TEMA 1: Introducción al Análisis Forense Informático

IES Zaidín-Vergeles

30 de noviembre de 2020

Tabla de contenidos

CAPÍTULO 1

Objetivos del tema

Este primer tema de la asignatura pretende ser un tema introductorio al mundo del análisis y la informática forense. Con este tema se pretenden conseguir unos conocimientos mínimos sobre los que posteriormente se asentará el resto de la asignatura. Los objetivos de este primer tema son:

- Conocer qué es la **informática forense** y qué se considera una **evidencia digital**.
- Tener una visión de cuáles son los **objetivos de un análisis forense**.
- Saber identificar cada una de las **etapas de un análisis forense**.
- Conocer la importancia de la **cadena de custodia** en el ámbito de trabajo de un analista forense.
- Conocer los delitos mas comunes que cometen lo ciberdelicuentes. Tambíen conocer aquellos que, como peritos, podemos cometer durante el ejercicio de nuestra labor.
- Conocer a quién se puede considerar **perito** según la legislación española.

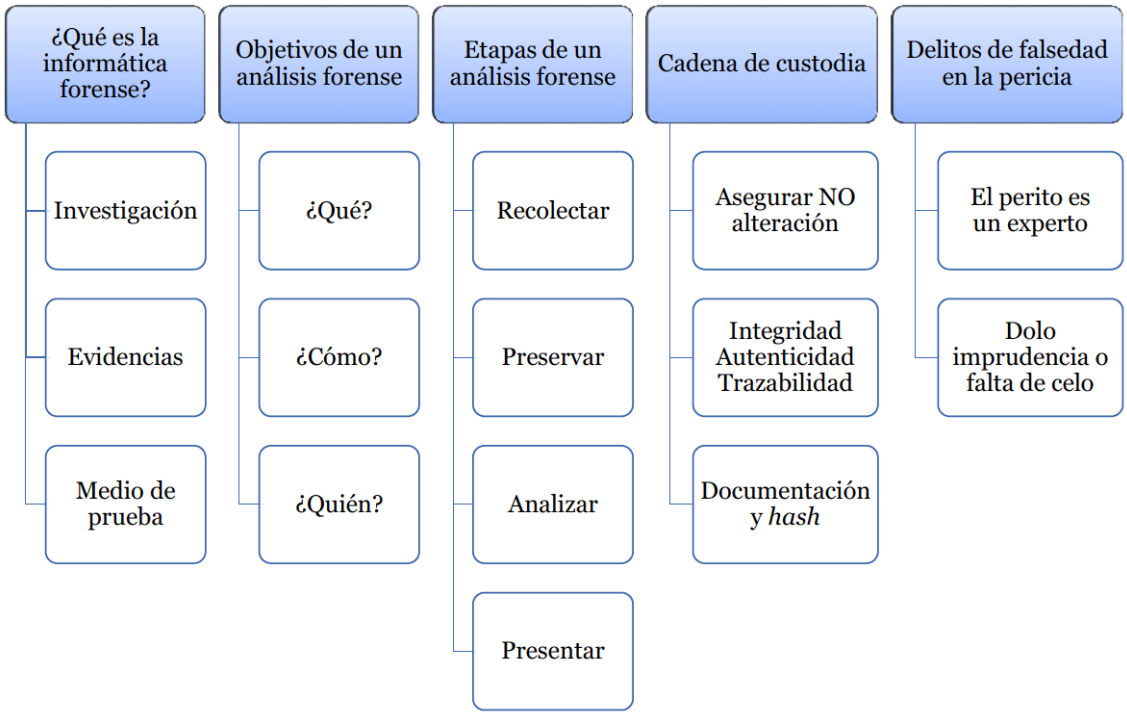
Para estudiar este tema lee los siguientes documentos, además de las **Ideas clave**:

Importante:

- El artículo **¿Qué es la informática forense o Forensic?**, publicado por Microsoft
- Entrevista a Juan Martos, ex responsable del área de informática forense de la empresa Recovery Labs (parte 1) ; (parte 2)
- What is Digital Forensics? El vídeo presenta a Bill Dean, director de Informática forense de la empresa Sword & Shield Enterprise Security
- ¿Como se llega a ser Perito Informático?
- En cuanto a las evidencias digitales, es recomendable la lectura del artículo **Taxonomy of Digital Evidence**, publicado por la New Mexico Tech University. Este

artículo introduce el concepto de evidencia digital, además de algunas de las características deseables de la misma

- También es interesante la lectura del artículo **Recovering and Examining Computer Forensic Evidence**, publicado por el FBI, especialmente, la introducción y la definición de informática forense que en él aparecen.
- Evidencia Digital. Una pericial informática me ayudó a ganar el caso



CAPÍTULO 2

La amenaza digital

En la actualidad, dependemos cada vez más y más de Internet y de herramientas de tecnologías de la comunicación y la información (TIC) en la medida que usamos aplicaciones en línea para comunicarnos via chat, dependemos del correo electrónico para comunicarnos con familiares y con el trabajo, nos mantenemos en contacto con nuestros amigos y actualizamos el estado utilizando redes sociales, trabajamos en línea manteniéndonos conectados a nuestra oficina usando Internet, hacemos compras on-line, enseñamos en línea, aprendemos en línea, recibimos nuestras facturas en línea, realizamos transferencias bancarias, etc. Nuestra dependencia de la informática e Internet ha aumentado tanto que estamos «en línea» la mayor parte de el tiempo. Por lo tanto, existe una mayor necesidad de proteger nuestra información para que no sea mal utilizada siguiendo las pautas de seguridad de la información. Sin embargo, si la seguridad de nuestro ordenador está comprometida, la informática forense es útil para la investigación posterior al incidente.

Cuando hablamos de ciberseguridad o seguridad informática solemos utilizar a menudo los términos **«amenaza»** y **«vulnerabilidad»**, pues representan una realidad con la que nos enfrentamos a menudo en este trabajo.

La **vulnerabilidad** es la debilidad o fallo que presenta un sistema de información. Este es capaz de poner en riesgo la seguridad de toda o parte de la información. Es decir, es un problema que tenemos nosotros, nuestro sistema.

El motivo es que este fallo o debilidad permite que el atacante comprometa la integridad, confidencialidad e incluso la disponibilidad de la información y los datos.

Los orígenes de las vulnerabilidades son muy diferentes. Pueden ser debidas a fallos en el diseño del sistema, carencia de procedimientos o simples errores de configuración.

La **amenaza** es la acción que se vale de una vulnerabilidad para actuar contra la seguridad del sistema de información. Estas actuaciones son siempre peligrosas pero, obviamente, si existe una vulnerabilidad su efecto se posibilita y multiplica. La amenaza forma parte del lado contrario, no de nuestro sistema.

Sus orígenes pueden ser muchísimos:

- **Código malicioso o malware:** Es el más general y permite ejecutar muchas acciones ofensivas muy variadas.
- **APTs (Advanced Persistent Threat):** Son ataques elaborados, bien coordinados, que se enfocan en una empresa u organización para realizar un ataque con un objetivo específico contra su información.
- **Ingeniería social:** Se utilizan técnicas persuasivas para aprovechar la buena voluntad de la gente; es decir, atacan al componente humano.
- **Botnets:** Son equipos infectados que se dedican a ejecutar, de manera automática, programas para realizar ataques sofisticados.
- **Servicios en la nube:** La nube es tremendamente vulnerable, por ello, es necesario que si contratas algún servicio exijas la misma seguridad que tienes en tus sistemas, con acuerdos de nivel de servicios firmados. Si no, se abrirán brechas muy rápidamente y quedaréis tremendamente expuestos.
- **Redes sociales:** La reputación de la empresa se puede ver en entredicho con un uso descontrolado de estas, que, por otro lado, son tremendamente accesibles.

Por este motivo, es esencial estar perfectamente protegido. Las amenazas existentes son muchas y los atacantes están al acecho esperando su oportunidad.

Tenemos así que **las vulnerabilidades son las condiciones de nuestro sistema que los hacen ser susceptibles a las amenazas**, que son las circunstancias ajenas capaces de suponer un riesgo o ser un peligro.

El **riesgo** es una probabilidad de que se pueda producir un incidente relacionado con la ciberseguridad empresarial, industrial o doméstica, y tiene como principales factores la existencia tanto de una vulnerabilidad como de una amenaza. (Riesgo = probabilidad amenaza x impacto)

Se trata de una cifra que indica cómo de posible es que una amenaza, con el aprovechamiento de una vulnerabilidad presente, se materialice produciendo impactos negativos en el sistema de información

2.1 El delito informático

Delito informático, delito cibernético o ciberdelito es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet. Ante el extendido uso y utilización de las nuevas tecnologías en todas las esferas de la vida (economía, cultura, industria, ciencia, educación, información, comunicación, etc) y el creciente número de usuarios, consecuencia de la globalización digital de la sociedad, la delincuencia también se ha expandido a esa dimensión. Gracias al anonimato y a la información personal que se guarda en el entorno digital, los delincuentes han ampliado su campo de acción y los delitos y amenazas a la seguridad se han incrementado exponencialmente.

Además de los ataques que tienen como objetivo destruir y dañar activos, sistemas de información u otros sistemas de computadoras, utilizando medios electrónicos y/o redes de Internet, se producen nuevos delitos contra la identidad, la propiedad y la seguridad de las personas, empresas e instituciones, muchos de ellos como consecuencia del valor que han adquirido los activos digitales para la big data empresarial y sus propietarios

bien sean entes jurídicos o personas naturales. Existen también otras conductas criminales que aunque no pueden considerarse como delito, se definen como ciberataques o abusos informáticos y forman parte de la criminalidad informática. La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, son llevados a cabo utilizando un elemento informático.

La Organización de Naciones Unidas reconoce los siguientes tipos de delitos informáticos:

- **Fraudes cometidos mediante manipulación de computadoras**; en este se reúne: la manipulación de datos de entrada (sustraer datos), manipulación de programas (modificar programas del sistema o insertar nuevos programas o rutinas), manipulación de los datos de salida (fijación de un objeto al funcionamiento de sistemas de información, el caso de los cajeros automáticos) y fraude efectuado por manipulación informática (se sacan pequeñas cantidades de dinero de unas cuentas a otras).
- **Manipulación de datos de entrada;** como objetivo cuando se altera directamente los datos de una información computerizada. Como instrumento cuando se usan las computadoras como medio de falsificación de documentos.
- **Daños o modificaciones de programas o datos computarizados;** entran tres formas de delitos: sabotaje informático (eliminar o modificar sin autorización funciones o datos de una computadora con el objeto de obstaculizar el funcionamiento) y acceso no autorizado a servicios y sistemas informáticos (ya sea por curiosidad, espionaje o por sabotaje).

Existen leyes que tienen por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos en las variedades existentes contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías.

Una misma acción dirigida contra un sistema informático puede aparejar la violación de varias leyes penales, algunos autores expresan que el «uso de la informática no supone más que un modus operandi nuevo que no plantea particularidad alguna respecto de las formas tradicionales de comisión». Una clara dificultad para la persecución de estos ilícitos, ha sido que el ciudadano no considera delincuente al autor de estos delitos, entre los propios victimarios algunas veces existe una reivindicación que subyace a toda su actividad, como es el caso de los hackers, quienes cuentan con todo una «filosofía» preparada para respaldar su actividad afirmando que propenden a un mundo más libre, que disponga de acceso a todas las obras de la inteligencia, y basándose en ese argumento divulgan las claves que tienen en su actividad.

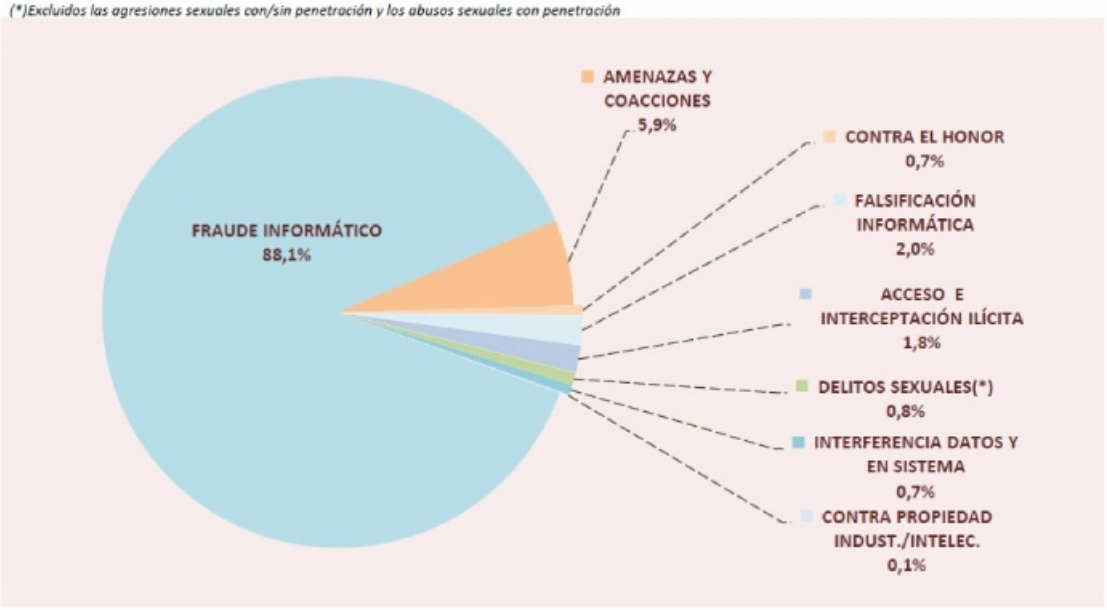
Clasificación según la página de la Brigada de Investigación Tecnológica de la Policía Nacional Española:

- **Ataques que se producen contra el derecho a la intimidad:** Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal)
- **Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor:** Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal)

- **Falsedades:** Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (Artículos 386 y ss. del Código Penal)
- **Sabotajes informáticos:** Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal)
- **Fraudes informáticos:** Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal)
- **Amenazas:** Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal)
- **Calumnias e injurias:** Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal)
- **Pornografía infantil:** Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.
- La inducción, promoción, favorecimiento o facilitamiento de la **prostitución** de una persona menor de edad o incapaz. (art 187)
- La producción, venta, distribución, exhibición, por cualquier medio, de **material pornográfico** en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (art 189)
- El **facilitamiento de las conductas anteriores** (El que facilitare la producción, venta, distribución, exhibición...). (art 189)
- La **posesión de dicho material** para la realización de dichas conductas. (art 189)

HECHOS CONOCIDOS	2016	2017	2018	2019
ACCESO E INTERCEPTACIÓN ILÍCITA	3.243	3.150	3.384	4.004
AMENAZAS Y COACCIONES	12.036	11.812	12.800	12.782
CONTRA EL HONOR	1.546	1.561	1.448	1.422
CONTRA PROPIEDAD INDUST./INTELEC.	129	121	232	197
DELITOS SEXUALES(*)	1.231	1.392	1.581	1.774
FALSIFICACIÓN INFORMÁTICA	3.017	3.280	3.436	4.275
FRAUDE INFORMÁTICO	70.178	94.792	136.656	192.375
INTERFERENCIA DATOS Y EN SISTEMA	1.336	1.291	1.192	1.473
Total HECHOS CONOCIDOS	92.716	117.399	160.729	218.302

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



Casi nueve de cada 10 ciberdelitos consisten en fraude informático | INTERIOR

2.2 Evaluación del riesgo

La probabilidad de que una amenaza digital llegue a producirse depende de varios factores:

(a) frecuencia de la misma según la estadística y la experiencia histórica

(b) vulnerabilidad de los sistemas atacados

(c) valor de los datos

(d) motivación del atacante

(e) relevancia mcdiática de la entidad atacada

En la práctica resulta posible evaluar el riesgo en función de dos factores principales: un primer lugar la misma probabilidad del hecho hostil —intrusión en sistemas, sabotaje, robo de datos— y, segundo, el valor del bien comprometido —información confidencial, documentos de clientes o proveedores, datos críticos para el funcionamiento de los sistemas, etc.—. Seria aconsejable que con carácter preventivo se lleve a cabo un análisis de riesgos centrado en la probabilidad de los ataques y una evaluación de los daños económicos asociados a los mismos, tomando a renglón seguido las medidas técnicas, organizativas, legales o de infraestructura que se consideren oportunas. En cualquier caso, una vez

que las actuaciones ilícitas han tenido lugar, tales procedimientos resultan inexcusables si se desea evitar que los incidentes vuelvan a producirse en el futuro.

Durante los últimos años la escena del delito digital ha experimentado un profundo cambio, pasando de ser un entorno en cl que de vez en cuando se cometían hechos aislados a convertirse en un fenómeno de masas, con millares de delincuentes, activistas políticos, miembros de bandas organizadas y simples gamberros. La culpa la tienen por un lado el monocultivo de sistemas operativos y aplicaciones, y por otro la explosión de Internet con su enorme variedad de servicios, la estandarización de sus protocolos y la presencia inevitable de fallos de configuración y diseño en el software. Todo ello ha conducido a una multiplicación exponencial de los incidentes de seguridad.

2.3 Motivos del agresor

La ciberdelincuencia presenta perfiles tan variopintos como clasificaciones criminológicas quieran hacerse. Por lo tanto, no existe un perfil único para encasillar a un cibercriminal o para determinar que alguien lo sea porque cumpla tales requisitos, por ello no podemos hablar de perfil típico sino de características comunes, desde el punto de vista de la probabilidad. Estas características se pueden agrupar en:

- **Capacidades tecnológicas.** Por lo general se consideran delincuentes especializados, es decir es necesario el requerimiento de cierta destreza tecnológica para llevar a cabo cualquier ilícito: Fraude, Phising, acceso no autorizado a un dispositivo, Pharming, etc. Sin embargo, dependerá del delito que se quiera cometer, ya que no se necesitarán las mismas habilidades para suplantar una identidad que para acceder a un sistema o crear un Malware.
- **Expectativas sociales.** El delincuente que nos solemos encontrar en las redes tienden a realizar los delitos movidos por fantasías y motivaciones. En lo que respecta a las fantasías, algunos de estos criminales tienden a imaginarse una idealidad de consecuencias al vulnerar un sistema o realizar un fraude; como el falso reconocimiento de amigos o entorno, sentimiento de superioridad frente a otros o tener el control sobre webs o temas para encontrar un reconocimiento a sus habilidades.
- **Sentimiento de seguridad.** Al moverse en un ámbito de clandestinidad como es Internet, el delincuente puede cometer las acciones delictivas bajo cualquier seudónimo o restricción de su identidad, por lo tanto estaríamos ante condiciones de anonimato que le permitirían realizar los delitos desde una comodidad y una seguridad propia de estas características. En este aspecto también influye la transnacionalidad del ciberdelito, característica que fomenta el anonimato y que obtiene las mismas consecuencias de falsa seguridad.
- **Sentimiento de superioridad.** El cibercriminal, como cualquier otro delincuente, tiende a sentirse por encima de la ley y por ello la vulnera, unido a las expectativas que acabamos de explicar, sirve como detonante para realizar cualquier tipo delictivo. Desde la criminología estas conductas tienden a explicarse por teorías criminológicas, que en síntesis, hablan de una elección entre la buena conducta (utilizar Internet con fines útiles) y una elección de una mala conducta (utilizar Internet con fines delictivos), valorando como más fructíferas para el delincuente las acciones negativas.

Sin embargo, el motivo principal por el que un cibercriminal delinque, al igual que cualquier otro, es la motivación, o sea, el conjunto de impulsos que le llevan a realizar cualquier ilícito ya sea fraude, robo de información, suplantación de identidad... Las motivaciones pueden ser de diferente tipología, las más relevantes desde la criminología son:

- **Por diversión:** el interés únicamente por el morbo de llegar un poco más lejos de lo que un usuario "estándar" de la red o de tecnología pueda llegar.
- **Por beneficio económico:** utilizar la pericia o los conocimientos para poder obtener un ánimo de lucro. Aquí encontraríamos casos de estafa o de Phising cuyo objetivo es obtener una ganancia económica.
- **Por sentimientos de ira, rabia, venganza, indignación:** en este caso encontraríamos delitos de cualquier corte, por ejemplo un trabajador despedido que tumba una página web, mediante un ataque DDos, y esta pierde millones de euros.
- **Por incitación sexual:** en esta ocasión veríamos un ciberdelincuente que utilizaría los medios técnicos oportunos para conseguir imágenes o grabaciones sexualizadas, hablamos de casos de pedofilia o sexting. Estos delitos pueden perpetrarse mediante conductas de acceso no autorizado al sistema de vigilancia de una vivienda.
- **Por cuestiones políticas o religiosas:** con el objetivo de derrocar el gobierno o de llamar la atención ante la sociedad. Un ejemplo sería el hacktivismo.

2.4 Amenazas internas y externas

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, y con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo, el hecho de que la red no esté conectada a un entorno externo, como Internet, no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas:

- **Amenazas internas:** Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:
  - Si es por usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos.
  - Los sistemas de prevención de intrusos o IDS, y firewalls son mecanismos no efectivos en amenazas internas por no estar orientados al tráfico interno. Que el ataque sea interno no tiene que ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red directamente: rosetas accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etc.
- **Amenazas externas:** Son aquellas amenazas que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacar. La ventaja

que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

CAPÍTULO 3

Dinámica de una intrusión

Un ataque informático puede ser de muchos tipos, tantos como hayan tipificado en el código penal, claro está, requerirán de un ordenador para ser llevados a cabo. Muchas veces la persona que comete el delito informático en cuestión pueden llegar a paralizar gran número de máquinas e incluso la página web de alguna organización importante. O por el contrario puede que tengamos al enemigo en casa y un empleado vengativo quiera dejar nuestra red corporativa al descubierto saboteando para ello nuestro router, saca un disco duro del servidor de la empresa o por el contrario roba la base de datos de la empresa un dispositivo usb.

Ante todo lo que acabamos de describir las medidas que el investigador en cuestión tenga que tomar van a depender siempre de las circunstancias que vengan sobrevenidas del hecho delictivo en cuestión. Antes que podamos sufrir algunos de los percances que acabamos de describir un ejército descoordinado y anónimo compuesto por miles de aficionados, frikis o script kiddles habrá probado fortuna atacando a la empresa usando herramientas descargadas de internet, cuyo funcionamiento no entienden pero que seguro a través de algún foro de hacker, o mediante la descarga un documento adjunto tendrán las instrucciones precisas, para ser ejecutadas contra cualquier objetivo remoto como oportunistas sin ningún conocimiento alguno sobre informática. Por su parte si se tratara de un atacante profesional que se haya propuesto abrirse camino hacia el interior de cualquier servidor dentro de una organización no actuará de manera aleatoria sino que seguirá una estrategia planificada de manera concienzuda. Cualquiera que sea el motivo, o se trate de una intrusión interna o externa, desde la misma red local, o externa se desarrollará con un esquema bien definido. El informático forense debe conocer el modus operandi, para verificar así la existencia de la intrusión y elaborar una línea de tiempo que permita descubrir cuáles han sido los pasos seguidos para atacar el sistema, y que permita esclarecer los delitos.

3.1 FootPrinting (Reconocimiento)

El footprinting ('reconocimiento') es el proceso de recogida de información en internet sobre algo muy concreto. Se trata de un concepto relacionado con la seguridad informática, ya que, en general, está ligado a los métodos empleados por los hackers informáticos. Aunque no siempre: es una técnica que también utilizan investigadores, periodistas, académicos, estudiantes, etc. Cualquiera de nosotros usamos el footprinting al hacer una búsqueda habitual en la red.

lo primero que debemos hacer es navegar por todas las páginas del sitio web que queramos investigar. Así podremos descubrir tanto el contenido que ha sido publicado intencionadamente como el que no.

Las principales huellas que quedan cuando buscamos un objetivo concreto (direcciones IP, cuentas de correo de los usuarios, credenciales, impresoras, metadatos...) también son información valiosa. Pueden ayudarnos a localizar los datos bancarios de un defraudador, la identidad de un ciberacosador o conseguir documentos desprotegidos. Así pues, cuando hacemos footprinting podemos trabajar a favor de la seguridad informática o en contra de ella.

Un paso imprescindible dentro del proceso de footprinting es preguntar al buscador (Google, Bing, etc.) por la información que queremos localizar. Los crawlers o arañas web de los buscadores suelen indexar algunas páginas que no deberían haber sido publicadas y que se han guardado en la caché. El servicio archive.org nos permitirá verlas.

Seguiremos refinando la búsqueda con diferentes verbos y combinaciones de palabras, como puede ser «-» (guión), que indica que queremos ver todos los resultados menos los del dominio objetivo.

Podemos distinguir algunos operadores:

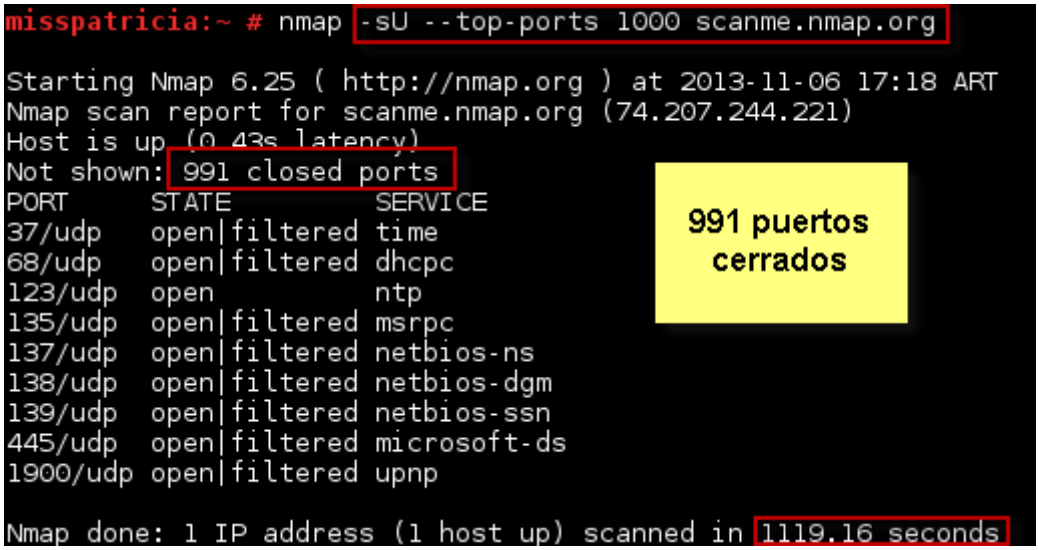
«site»: lista toda la información que aparece en un dominio concreto y sobre una búsqueda específica.

«filetype» o «ext»: busca archivos de un formato determinado, como PDF, JPG, RPD, imágenes, etc.

«intitle»: busca páginas con ciertas palabras en el campo «title».

«inurl»: para buscar páginas con ciertas palabras en la URL.

3.2 Escaneo de puertos



El término **escáner de puertos o escaneo de puertos** se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido por un cortafuegos.

Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos. Es usado por administradores de sistemas para analizar posibles problemas de seguridad, pero también es utilizado por usuarios malintencionados que intentan comprometer la seguridad de la máquina o la red.

Existen varios programas para escanear puertos por la red. Uno de los más conocidos es Nmap, disponible tanto para Linux como Windows.

Cuando se ha completado el escaneo de la red y se ha compilado una lista de hosts disponibles, puede usar un escáner de puerto para identificar el uso de los puertos de hosts disponibles. El escaneo de puertos típicamente clasificará los puertos en una de tres categorías:

- **Abierto:** el host deseado responde con un paquete que indica que está activo en ese puerto. También indica que el servicio que se usó para el escaneo (típicamente TCP o UDP) también está en uso.
- **Cerrado:** el host de destino recibe el paquete de solicitud e indica que no hay ningún servicio activo en ese puerto.
- **Filtrado:** un escáner de puertos clasifica un puerto como filtrado cuando se envía un paquete de solicitud, pero no se recibe una respuesta. Esto generalmente indica que el paquete de solicitud ha sido filtrado y eliminado por un firewall.

3.3 Enumeración

La enumeración de red (network enumeration) es una actividad de la informática en la cual se consigue información de usuarios , grupos o dispositivos y demás servicios relacionados de una red de computadoras. No debe ser confundido con mapeo de red, el cual sólo recupera la información sobre qué servidores están conectados a una red concreta y qué sistemas operativos corren en ellos.

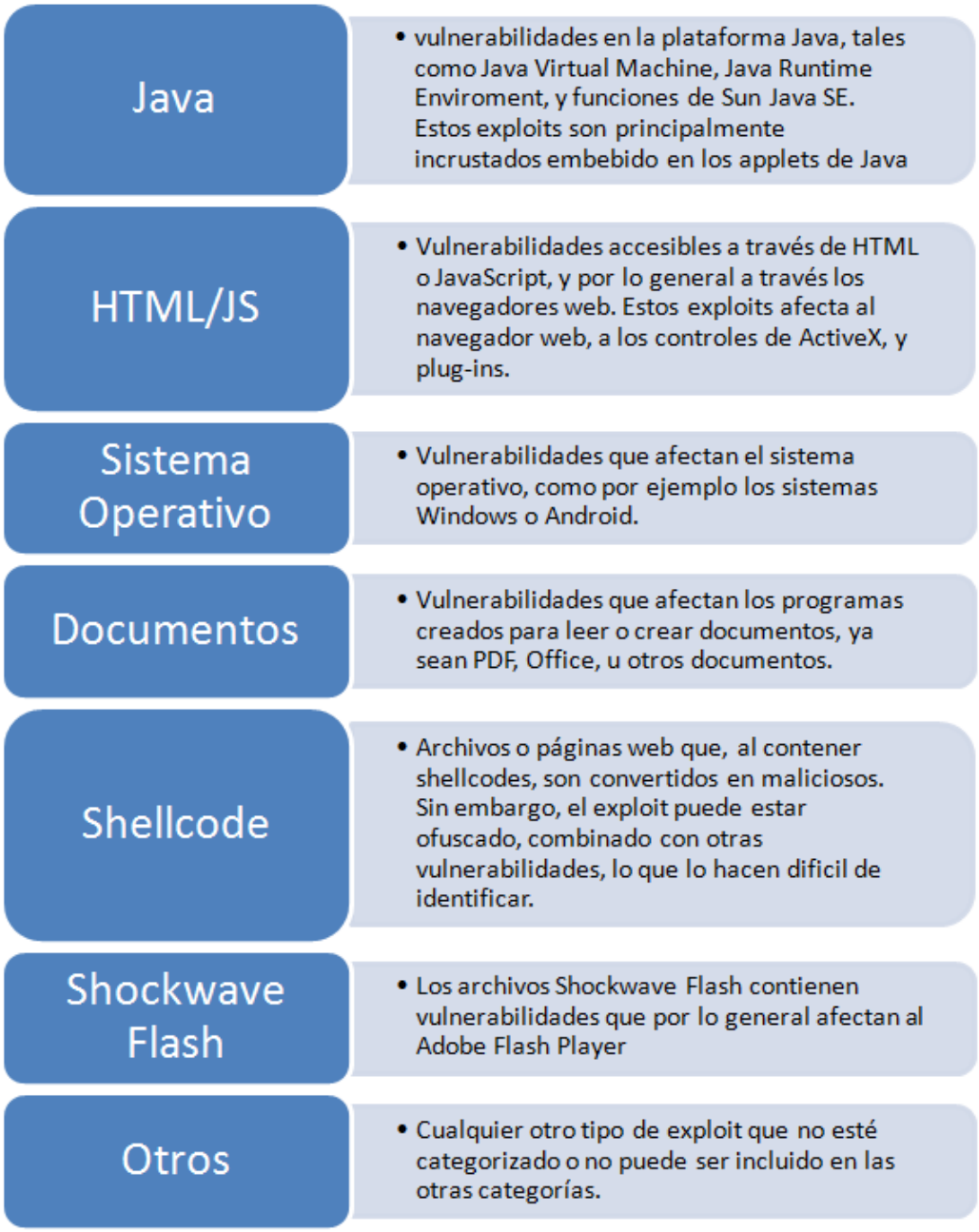
Netflows

Host	Process	Create Time	Protocol	Local Address	Remote Address
XU76QW	C:\RECYCLER\sharescan.exe	2015-09-28T19:20:58.171333	UDP	192.168.0.247:56793	192.168.0.168:137
XU76QW	C:\RECYCLER\sharescan.exe	2015-09-28T19:20:58.186958	UDP	192.168.0.247:56794	192.168.0.160:137
XU76QW	C:\RECYCLER\sharescan.exe	2015-09-28T19:20:58.421333	UDP	192.168.0.247:59101	192.168.0.254:137
XU76QW	C:\RECYCLER\sharescan.exe	2015-09-28T19:20:58.686958	UDP	192.168.0.247:64315	192.168.0.78:137
XU76QW	C:\RECYCLER\sharescan.exe	2015-09-28T19:20:59.046333	UDP	192.168.0.247:56913	192.168.0.80:137
XU76QW	C:\RECYCLER\sharescan.exe	2015-09-28T19:20:59.874458	UDP	192.168.0.247:56817	192.168.0.169:137
XU76QW	C:\RECYCLER\sharescan.exe	2015-09-28T19:21:01.155708	UDP	192.168.0.247:49383	192.168.0.150:137
XU76QW	C:\RECYCLER\sharescan.exe	2015-09-28T19:21:01.327583	UDP	192.168.0.247:49384	192.168.0.151:137
XU76QW	C:\RECYCLER\sharescan.exe	2015-09-28T19:21:01.515083	UDP	192.168.0.247:49385	192.168.0.152:137
XU76QW	C:\RECYCLER\sharescan.exe	2015-09-28T19:21:01.577583	UDP	192.168.0.247:49386	192.168.0.237:137

Esta práctica consiste en el descubrimiento de anfitriones o dispositivos en una red de computadoras.Esta actividad tiende a utilizar protocolos de descubrimiento como ICMP y SNMP para recopilar información. También puede escanear varios puertos en anfitriones remotos para buscar servicios conocidos en un intento de identificar la función de un anfitrión remoto. La siguiente etapa de la enumeración es hacer fingerprinting al sistema operativo del anfitrión remoto.

3.4 Perpetración y despliegue de Exploits

Exploit es una palabra inglesa que significa explotar o aprovechar, y que en el ámbito de la informática es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.



Su uso principal es como vector para la inyección de una carga útil (en inglés payload) que ofrezca al atacante algún tipo de acceso y/o control del equipo comprometido. Un payload puede ser utilizado por varios exploits y un mismo exploit puede utilizar varios payloads.

Según la forma en la que el exploit contacta con el software vulnerable:

- **Exploit remoto.** Si utiliza una red de comunicaciones para entrar en contacto con el sistema víctima. Por ejemplo puede usar otro equipo dentro de la misma red interna o tener acceso desde la propia Internet.
- **Exploit local.** Si para ejecutar el exploit se necesita tener antes acceso al sistema vulnerable. Por ejemplo, el exploit puede aumentar los privilegios del que lo ejecuta. Este tipo de exploits también puede ser utilizado por un atacante remoto que ya tiene acceso a la máquina local mediante un exploit remoto.
- **Exploit en cliente.** Aprovechan vulnerabilidades de aplicaciones que típicamente están instaladas en gran parte de las estaciones de trabajo de las organizaciones.

Ejemplos típicos de este tipo de software son aplicaciones ofimáticas (p. ej. Microsoft Office, Open Office), lectores de PDF (p. ej. Adobe Acrobat Reader), navegadores (p. ej. Internet Explorer, Firefox, Chrome, Safari), reproductores multimedia (p. ej. Windows Media Player, Winamp, iTunes). El exploit está dentro de ficheros interpretados por este tipo de aplicaciones y que llega a la máquina objetivo por distintos medios (p. ej. mediante un correo o en una memoria USB). El archivo será usado por el programa y si no es detenido por ningún otro programa (p. ej. cortafuegos o antivirus) aprovechará la vulnerabilidad de seguridad. Las peculiaridades de este tipo de ataques son:

- Requieren la intervención del usuario del lado del cliente. Por ejemplo, necesitan que abra cierto archivo o que haga clic en cierto enlace.
- Es un ataque asincrónico porque el momento en que se lanza no es el mismo en que se consigue ejecutar el exploit (ya que necesita la acción del usuario).
- Se lanza a ciegas, no se sabe qué aplicaciones y versiones de esta utiliza el objetivo real.

Según el propósito de su ataque:

- Curiosidad
- Fama personal
- Beneficio personal
- Espionaje

3.5 Puertas traseras

Una puerta trasera o backdoor es una vulnerabilidad que permite entrar en un servidor, página web, red local o empresarial sin ser detectado y con ciertos privilegios (o no, depende) para poder hacer casi lo que quieras. La inmensa mayoría de las puertas traseras son errores genuinos, es decir, o bien se generan por un error del usuario o del programador, o de los administradores de red. Esto es peligroso porque el usuario desconoce que existe esa puerta abierta sin protección.

Ver también:

- https://www.redeszone.net/2016/06/16/descubren-una-nueva-backdoor-los-procesadores-intel-x86-i
- https://hipertextual.com/2013/07/edward-snowden-microsoft-colaboro-con-prism
- https://www.genbeta.com/actualidad/microsoft-confirma-que-la-nsa-desarrollo-el-fallo-del-que-se-a
- https://spa.small-business-tracker.com/snowden-nsa-planted-backdoors-cisco-products-468964
- https://www.europapress.es/portaltic/ciberseguridad/noticia-dos-marcas-routers-baratos-chinos-incluyen-puerta-trasera-permite-controlar-trafico-disposi html
- https://www.theregister.com/2013/09/19/linux_backdoor_intrigue/
- https://sneak.berlin/20201112/your-computer-isnt-yours/

Otro pequeño porcentaje de puertas traseras se generan con conocimiento de causa, simplemente como un recurso de un programador (con buenas o malas intenciones, aunque sea más frecuente lo segundo) para acceder a «su» sistema cuando así lo desee. Las razones para dejar una puerta abierta y acceder más tarde a un servidor, una página web o un servicio determinado para realizar la tarea que sea son múltiples.

En esencia hay dos tipos de backdoor o puertas traseras: las que se intentan instalar en nuestro sistema y las que ya existen en nuestro sistema (en el sistema operativo o en aplicaciones conocidas).

El primer tipo de puerta trasera es fácilmente detectable por los antivirus modernos, y se elimina con igual facilidad. En el caso de las puertas traseras en aplicaciones lícitas, hemos de confiar en que la empresa desarrolladora haga un buen uso de ellas, o bien la comunidad de desarrolladores si nos referimos al software libre. Como siempre, nuestra recomendación principal es mantener nuestro sistema limpio, actualizado y con un buen antivirus instalado.

3.6 Borrado de huellas

Una vez que el atacante ha comprometido un sistema evitará ser descubierto, para lo que borrará toda traza de sus movimientos en los equipos comprometidos. Para evitar que pueda conseguirlo, lo mejor es que los **empleados utilicen sus equipos sin permisos de administración**, de manera que si su equipo es comprometido, el atacante tendrá los mismos permisos que éste y no podrá eliminar los registros de actividad. Además es interesante **centralizar los registros de actividad** en un servidor central.

CAPÍTULO 4

¿Qué es la informática forense?

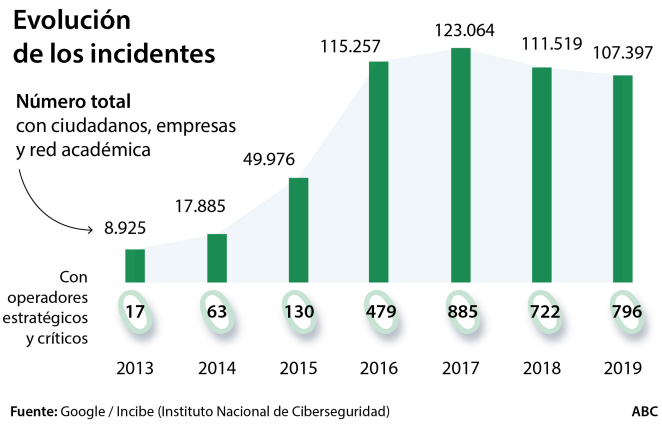
4.1 Motivación

El análisis forense es un área perteneciente al ámbito de la seguridad informática surgida a raíz del incremento de los diferentes incidentes de seguridad. En el análisis forense se realiza un análisis posterior de los incidentes de seguridad, mediante el cual se trata de reconstruir cómo se ha penetrado o vulnerado el sistema. Por tanto, cuando se está realizando un análisis forense se intenta responder a las siguientes preguntas:

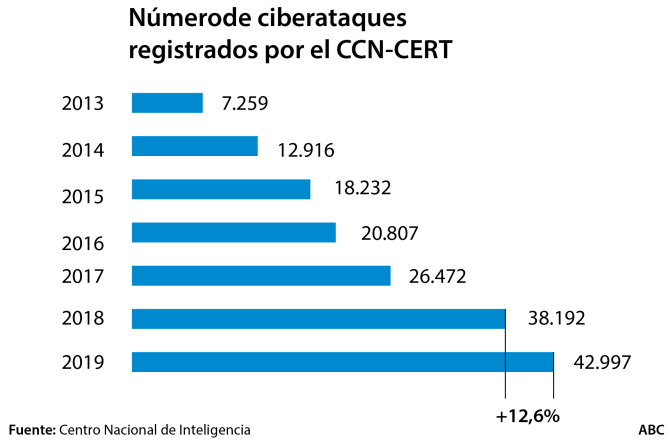
- ¿Quién ha realizado el ataque?
- ¿Cómo se realizo?
- ¿Qué vulnerabilidades se han explotado?
- ¿Qué hizo el intruso una vez que accedió al sistema?

El área de la ciencia forense es la que más ha evolucionado dentro de la seguridad, ya que (tal y como se muestra en las siguientes figuras) los incidentes de seguridad han incrementado en los últimos años. Además, los ataques son diferentes y por tanto hay que actualizar las técnicas de análisis en cada mo- mento.

En la figura siguiente se ve la evolución de los incidentes de seguridad desde 2013 a ciudadanos, empresas y a la red académica española. Como se puede observar, en el año 2013 nos en contrábamos con menos de 9000 incidentes y en el 2019 llegaron casi a 108.000



En la siguiente figura se puede observar el número de ciberataques registrados por el Centro Criptológico Nacional Computer Emergency Response Team (CCN-CERT). CCN-CERT es el organismo español, creado en 2006, encargado de contribuir a la ciberseguridad de la administración pública, los organismos públicos y empresas estratégicas del país. El CCN está intregrado en el servicio de inteligencia español (CNI).



4.2 Evolución de la informática forense

Es difícil precisar el primer examen «informático forense» o el comienzo de la materia. La mayoría de los expertos coinciden en que el campo de la informática forense comenzó a evolucionar hace más de 30 años. El campo comenzó en los Estados Unidos, en gran parte, cuando los agentes de la ley y los investigadores militares comenzaron a ver cómo los criminales se volvían técnicos. El personal del gobierno encargado de proteger información importante, confidencial y secreta llevó a cabo exámenes forenses en respuesta a posibles violaciones de seguridad no solo para investigar la infracción en particular, sino también para aprender cómo prevenir futuras infracciones potenciales. En última instancia, los campos de la seguridad de la información, que se centra en proteger la información y activos informáticos, y la informática forense, que se centra en la respuesta a delitos de alta tecnología, se comenzaron a entrelazar.

Durante las próximas décadas, y hasta hoy, el campo está continuamente evolucionando. Tanto el gobierno como las organizaciones privadas han seguido su ejemplo, contratando profesionales de seguridad de la información y profesionales de informática forense.

Recientemente el sector legal ha visto la necesidad de utilizar exámenes forenses informáticos en disputas legales civiles, lo que ha provocadp una explosión en est campo.

La historia de la ciencia forense se remonta a miles de años. La toma de huellas dactilares fue una de sus primeras aplicaciones. Los antiguos chinos usaban huellas dactilares para identificar documentos comerciales. En 1892, un eugenista llamado Sir Francis Galton estableció el primer sistema para clasificar huellas dactilares. Sir Edward Henry, comisionado de la Policía Metropolitana de Londres, desarrolló su propio sistema en 1896 basado en la dirección, el flujo, el patrón y otras características de las huellas dactilares. El sistema de clasificación de Henry se convirtió en el estándar para técnicas de huellas dactilares criminales en todo el mundo.

En 1835, Henry Goddard de Scotland Yard se convirtió en la primera persona en utilizar el análisis físico para conectar una bala al arma homicida. El examen de balas se volvió más preciso en la década de 1920, cuando el médico estadounidense Calvin Goddard creó el microscopio de comparación para ayudar a determinar qué balas provienen de qué casquillos. Y en la década de 1970, un equipo de científicos en la Corporación Aeroespacial de California desarrolló un método para detectar residuos de disparos utilizando microscopios electrónicos de barrido.

En 1836, un químico escocés llamado James Marsh desarrolló una prueba química para detectar arsénico, que se utilizó durante un juicio por asesinato. Casi un siglo después, en 1930, el científico Karl Landsteiner ganó el Premio Nobel por clasificar la sangre humana en sus diversos grupos. Su trabajo allanó el camino para el futuro uso de sangre en investigaciones criminales. Otras pruebas fueron desarrollado a mediados del siglo XX para analizar la saliva, el semen y otros fluidos corporales, así como para análisis de sangre más precisos.

En 1984, el programa Magnetic Media del FBI, que más tarde pasó a llamarse Computer Analysis y Response Team (CART), fue creado y se cree que es el comienzo de la informática forense.

En 1988, se funda la Asociación Internacional de Especialistas en Investigación en Computación (IACIS), corporación internacional sin ánimo de lucro compuesta por profesionales forenses informáticos voluntarios dedicada a la formación y certificación de profesionales en el campo de la informática forense.

Fue seguido por la formación de la Organización Internacional de Evidencia Informática (IOCE) en 1995, que tiene como objetivo reunir a organizaciones comprometidas activamente en el campo de la tecnología digital y evidencia multimedia para fomentar la comunicación y la cooperación, así como para garantizar la calidad y coherencia dentro de la comunidad forense.

Con el aumento de los delitos cibernéticos, las naciones del G8 se dieron cuenta de la importancia de la informática forense y en 1997 declaró que “el personal encargado de hacer cumplir la ley debe estar capacitado y equipado para abordar los delitos de alta tecnología”. En 1998, el G8 nombró al IICE para crear principios y directrices internacionales y procedimientos relacionados con la evidencia digital. En el mismo año, tuvo lugar el simposio «INTERPOL Forensic Science». El primer laboratorio forense informático regional del FBI se estableció en 2000 en San Diego.

4.3 Informática Forense

La informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en soportes informáticos. Se trata de una práctica cada vez más habitual debido al uso que actualmente todos realizamos de las nuevas tecnologías, y que permite resolver casos policiales o judiciales.

Aunque un delito no sea informático, sí que hay evidencias digitales, y puesto que todas las actividades que se realizan con un dispositivo (de forma manual o automática) dejan una prueba, es posible que la misma sea analizada junto con el resto de pruebas de un caso.

Esta ciencia está adquiriendo un papel muy importante en los últimos años ya que cada día es más habitual tener que hacer frente a diferentes incidentes relacionados con la seguridad informática como por ejemplo: intrusiones, robos de información, infecciones, etc.

Su uso está extendido por muy diversos campos, entre los que destacan:

- Persecución de delitos como fraude financiero y evasión de impuestos.
- Pornografía infantil.
- Casos de discriminación o acoso.
- Investigación de seguros.
- Recuperación de ficheros eliminados.
- Casos de robo de la propiedad intelectual.
- Ciberterrorismo.
- Asegurar la resiliencia de las empresas, es decir, la capacidad de recuperación frente a ataques.

El Incibe (Instituto Nacional de Tecnologías de la Comunicación) define la informática forense como:

Importante: El proceso de investigación de los sistemas de información para detectar toda evidencia que pueda ser presentada como medio de prueba fehaciente para la resolución de un litigo dentro e un procedimiento judicial.

De la definición anterior hay que sacar dos ideas clave, que la informática forense es un **proceso de investigación** y que las **evidencias** que obtengamos deben de poder ser presentadas como **medio de prueba** en un procedimiento judicial.

Otros autores (Brown, 2010) definen la informática forense como **«The art and science of applying computer science knowledge and skills to aid the legal process»**.

Brown cataloga a la vez a la informática forense como arte y como ciencia. Porque, como comenta el autor, aunque la informática forense se base en procedimientos ya definidos o en el uso de herramientas que ayuden al investigador, los buenos investigadores forenses tienen la habilidad de ir un paso más allá en la investigación y llegar a pensar como el autor al que se está intentando encontrar.

Nota: Un buen analista forense, tiene que disfrutar de su trabajo siendo a la vez un gran profesional.

Desde un punto de vista más empresarial, podríamos ver la informática forense como un fin:

Importante: La informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos. Gracias a ella, las empresas obtienen una respuesta a problemas de privacidad, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial surgidos a través de uso indebido de las tecnologías de la información. Mediante sus procedimientos se identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal.

Tanto las fuerzas y cuerpos de seguridad del Estado como los peritos informáticos forenses utilizan herramientas y procedimientos específicos para la recolección de evidencias de dispositivos que van desde ordenadores o teléfonos móviles hasta servidores de correo electrónico, por ejemplo.

4.4 La evidencia digital

Otro concepto relacionado con la informática forense y que también debemos de conocer es el concepto de **evidencia digital**.

Importante: Evidencia digital es todo elemento que pueda almacenar información en formato electrónico, de forma física o lógica y que permita constatar un hecho investigado o el esclarecimiento del mismo.

La evidencia digital abarca todos y cada uno de los datos digitales que pueden establecer que se ha cometido un delito o puede proporcionar un vínculo entre un delito y su víctima o un delito y su autor. Algunos ejemplos de evidencias digitales serían:

- Documento electrónico de texto
- Archivo de imagen o vídeo
- Historiales de navegación
- Archivos temporales de navegación
- Cookies del explorador
- Registros de eventos del sistema operativo
- Ficheros de logs (accesos a sistemas)
- Registros del tráfico de red del equipo
- Envíos de correos electrónicos

- Direcciones IP
- Localizaciones geográficas
- Chats
- Borrado de datos

y un sinfín de información es analizada para investigar delitos contra la propiedad intelectual, espionaje industrial, vulneración de la intimidad y/o robo de datos entre otros delitos

Los sistemas de detección de intrusos (IDS) son una gran fuente de evidencias digitales. Recopilan información de una gran variedad de fuentes, como pueden ser sistemas y redes, y luego analizan esta información en busca de signos de intrusión y mal uso. Hay dos tipos de IDS: basados en host y en red.

En la arquitectura de detección de intrusiones basada en host, el sistema se utiliza para analizar datos que se originan en computadoras (hosts). Por tanto, esta arquitectura se utiliza para detectar ataques internos y uso indebido. Por ejemplo, un empleado que abusa de sus privilegios, oestudiantes cambiando sus calificaciones. Los sistemas basados en host examinan eventos como qué archivos son accedidos y qué aplicaciones se ejecutan. Los registros se utilizan para recopilar estos datos de eventos. Sin embargo, la política de auditoría que se esté empleando resulta muy importante porque define qué acciones del usuario final dará como resultado que un registro de eventos se escriba en un registro de eventos, por ejemplo, registrando todos accesos de archivos de misión crítica. Los sistemas de detección de intrusos basados en host residen en cada sistema y generalmente informan a una consola de comando central. Para detectar mal uso, firmas o patrones predefinidos de mal uso que se comparan con los datos de los archivos de registro. Cuando existe una correlación, o se notifica al administrador de seguridad del posible uso indebido o se ejecuta una respuesta predefinida al mal uso.

En la arquitectura de detección de intrusos basada en red, el sistema se utiliza para analizar paquetes de red. Las arquitecturas basadas en red se utilizan para detectar intentos de acceso e intentos de denegación de servicio que se originan fuera de la red. Esta arquitectura consiste en una conjunto de sensores desplegados en una red. Estos sensores informan a una consola central. De forma similar a las arquitecturas basadas en host, se utilizan las firmas de contenido de los paquetes para identificar el mal uso. Estas firmas se basan en el contenido de paquetes, encabezados y flujo de tráfico. Sin embargo, es importante tener en cuenta que el cifrado evita la detección de cualquier patrón en el contenido del paquete.

Sin embargo, debido a que la detección de intrusos basada en la red puede relacionar información tal como direcciones IP falsificadas (spoofing) con usuarios válidos, podría darse el caso de que se atribuyan erróneamente acciones de mal uso del sistema. Esto hace que la detección de intrusiones basada en la red proporcione datos inválidos, lo que también invalida la mayoría, pero no toda la evidencia digital de la red. Sin embargo, los datos de detección de intrusos basados en el host pueden ser una evidencia digital válida.

4.5 Cadena de custodia de las evidencias digitales

Como se ha comentado al principio del apartado, las evidencias que obtengamos de un análisis forense deben de poder ser presentadas como medio de prueba en un procedimiento judicial. Pero, para que un elemento pueda servir como elemento probatorio en un procedimiento judicial se tiene que poder asegurar que dicho elemento no ha sido alterado desde el momento de su recolección hasta su análisis y presentación. Para ello se utiliza la cadena de custodia.

La cadena de custodia es el proceso mediante el cual la evidencia es transmitida sin modificación alguna, desde quien la ocupa, hasta quien la analiza. Los objetivos que se a conseguir mediante el uso de la cadena de custodia son:

1) Garantizar la integridad de la evidencia, impidiendo que se realice cualquier cambio sobre la misma.
2) Garantizar su autenticidad, permitiendo contrastar su origen.
3) Garantizar la posibilidad de localización, permitiendo saber en cualquier momento dónde se encuentra una evidencia.
4) Garantizar la trazabilidad de los accesos a la evidencia.
5) Garantizar su preservacióna largo plazo.

En el ámbito del análisis forense, el mantenimiento de la cadena de custodia se suele llevar a cabo mediante la documentación de las personas custodiantes de la evidencia y el uso de funciones hash que garanticen la integridad de la misma.

Así mismo, se ha de llevar un registro de las personas que realicen cualquier operación con la evidencia, indicando la operación realizada, la fecha en que dicha operación ha sido realizada (inicio y finalización) y la persona que la ha realizado.

4.6 Objetivos de un análisis forense

Importante: Los objetivos de la informática forense son proporcionar pautas para:

- Seguir el procedimiento de respuesta inmediata y acceder al sistema informático de la víctima después de un incidente de seguridad.
- Diseñar procedimientos en la escena del crimen para asegurar que las evidencias digitales obtenidas no están dañadas.
- Adquisición y duplicación de datos.
- Recuperar archivos borrados y particiones borradas de medios digitales para extraer las evidencias y validación de las mismas.
- Proporcionar pautas para analizar medios digitales para preservar las evidencias, analizar registros y derivar conclusiones, investigar el tráfico de red y los registros para correlacionar eventos, investigar ataques inalámbricos y web, rastrear correos electrónicos e investigar delitos de correo electrónico.

- Elaboración de informes forenses que proporcionen información completa del proceso de investigación forense en el sistema informático.
- Conservar las evidencias siguiendo la cadena de custodia.
- Emplear los procedimientos rigurosos necesarios para que los resultados forenses resistan escrutinio en un tribunal de justicia.
- Presentar resultados de análisis forense digital en un tribunal de justicia como testigo experto.

El fin último de toda investigación forense es el esclarecimiento de los hechos ocurridos de acuerdo a las evidencias recogidas en la **escena del delito**.

Para ello, dependiendo del delito que se esté investigando, deberemos responder estas tres preguntas:

1. ¿Qué se ha hecho?
2. ¿Cómo se ha hecho?
3. ¿Quién lo ha realizado?

Para responder a la primera de las preguntas, hay que ser capaz de **detectar los accesos o cambios no autorizados** que se han realizado en el sistema. Estos cambios no tienen que consistir únicamente en la alteración física de un fichero, modificándolo o eliminándolo, también hay que ser capaces de saber qué ficheros fueron accedidos, aunque solo se trate de la lectura y/o copia de los mismos.

Un ejemplo de acceso no autorizado, podría ser el **acceso a la información del teléfono móvil de una persona**, cómo ha sucedido con el teléfono de algunos famosos, en los que un atacante accede a los datos contenidos en el mismo, sin alterarlos.

Con la pregunta *«¿Cómo se ha hecho?»*, lo que se busca es **reconstruir los pasos dados por el autor** de los hechos para llegar a comprender cómo hizo lo que hizo, y ser capaces de evitar en un futuro que el método utilizado para realizar la alteración se repita.

La última de las preguntas plantea el reto de saber **quién fue el autor material de los hechos**. Quién ha realizado las modificaciones que han sido detectadas.

En otros ámbitos de la investigación forense, como pueden ser el análisis dactiloscópico (análisis de las huellas dactilares) o el de ADN, es posible identificar plenamente a la persona autora de los hechos; en el análisis forense no se puede llegar a ser tan precisos.

Nota: Cuando se realiza un análisis forense, la conclusión más concreta a la que se va a llegar va a ser el usuario (local o remoto) que realizo las modificaciones y/o la dirección IP o MAC de la máquina desde la cual dichas modificaciones fueron realizadas. Por lo que tenemos que ayudarnos de otras técnicas de investigación si se quiere dar con la persona física autora de los hechos.

4.7 Etapas de un análisis forense

Las etapas de un análisis forense son (NIST 2006):

1. Recolectar
2. Preservar
3. Analizar
4. Presentar

La **recolección** de las evidencias es el **primer paso** que se da a la hora de realizar un análisis forense. Consiste en **obtener las evidencias** que consideremos de **interés** de manera que posteriormente puedan ser analizadas. Asemejando el hecho al ámbito forense tradicional, la recolección de las evidencias sería algo así como la recogida de una muestra de sangre dentro de la escena de un crimen. La diferencia es que nuestra escena del crimen no es la habitación de un domicilio, si no que es un equipo informático y la sangre que tenemos que recoger puede ser desde un sencillo archivo de logs, hasta el disco (o discos) duro completo.

Como hemos nombrado anteriormente, algunos ejemplos de evidencias digitales podrían ser: un documento electrónico de texto, un archivo de imagen o vídeo, los archivos temporales de navegación, etc. Incluyendo también otro tipo de evidencias como pendrives, DVDs, discos duros externos, etc.

Importante: En definitiva, habría que recolectar cualquier elemento generado o almacenado en un sistema de la información, y que pueda ser utilizado como prueba en un proceso legal.

La recolección de las evidencias tiene que hacerse con medios que aseguren, en la medida de lo posible, la **no modificación** de las mismas:

> **Atención:** Artículo 482.3 de la Ley de Enjuiciamiento Criminal (LECrim). [...] el Juez o quien lo represente adoptará las precauciones convenientes para evitar cualquier alteración en la materia de la diligencia pericial.

Siendo necesaria la **documentación de los cambios** que tengamos que haber realizado en el equipo para la recolección, si no ha sido posible evitar su modificación.

> **Atención:** Artículo 479 de la LECrim. Si los peritos tuvieren necesidad de destruir o alterar los objetos que analicen, deberá conservarse, a ser posible, parte de ellos a disposición del Juez, para que, en caso necesario, pueda hacerse nuevo análisis.

La **preservación** de las evidencias tiene por objetivo el garantizar que lo que se **analiza es lo mismo que previamente se ha recolectado** cumpliendo así con el procedimiento de cadena de custodia, requisito indispensable para que una evidencia tenga validez judicial.

En el ámbito del análisis forense, el hecho de realizar una imagen o clonado de un dispositivo (como puede ser un disco duro, o un pendrive) con medios certificados para ello (clonadoras hardware como la Logicube Forensic Talon o la Tableau Imager, entre otras, han sido testeadas y aprobadas por el Departamento de Justicia de Estados Unidos), ya es una garantía de que lo que se copia es imagen fiel y exacta de lo que se ocupa; pero dada la relativa facilidad de modificación de la evidencia y/o de la copia, se debe garantizar la integridad a lo largo de todos los procesos a los que estas sean sometidas.

Nota: Puedes encontrar más información sobre las herramientas testeadas y aprobadas por el Departamento de Justicia de Estados Unidos en: http://nij.ncjrs.gov/App/publications/Pub_search.aspx?searchtype=basic&category=9&location=top&PSID=

Para ello, se hace uso de funciones resumen hash (como MD5 o SHA1). El procedimiento (que será explicado más detalladamente en posteriores temas) consiste en realizar un resumen digital a la evidencia original y a la copia, de manera que si ambos resúmenes coinciden, se asegura que el contenido de la evidencia original y el de la copia son exactamente iguales.

Posteriormente, y a lo largo de todos los procesos que se realicen, se puede verificar que se **está analizando lo que en su momento se ocupó** realizando nuevamente un resumen digital y comparando el resultado con el primer resultado obtenido.

El **análisis** de las evidencias es la etapa en la que se intenta responder a las tres preguntas mencionadas:

- ¿**Qué** se ha hecho?
- ¿**Cómo** se ha hecho?
- ¿**Quién** lo ha hecho?

Durante el análisis, las evidencias que han sido recolectadas y preservadas previamente se estudian, con el fin de concluir si los hechos objeto de la investigación son ciertos o no.

La **presentación** es la última etapa de un análisis forense y consiste en la **realización de un informe pericial** en el que se detallen (Artículo 478 de la LECrim.):

1. La **descripción** del equipo informático o dispositivo objeto del mismo.
2. Los **procedimientos** realizados por los peritos y sus **resultados**.
3. Las **conclusiones** a las que los peritos han llegado en base a los resultados obtenidos.

4.8 Tipos de análisis forense

Dependiendo del punto de vista nos vamos a encontrar diferentes tipos de análisis forense. Si lo vemos desde el punto de vista de lo que se va a analizar, nos encontraremos los siguientes tipos:

- **Análisis forense de sistemas:** en este análisis se tratarán los incidentes de seguridad acaecidos en servidores y estaciones de trabajo con los sistemas operativos:

Mac OS, sistemas operativos de Microsoft (Windows 9X/Me, Windows 2000 server/workstation, Windows 2003 Server, Windows XP, Windows Vista, Windows 2008 Server, etc.), sistemas Unix (Sun OS, SCO Unix, etc.) y sistemas GNU/Linux (Debian, RedHat,Suse, etc.).

- **Análisis forense de redes:** en este tipo se engloba el análisis de diferentes redes (cableadas, wireless, bluetooth, etc.).
- **Análisis forense de sistemas embebidos:** en dicho tipo se analizaran incidentes acaecidos en móviles, PDA, etc. Un sistema embebido posee una arquitectura semejante a la de un ordenador personal.

CAPÍTULO 5

Entorno Legal

En este punto veremos las leyes de la legislación española que debemos tener en cuenta a la hora de realizar el análisis forense de un sistema telemático en este país.

5.1 Ley de Enjuiciamiento Civil

La Ley de Enjuiciamiento Civil establece el marco legal, mediante el cual se regulan los procesos civiles, los tribunales y quienes ante ellos acuden e intervienen.

5.2 Derechos fundamentales

Los derechos fundamentales son aquellos derechos humanos garantizados con rango constitucional que se consideran como esenciales en el sistema político que la Constitución funda y que están especialmente vinculados a la dignidad de la persona humana.

La Constitución española otorga a todos los ciudadanos una serie de derechos fundamentales y libertades públicas, reguladas por el título I de la Constitución, capítulo 2, sección 1.

Los derechos se dividen fundamentalmente en 3 tipos, según el ámbito:

1) personal.
2) público.
3) económico y social.

Dentro de estos derechos son de particular interés los siguientes:

- Derecho a la seguridad jurídica y tutela judicial, la cual nos garantiza un proceso penal con garantías.

- Derecho al secreto de las comunicaciones.
- Derecho a la vida privada. En este derecho se incluye el derecho a la intimidad, una vida privada, derecho al honor y la propia imagen. Asimismo se incluye la limitación del uso de la informática para proteger la intimidad.
- Derecho fundamental a la protección de datos. En el año 2000 en la sentencia 292/2000, el Tribunal Constitucional crea el derecho fundamental a la protección de datos como un derecho diferente al de intimidad.

5.3 Normativa de ciberseguridad

En nuestro país existe un Código de Derecho de la Ciberseguridad, publicado en el Boletín Oficial del Estado, que cita las principales normas a tener en cuenta con relación a la protección del ciberespacio.

5.3.1 Normativas de seguridad nacional

- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que regula los principios y organismos clave así como las funciones que deberán desempeñar para la defensa de la Seguridad Nacional.
- Orden TIN/3016/2011, de 28 de Octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.

5.3.2 Normativas de seguridad

- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.
- Ley 5/2014, de 4 de abril, de Seguridad Privada.

5.3.3 Referidas a las telecomunicaciones

- Ley 34/2002, de 11 de julio, de servicios a la sociedad de la información y comercio electrónico.
- Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido o irregular con fines fraudulentos en comunicaciones electrónicas.
- Ley 50/2003, de 19 de diciembre, de firma electrónica.
- La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Todas esas leyes relacionadas con la seguridad de la información están diseñadas con el objetivo de ofrecer un marco normativo que permita garantizar la seguridad de la información digital y establecer una legislación común a nivel europeo.

5.4 Ley Orgánica de Protección de Datos

LOPD son las siglas abreviadas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Esta Ley fundamentalmente tiene el objetivo de proteger a las personas físicas con respecto al tratamiento que se pueda realizar de sus datos propios por distintos sujetos, ya sean públicos o privados.

Dicha regulación pretende, fundamentalmente, establecer un control sobre quién tiene dichos datos, para qué los usa y a quién se los cede. Para ello, impone una serie de obligaciones a los responsables de dichos ficheros de datos:

- Recabar el consentimiento de los titulares de los datos para poder tratarlos
- Comunicar a un registro especial la existencia de dicha base de datos y su finalidad, así como mantener unas medidas de seguridad mínimas de la misma, en función del tipo de datos recogidos.
- Reconoce una serie de derechos al individuo sobre sus datos, como son los de información, acceso, rectificación e, incluso, de cancelación de los mismos en determinados supuestos.

Finalmente, se designa a una entidad: la Agencia de Protección de Datos, como órgano administrativo encargado de hacer cumplir la LOPD y sus reglamentos, pudiendo inspeccionar e imponer fuertes sanciones a aquellos sujetos que no cumplan con la misma.

Dentro del Reglamento de Desarrollo de la LOPD (RD 1720/2007), existen tres niveles de seguridad distintos: el básico, el medio y el alto. Para saber qué nivel debemos de aplicar, debemos referirnos al tipo de datos personales almacenados en el fichero. Para ello, estaremos a lo dispuesto en el artículo 81 del Reglamento, del que se deduce lo siguiente:

1) Nivel básico:
   - Aplicable a todos los sistemas con datos personales en general.
2) Nivel medio:
   - Datos de comisión de infracciones administrativas o penales.
   - Datos de Hacienda pública.
   - Datos de servicios financieros.
   - Datos sobre solvencia patrimonial y crédito
   - Conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.
3) Nivel alto:
   - Datos sobre ideología.
   - Datos sobre religión.

- Datos sobre creencias.
- Datos sobre origen racial.
- Datos sobre salud o vida sexual.
- Datos recabados para fines policiales, y
- Datos sobre violencia de género.

Estas medidas de seguridad se aplican de forma acumulativa, así, el nivel alto deberá cumplir también las reguladas para el nivel medio y el nivel bajo de seguridad.

La Ley Orgánica de Protección de Datos y de Garantía de Derechos Digitales de 2018 (LOPDGDD), fue aprobada por el Congreso el 18 de octubre. Sus siglas son un complemento de su antecesora, la LOPD, y "reflejan los nuevos derechos" consignados en esta nueva normatividad.

Dentro de los 97 artículos dispuestos por la nueva Ley Orgánica, se pueden encontrar algunos puntos relevantes como:

- **El derecho al olvido:** la LOPDGDD privilegia la defensa de la privacidad, intimidad y protección de los datos otorgados a través de Internet, por lo cual el usuario podrá reclamar y exigir la supresión de sus datos personales presentes en redes sociales o buscadores. Existen tres casos por los cuales se puede solicitar dicha eliminación:
  - Cuando la finalidad de los datos recogidos ha sido alcanzada,
  - Cuando el usuario retira su consentimiento del uso de los datos, y
  - Cuando la obtención y el tratamiento de los datos hayan sido por la vía ilícita.

Con esta nueva disposición, el derecho al olvido supera el enfoque del RGPD, ampliando así el alcance del nuevo artículo.

- **El acceso digital a los menores de edad:** esta nueva ley establece una nueva edad mínima de acceso a las redes sociales por parte de los menores. Ahora, solo los mayores de 14 años están autorizados a dar su consentimiento para el uso de sus datos en Internet, contrario a la antigua ley que establecía los 13 años de edad.

Esta consigna sigue lo establecido por el RGPD, respetando la banda de edad entre los 13 y 16 años.

- **El derecho a la neutralidad de Internet:** los proveedores de servicios de Internet no podrán hacer una oferta en función de una discriminación tecnica o economica. Es decir, que todo tráfico de información que transita por la red, deberá hacerlo de manera transparente, sin que haya lugar al pago de tarifas, por parte de los usuarios, a los contenidos, plataformas o páginas web consultados o accedidos.

Tampoco debe tenerse en cuenta el tipo de equipamiento, dispositivo o método de comunicación que utilizan para el acceso.

- **El derecho al testamento digital:** el título X de la nueva normativa recoge el derecho al testamento digital, el cual establece que "las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión".

5.5 Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico

LSSI-CE son las siglas abreviadas de la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico aprobada el 11 de julio del 2001. Esta ley tiene el objetivo fundamental de regular y proteger a todos aquellos que intervienen en las relaciones ofrecidas por Internet. Dicha regulación pretende, fundamentalmente, establecer una normativa de Internet desde un punto de vista comercial y promocional obligando, por ejemplo a los propietarios de las webs, a incluir los datos de identificación de la empresa de modo perfectamente accesible y claro.

Además prohíbe el correo electrónico comercial no solicitado, también conocido con el nombre de spam.

5.6 Ley de conservación de datos relativos a las comunicaciones y las redes públicas

Esta ley tiene como objetivo conservar los datos que pueden ser relevantes para rastrear las actividades ilícitas y así mejorar la seguridad de los ciudadanos frente a actividades terroristas. Por tanto, pretende establecer una regulación a los operadores de telecomunicaciones para retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados (son los miembros de los Cuerpos de Policia autorizados para ello en el marco de una investigación criminal).

En su artículo 3 nos define los datos objeto de conservación dividiéndolos en diferentes tipos:

- telefonía fija
- telefonía móvil
- acceso a Internet, correo electrónico y telefonía por Internet Los datos que solicitan que sean conservados son todos los necesarios para la trazabilidad de origen a destino de cualquier comunicación telemática.

El periodo de conservación de los datos impuesta cesa a los doce meses, siempre computados desde la fecha en que se haya producido la comunicación.

Aunque podría haber alguna excepción, cuyo periodo mínimo deberá ser de 6 meses y máximo 2 años.

5.7 Ley sobre la seguridad de las redes y sistemas de información

El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información tiene por objeto:

- Regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales.
- Establecer un sistema de notificación de incidentes.

5.8 Código penal

El Código penal nos muestra las actitudes que se han tipificado como delito. El concepto de delito viene descrito en el artículo 10 del Código Penal (Ley Orgánica 10/1995, de 23 de noviembre actualizada el 31/03/2015) (CP): «son delitos o faltas las acciones y omisiones dolosas o imprudentes penadas por la Ley.»

Por tanto, en este apartado comentaremos todas aquellas acciones que se pueden considerar como delitos telemáticos según la LO 10/1995 y varias modificaciones posteriores:

- **Acoso**
  - Artículo 172 ter.: «el que **acose** a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana: 1.ª La vigile, la persiga o busque su cercanía física. 2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas. 3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.»
- **Descubrimiento y revelación de secretos**
  - Artículos 197, 197 bism 197 ter: «descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación»
  - «Por datos personales habrían de entenderse no solo los datos de identidad oficial, en sentido estricto, sino cualesquiera otros, propios de una persona o utilizados por ella, que le identifiquen o hagan posible su identificación frente a terceros tanto en un entorno físico como virtual. Tienen tal consideración no solo el nombre y apellidos, sino también, entre otros, los números de identificación personal como el correspondiente al DNI, el de afiliación a la Seguridad Social o a cualquier institución u organismo público o privado, el número de teléfono asociado a un concreto titular, la dirección postal, el apartado de correos, la dirección de correo electrónico, la dirección IP, la contraseña/usuario de carácter personal, la matrícula del propio vehículo, las imágenes de una

persona obtenidas por videovigilancia, los datos biométricos y datos de ADN, los seudónimos y en general cualquier dato identificativo que el afectado utilice habitualmente y por el que sea conocido.»

- **Delito de acceso ilegal a sistemas informáticos**
  - Artículo 197 bis 1º: «El delito se consuma por el mero hecho de acceder -o facilitar a otro el acceso- a un sistema informático o a parte del mismo aun cuando la acción no vaya seguida del apoderamiento de datos, informaciones o documentos ajenos. En todo caso, cuando para sortear las medidas de seguridad fuera preciso utilizar datos de carácter personal de la víctima, la apreciación del Artículo 197 bis 1º junto con el artículo 197, 4 b) supondría una infracción del principio non bis in idem, debiendo aplicarse en estos casos este último precepto, por mor del principio de especialidad establecido en el artículo 8.1 del CP.»
- **El delito de interceptación ilegal de datos informáticos**
  - Art 197 bis 2º: «Que quien efectúa la interceptación no esté autorizado para ello y que la misma se realice utilizando como medio artificios o instrumentos técnicos, debiendo entenderse por tales cualesquiera herramientas o mecanismos que hagan posible este objetivo aunque no estén específicamente destinados a ello.»
- **El delito de abuso de dispositivos**
  - Artículo 197 ter: «Dichos instrumentos y herramientas pueden ser: programas informáticos y/o contraseñas, códigos de acceso o datos similares que hagan posible el acceso a un sistema. Respecto a los primeros la exigencia legal de que se trate de programas concebidos o adaptados principalmente para cometer determinados delitos remite al software malicioso o malware diseñado para infiltrarse y/o obtener información (programas espía) en un dispositivo o un sistema de información sin el consentimiento de su propietario, quedando excluidos cualquier otro tipo de programas que no reúnan dicha característica, aunque puedan ocasionalmente servir para esa misma finalidad, circunstancia cuya determinación hará necesario generalmente un informe pericial.»
- **Estafas**
  - Artículo 248: «a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.»
- **Exhibicionismo y provocación sexual**
  - Artículo 185: «El que ejecutare o hiciere ejecutar a otra persona actos de exhibición obscena ante menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses»
  - Artículo 186: «El que, por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico entre menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses»

- **Prostitución**
  - Artículo 187: «El que, empleando violencia, intimidación o engaño, o abusando de una situación de superioridad o de necesidad o vulnerabilidad de la víctima, determine a una persona mayor de edad a ejercer o a mantenerse en la prostitución, será castigado con las penas de prisión de dos a cinco años y multa de doce a veinticuatro meses»
  - Artículo 189.1: «1. Será castigado con la pena de prisión de uno a cinco años: a) El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas. b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.»
- **Apología del delito**
  - Artículo 18.1, párrafo 2º: «Es apología, a los efectos de este Código, la exposición, ante una concurrencia de personas o por cualquier medio de difusión, de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor. La apología sólo será delictiva como forma de provocación y si por su naturaleza y circunstancias constituye una incitación directa a cometer un delito»
- **Apología del genocidio**
  - Artículo 608.2: «Los prisioneros de guerra protegidos por el III Convenio de Ginebra de 12 de agosto de 1949 o por el Protocolo I Adicional de 8 de Junio de 1977»
- **Calumnias**
  - Artículo 205: «Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad».
  - Artículo 206: «Las calumnias serán castigadas con las penas de prisión de seis meses a dos años o multa de doce a 24 meses, si se propagaran con publicidad y, en otro caso, con multa de seis a 12 meses».
- **Injurias**
  - Artículo 208: «Es injuria la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.»
  - Artículo 174.3: «quien sea o haya sido su cónyuge o sobre persona que esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia, o sobre los descendientes, ascendientes o hermanos por naturaleza, adopción o afinidad, propios o del cónyuge o conviviente, o sobre los menores o personas con discapacidad necesitadas de especial protección que con él convivan o que se hallen sujetos a la potestad, tutela, curatela, acogimiento o guarda de hecho del cónyuge o conviviente, o sobre persona amparada en cualquier otra relación por la que se encuentre integrada en el núcleo de

su convivencia familiar, así como sobre las personas que por su especial vulnerabilidad se encuentran sometidas a custodia o guarda en centros públicos o privados, será castigado con la pena de prisión de seis meses a tres años, privación del derecho a la tenencia y porte de armas de tres a cinco años y, en su caso, cuando el juez o tribunal lo estime adecuado al interés del menor o persona con discapacidad necesitada de especial protección, inhabilitación especial para el ejercicio de la patria potestad, tutela, curatela, guarda o acogimiento por tiempo de uno a cinco años, sin perjuicio de las penas que pudieran corresponder a los delitos en que se hubieran concretado los actos de violencia física o psíquica.»

- **Delitos contra la intimidad**
  - Artículo 197: «1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.»
- **Estafa**
  - Artículo 248.2: «También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante, consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.»
- **Apropiación indebida**
  - Artículo 252: «los que teniendo facultades para administrar un patrimonio ajeno, emanadas de la ley, encomendadas por la autoridad o asumidas mediante un negocio jurídico, las infrinjan excediéndose en el ejercicio de las mismas y, de esa manera, causen un perjuicio al patrimonio administrado.»
- **Uso ilegal de terminales**
  - Artículo 264.2: «El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.»
- **Daños a ficheros informáticos**
  - Artículo 264.2: «La misma pena (prisión de uno a tres años y multa) se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.»
  - «Habrían de considerarse graves, y por tanto encuadrables por su resultado en el Artículo 264.1 CP, todas aquellas acciones ilícitas que tuvieran trascendencia significativa o generaran consecuencias apreciables en datos, programas informáticos o documentos electrónicos o en los intereses en juego, quedando la aplicación del subtipo que nos ocupa para los supuestos en que los efectos del delito fueran especialmente relevantes y no se hicieran merecedores, por su especial intensidad, de la calificación de extrema gravedad.»

- **Piratería informática**
  - Artículo 270: «Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.»
  - Artículo 270.3: «Será castigado también con la misma pena quien fabrique, importe, ponga en circulación o tenga cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en el apartado 1 de este artículo.»
- **Delitos relativos a la propiedad industrial**
  - Artículo 273: «Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses el que, con fines industriales o comerciales, sin consentimiento del titular de una patente o modelo de utilidad y con conocimiento de su registro, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio objetos amparados por tales derechos.»
- **Delitos relativos al mercado y a los consumidores**
  - Artículo 278: «El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses»
- **Falsificación de documento público**
  - Artículo 390: «Será castigado con las penas de prisión de tres a seis años, multa de seis a veinticuatro meses e inhabilitación especial por tiempo de dos a seis años, la autoridad o funcionario público que, en el ejercicio de sus funciones, cometa falsedad: 1.º Alterando un documento en alguno de sus elementos o requisitos de carácter esencial. 2.º Simulando un documento en todo o en parte, de manera que induzca a error sobre su autenticidad. 3.º Suponiendo en un acto la intervención de personas que no la han tenido, o atribuyendo a las que han intervenido en él declaraciones o manifestaciones diferentes de las que hubieran hecho. 4.º Faltando a la verdad en la narración de los hechos.»
- **Falsificación de documento privado**
  - Artículo 395: «El que, para perjudicar a otro, cometiere en documento privado alguna de las falsedades previstas en los tres primeros números del apartado 1 del artículo 390, será castigado con la pena de prisión de seis meses a dos años.
- **Falsificación de certificados**

  - Artículo 397: «El facultativo que librare certificado falso será castigado con la pena de multa de tres a doce meses.»
  - Artículo 398: «La autoridad o funcionario público que librare certificación falsa con escasa trascendencia en el tráfico jurídico será castigado con la pena de suspensión de seis meses a dos años.»

- **Falsificación de tarjetas de crédito**
  - Artículo 399 bis: «El que altere, copie, reproduzca o de cualquier otro modo falsifique tarjetas de crédito o débito o cheques de viaje, será castigado con la pena de prisión de cuatro a ocho años. Se impondrá la pena en su mitad superior cuando los efectos falsificados afecten a una generalidad de personas o cuando los hechos se cometan en el marco de una organización criminal dedicada a estas actividades.»
- **Infidelidad en la custodia**
  - Artículo 413: «La autoridad o funcionario público que, a sabiendas, sustrajere, destruyere, inutilizare u ocultare, total o parcialmente, documentos cuya custodia le esté encomendada por razón de su cargo, incurrirá en las penas de prisión de uno a cuatro años, multa de siete a veinticuatro meses, e inhabilitación especial para empleo o cargo público por tiempo de tres a seis años.»
- **Protección de la contraseña**
  - Artículo 414.2: «El particular que destruyere o inutilizare los medios a que se refiere el apartado anterior (los puestos para impedir el acceso no autorizado a los documentos) será castigado con la pena de multa de seis a dieciocho meses.»
- **Delitos de falsedad en la pericia**
  - La figura del perito se corresponde con la de un **experto** (no requiere titulación) en alguna materia (artística o científica) en la cual el juez no tiene los conocimientos suficientes. De esto se desprende que un perito puede ser **cualquier persona**, siempre y cuando sea un experto en la materia sobre la cual pretenda realizar la pericia.
  - La **responsabilidad penal** del perito, no solo se da por la realización del hecho con **dolo, sino también por la imprudencia o falta de celo** a la hora de realizar la pericial. Por ello tenemos una serie de artículos del código penal dedicados en exclusiva a castigar este tipo de actos; los artículos 458 y siguientes del Capítulo VI (Del falso testimonio) del Título 20 del Código Penal de los cuales se pueden extraer los siguientes fragmentos de interés:

Importante: Artículo 458.1: El testigo que faltare a la verdad en su testimonio en causa judicial, será castigado con las penas de prisión de seis meses a dos años y multa de tres a seis meses.

Artículo 459: Las penas de los artículos precedentes se impondrán en su mitad superior a los peritos o intérpretes que faltaren a la verdad maliciosamente en su dictamen...

Artículo 460: Cuando el testigo, perito o intérprete, sin faltar sustancialmente a la verdad, la alterare con reticencias, inexactitudes o silenciando hechos o datos relevantes que le

fueran conocidos...

5.9 Normativas y estándares del sector

En este capítulo se repasarán algunas de las normativas y estándares, tanto a nivel nacional como internacional, más relevantes. Por un lado la RFC 3227 y por otro lado la ISO 27037 y las UNE 71505 y UNE 71506 .

5.9.1 ISO 27037

Dentro de la seguridad informática cabe destacar una normativa ampliamente conocida, es la familia ISO 27000. Esta serie de normas son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Esta serie contiene diversas normas todas relacionadas con las mejores prácticas recomendadas en Seguridad de la Información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Concretamente, existe una norma dedicada en exclusiva al análisis forense, se trata de la ISO 27037 Directrices para la identificación, recolección, adquisición y preservación de la prueba digital.

Esta norma ofrece orientación para tratar situaciones frecuentes durante todo el proceso de tratamiento de las pruebas digitales. Además define dos roles especialistas:

- DEFR (Digital Evidence First Responders): Expertos en primera intervención de evidencias electrónicas.
- DES (Digital Evidence Specialists): Experto en gestión de evidencias electrónicas.

ISO 27037 proporciona orientación para los siguientes dispositivos y circunstancias:

- Medios de almacenamiento digitales utilizados en equipos varios como por ejemplo discos duros, disquetes, discos magneto-ópticos y ópticos y otros similares.
- Teléfonos móviles, PDAs, tarjetas de memoria.
- Sistemas de navegación móvil (GPS).
- Cámaras de video y cámaras digitales (incluyendo circuitos cerrados de televisión).
- Ordenadores estándares con conexiones a redes.
- Redes basadas en protocolos TCP/IP y otros protocolos digitales.
- Otros dispositivos con funcionalidades similares a las descritas anteriormente.

Resumiendo, se puede destacar que esta norma ofrece orientación sobre el manejo de las pruebas digitales. Siguiendo las directrices de esta norma se asegura que la evidencia digital potencial se recoge de manera válida a efectos legales para facilitar su aportación en juicios y procesos legales. Además cabe destacar que cubre una amplia gama de tipos de dispositivos y situaciones, por lo que la orientación dentro de la norma es ampliamente aplicable.

5.9.2 RFC 3227

Otra norma destacable para mencionar es la RFC 3227. Este documento publicado por la Internet Engineering Task Force (IETF) recoge directrices para recopilar y almacenar evidencias sin ponerlas en riesgo.

En cuanto a los principios para la recolección de evidencias destacan básicamente tres, el orden de volatilidad de los datos, las acciones que deben evitarse y las consideraciones sobre la privacidad.

Relativo al procedimiento de recolección destaca que debe ser detallado, procurando que no sea ambiguo y reduciendo al mínimo la toma de decisiones.

Sobre el procedimiento de almacenamiento tiene en cuenta la cadena de custodia de las pruebas recogidas anteriormente y dónde y cómo se deben almacenar estas para que estén a buen recaudo.

Para acabar detalla qué tipo de herramientas son las más útiles y qué características deben tener para evitar conflictos, haciendo hincapié en que las herramientas deben alterar lo menos posible el escenario. Según este documento el kit de análisis debe incluir las siguientes herramientas:

- Programas para listar y examinar procesos.
- Programas para examinar el estado del sistema.
- Programas para realizar copias bit a bit.

Todas estas recomendaciones tienen como epicentro el principio de intercambio de Locard, que señala que: “siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto”.

5.9.3 UNE 71505 y UNE 71506

Estas normas, publicadas por la Asociación Española de Normalización y Certificación tienen como finalidad dar una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales.

Según la asociación esta norma debe dar respuesta a las infracciones legales e incidentes informáticos en las distintas empresas y entidades. Con la obtención de dichas pruebas digitales, que serán más robustas y fiables siguiendo la normativa, se podrá discernir si su causa tiene como origen un carácter intencional o negligente.

Estas normativas son de aplicación a cualquier organización con independencia de su actividad o tamaño, así como a cualquier profesional competente en este ámbito. Se dirige especialmente a incidentes y seguridad, así como al personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas.

CAPÍTULO 6

Más información

6.1 Webgrafía

6.1.1 Informática forense

Para comenzar en el mundo de la informática forense, aquí tenéis algunas direcciones de páginas web específicas donde podréis encontrar multitud de recursos relacionados con el mundo forense.

- European Union Agency for Cybersegurity(https://www.enisa.europa.eu/)
- Un informático en el lado del mal (http://www.elladodelmal.com/)
- Forensics Focus (http://www.forensicfocus.com/)
- Computer Forensics World (http://www.computerforensicsworld.com/)
- Forensics Magazine (http://www.forensicmag.com/)
- SANS (http://www.sans.org/)
- Cert (http://www.cert.org/)
- National Criminal Justicie Reference Service (https://www.ncjrs.gov/)
- National Institute of Justice (http://nij.gov/)
- FBI: Cyber Crime (http://www.fbi.gov/about-us/investigate/cyber/cyber/)

6.2 Bibliografía

- Brown, C. L. T. (2010). Computer evidence. Collection and preservation. Boston: Course Technology PTR.
- NIST. (2006). Performing the Forensic Process. En Guide to integrating forensic techniques into incident response.
- Lazaro Dominguez, F. Introducción a la Informática Forense. Editorial Ra-Ma