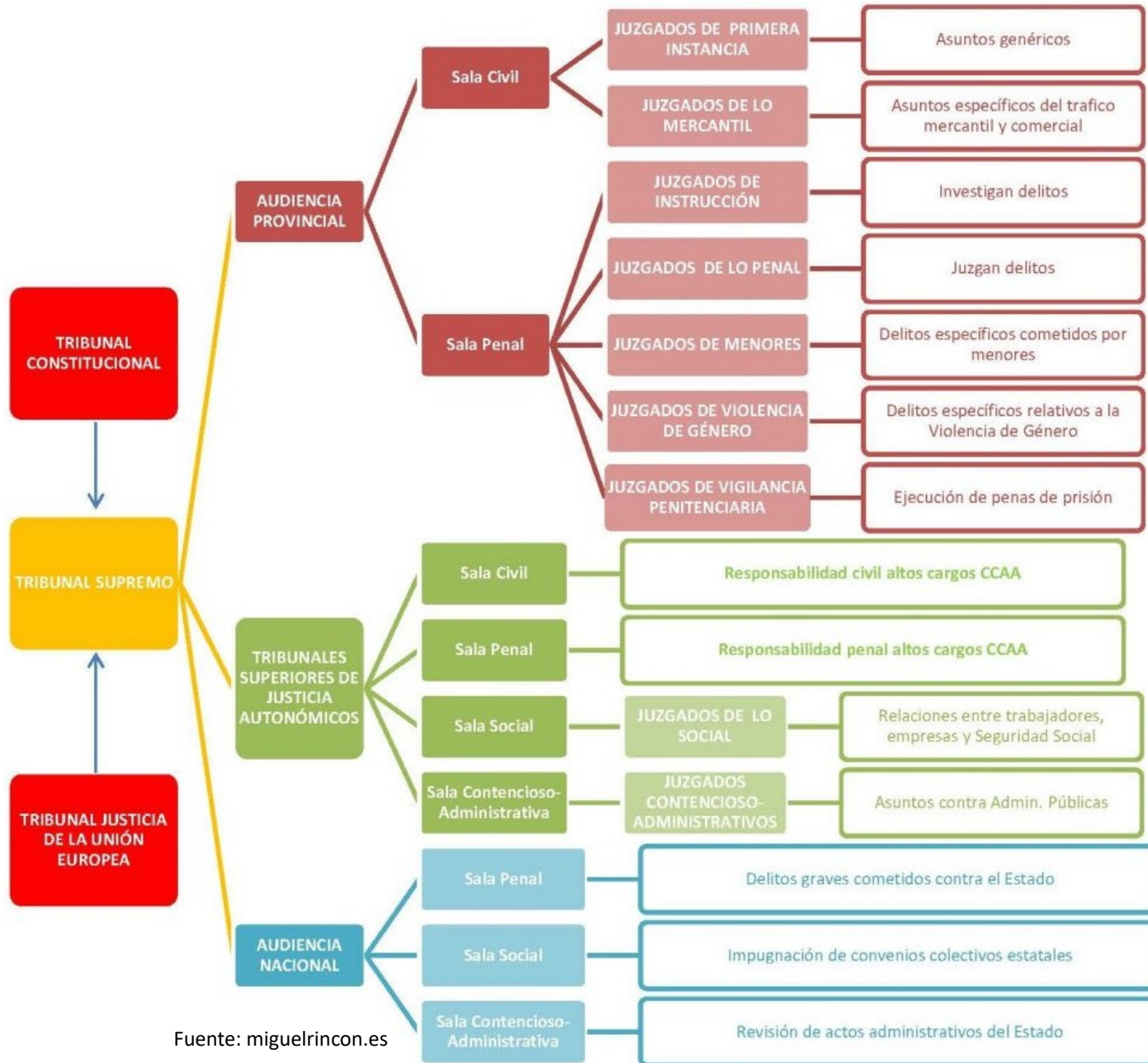
- **Su misión es suministrar información u opinión fundada a los tribunales de justicia**
- El 85% de los procesos penales en la UE incorporan pruebas con componente electrónico.

<https://www.consilium.europa.eu/es/policies/e-evidence/#>

Proceso



Los Tribunales de Justicia



El caso penal y el caso civil: diferencias

- El **derecho civil** contempla las relaciones entre personas físicas y/o jurídicas. Mientras que el **derecho penal** pone al imputado contra la sociedad cuando infringe la ley.
- En un **caso penal**, el acusado puede ser condenado a **multas muy elevadas** o incluso a la **cárcel**. Un caso civil se puede resolver con una negociación económica o bien una sanción impuesta por el juez. En el **caso civil** el condenado **no va a prisión**.
- La ley penal es la que castiga los delitos. Para que una persona sea declarada culpable de haberlos cometido, la fiscalía tiene que demostrarlo.

Historia de los peritos (I)

- ¿Fue el primero Arquímedes de Siracusa?
- Ya eran usados en juicios en la antigua Roma
 - Para disputas de lindes de tierras, embarazos, etc.



Historia de los peritos (II)

- Después se van extendiendo a otras áreas
 - P. ej.: caligrafía
- En la Edad Media en España aparecen los peritos especializados en Medicina Forense
 - La Inquisición (infanticidio, abortos, etc.)
- En el entorno industrial, el título en España se crea en el R.D. del 17 de agosto de 1901
 - Conde de Romanones

El perito judicial (I)

- El perito judicial civil se recoge en la [Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil](#)
 - Sección 5ª, arts. 335-352
- El perito judicial criminal se recoge en el [Real Decreto de 14 de septiembre de 1882](#) por el que se aprueba la Ley de Enjuiciamiento Criminal (LECrim)
 - arts. 456-485, 661-663, 723-725 y 334-367

El perito judicial (II)

- También hay peritos en lo social ([Ley 36/2011, de 10 de octubre](#)) y en lo contencioso-administrativo ([Ley 29/1998, de 13 de julio](#))
 - Sin embargo, la legislación sobre peritos es escasa y se suele seguir la Ley de Enjuiciamiento Civil siempre y cuando no contradiga a las otras
- En los siguientes apartados nos centraremos más en los peritos según la LEC
 - Aunque en muchos aspectos la LECrim es similar

Requisitos de los peritos judiciales

- Poseer el **título oficial** en la materia
 - O ser *personas entendidas* si no hay título oficial
- Promesa de **decir la verdad** y actuar con la mayor **objetividad** posible
 - Tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a las partes
- **Conocer las sanciones** penales en las que podría incurrir si incumple su deber

Funciones de los peritos

- **Formular dictamen escrito**
 - Acompañar de documentos o instrumentos o materiales adecuados
- **Intervenir en el juicio**
 - Exposición del dictamen
 - Explicación del dictamen
 - Respuesta a preguntas y objeciones
 - Respuesta a solicitudes de ampliación
 - Crítica del dictamen de la parte contraria
 - Formulación de tachas (advertencia al tribunal de la posibilidad de la parcialidad del perito, no supone perito inhábil)

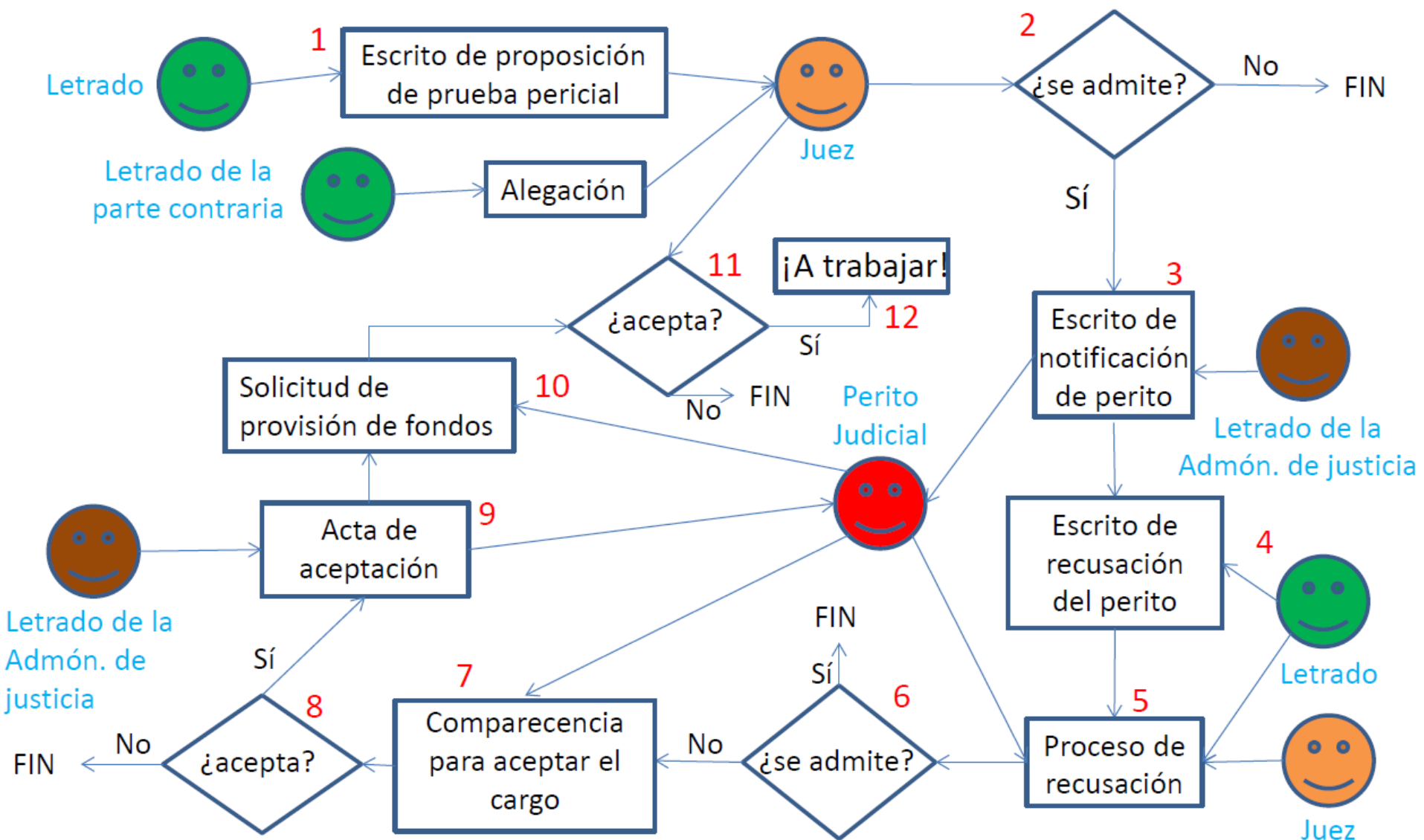
Habilidades de los peritos

- Aseguramiento de la escena
- Recolección de pruebas
- Preservación de pruebas
- Manejo de la cadena de custodia
- Análisis de evidencias
- Generación de dictámenes
- Conocimiento legislativo

Nombramiento del perito (I)

- Peritos nombrados **judicialmente**
 - A partir de una lista de titulados creada por el Colegio profesional o asociación similar
 - Pueden ser recusados
 - Pueden excusarse de participar
 - Bajo **causa justificada** (p. ej.: no tener conocimiento o experiencia suficiente en la materia)
 - **Si no se le asigna la provisión que solicite** en plazo
 - Sólo civil, en penal el juez pide los medios y se cobra al final

Nombramiento del perito (II)



Nombramiento del perito (III)

- Peritos nombrados **por una o ambas partes**
 - Tienen que ser aceptados por el juez o fiscal
 - No necesitan ser titulados
 - Pueden ser tachados por nepotismo, etc.
 - Tachado significa que **no se le recusa** aunque sí se tiene en cuenta la circunstancia
 - P. ej.: si el perito de una empresa es un propio trabajador de la empresa

Nombramiento del perito (IV)

- En el libro “Informática Forense – 55 Casos reales” se pueden ver ejemplos de los escritos
 - Proposición de prueba (págs. 212-213)
 - Se incluyen las cuestiones a tratar en la misma
 - Notificación de designación de perito (pág. 215)
 - Acta de aceptación (pág. 219)
 - Presentación de informe y ratificación (págs. 220-221)

Código deontológico:

Responsabilidad civil

- Sujeto a **responsabilidad civil**
 - Por acción u omisión
 - Obligado a reparar el daño a un particular
- Causas:
 - Faltar al Secreto Profesional
 - Daño patrimonial
 - Pérdida o deterioro de objetos, bien mal valorado, etc.)
 - Falsedad en documento privado
 - Responsabilidad contractual
 - No hacer la tarea, hacerlo fuera de plazo o errores flagrantes

Código deontológico: Responsabilidad penal

- Sujeto a **responsabilidad penal**
 - Hecho delictivo voluntario
 - Obligado a reparar el daño a la sociedad
- Causas:
 - Falso testimonio o perjurio
 - Cohecho o soborno
 - Denegación de auxilio a la justicia
 - Desobediencia al Juez o Tribunal
 - Perturbación del orden en el Juzgado o Tribunal

Código deontológico: Responsabilidad disciplinaria y profesional

- Sujeto a **Responsabilidad disciplinaria**
 - No comparecer en juicio o vista cuando sea requerido judicialmente (por escrito) para ello
- Sujeto a **Responsabilidad profesional**
 - No cumplir el código deontológico o el procedimiento disciplinario Colegial

El colegio de ingenieros técnicos en Informática "alerta" al juez de que el perito está "difundiendo" el contenido del informe

- Considera "palmaria la violación del derecho al secreto de las comunicaciones y a la intimidad"
- El Colegio de Ingenieros Informáticos advirtió al juzgado de que el perito del caso Marta no tiene titulación
- El informe del teléfono de Carcaño no revela nuevos movimientos la noche del asesinato
- El clonado permite recuperar varias fotografías y mensajes de texto



Manuel Huerta de la Morena, en su despacho. / M. G.

Otras funciones de los peritos (I)

- Los peritos pueden ser contratados con fines **preventivos, correctivos o probatorios**
 - Asesoría técnica contra el Cibercrimen
 - Localización de evidencias electrónicas
 - Auditorías
 - Análisis forenses preventivos
 - Valoración y Tasación de equipos tecnológicos
 - Certificaciones y Homologaciones
 - Recuperación de Datos

Otras funciones de los peritos (II)

- Los peritos pueden ser contratados con fines **preventivos, correctivos o probatorios** (cont.)
 - Asesoría Informática y formación a profesionales del Derecho, Administración pública, Cuerpos y Fuerzas de Seguridad del Estado...
 - Supervisión de actividad laboral informática
 - Detección y asesoría en casos de competencia desleal
 - Seguimiento de correos, autores de publicaciones, propietarios de páginas Web

Otras funciones de los peritos (III)

- Los peritos pueden ser contratados con fines **preventivos, correctivos o probatorios** (cont.)
 - Análisis informático forense de videos, imágenes digitales y audio
 - Asesoría sobre falsificación de correos, imágenes, violaciones de seguridad, infiltraciones, doble contabilidad, fraude financiero y de sistemas informáticos, robo de claves, información sensible, secretos industriales, errores en la cadena de custodia, etc.

Cobro de honorarios

- Solicitado por una de **las partes** => se trata como un contrato privado más
- Solicitado por **el juez** => pagado por las partes
 - A través del juzgado o directamente por ellas
 - Puede presentar escrito al juez o renunciar si no le pagan en tiempo y forma
- **Justicia gratuita** => pago por parte de Admon. de Justicia que no cubre los gastos ni de lejos
 - Puede cobrar más si hay beneficio económico

La alternativa: el Arbitraje

- Más rápido y barato que el proceso judicial
 - Contemplado en las leyes [60/2003](#) y [11/2011](#)
 - Debe ser de mutuo acuerdo y renuncia a la vía judicial
- En lugar del juez hay uno o varios *árbitros*
 - En arbitraje de derecho, han de ser abogados
 - **En el de equidad, serán profesionales de la materia**
- A la sentencia se le llama *laudo*
 - De obligado cumplimiento y no recurrible, pero se puede solicitar su anulación

Parte III: Legislación aplicable al Análisis Forense Informático

Constitución Española

- Garantizar los siguientes derechos fundamentales
 - A la **seguridad jurídica** (art. 9.3) y **tutela judicial efectiva** (art. 24.1)
 - Proceso judicial con garantías.
 - Al **honor, a la intimidad personal y familiar, y la propia imagen** (art. 18.1)
 - Limitación del uso de la informática para proteger el honor y la intimidad (art. 18.4)
 - Al **secreto de las comunicaciones** (art. 18.3)
 - A la **protección de datos** ([STC 292/2000](#))

Enjuiciamiento civil y criminal

- [Ley 1/2000](#), de 7 de enero, de Enjuiciamiento Civil (LEC)
- [Real Decreto de 14 de septiembre de 1882](#) ... Ley de Enjuiciamiento Criminal (LECrim)
 - Art. 326, recogida de pruebas
 - Arts. 456-485, 661-663, 723-725 y 334-367, sobre peritos e informes periciales
 - Art. 588, sobre interceptación de comunicaciones
 - Muy modificado por la [LO 13/2015, de 5 de octubre](#)
- [Circular 5/2019, de 6 de marzo](#), de la FGE, sobre registro de dispositivos y equipos informáticos

Sistemas de información y Comercio electrónico

- [Directiva 2013/40/UE](#) ..., de 12 de agosto de 2013, relativa a los **ataques contra los sistemas de información**
- [Ley 34/2002](#), de 11 de julio, de servicios de la **sociedad de la información y de comercio electrónico**

Protección de datos personales

- [Reglamento \(UE\) 2016/679](#) ..., de 27 de abril de 2016, relativo a la **protección** de las personas físicas en lo que respecta al tratamiento **de datos personales** y a la libre circulación de estos datos
- [Ley Orgánica 3/2018](#), de 5 de diciembre, de **Protección de Datos Personales** y garantía de los derechos digitales.

Conservación de datos de comunicaciones electrónicas

- [Directiva 2006/24/CE](#) ..., de 15 de marzo de 2006, sobre la **conservación de datos** generados o tratados en relación con la prestación de servicios de **comunicaciones electrónicas** de acceso público o de redes públicas de comunicaciones
- [Ley 25-2007](#), de 18 de octubre, de **conservación de datos relativos a las comunicaciones electrónicas** y a las redes públicas de comunicaciones

Secretos empresariales y propiedad intelectual

- [Ley 1/2019](#), de 20 de febrero, de Secretos Empresariales
 - Art. 2 punto 3, letra b (investigaciones, etc.)
- [Real Decreto Legislativo 1/1996](#), de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia
 - Artículo 100 (decompilación, modificación, etc.)

Código Penal (I)

- [Ley Orgánica 10/1995](#), de 23 de noviembre, del Código Penal
 - Corrupción de menores (Título VIII, Capítulo V)
 - Delitos contra la intimidad (Título X, Capítulo I)
 - Delitos contra el honor (Título XI):
 - Calumnias (Capítulo I, art. 205-207)
 - Injurias (Capítulo II, art. 208-210)
 - Defraudación electrónica (Título XIII, Capítulo VI):
 - Estafa (art. 248.2)
 - Apropiación indebida (art. 252)
 - Uso ilegal de terminales (art. 256)

Código Penal (II)

- [Ley Orgánica 10/1995](#), de 23 de noviembre, del Código Penal (cont.)
 - Daños a ficheros informáticos (art. 264.2)
 - Piratería informática (Título XIII, Capítulo XI)
 - Delitos documentales (Título XVIII)
 - En el artículo 26 se define el concepto de documento
 - Falsedades documentales (Título XVIII, Cap. II, arts. 390-400)
 - Infidelidad en la custodia (Título XIX, Cap. IV, arts. 413-416)
 - Protección de la contraseña (art. 414.2)
 - Apología del delito (art. 18)

Reglas de exclusión y la doctrina del fruto del árbol envenenado (I)

- Reglas de exclusión
 - **Desestimar cualquier medio probatorio obtenido por vías ilegítimas**
- Doctrina del fruto del árbol envenenado
 - **Desestimar evidencia secundaria o derivada de la anterior**
 - Silverthorne Lumber Company c/ EE. UU, 1920
 - [STC 114/1984](#) y artículo 11 de la [Ley Orgánica 6/1985 del Poder Judicial](#) en España

Reglas de exclusión y doctrina del fruto del árbol envenenado (II)

- Excepciones en las cuales se admite evidencia:
 - Obtención por fuente independiente a la investigación ilegal ([STC 49/1996](#))
 - Hallazgo inevitable ([STS 974/1997](#)) o casual ([STS 284/2000](#))
 - Nexos atenuados entre la evidencia y la conducta ilegal ([STC 86/1995](#))
 - Actos de buena fe: los investigadores se basan en algo que más tarde resulta no ser válido ([STC 22/2003](#))
 - Falta de nexos con la prueba primaria ([STC 81/1998](#))

Parte IV: Metodologías de Análisis Forense Informático

Metodologías y guías (I)

- **No existe un estándar obligatorio**
- Existen algunas metodologías y guías con cierta aceptación
 - Normas ISO y UNE
 - RFC (Request For Comments) del IETF
 - Guías y manuales creados por instituciones varias

Metodologías y guías (II)

- Algunas guías se especializan en dispositivos móviles
 - [Guidelines on Mobile Device Forensics](#) de NIST
 - [Developing Process for Mobile Device Forensics](#) de SANS
 - [Best Practices for Mobile Phone Forensics](#) de SWGDE
 - Good Practice Guide for Mobile Phone Seizure and Examination de la Interpol

Metodologías y guías (III)

- Estándares UNE
 - Familia UNE 71505:2013 – Sistema de Gestión de Evidencias Electrónicas ([Parte 1](#), [Parte 2](#), [Parte 3](#))
 - [UNE 71506:2013](#) – Metodología para el análisis forense de las evidencias electrónicas
 - [UNE 197010:2015](#). Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)

Metodologías y guías (IV)

- Estándares UNE (cont.)
 - [UNE-EN ISO/IEC 27037:2016](#) - Directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas (ISO/IEC 27037:2012)
 - [UNE-EN ISO/IEC 27040:2016](#) – Seguridad en el almacenamiento (ISO/IEC 27040:2015)
 - [UNE-EN ISO/IEC 27042:2016](#) - Directrices para el análisis y la interpretación de las evidencias electrónicas (ISO/IEC 27042:2015)

Metodologías y guías (V)

- Estándares RFC (Request For Comments)
 - [RFC 3227](#) - *“Guidelines for Evidence Collection and Archiving”*
 - [RFC 4810](#) - *“Long-Term Archive Service Requirements”*
 - [RFC 4998](#) - *“Evidence Record Syntax (ERS)”*
 - [RFC 6283](#) - *“Extensible Markup Language Evidence Record Syntax (XMLERS)”*

Grupos y organizaciones

- Scientific Working Group on Digital Evidence
 - Desde 1998 (<https://www.swgde.org/>)
 - Buscan comunicación y cooperación entre participantes, y asegurar calidad y consistencia
- European Network of Forensic Science Institutes
 - Desde 1993 (<https://enfsi.eu/>)
 - Intercambio de info. en todo tipo de ciencias forenses

Características comunes de las metodologías (I)

- **Verificable:** se debe poder comprobar la veracidad de las conclusiones extraídas a partir del análisis
- **Reproducible:** se deben poder reproducir en todo momento las pruebas realizadas durante el proceso, obteniendo siempre el mismo resultado
- **Repetible:** un estudio empleando la misma metodología pero otros datos debe obtener un resultado consistente

Características comunes de las metodologías (II)

- **Independiente:** las conclusiones obtenidas deben ser las mismas, independientemente de la persona que realice el proceso y de la metodología empleada
- **Documentado:** todo el proceso debe de estar correctamente documentado, de forma comprensible y detallada

Fases (I)

- Se suelen estudiar estas cuatro:
 1. Identificación y adquisición de evidencias
 2. Preservación de las evidencias
 3. Análisis de las evidencias
 4. Documentación y presentación de los resultados
- No es algo fijo, hay variantes
 - P. ej.: Descomponer algunas fases en varias
 - P. ej.: Poner preservación antes que adquisición

Fases (II)

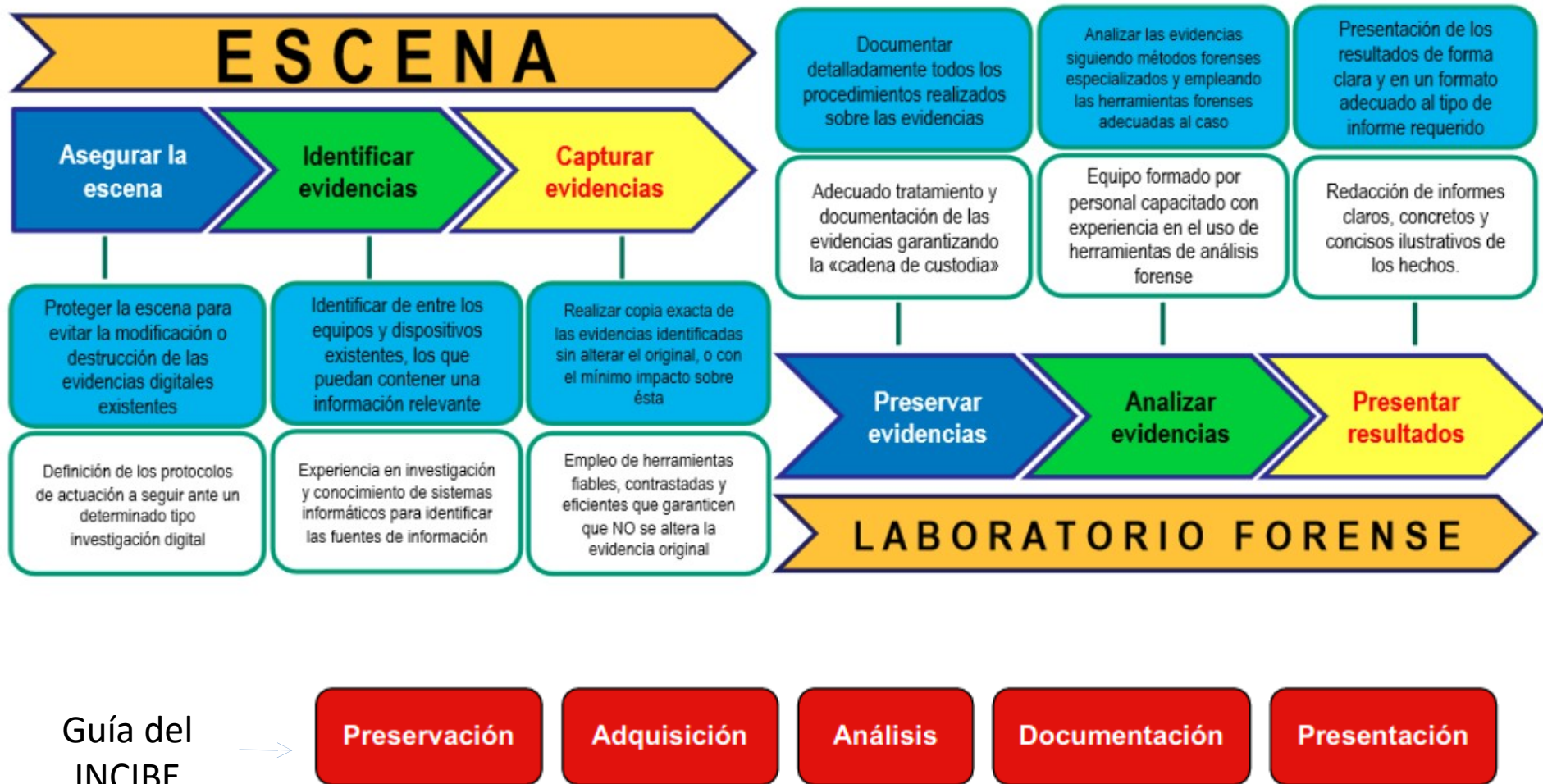


Ilustración 2: Fases del análisis forense digital.

Identificación y adquisición

- En una actuación forense orientada a pericial se podrían realizar las siguientes tareas
 1. Identificación del incidente
 2. Entrevista aclaratoria
 3. Inspección ocular
 4. Recopilación de evidencias

Identificación

- ¿Qué dispositivos físicos pueden contener evidencias digitales?
- ¿Cuáles son sus antecedentes?
- ¿Depende de otros dispositivos?
 - P. ej.: ¿está conectado a una red?
- ¿Está sometido a reglamento? ¿se aplicó?
- ¿En qué período de tiempo sucedió el incidente?
- ¿Cuáles son los siguientes pasos a dar?

Adquisición (I)

- Según el RFC 3227, la evidencia ha de ser:
 - **Admisible**: Válida en un proceso legal
 - **Auténtica**: Poder demostrar que no ha sido manipulada
 - **Completa**: Debe contar toda la historia y no una única perspectiva
 - **Fiable**: No puede haber duda sobre su autenticidad y veracidad
 - **Creíble** y comprensible por un jurado

Adquisición (II)

- Evidencia física
 - Discos duros, pendrives, etc.
- Evidencia digital
 - Ficheros, procesos en ejecución, logs, entradas de registro, archivos temporales...
- Generar imágenes forenses de la evidencia digital
 - Proceso de duplicación empleando tecnología puntera para mantener la integridad de la evidencia
 - Trabajar con una o más copias de dicha imagen

Preservación

- No se deben perder las evidencias sobre las que se va a hacer el análisis
 - Cuidado con la información volátil
 - Rotular bien todos los elementos
- Registro de todas las acciones que se realizan
- Transportar con sumo cuidado
 - Temperaturas extremas y campos electromagnéticos
- Mantener la **cadena de custodia**
 - Romperla puede anular la validez de la prueba

Análisis

- Proceso de aplicar técnicas científicas y analíticas
 - Búsquedas de cadenas de caracteres
 - Acciones específicas de los usuarios de la máquina
 - P. ej.: uso de dispositivos de USB (marca, modelo)
 - Recuperación de archivos específicos, correos electrónicos, últimos sitios visitados, caché del navegador de Internet
 - Estudio de *artefactos* como la Master File Table (MFT), archivo de paginación, papelera de reciclaje, espacio no asignado, slack space, registro de Windows, tráfico de red, procesos del sistema, logs, etc.

Documentación y Presentación (I)

- Recopilar toda la información que se obtuvo en el análisis para realizar el informe para su presentación a los abogados
 - Documentar todos los pasos del proceso
 - Manteniendo fechas y hora de cada acción
 - Incluir fotografías de las pruebas
 - Ser objetivos, no hacer juicios de valor
 - Detallar las conclusiones

Documentación y Presentación (II)

- Generación de una pericial
 - **Informe ejecutivo**
 - Corto y simple
 - **Informe técnico**
 - Más largo y complejo
- Interpretación de forma pedagógica, clara y sencilla
 - Sin usar muchos tecnicismos

Bibliografía y webgrafía

Bibliografía y webgrafía (I)

- Pilar Vila Avendaño *“Técnicas de Análisis Forense Informático para Peritos Judiciales Profesionales”*
 - 2018, ISBN: 978-84-697-7700-8, Editorial OxWord
- Ernesto Martínez de Carvajal Hedrich:
“Informática Forense – 55 Casos reales”
 - 2021, ISBN: 978-84-615-8121-4, 4ª Ed.

Bibliografía y webgrafía (II)

- McKemmish, Rodney “*What is Forensic Computing?*” En: Trends & issues in crime and criminal justice, No. 118
 - [https://
www.aic.gov.au/sites/default/files/2020-05/tandi118.pdf](https://www.aic.gov.au/sites/default/files/2020-05/tandi118.pdf)
- INCIBE. “*RFC 3227 – Directrices para la recopilación de evidencias y su almacenamiento*”
 - <https://www.incibe-cert.es/blog/rfc3227>

Bibliografía y webgrafía (III)

- Augusto Javier Mosquera Blanco “*La prueba ilícita tras la sentencia Falciani: Comentario a la STS 116/2017, de 23 de Febrero*”
 - [https://
raco.cat/index.php/InDret/article/download/341931/432993/0](https://raco.cat/index.php/InDret/article/download/341931/432993/0)
- Peritos
 - <https://perito.biz/historia/>
 - [https://
uvadoc.uva.es/bitstream/handle/10324/33650/TF-G-N.1025.pdf?sequence=1&isAllowed=y](https://uvadoc.uva.es/bitstream/handle/10324/33650/TF-G-N.1025.pdf?sequence=1&isAllowed=y)

Bibliografía y webgrafía (IV)

- Peritos
 - https://formacion.istas.net/ficheros/curso777/Peritaje_UDAD2.pdf
 - Judith Tiral *“Así se resolvió el primer crimen de la historia – Tenía La Duda 1x01”*
 - <https://www.youtube.com/watch?v=D1lo7HTUCgQ>
 - Universitat Politècnica de Valencia (UPV) *“El perito a través de la historia”*
 - https://www.youtube.com/watch?v=Ta_BsbE3bAA

Bibliografía y webgrafía (V)

- Palabra de hacker “*Análisis forense digital: qué es y como se investigan las evidencias*”
 - <https://www.youtube.com/watch?v=EbH7tPSiaYk>
- Juicios
 - iurisfacil.com “*Cómo funciona un juicio: quién interviene en un juicio*”
 - <https://iurisfacil.com/como-funciona-un-juicio-quien-interviene-en-un-juicio/derecho-penal>
/

Bibliografía y webgrafía (VI)

- Foro de evidencias electrónicas
 - <http://foroevidenciaselectronicas.org/>