Conceptos básicos

Seguridad informática, análisis forense, sistema legal y estándares

PID_00273517

Josep Maria Arqués Soldevila
Miquel Colobran Huguet
Erik de Luis Gargallo

Tiempo mínimo de dedicación recomendado: 5 horas

Universitat Oberta de Catalunya

Josep Maria Arqués Soldevila

Ingeniero en informática por la Universitat Autònoma de Barcelona. Hizo el trabajo de investigación en el Departamento de Ingeniería de la Información y de las Comunicaciones (DEIC) de la mencionada universidad. Ha trabajado, como profesor ayudante y asociado, en el DEIC, y ha ejercido de profesor docente colaborador de varias asignaturas de la Universitat Oberta de Catalunya. Actualmente, ejerce de analista en informática forense y especialista en gestión de la calidad en ciencias forenses.

Miquel Colobran Huguet

Doctor en informática por la Universitat Autònoma de Barcelona. Es profesor docente colaborador en la UOC y coautor de varios materiales centrados en la administración y seguridad de sistemas e informática forense. Su investigación se enmarca dentro de la seguridad y del *social computing*, es decir, cómo los ordenadors influyen y son influidos por la sociedad, y cómo interviene la seguridad informática en este proceso.

Erik de Luis Gargallo

Ingeniero en informática y Máster en Seguridad de la Información por la Universitat Oberta de Catalunya. Tiene más de 10 años de experiencia en seguridad de la información, auditorías informáticas, informática forense e ingeniería de seguridad. Actualmente, trabaja estableciendo líneas estratégicas en el ámbito de la seguridad de las TIC y despliegue de las tecnologías que las aseguren. También es profesor colaborador de varios cursos y asignaturas de la Universitat Oberta de Catalunya.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Jordi Serra (2020)

Primera edición: febrero 2020

Avda. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

La informática se ha convertido en el eje vertebrador de todas las organizaciones y de buena parte de la sociedad. La información que circula por sus redes es vital para su funcionamiento y, en consecuencia, se ha convertido en el nuevo objetivo de los criminales del siglo XXI. La información es un valor en sí misma y, por lo tanto, un objeto codiciado por los nuevos delincuentes y una vía para provocar cuantiosos daños. Así mismo, su destrucción puede comportar pérdidas económicas importantes a sus propietarios, e incluso comprometer la continuidad de las organizaciones.

Cualquier organización se tiene que plantear la implantación de medidas de seguridad en los sistemas de información (tanto de carácter tecnológico como organizativo) y tendrá que buscar los siguientes objetivos: evitar los incidentes de seguridad y reducir las consecuencias de los que no se puedan evitar.

A pesar de esto, conviene ser consciente de que, por más recursos que se destinen a mejorar la seguridad, nunca se podrá conseguir en su máxima expresión, puesto que siempre se estará expuesto a sufrir algún tipo de incidente que provocará algún impacto en la organización (en más o menos medida). Por lo tanto, lo adecuado es que las organizaciones se planteen cómo actuar ante un incidente de seguridad. La gestión de incidentes permite a las organizaciones estructurar un protocolo de actuación ante una incidencia para minimizar el impacto y el tiempo de resolución.

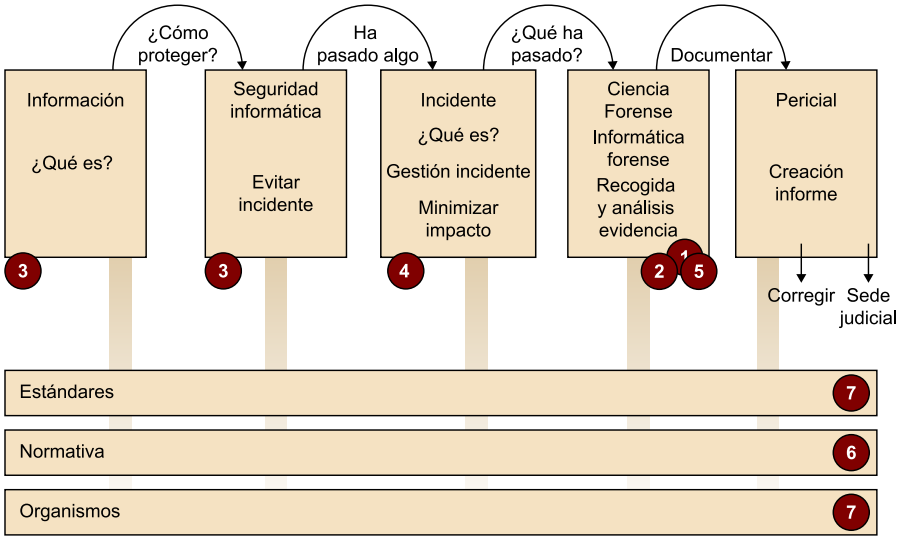
Cuando se produce un incidente, se tiene que determinar qué ha pasado. El conjunto de técnicas, conocido de manera genérica como informática forense, además de esclarecer los hechos, nos permitirá reunir pruebas de manera ordenada y metódica. Estas, probablemente, tengan que tener valor probatorio para poderlas utilizar posteriormente en el ámbito procesal (ante un juez).

Las técnicas de informática forense no solo son útiles a la hora de reunir las pruebas de un incidente de seguridad, sino que en general también se pueden emplear para preservar, analizar y presentar (mediante un informe pericial) cualquier evidencia contenida en un dispositivo digital o almacenada en la red. El informe mediante el que se presentan, de manera ordenada, estas evidencias, puede ir, pues, dirigido a múltiples destinatarios: jueces, responsables de una empresa, técnicos, etc.

Finalmente, no hay que perder de vista que tanto la protección de la información como las técnicas de seguridad y la informática forense están muy ligadas a estándares y al sistema legal.

El texto relaciona estándares, normativa y organismos con los 5 conceptos básicos que veremos en el módulo. En rojo hay los apartados donde aparecen cada uno de estos conceptos.

Figura 1. Representación de los diferentes conceptos, relación y lugar del módulo en que se desarrollan



Objetivos

Con el trabajo para realizar con estos materiales didácticos, pretendemos que el estudiante logre los siguientes objetivos:

1. Saber qué son las ciencias forenses y en especial la informática forense.

2. Comprender la relación que se produce entre la información, la seguridad informática, el incidente, el análisis forense y el sistema legal.

3. Conocer la regulación legal más importante para tener en cuenta.

4. Adquirir las nociones básicas en seguridad informática, gestión de incidentes y su tratamiento mediante las ciencias forenses.

5. Facilitar la comprensión del contexto de seguridad de la información y el vocabulario básico en este ámbito.

6. Conocer un vocabulario técnico básico en este ámbito.

7. Saber cuáles son los fundamentos básicos de seguridad.

8. Tener conocimiento del origen de la informática forense y de su vinculación con la criminalística.

9. Tener conocimiento sobre los incidentes de seguridad y su gestión.

10. Tener conocimiento de los delitos informáticos y la legislación asociada.

1. Disciplina forense

La palabra *forense* es latina (*forensis*), «perteneciente o relativo al foro». El origen es de la antigua Roma donde la acusación, la argumentación y las pruebas de un crimen requerían ser presentadas en un foro de personas consideradas notables. Eran estas las que determinaban el veredicto.

Rápidamente la fundamentación de los casos requirió otros conocimientos, como por ejemplo el conocimiento médico (medicina forense). A lo largo de la historia, se han desarrollado otras disciplinas como la criminología, la psiquiatría forense y la criminalística a partir de la medicina forense.

1.1. Ciencia forense

Conocemos por *ciencia forense* aquella que tiene por objeto la aplicación de prácticas científicas dentro del proceso legal. Normalmente, la ciencia forense está referida solo con el término ***forense***, el cual, aceptado en todo el mundo, se usa a menudo como sinónimo de legal. La ciencia forense incluye tanto la rama civil del derecho como la penal.

Ciencias forenses

El conjunto estructurado y sistematizado de conocimientos, de carácter técnico y científico, generados por la investigación y el análisis de los indicios de un hecho presuntamente delictivo, con el fin de presentar estos resultados ante la autoridad jurídica correspondiente y coadyuvar en la prevención del delito, y en la procuración y administración de la justicia.

Es decir, cualquier disciplina cuyos principios científicos se utilicen para ayudar a la justicia.

La ciencia forense se ha expandido tanto, que actualmente hay muchísimas ramas de las ciencias que la apoyan en la resolución de los problemas que plantea el derecho. A título orientativo, algunas son las siguientes[1]:

(1)La última en incorporarse a esta larga lista ha sido la informática forense.

- **Contabilidad forense**: adquisición, interpretación y estudio de la contabilidad.

- **Informática forense**[2]: recuperación, reconstrucción e interpretación de los medios digitales que están almacenados en un ordenador, para su utilización como prueba.

(2)Su uso y su utilidad se han extendido mucho más allá de los tribunales, como veremos más adelante.

- **Economía forense**: adquisición, estudio e interpretación de las pruebas relacionadas con el daño económico. Incluye la determinación de la pérdida de beneficios y ganancias, el valor del negocio y la pérdida de beneficios, etc.

- **Ingeniería forense**: reconstrucción, estudio e interpretación de un fallo mecánico o estructural (de edificios, puentes, etc.).

- **Lingüística forense**: estudio e interpretación de la lengua para utilizarla como prueba jurídica.

- **Psicología y psiquiatría forense**: estudio, evaluación e identificación de enfermedades relacionadas con el comportamiento humano y su mente, para la obtención de pruebas jurídicas.

- **Odontología forense**: estudio de los dientes, específicamente la unicidad de la dentición.

- **Patología forense**: combina las disciplinas de la medicina y la patología para determinar las causas de las lesiones o de la muerte.

- **Toxicología forense**: estudio, evaluación e identificación de los efectos de los venenos, productos químicos o de las drogas en el cuerpo humano.

1.2. Informática forense

El análisis forense en informática surgió de la necesidad de poder aportar elementos relevantes en los procesos judiciales en los que las nuevas tecnologías estaban presentes, bien como objetivo (por ejemplo, una intrusión que comporte daños en un sistema informático) o bien como medio (por ejemplo, el envío de correos electrónicos amenazantes a un personaje público). Así pues, es una ciencia forense que se ocupa del uso de los métodos científicos aplicables a los sistemas informáticos[3].

(3)Todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

La informática forense es la **ciencia forense** que se encarga de **asegurar, identificar, recoger, preservar, analizar y presentar** la evidencia[4] digital, de forma que esta sea aceptada en un proceso judicial.

(4)Cualquier elemento que proporcione información de la que se pueda inferir alguna conclusión o bien que constituya un hallazgo relacionado con el hecho que se investiga.

Sin embargo, la informática forense también se ha revelado como un área de la informática con muchas más utilidades, de forma que la definición anterior solo se aplica a parte de su uso. Así pues, también podríamos considerar la informática forense bajo la siguiente definición:

La informática forense investiga los sistemas de información con objeto de detectar evidencias de vulnerabilidad.

Esta definición subraya que se aplican las técnicas, los procedimientos y las herramientas de *hardware* y *software* necesarias para determinar datos y hechos relevantes. Estas técnicas se pueden llevar a cabo antes o después de que se produzca un suceso y con finalidades judiciales o no.

Bajo esta óptica, la informática forense aparece con diferentes finalidades y objetivos:

		Objetivos	
		Preventivo	**Correctivo**
Finalidad	Probatoria	---	Ha habido un incidente y deben reunir pruebas para un proceso judicial.
	Auditora / monitorización	Verificación que el sistema informático está funcionando correctamente usando técnicas forenses.	Ha habido un incidente y hay que conocer los hechos para modificar las políticas de seguridad.

- **Objetivos preventivos**: se pretende anticipar al problema. En este escenario la informática forense forma parte del sistema de seguridad. Se utiliza para verificar y para auditar. Mediante la práctica de varias técnicas se verifica que los sistemas de seguridad instalados cumplen con ciertas condiciones básicas de seguridad. Los resultados de las auditorías servirán para poder corregir los errores encontrados y poder mejorar el sistema.

- **Objetivos correctivos**: este escenario supone la detección de un incidente. Se tiene que conocer la causa para poder aplicar las medidas correctivas que permitan evitar nuevos incidentes por esta misma vía.

- **Finalidad probatoria**: especialmente si el incidente ha ocasionado daños, estamos ante un escenario que hay que gestionar de forma muy cuidadosa. La obtención de pruebas es muy importante. La informática forense permite realizar un rastreo de la intrusión, descubrir el daño realizado y recopilar las evidencias digitales. En este contexto hablamos de recuperación de información e incluso de descubrimiento de información. Podemos llegar a conocer el origen del ataque y los cambios realizados en el sistema (fugas de información, pérdida o manipulación de datos). Posteriormente, las evidencias encontradas podrán ser utilizadas en el marco legal.

Ved también

Se puede consultar el apartado «Gestión de incidentes de seguridad» para conocer las etapas con más detalle.

- **Finalidad auditora**: periódicamente se tiene que comprobar, a todos los niveles, la robustez del sistema informático. Las técnicas forenses se han revelado como extremadamente útiles en estos escenarios.

1.3. La informática en el delito

En el ámbito de la informática forense el delito se denomina coloquialmente *ciberdelito*, en cuanto que, de alguna manera, está casi siempre vinculado a las tecnologías de la información. Es especialmente destacable que hay pocas áreas de delincuencia donde no es posible aplicar la investigación forense ligada a las TIC.

Dentro de este ámbito, los ordenadores pueden constituir:

- **Objeto** del delito. Por ejemplo, con ataques de piratería, denegación de servicio, intrusión informática[5] o *hacking*[6].

- **Medio** para cometer el delito. Es el caso más corriente, puesto que incluye la mayoría de delitos «tradicionales» en los que se ha incorporado la tecnología (ya sea usando ordenadores o dispositivos móviles como teléfonos o tabletas). El abanico es muy variado y se puede encontrar, por ejemplo, la extorsión, la estafa (*phishing*), el tráfico de drogas, la pornografía infantil, el *ciberbulling*, el ciberacoso o el *sexting*.

- **Elemento material probatorio**[7] en un delito. En muchos delitos los ordenadores aparecen en «la escena de un delito» de manera circunstancial. Así, por ejemplo, pueden contener pruebas en forma de mensajes de correo electrónico o ficheros relevantes para delitos como asesinatos, secuestros, consultas a Internet, etc.

(5)Acceso a un sistema informático «saltándose» la seguridad establecida. Artículo 197bis del Código Penal.

(6)Acceder de manera ilegal a datos almacenados en un ordenador o servidor.

(7)Objeto que sirve para probar unos hechos (por ejemplo una pistola que se encuentra en la escena del crimen).

2. Marco conceptual de la informática forense

2.1. Breve reseña histórica

Antes del 1985. De hecho, el término simplemente no existía. Desde los años sesenta hasta principios de los ochenta, los ordenadores eran principalmente un aparato industrial, propiedad de empresas y operado por estas y por universidades, centros de investigación y agencias gubernamentales. Necesitaban una gran infraestructura física, que incluía cantidades masivas de energía y aire acondicionado, y un personal dedicado y altamente calificado. El libro de Donn Parker (1976), *Crime by Computer*, es el primero en describir el uso de la información digital para investigar y procesar delitos cometidos con la ayuda de un ordenador. El gobierno y el FBI notaron que los criminales empezaban a usar la tecnología como medio para cometer delitos. En 1984, el FBI inició un programa denominado Programa de Medios Magnéticos que fue el origen del CART (*Computer Analysis and Response Team*), un equipo de análisis por ordenador.

Década del 85 al 95. La llegada del ordenador personal en la década de los 80 provocó la aparición de muchos ordenadores en hogares y pequeñas organizaciones, y puso de relieve la existencia de problemas de seguridad.

> Entre los aficionados a la informática había gente de muchas organizaciones. Algunas de las personas clave fueron Mike Anderson, Danny Madres y Andy Fried de la IRS; Ron Peters y Jack Lewis del servicio secreto de los Estados Unidos; Jim Christy y Karen Matthews del Departamento de Defensa; Tom Seipert, Roland Lascola y Sandy Mapstone de las agencias locales de aplicación de la ley de los EE. UU.; y los canadienses, Gord Hama y Steve Choy.

En 1988, Michael Anderson, un agente del IRS (Internal Revenue Service), creó junto con un grupo de especialistas y tres compañías, un grupo especializado en la recuperación de datos. También este año se creó la Asociación Internacional de Especialistas en la Investigación Computacional (IACIS).

En 1993, el FBI acogió la Primera Conferencia Internacional sobre evidencia informática, donde asistieron representantes de 26 países. En 1995, la segunda conferencia se celebró en Baltimore y se fundó la Organización Internacional para la Evidencia Computacional (IOCE).

> Se quería proveer un foro internacional para el intercambio de la información relacionada con la investigación computacional y la informática forense.

Los casos investigados eran muy básicos. Gran parte del enfoque era la recuperación de datos de manera independiente de ordenadores. Internet todavía no era popular, pero los delincuentes usaban el acceso telefónico para comprometer ordenadores. Los temas de las investigaciones sobre delitos por orde-

nador eran generalmente delitos tradicionales que utilizan ordenadores para apoyar sus actividades o jóvenes que utilizaron sus habilidades técnicas para obtener acceso a ordenadores de manera ilegal.

Sin embargo, se vio la necesidad y el potencial de la ciencia forense digital. Se creó, por ejemplo, el programa Especialista en Recuperación de Evidencias Informáticas (SCERS) en la agencia tributaria, el Programa de Agentes Especiales de Delitos Electrónicos (ECSAP) en el Servicio Secreto de los Estados Unidos, el equipo de respuesta y de análisis computacional (CART[8]) en el FBI. Cada organismo lo hacía a su manera y la mayoría de las investigaciones forenses digitales fueron realizadas por personas con formación mínima, a menudo con equipamiento personal y sin ningún tipo de supervisión o control de calidad formal.

(8)El CART empezó a operar en 1991. Fue la respuesta al incremento del número de casos en los que estaba involucrada la evidencia digital. Proporcionaba exámenes de los ordenadores y discos (realizados en los laboratorios del FBI) como apoyo a investigaciones y juicios.

Algunos países empezaron a crear asociaciones y entidades, y estas organizaciones ofrecían formación. La formación forense se desarrolló y sistematizó ofreciendo una formación asequible y de calidad. Como consecuencia, la demanda de esta formación se disparó. Mientras tanto la comunidad académica no estaba interesada en este campo, con dos excepciones notables: Gene Spafford y Dorothy Denning.

Década del 95 al 2005. Es la etapa de la formalización de la ciencia forense digital. La explosión de la tecnología, la llegada de la telefonía celular (muy incipiente), Internet como eje vertebrador y su masiva difusión, cambiaron el escenario. A finales del 2005 prácticamente todo el mundo ya tenía correo electrónico y alguna manera de poder acceder a la red. Este fue un entorno que los delincuentes supieron aprovechar muy bien.

A raíz de esto, en pocos años hubo una explosión de casos de pornografía infantil. El primero, el caso George Stanley Burdynski, Jr., en 1993, reveló que los ordenadores se utilizaban para hacer tránsito ilegal de imágenes de menores. Pocos años más tarde, todos los organismos tenían grupos dedicados a ello. El resultado de todo este trabajo supuso la confiscación de volúmenes digitales cada vez más grandes y fue uno de los principales motores en el crecimiento de la investigación forense digital.

> En 1999, el CART trabajaba ya en más de 2.000 casos anuales, y examinaba del orden de 17 *terabytes* de datos. Tres años más tarde, en 2003, el CART trabajaba en 6.500 casos y estaba examinando 782 *terabytes* de datos.

Mientras tanto, las herramientas forenses cambiaron radicalmente. De las herramientas en línea de comando y montajes caseros se pasó a herramientas complejas, con entornos gráficos y paquetes de interfaz de usuario. La primera de las nuevas herramientas fue Expert Witness, un producto diseñado por Andy Rosen para la técnica forense de Macintosh que evolucionó a EnCase. EnCase, junto con Forensic ToolKit (FTK), son ahora herramientas forenses estándares.

Del 2005 hasta ahora. Es desde 2005 que la investigación forense digital ha crecido en profundidad y amplitud. Tiene muchos más practicantes y una gran variedad de formación reglada muy estricta que permite obtener certificaciones que avalan la profesionalidad del informático forense.

En 2006, los tribunales de los Estados Unidos adoptaron nuevas normas para el procedimiento civil que definían la información digital como una nueva forma de evidencia e implementaron un sistema obligatorio llamado descubrimiento electrónico o eDiscovery, para tratar pruebas digitales.

Nota

En 2007, el FBI anunció que su análisis informático y el equipo de respuesta (CART) examinaron más de 2,5 *petabytes* de pruebas.

Prácticamente todos los dispositivos que utilizan electricidad ahora tienen algún tipo de almacenamiento digital, las redes conectan muchos de los dispositivos que utilizamos en nuestra vida cotidiana. Esto, a su vez, ha impulsado el desarrollo de muchos servicios basados en red y web, incluida la informática en la nube.

Los profesionales de la seguridad de la información ahora reconocen la ciencia forense digital como una de las habilidades básicas. A pesar de que sus objetivos y sus necesidades difieren de estos, en lo referente a la aplicación de la ley, los conceptos y las herramientas a menudo son idénticos.

Las herramientas forenses han seguido evolucionando, y se han movido en el entorno de la red e incluso en la nube. Estas mismas herramientas se adaptan a los nuevos entornos y aparecen los laboratorios virtualizados (utilizando productos como por ejemplo VMWare) y redes de área de almacenamiento (SAN).

En menos de cuarenta años, la ciencia forense digital ha pasado de ser un conocimiento desarrollado y difundido por unos cuantos profesionales, a su estado actual, una disciplina sólida y muy fundamentada.

La investigación forense en la nube (2019)

La demanda de computación y servicios en la nube está aumentando debido a la popularidad de los dispositivos digitales, de los dispositivos móviles y del uso intensivo de Internet.

Así pues, aparecerán usos maliciosos de estos servicios. Este tipo de investigación forense está todavía en una etapa muy inicial.

2.2. Ámbito de actuación

Actualmente la informática forense ya no trata solo del contenido de correos electrónicos, documentos y otros ficheros que puedan ser de interés para los investigadores, sino también de los metadatos asociados a estos ficheros y la secuencia temporal de acontecimientos. Un examen forense informático pue-

de desvelar cuándo un documento apareció por primera vez en un ordenador, cuándo se editó por última vez, cuándo se guardó o imprimió por última vez y qué usuarios llevaron a cabo estas acciones.

El ámbito más conocido es el judicial, pero la informática forense se ha difundido más allá del ámbito criminalístico y se utiliza también en otras vertientes, como por ejemplo:

1) Persecución criminal: Evidencia incriminatoria que puede ser usada para procesar delitos y crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.

2) Litigación civil: Casos relativos a fraude, discriminación, acoso, divorcio, etc. Estudios jurídicos que necesitan pedir información, ya sea para presentarla ante un tribunal, o bien para negociar con las partes un acuerdo extrajudicial, resarcimiento, una renuncia, etc.

3) Investigación de seguros: La evidencia encontrada en ordenadores puede ayudar a las compañías de seguros a disminuir costes de reclamaciones por accidentes o compensaciones.

4) Temas corporativos: Se puede recoger información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o espionaje industrial. Empresas que realizan juicios laborales con sus empleados o con sus asociados por conflictos de intereses.

5) Finalidad preventiva: Como medida preventiva sirve a las empresas para auditar, mediante la práctica de varias pruebas técnicas, que los mecanismos de protección instalados y las condiciones de seguridad aplicadas a los sistemas de información son suficientes. Permite detectar las vulnerabilidades de seguridad para corregirlas.

6) Recuperación de datos: Situación en la cual hay que recuperar información que ha sido eliminada por error, durante una subida de tensión o una caída de servidores. En este escenario habitualmente se conoce la información que se está buscando.

7) *Network forensics*: Saber cómo un atacante ha accedido al sistema informático y las acciones que ha podido llevar a cabo.

8) Cuando la investigación forense se tenga que presentar ante un juzgado se tienen que tomar medidas especiales. Una de las más importantes es asegurar que la evidencia ha sido correctamente recogida y documentar la cadena de custodia, desde la escena del delito hasta el juzgado para garantizar de este modo la integridad de la evidencia digital.

Ved también

Se puede ver con más detalle en el módulo «Fases y metodología del análisis forense».

9) Dentro del ámbito de la investigación de delitos, la informática forense estará presente siempre que haya elementos digitales involucrados. Por lo tanto, puede formar parte de cualquier investigación por delitos no relacionados con las tecnologías de la información. Como ejemplos, puede ser necesario en un robo donde se hayan usado teléfonos móviles, en delitos donde haya correos electrónicos o en robo o falsificación de información en bases de datos.

La informática forense se convierte en imprescindible desde el momento en que gran parte de la información generada se encuentra almacenada en soportes digitales.

2.3. Principios de la informática forense

Como la informática forense es una disciplina de la ciencia forense, comparte muchos de los principios claves a la hora de examinar y manipular la información. Estos principios[9] son:

(9)Elaborados por la Association of Chief Police Officers (ACPO) y seguidos por la policía británica.

- **Evitar la contaminación**: no se realizará ninguna acción que modifique los datos contenidos en un ordenador o dispositivo de almacenamiento. Para poder obtener un análisis veraz y preciso, la información se debería almacenar en un medio lo más estéril posible.
  Con la evidencia electrónica (imágenes de discos y memoria, ficheros de datos y ejecutables, etc.) la práctica consiste en obtener *hashes* de la información en el momento de la obtención, de forma que se pueda comprobar en cualquier momento si la evidencia ha sido modificada.
  Los algoritmos de *hashing* aceptados como estándares son el MD5 y el SHA-1. A pesar de que se han descubierto vulnerabilidades, siguen utilizándose, puesto que la posibilidad de obtener una colisión es infinitesimal.

- **Actuar metódicamente**: el investigador tiene que ser responsable de sus procedimientos y del desarrollo de la investigación, por lo tanto, es importante que se documenten claramente los procesos, las herramientas y metodologías de análisis empleados durante todo el proceso.

- **Tener control sobre la evidencia**: hay que mantener en custodia cualquier evidencia relacionada con el caso, y documentar así mismo cualquier acontecimiento que la pueda afectar: quién entregó la evidencia, cómo se transportó, quién tuvo acceso a la evidencia, etc. De este modo, un tercer analista independiente debe ser capaz de examinar estos registros y lograr el mismo resultado.

- **En circunstancias excepcionales**: si se da la circunstancia de que hay que acceder a los datos originales contenidos en un ordenador o dispositivo de

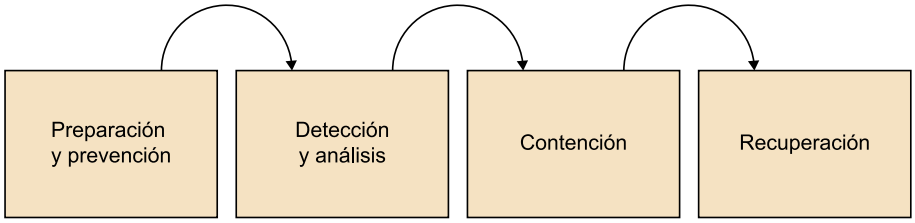
almacenamiento, la persona tiene que ser competente en esta práctica, y explicar la relevancia y las implicaciones de sus acciones.

2.4. La informática forense en las organizaciones

Actualmente, la informática forense tiene una relevancia considerable dentro de las organizaciones y juega un papel clave en la seguridad. Desde el punto de vista de la organización, la informática forense debe integrarse dentro de la seguridad global del sistema informático. Este, a su vez, depende del buen diseño de las medidas de prevención, detección, contención y recuperación de los **incidentes**[10] **informáticos**.

(10)Entenderemos por incidente cualquier hecho anómalo que afecte al funcionamiento del sistema. En próximos apartados detallaremos más el concepto.

Figura 2. Esquema básico de la gestión de incidentes



- **Medidas de prevención**: estas medidas integran todos los aspectos relativos a evitar que se produzca un incidente o suceso. La informática forense se integra en esta etapa a través de las auditorías y sus correspondientes técnicas como, por ejemplo, los llamados *penetration tests*, y el *Black box*, *Gray box* o el *White box*, para evaluar el estado del sistema[11].

  Una de las medidas organizativas fundamentales es el plan de prevención de riesgos. Para preparar un plan de riesgo, el primer paso es identificar los riesgos a los que estamos sometidos. Por eso, tenemos que determinar qué riesgos nos pueden provocar un fallo en el sistema y determinar cuáles son probables, cuáles son posibles y cuáles son críticos. Después, necesitamos determinar las prioridades de estos riesgos basándonos en el entorno de nuestra empresa. Es decir, a pesar de que los riesgos informáticos son parecidos para la mayoría de las empresas, la prioridad que se les asigna depende del uso informático que lleva a cabo la empresa. Una vez tenemos identificados y priorizados los riesgos, podemos decidir cuáles generarán un plan de riesgo y cuáles no hay que tener implementados en un plan como este, además de las características del plan.

(11)No es objeto de estos materiales detallar estas técnicas, las cuales utilizan la informática forense como un elemento más para cumplir sus objetivos.

- **Medidas de detección**: dado que es inevitable que el incidente suceda tarde o temprano, las medidas de detección sirven para descubrir violaciones de la seguridad del sistema. La informática forense se integra perfectamente en herramientas como por ejemplo los analizadores de tránsito, *honeypots* y *honeynets*, o los IDS[12].

(12)Una vez más, no es objeto de estos materiales detallar estas técnicas.

- **Medidas de contención**: una vez detectado e identificado el incidente, hay que procurar por todos los medios restringir la expansión. Para lo cual, se deben tomar medidas protocolizadas. Las técnicas de *network forensics* ayudan a identificar el origen del incidente y, por lo tanto, a contener y eliminar el problema.

- **Medidas de recuperación**: finalmente, es necesario determinar el origen del ataque y los daños ocasionados (entre otros), y emprender acciones legales, si procede. Este es el campo de trabajo de la informática forense (en concreto del análisis forense). Así mismo, también es de vital importancia la recuperación del estado normal del sistema informático[13].
  En el ámbito organizativo, el plan de contingencia o recuperación es muy importante, puesto que tiene que detallar los pasos que hay que seguir para recuperarnos de diferentes situaciones de crisis, e indicar claramente lo que hay que hacer, lo que no se ha hacer y quién es responsable de cada paso. Es importante también tener presente durante la recuperación el poder estar seguros que somos capaces de acumular los indicios y los datos que facilitarán las tareas de informática forense y el posterior saneamiento de la vulnerabilidad explotada.

[13] Forma parte del plan de contingencia o *Disaster Recovery Plan* (DRP), muy vinculado a las políticas de copia de seguridad.

3. Seguridad informática

El concepto *seguridad* lleva asociado otro concepto que le da sentido: *valor*. Solo protegemos aquello que creemos que tiene un valor importante para nosotros y, por lo tanto, la seguridad va íntimamente asociada al valor que le damos al objeto o a los objetos protegidos.

Así pues, si en el sistema informático nos preocupa tanto la seguridad, ¿qué queremos proteger?

3.1. El valor de la información

Los tres elementos básicos que deseamos proteger en cualquier sistema informático son: el ***software***, el ***hardware*** y los **datos** o la **información**.

- Por ***hardware*** entendemos todos los elementos físicos de un sistema informático, como servidores, estaciones de trabajo, cableado, cintas de copia, DVD, etc.

- Por ***software*** entendemos todos los programas que hacen funcional el *hardware*, tanto los sistemas operativos como las aplicaciones.

- Por **datos** entendemos el conjunto de información lógica que manejan tanto el *software* como el *hardware*.

Datos e información

Hay una diferencia en estos dos conceptos, a pesar de que a menudo se usan de manera indistinta.

Datos: conjunto discreto de factores objetivos sobre «algo». Puede ser un número, una letra…

Información: la reunificación y estructuración de los datos en un contexto que le da sentido.

Ejemplo

Dato: 17

Información: Juan tiene 17 años. El número de personas en la habitación es de 17…

En esencia, lo que más nos importa proteger, porque es propio de la organización, es la información, puesto que sin duda constituye uno de los activos más grandes de cualquier organismo. Por eso, se destinan muchos recursos a su protección y a su uso de forma controlada, puesto que en muchos casos, además constituye su conocimiento o *know-how*[14].

(14) Saber hacer en términos empresariales.

El problema más grande de la información, por su naturaleza, es la dificultad de protegerla, puesto que no se puede proteger como los objetos materiales, depositándola en un recinto custodiado. Esto comporta que la información sea susceptible de copia, robo, destrucción, etc., con las consiguientes pérdidas que puede suponer para la organización.

La información es uno de los bienes más grandes de la organización.

La información, a pesar de ser uno de los bienes que requiere más esfuerzo en cuanto a protección, no es el único bien para proteger. En seguridad tenemos que considerar otros bienes como por ejemplo los equipos físicos.

3.2. ¿Qué es la seguridad informática?

Aunque sea de forma intuitiva, todo el mundo entiende que un sistema informático se considerará seguro si se encuentra libre de todo riesgo y daño. Aún así, no es nada fácil formalizar el concepto de *seguridad informática*. Lo entenderemos como el conjunto constituido por las diversas metodologías, los documentos, el *software* y *hardware*, que determinan que los accesos a los recursos de un sistema informático sean empleados únicamente por los elementos autorizados a hacerlo. Como es totalmente imposible garantizar la seguridad o inviolabilidad de un sistema informático, en lugar del inalcanzable concepto de *seguridad* es preferible emplear el término de *fiabilidad*. Por lo tanto, no podremos entender la seguridad informática como un concepto cerrado, consecuencia de la aplicación de métodos, sino como un proceso que puede verse comprometido en cualquier momento de la manera más insospechada.

En general, pues, diremos que un sistema informático es fiable cuando se satisfacen las tres propiedades siguientes:

- **Confidencialidad**: los recursos que integran el sistema solo pueden ser accedidos por los elementos autorizados a hacerlo. Por recursos del sistema no solo entenderemos la información, sino también cualquier recurso en general: impresoras, procesador, etc.

- **Integridad**: los recursos del sistema solo pueden ser modificados o alterados por los elementos autorizados a hacerlo. La modificación incluye varias operaciones, como el borrado y la creación, además de todas las posibles alteraciones que se puedan realizar sobre un objeto.

- **Disponibilidad**: los recursos del sistema deben poder ser accesibles a los elementos autorizados.

Tríada CIA / CID

Las tres propiedades juntas se conocen como la tríada CID, por las iniciales:
- **C**onfidencialidad
- **I**ntegridad
- **D**isponibilidad
- Estas mismas siglas en inglés forman el acrónimo CIA

Como podemos imaginar, es muy difícil encontrar un sistema informático que maximice las tres propiedades. Normalmente, y según la orientación del sistema, se priorizará alguno de los tres componentes. Por ejemplo, en un sistema

que almacene datos de carácter personal, el elemento que hay que priorizar es la confidencialidad de la información, a pesar de que también hay que tener muy presente el de la preservación (en tanto que sea posible) de la integridad y la disponibilidad. Observamos que no sirve de nada garantizar la confidencialidad por medio de algún método criptográfico, si permitimos que un intruso pueda borrar fácilmente la información almacenada en el disco duro del servidor (ataque contra la integridad).

Existe alguna otra definición, que sin ser tan «informática», nos puede ser útil conocer. Esta observa la seguridad informática en un entorno de trabajo.

La seguridad informática es el conjunto de reglas, planes y acciones encaminados a garantizar tres objetivos:

- La capacidad de trabajo (disponibilidad), es decir, que el sistema sea operativo en todo momento, o haya mecanismos de contingencia que permitan un ritmo de trabajo aceptable mientras se soluciona el problema.

- La integridad de la información (consistencia), de forma que la información a disposición del usuario permanezca inalterada.

- La confidencialidad de los datos (confidencialidad, control de acceso, autenticación), a fin de que cada usuario tenga acceso solo a la información que le corresponde.

Y para proteger mejor nuestro sistema es necesaria una buena visión global sobre cómo este puede ser atacado, a fin de detectar vulnerabilidades, analizar cómo solucionarlas y tener planes de contingencia detallados y probados para una rápida y satisfactoria solución del incidente.

3.3. Conceptos básicos de la seguridad

El primer paso en seguridad informática es tener muy claro de qué nos queremos proteger y de qué no queremos o no podemos (coste, dificultad y/o imposibilidad) protegernos. La seguridad informática tiene diferentes ámbitos, entre los que destacaremos el acceso físico a los dispositivos, cableado o copias de seguridad, los procesos, las operaciones y los permisos de acceso, la arquitectura y la seguridad de la red, la redundancia del *hardware*, la integridad de los datos, y los permisos de los usuarios. La seguridad debe funcionar correctamente en los distintos ámbitos. El sistema es tan seguro como el menos resistente de sus elementos. Veamos algunas definiciones y conceptos básicos.

Fortaleza de la seguridad

Un sistema informático es tan seguro como lo es su eslabón más débil.

En otras palabras, el punto más débil de la seguridad será el punto de entrada.

3.3.1. Vulnerabilidad, amenaza y riesgo

- **Vulnerabilidad**: debilidad en cualquiera de los puntos de los sistemas de información (acceso, datos, suministros, programas, *hardware*, diseño,

etc.) que podría ser explotada accidental o intencionadamente, y que comportaría una violación de la política de seguridad de sistemas.

- **Amenaza**: indicio por el que se manifiesta un peligro.

- **Riesgo**: peligro incierto.

A modo de ejemplo, podemos decir que dejar nuestro terminal de trabajo sin estar protegido por una contraseña es una vulnerabilidad que alguien (amenaza) puede aprovechar y corremos el riesgo de que entre en nuestra cuenta y se haga pasar por nosotros o nos borre o modifique ficheros.

3.4. Tipos de seguridad

Distinguimos dos tipos de seguridad, la activa y la pasiva.

La seguridad activa busca proteger y evitar posibles daños en los sistemas informáticos, que comprenden los datos, el *software* y el *hardware*, es decir, en los sistemas y los datos que almacenamos. Queremos evitar los problemas antes de que pasen.

La seguridad pasiva busca minimizar los impactos causados por *malware*, accidentes (cortes de corriente o red, mal funcionamiento de dispositivos críticos, etc.), usuarios (autorizados o no autorizados), y cualquier otro posible agente perturbador. Queremos minimizar las consecuencias una vez los accidentes han pasado y recuperarnos lo más rápidamente posible.

3.4.1. Activa

Con la seguridad activa nos protegemos de todos los posibles ataques maliciosos que puedan venir, básicamente por la red, y tomamos conciencia de que hay que implementar medidas adicionales para que los intrusos no tengan acceso a la información de la organización.

Para protegerse de lecturas no deseadas de la información guardada en un fichero o de los datos que circulan por Internet, basta con cifrar los mensajes o archivos con un par compuesto por una clave pública y otra privada, para que nadie a quien no se haya dado permiso expreso antes pueda acceder a la información.

Además, todas las aplicaciones para ejecutar que requieran tener el acceso mediante la red pueden autenticarse. Es decir, podemos pedir que el usuario se autentique para utilizar estas aplicaciones.

Por ejemplo, en vez de utilizar el protocolo HTTP de intercambio de ficheros por Internet, se puede usar el protocolo HTTPS, que debe autenticar al usuario que intenta acceder al servidor web para descargar la información.

Otra manera de asegurarnos de que no se acceda a la información privada son las extensiones IPsec (Internet Protocol security), que proporcionan vías de comunicación segura de la información que es transportada por Internet.

Una de las tareas de un administrador de sistemas, aparte de estas que hemos indicado, es la monitorización de la red. El tránsito de información de la red da mucha información de la manera cómo se puede acceder a los datos y quién ha accedido a cada uno de los recursos compartidos.

3.4.2. Pasiva

Es un aspecto muy importante que debemos tener en cuenta a la hora de administrar o instalar un equipo informático. En principio, una vez configuradas las políticas de seguridad pasiva, no hace falta que nos preocupemos mucho del funcionamiento que tienen y, por lo tanto, esto hace que las olvidemos fácilmente y si hay algún error o problema no nos damos cuenta hasta que muchas veces es demasiado tarde. Sin embargo, el hecho de tener que estar constantemente pendientes de la seguridad pasiva significa que las decisiones tomadas en el momento de configurarla han sido erróneas y, por lo tanto, realmente no funciona correctamente esta seguridad. Por ejemplo, un caso típico es la caída de fluido eléctrico. Para solucionar este problema se puede decidir entre instalar un sistema de alimentación ininterrumpida (SAI) o contratar una doble compañía de suministro eléctrico (así, en caso de que falle una compañía se puede utilizar la otra) e incluso instalar dos fuentes de alimentación o más (la mayoría de los fabricantes de servidores ya tienen esta doble fuente de alimentación en los equipos).

Algunos puntos clave de la seguridad pasiva son las políticas de copias de seguridad, los planes de prevención de riesgos y los planes de contingencia que hay que seguir ante diferentes situaciones. También los elementos redundantes (alimentación, red, CPU, discos, etc.) nos ayudarán a recuperar rápidamente, y quizás de manera automática, las funcionalidades del sistema en caso de accidente fortuito o deliberado.

Una de las medidas principales para asegurar la continuidad de los servicios es determinar los riesgos a los que nos enfrentamos ante un fallo en el sistema. Esto implica conocer el alcance de los servicios críticos que están involucrados, la incidencia interna y externa que tienen y haber medido las posibles consecuencias de un fallo. Por lo tanto, hay que preparar un conjunto de acciones que se deben tomar en caso de fallo, teniendo en cuenta que puede ser por un problema con el *hardware* o con el *software* (como virus, troyanos, ataques maliciosos, etc.). En esto consiste, precisamente, un plan de riesgo.

4. Gestión de incidentes de seguridad

A pesar de todo lo que hacemos para evitar que «pasen cosas» en un sistema informático, siempre existe esta posibilidad y por lo tanto incidentes como un ciberataque por Internet, un corte de corriente o simplemente que un ordenador se estropee son muy difíciles de prever (y muchas veces el coste de hacerlo es demasiado elevado). Por lo tanto, toda organización tiene que tener presente cómo gestionar estas situaciones.

4.1. Concepto de vulnerabilidad e incidente

Entenderemos por *incidente* cualquier hecho anómalo que afecte al funcionamiento del sistema. Dado que los incidentes son imprevisibles, lo único que se puede hacer es gestionarlos de la mejor manera posible, puesto que es imposible que no existan. Así pues, la gestión de un incidente informático tiene que incluir la monitorización y la detección del incidente, y la respuesta ante este, que en general se puede considerar un incidente de seguridad.

Activo

Son los componentes indispensables para el correcto funcionamiento de un sistema informático. En general, el *hardware*, el *software* y los datos.

Política de seguridad

Conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la organización.

Definición de vulnerabilidad de un activo

La potencialidad o posibilidad de la materialización de una amenaza sobre este activo. Se determina por dos medidas: frecuencia y degradación causada.

Definición de incidente de seguridad informática

La violación o el intento de violación de la política de seguridad.

Así, se convierte en esencial **la gestión de riesgos y la planificación**. Partiendo del hecho de que el incidente será inevitable, hay que asegurar que los **planes de respuesta** diseñados reducen el impacto en la organización. La planificación de respuesta de incidentes, globalmente, está muy relacionada con el conocimiento de procesos y con el desarrollo y la aplicación de contramedidas proactivas de detección, prevención y reacción para cada fallo potencial.

Los incidentes que el equipo de soporte al usuario no puede resolver rápidamente son asignados a un especialista del equipo de apoyo técnico. La resolución del incidente tiene que ser ejecutada tan pronto como sea posible para restaurar el servicio rápidamente. El proceso habitual de gestión de incidentes es el siguiente:

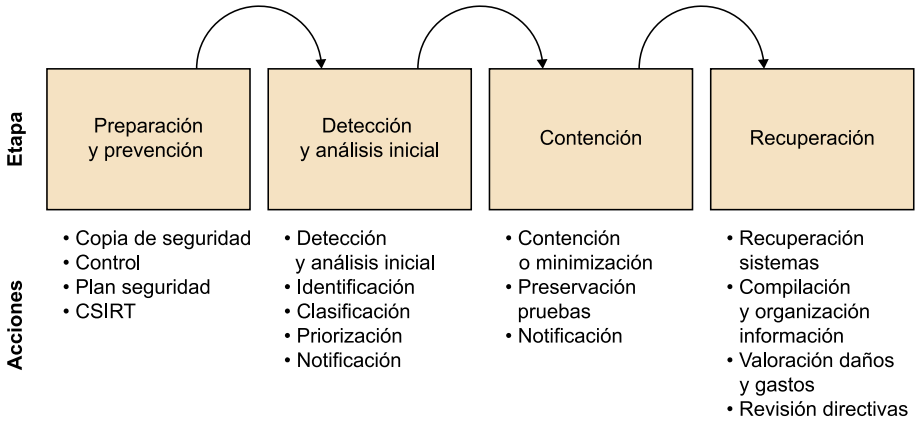
- Detección y registro del incidente.
- Clasificación y apoyo inicial.
- Investigación y diagnóstico.
- Resolución y recuperación.
- Cierre del incidente.
- Monitorización, seguimiento y comunicación del incidente.

4.2. Ciclo de vida del incidente

Desde el punto de vista de la organización, la gestión del incidente debe integrarse dentro de la seguridad global del sistema informático. A su vez, esta depende del buen diseño de las medidas de prevención, detección y recuperación.

El ciclo de vida general de los incidentes de seguridad se puede ver en la figura 3.

Figura 3. Esquema detallado de las etapas en la gestión de incidentes



Cada una de estas etapas contiene un conjunto de acciones que requieren ser llevadas a buen término para que el conjunto sea efectivo.

La seguridad global de un sistema informático depende, en gran medida, del diseño detallado de las etapas siguientes:

- **Prevención o preparación**. El objetivo consiste en intentar eliminar las causas que pueden ocasionar los incidentes. Por eso, se habla de análisis y gestión de riesgos. Esta etapa incluye tanto la prevención de los ataques como la preparación para responder a ellos correctamente. Para minimizar el daño potencial de un ataque se requiere estar preparado y seguir unas prácticas, como hacer copias de seguridad de los datos críticos de manera periódica, controlar y actualizar el *software* periódicamente, y tener implementada y documentada una política de seguridad. Las políticas de copia de seguridad hechas con regularidad minimizan la pérdida potencial de datos. El control con los proveedores, sitios web de seguridad y las listas de distribución es una manera de estar al día sobre el estado del *software* y los parches de seguridad. Es necesario actualizar el *software* para corregir

las vulnerabilidades que se van descubriendo. También es vital actualizar el *software* antivirus para mantener la protección del sistema actualizada.

- **Detección y análisis**. Dado que el riesgo es imprevisible, hay muchas probabilidades que tarde o temprano se materialice, de forma que el escenario más adecuado es la gestión de los incidentes. El primer paso en la gestión de incidentes es identificarlos. Hace falta identificar varias características de un ataque antes de que se pueda contener correctamente: determinar que realmente se está produciendo un ataque, sus efectos sobre la red (local y remota si hubiera), el posible daño a los sistemas y dónde se origina.

- **Contención**. Con el ataque identificado, hay que considerar los pasos necesarios para minimizar los efectos. La contención permite proteger otros sistemas y redes del ataque y limitar el daño. En esta fase, se hacen los pasos necesarios para detener el ataque. Una vez se ha contenido el ataque, la fase final es la recuperación.

- **Recuperación**. Finalmente, cuando el incidente ha tenido lugar, hay que responder a este. De forma que se debe recuperar el sistema en un estado seguro, aplicar acciones correctivas y reunir las pruebas del incidente. Hay que valorar el daño, qué información se ha perdido. ¿Por qué se ha producido? ¿Se ha controlado inmediata y correctamente? ¿Se podría haber controlado mejor? La fase de análisis permite a los administradores determinar la razón del ataque y las acciones correctivas para protegerse contra ataques futuros.

La seguridad se puede ver como la gestión del riesgo.

4.3. Clasificación de los ataques

Cualquier equipo conectado a una red informática puede ser vulnerable a un ataque. Por lo tanto, hay multitud de ataques diferentes, y es muy importante poderlos clasificar de alguna manera. Los podemos agrupar según la motivación, la manera de actuar o en función de quién los origina.

La protección de un sistema informático se tiene que dirigir al *hardware*, al *software* y de manera muy especial a los datos, tanto aquellos que se encuentren circulando a través de la red, como los que están almacenados en discos duros u otros soportes de similares propósitos. Observamos que si bien es posible reemplazar los componentes del *hardware* y del *software* de un sistema informático, los datos no tienen sustituto posible en caso de pérdida definitiva.

4.3.1. Motivos detrás de un ataque

Los motivos existentes detrás de un ataque son muchos y muy diversos como por ejemplo:

- Obtener acceso al sistema.
- Robar información, secretos industriales o propiedad intelectual.
- Recopilar información personal sobre alguien (un usuario).
- Obtener información de cuentas bancarias.
- Obtener información de una organización (la compañía del usuario, etc.).
- Afectar al funcionamiento normal de un servicio o un sistema informático.
- Utilizar el sistema de un usuario como un «trampolín» para un ataque a otro lugar.
- Suplantación de identidad.
- Ganancia económica.
- Usar los recursos del sistema de la víctima para fines diversos, en particular cuando la red en la que se localiza el sistema atacado tiene un ancho de banda considerable.
- Antiguo trabajador de una organización.

4.3.2. Según cómo actúa

Los ataques que pueden sufrir el *hardware*, el *software* y, de una manera muy especial, los datos, se clasifican en cuatro grandes grupos:

- **Interrupción**. Ataque contra la **disponibilidad**, en el cual se destruye un recurso del sistema o queda no disponible. Un ejemplo de ataque de interrupción es cortar una línea de comunicación o deshabilitar el sistema de ficheros del servidor. Otro ejemplo es un ataque de denegación de servicio.

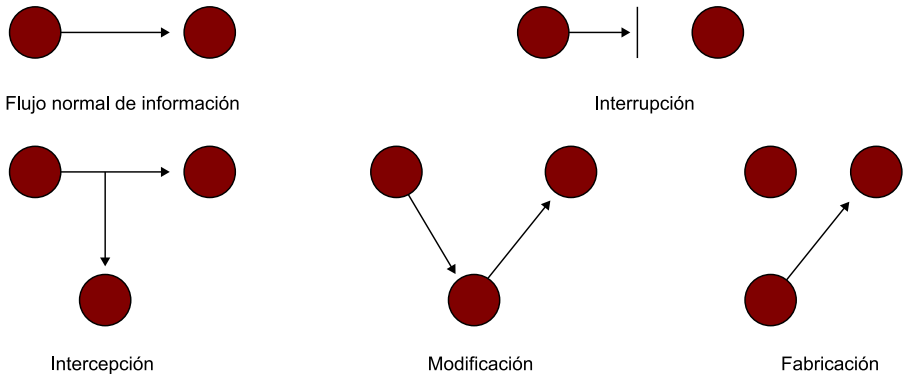
- **Interceptación**. Ataque contra la **confidencialidad**, en el cual un elemento no autorizado consigue acceder a un recurso. En este tipo de ataque no nos referimos únicamente a posibles usuarios que actúen como espías en la comunicación entre emisor y receptor. Por ejemplo, un proceso que se ejecuta subrepticiamente en un ordenador y que almacena en un fichero las teclas que pulsa el usuario que utiliza el terminal constituiría un ataque de interceptación.

- **Modificación**. Ataque contra la **integridad**, en el cual, además de conseguir acceder de manera no autorizada a un recurso, también se consigue modificarlo, borrarlo o alterarlo de cualquier manera. Los ataques están hechos por los intrusos. Borrado de bases de datos, alteración de páginas web, etc. son ejemplos típicos de esta modalidad de ataque.

- **Fabricación**. Ataque contra la **integridad**, en el cual un elemento consigue crear o insertar objetos falsificados en el sistema. Un ejemplo de ataque

de fabricación es añadir, de una manera no autorizada, un nuevo usuario y la contraseña correspondiente en el fichero de contraseñas.

Figura 4. Representación de los diferentes tipos de ataques que puede sufrir la comunicación entre un emisor y un receptor



4.3.3. Según quién lo origina

Pueden ser una o varias personas las que, con diferentes objetivos, originan un ataque a un sistema informático con el fin de intentar acceder a información confidencial, destruirla o simplemente conseguir el control absoluto del sistema atacado. Conocer los objetivos de los atacantes y sus motivaciones resulta, pues, esencial para prevenir y detectar las acciones.

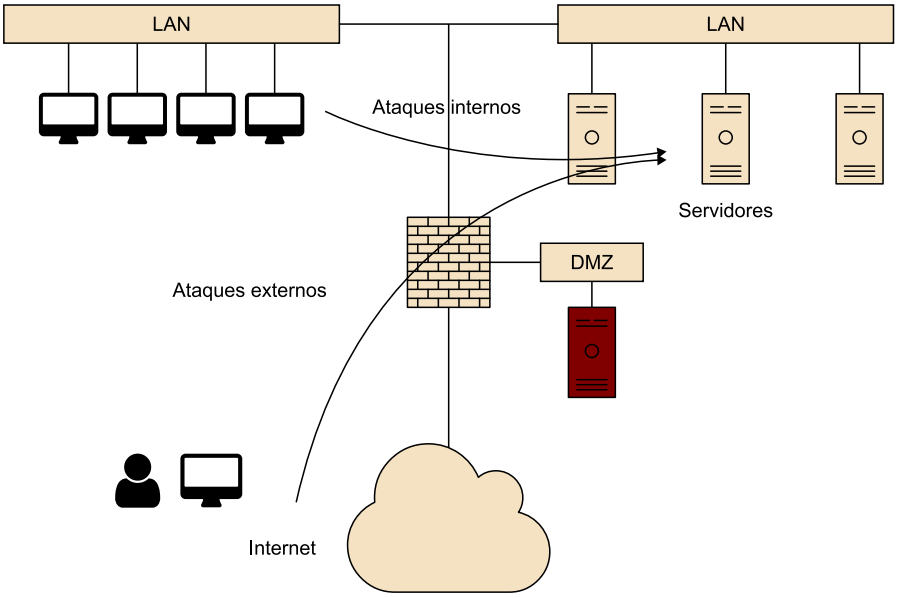
Los ataques provenientes de personas se pueden clasificar en dos grandes grupos: ataques pasivos y ataques activos.

- **Ataques pasivos**. El atacante no modifica ni destruye ningún recurso del sistema informático, simplemente lo observa, normalmente con el fin de obtener alguna información confidencial. A menudo, este ataque se produce sobre la información que circula por una red. El atacante no altera la comunicación, sino que sencillamente la escucha y obtiene la información que se transmite entre el emisor y el receptor. Como la información que se transmite no resulta alterada, la detección de este tipo de ataque no es una tarea sencilla, porque la escucha no tiene ningún efecto sobre la información que circula. Una solución muy eficaz, que permite resolver este tipo de problema, consiste en el uso de técnicas criptográficas para hacer que la información no se transmita en claro (visible) y no sea comprensible para los espías.

- **Ataques activos**. En una acción de este tipo, el atacante altera o destruye algún recurso del sistema. Ejemplos de ataques activos son la suplantación de identidad, la degradación fraudulenta del servicio o la modificación de mensajes.

Como ya se ha indicado previamente, conocer las motivaciones que pueden tener las personas para atacar a los sistemas informáticos puede ser vital para prevenir todo tipo de intrusiones. Hay que tener presente que un ataque puede provenir tanto del interior de la red (*insiders*) como del exterior (*outsiders*).

Figura 5. Ataques internos y externos (*insiders* y *outsiders*)



Veamos, pues, el perfil de los posibles atacantes de un sistema informático:

- **Antiguos trabajadores**. Una parte muy importante de los ataques a sistemas informáticos son los que llevan a cabo antiguos trabajadores que, antes de dejar la organización, instalan todo tipo de *software* destructivo como, por ejemplo, virus o bombas lógicas que se activan en ausencia del trabajador que, despedido o descontento por las condiciones de trabajo, ha decidido cambiar de ocupación. La presencia de este tipo de *software* no siempre es fácil de detectar, pero al menos sí que se pueden evitar los ataques que el antiguo trabajador puede llevar a cabo desde fuera con el nombre de usuario y la contraseña de que disponía cuando todavía trabajaba en la organización. Por lo tanto, como norma general, hay que dar de baja todas las cuentas del extrabajador y cambiar las contraseñas de acceso al sistema cuanto antes mejor.

- **Personal de la misma organización**. Aunque por defecto el personal interno disfruta de la confianza de la organización, hay que tener en cuenta que algunos ataques se pueden producir desde dentro mismo de la institución. A menudo, no hace falta que estos ataques sean intencionados (aunque, cuando lo son, son los más devastadores que se pueden producir); pueden ser accidentes provocados por el desconocimiento del personal (por ejemplo, el formateo accidental de un disco duro).

- ***Crackers*** (intrusos informáticos). Normalmente, estas personas llevarán a cabo ataques pasivos orientados a obtener información confidencial (por

ejemplo, un examen de un curso universitario), o simplemente con el fin de ponerse a prueba para obtener el control del sistema atacado. Además, si el atacante es bastante habilidoso, incluso podría borrar las trazas de sus acciones en los ficheros que las registran (denominados genéricamente ficheros de registro o ficheros log). Como este tipo de acciones no producen ningún efecto «visible», no se detectan fácilmente. Los intrusos suelen aprovechar la vulnerabilidad conocida de sistemas operativos y de *softwares* para conseguir el control de todo el sistema informático. Para llevar a cabo este tipo de acciones, basta con ejecutar varios *softwares* que se pueden obtener en Internet y que automatizan los ataques a los sistemas informáticos sin que el intruso necesite disponer de muchos conocimientos técnicos.

Hackers* y *crackers

Hay que ser cuidadosos a la hora de emplear ciertos términos informáticos como estos.

A pesar de que popularmente se ha consolidado el concepto de *hacker* como el de pirata informático, este anglicismo sería el equivalente a experto informático.

Por otro lado, el término ***cracker*** sería el equivalente a pirata informático.

- **Intrusos remunerados**. La ciberdelincuencia crece a un ritmo muy rápido, y aparecen constantemente nuevas tendencias. Las organizaciones delictivas utilizan Internet cada vez más con el objetivo de facilitar sus actividades ilícitas y maximizar los beneficios en el menor tiempo posible. En este caso, los intrusos están perfectamente organizados (incluso pueden estar en diferentes lugares geográficos) y atacan de una manera conjunta al sistema de una organización determinada. Disponen de muchos medios técnicos y reciben remuneraciones muy elevadas de la organización rival que dirige el ataque, a menudo con el ánimo de acceder a información confidencial (un nuevo diseño, un nuevo *software*, etc.) o bien con la intención de provocar un daño importante en la imagen de la organización atacada (un banco).

5. Informática y ciencias forenses

La generalización del uso de las tecnologías de la información en la sociedad ha incrementado el valor de la información digital y ha creado, a su vez, la necesidad de protegerla ante los ataques malintencionados o atribuibles al desconocimiento de estas nuevas tecnologías. En los dos casos, los rastros o las trazas que podrían revelar la ejecución de un hecho (tanto si es constitutivo de delito como no) están almacenados en soportes digitales y se denominan genéricamente *pruebas digitales*.

La prueba digital presenta, a grandes rasgos, las siguientes propiedades:

- Se puede modificar o eliminar fácilmente.
- Es posible obtener una copia exacta de un fichero sin dejar ningún rastro.
- La adquisición de la prueba puede comportar la alteración de los soportes digitales originales.

El análisis forense surgió de la necesidad de poder aportar elementos relevantes en los procesos judiciales, en los que las nuevas tecnologías estaban presentes, o bien como objetivo (por ejemplo, una intrusión que comporte daños en un sistema informático), o bien como medio (por ejemplo, el envío de correos electrónicos amenazantes a un personaje público). En cualquier caso, la prueba digital es esencial para encontrar las respuestas a las preguntas habituales que se plantean en cualquier investigación:

Preguntas clave

- ¿Qué se ha cometido?
- ¿Cuándo se ha hecho?
- ¿Dónde se ha cometido?
- ¿Quién lo ha hecho?
- ¿Cómo se ha llevado a cabo?
- ¿Por qué se ha cometido?

5.1. Principio de intercambio de Locard

Un principio fundamental en ciencia forense, que usaremos continuamente para relacionar a los autores con los hechos que han llevado a cabo, es el principio de intercambio o transferencia de Locard.

Edmund Locard (1877-1966) elevó a la categoría de imprescindibles una serie de pruebas forenses que antes se consideraban inútiles o incluso se ignoraban. El principio de intercambio de Locard se puede resumir en la frase «cada contacto deja un rastro», que significa que, en la mayoría de las acciones cotidianas, hay un intercambio.

Por ejemplo, la rotura de un cristal por un puñetazo deja restos de sangre en el escenario y fragmentos de cristal en la persona. Del mismo modo, una pisada dejará una huella sobre el terreno y rastros de tierra en la suela. El principio de Locard nos asegura que, en la gran mayoría de situaciones, hay un intercambio. Solo hay que tener la mente despierta y buscarlo.

En el mundo digital, el principio se aplica porque cualquier interacción con un ordenador afecta a la operativa, al estado de la memoria, e incluso a lo que se escribe en el disco duro. De forma que un experto puede encontrar trazas de la interacción, e incluso detalles que permiten reconstruir los hechos e identificar a los autores. Si bien es cierto que las pruebas informáticas (o evidencias digitales) pueden ser frágiles, esto no quiere decir que no existan y, por lo tanto, que no se puedan obtener pruebas definitivas, verificables e irrefutables.

5.2. Ciberdelito

El delito informático no aparece explícitamente definido en el actual Código Penal (1995), ni en las reformas posteriores.

Se habla de delito informático o ciberdelito cuando el sistema informático es el objetivo o bien un medio de comisión de un delito.

En definitiva, la mayoría de delitos informáticos son los delitos habituales (amenazas, estafas, etc.), en los cuales el sistema informático es utilizado como medio de comisión. Evidentemente, desde el punto de vista informático, los que serán más interesantes para nosotros serán aquellos que tengan el sistema informático como objetivo. Con esta característica solo tenemos, prácticamente, dos tipos de delitos: las intrusiones y los daños (DoS, *defacements*, etc.) en sistemas informáticos.

El caso de la intrusión (acceso no autorizado, aunque se realice sin romper ninguna contraseña) es muy curioso, puesto que, como consecuencia de no tener definido un capítulo específico para los delitos informáticos, la intrusión aparecerá recogida en los delitos contra la intimidad (desde el año 2010).

5.3. Ejemplos de delitos informáticos

5.3.1. Conrad Murray

Es uno de los casos más destacados de los últimos años. Conrad Murray era el médico de Michael Jackson. A pesar de que la informática forense no fue decisiva para el caso, no ayudó nada que los investigadores forenses encontraran documentación médica en su ordenador que mostraba que autorizaba cantidades mortales de propofol para la estrella del pop.

5.3.2. BTK Killer

Este es probablemente el uso más famoso de la informática forense para la resolución de un caso. Durante más de 30 años, la policía intentó utilizar técnicas tradicionales para localizar a la persona que había estrangulado a varias mujeres durante un periodo de 16 años, de 1974 a 1991. Se conoció con las siglas BTK (*Bind, Torture and Kill*, es decir, «atar, torturar y matar»). A menudo se burlaba de la policía con letras y poemas que enviaba a la prensa. Después de 10 años de silencio, envió un aviso a la prensa en 2004 en un disquete con un documento de Word. En pocas horas, los expertos en informática forense descubrieron metadatos en el disco que lo conectaron a un hombre llamado Dennis, relacionado con la Christ Lutheran Church. Finalmente, se detuvo a un hombre llamado Dennis Rader, el cual, más tarde, admitió haber cometido los crímenes.

5.3.3. Krenar Lusha

Cuando la policía entró en su casa comisaron, entre otras cosas, un ordenador portátil. Cuando los expertos en informática forense examinaron este ordenador, descubrieron que había descargado instrucciones sobre cómo construir cinturones suicidas y otros tipos de explosivos. También solía tener conversaciones en directo con personas, con las que se había identificado como terrorista y había dicho que quería ver a norteamericanos y judíos asesinados. Todo esto provocó una investigación en su apartamento, donde los oficiales encontraron equipos de fabricación de bombas y otras armas.

5.3.4. Matt Baker

A pesar de no ser un caso famoso, constata que cuando se utiliza un ordenador para el delito, la evidencia no se desvanece rápidamente con el tiempo. La historia empezó cuando la mujer del señor Baker murió de sobredosis de pastillas para dormir, y dejó una nota de suicidio. Todo el mundo aceptó que se había suicidado, pero después de cuatro años de investigación y el análisis forense del ordenador del señor Baker, se descubrió que este había estado buscando

en Internet información sobre sobredosis de pastillas para dormir y que había visitado varios sitios web farmacéuticos, poco antes del «suicidio» de su mujer. Matt Baker fue sentenciado a 65 años de prisión.

5.3.5. La ocultación de evidencias es peor que el delito

A diferencia de los casos anteriores, en este se comprueba cómo la carencia de evidencias también puede conducir a conclusiones en relación con los delitos cometidos.

Harold Einstein y Jennifer Boyd realizaron una compra de una propiedad (por una cantidad importante de dinero) en una transacción en que The Corcoran Group actuaba como agente. Después de la compra, se determinó que había graves deficiencias en la propiedad, las cuales no habían sido notificadas a los compradores. El caso se encargó a un experto en informática forense, con objeto de encontrar las evidencias de esta operación de compra. A pesar de que no se encontró ninguna evidencia, la conclusión a la que se llegó, fue tan interesante o más: los correos electrónicos y otros ficheros que tendrían que haber estado en los dispositivos examinados, habían desaparecido. A pesar de que no se pudo demostrar que los acusados habían eliminado los correos electrónicos relevantes, el juez dictaminó que intentaban ocultar intencionadamente las pruebas y engañaban al tribunal. La sentencia fue muy dura, puesto que se consideró que los acusados eran conocedores de los problemas de la propiedad y que, por lo tanto, habían eliminado las evidencias electrónicas.

5.3.6. El asesino de Craigslist

Una mujer fue asesinada y otra fue atacada después de emplear un servicio para conocer personas denominado Craigslist. La policía tuvo a su sospechoso una semana después del asesinato, gracias a la investigación forense digital. Los investigadores rastrearon la dirección IP de los correos electrónicos utilizados en la correspondencia de Craigslist, y las evidencias los llevaron rápidamente hacia un sospechoso: un estudiante de medicina de 23 años llamado Philip Markoff.

5.3.7. Suplantación de identidades para obtener información

Muchas entidades (en especial los bancos) sufren a menudo casos de *phising* (suplantación de identidades). En enero del 2018 una conocida entidad bancaria supuestamente se puso en contacto con sus usuarios, advirtiéndoles de que había una nueva «oleada de fraude» en la cual los ciberdelincuentes falsificaban la marca de la entidad, con el objeto de obtener los datos personales y la información bancaria diversa. Los atacantes enviaban un correo electrónico con la imagen del banco y pedían a los usuarios que les facilitaran datos privados.

5.3.8. Ashley Madison

En 2015 un grupo de ciberdelincuentes autodenominado The Impact Team aseguró haber robado los datos de los más de 37 millones de clientes del web de citas Ashley Madison. Amenazaron con publicar toda la información si la página no cerraba inmediatamente. Sin embargo, Ashley Madison siguió funcionando, y los *crackers* publicaron 10 *gigabytes* de información, con los nombres, apellidos y las transacciones bancarias de más de 32 millones de usuarios del web. Los primeros análisis de los datos, realizados por una empresa especializada en seguridad, CSO, señalaron que había decenas de miles de direcciones de correo electrónico pertenecientes a organismos públicos, muy probablemente falsas la mayoría. Ashley Madison considera que no es un acto de *hacktivismo* sino un acto criminal.

5.3.9. Equifax

Equifax, una empresa de crédito norteamericana, reveló que había sufrido un ciberataque durante varios meses. Detectado en julio del 2017, la fuga de información contenía los datos personales (nombres, fechas de nacimiento, números de la Seguridad Social, números de carnets de conducir) de 143 millones de clientes norteamericanos, canadienses y británicos, así como 200.000 números de tarjetas de crédito. Los atacantes usaron una vulnerabilidad conocida del servidor web Apache Struts. Sospechosamente, varios ejecutivos de la empresa vendieron acciones pocos días antes de que se hiciera pública la violación de la seguridad.

5.3.10. Marriott Hoteles

La información de unos 500 millones de usuarios del grupo hotelero Starwood de Marriott fue comprometida, incluidos los datos bancarios. La información robada incluía información de pago, nombres, direcciones de correo, números de teléfono, direcciones de correo electrónico, números de pasaporte e, incluso, detalles sobre la cuenta Starwood Preferred Guest (SPG), una tarjeta de gama alta emitida por el emisor de tarjetas de crédito American Express para viajeros habituales.

5.3.11. Robo de palabras de paso

En agosto del 2014, la compañía de seguridad informática Hold Security reveló que unos piratas informáticos rusos habían robado 1.200 millones de conexiones y contraseñas a 420.000 sitios web de todo el mundo. Esto podría haber permitido al grupo de piratas informáticos CyberVor acceder a 500 millones de cuentas de correo electrónico. Los *crackers* utilizaron redes de zombis programadas para visitar lugares y realizar pruebas de vulnerabilidad para explotar las vulnerabilidades de inyección SQL y acceder a bases de datos. A pesar de que el ataque es importante por su escala, en última instancia, no

ha tenido consecuencias importantes. Según el FBI, la información solo se ha utilizado en una gran campaña de correo basura (*spam*) en las redes sociales. La intención real de este robo continúa siendo un misterio.

5.3.12. Facebook

Facebook ha reconocido en una nota que un ataque informático ha comprometido información de 30 millones de usuarios, sobre todo datos personales y de contacto.

Los ciberdelincuentes controlaron unas 400.000 cuentas a través de una «vulnerabilidad» del código de la plataforma que afectó a la funcionalidad *Ver como* (una herramienta que permite a los usuarios ver su perfil como si fueran otras personas) de unas 400.000 cuentas y, desde aquí, llegaron a 30 millones de usuarios.

De los 30 millones de usuarios afectados, 15 millones vieron expuestos sus nombres y sus datos de contacto (número de teléfono, correo electrónico, o los dos, según el perfil del usuario). A 14 millones les fueron sustraídos, además, datos que tenían en su perfil de Facebook, como por ejemplo su nombre de usuario, sexo, idioma, religión, fecha de nacimiento, lugar de nacimiento, etc. Los piratas informáticos también se apropiaron de información relacionada con los últimos 10 lugares que estos internautas habían visitado en la red social, así como sus últimas 15 investigaciones, los dispositivos desde los cuales se conectaban a Facebook y las páginas que seguían.

5.3.13. Sexting

En mayo del 2019, V.R. se suicidó a raíz de la difusión de varios vídeos sexuales en los cuales aparecía. En pocos días estos vídeos se habían difundido a través de mensajes privados y grupos de WhatsApp dentro de la empresa donde trabajaba. Esto provocó en la mujer, de 32 años, una situación de presión y angustia. La mujer temía que las imágenes, grabadas antes de casarse, llegaran a su marido, hecho que, al parecer, se produjo. La policía tenía a su disposición el teléfono móvil de la mujer muerta y se realizó el análisis forense para tratar de averiguar si también pudo sufrir acoso por parte de algún compañero, tal como apuntaban círculos cercanos a la víctima.

5.3.14. Ciberacoso

La policía pudo evitar el suicidio de un menor de edad que estaba siendo acosado sexualmente a través de Internet. Los dos arrestados contactaban con los menores a través de Internet, desde Guatemala y, después de ganarse su confianza, les solicitaban material pornográfico de ellos mismos. Este es el resultado de una operación internacional entre agentes españoles, el departamento Homeland Security Investigation (HSI) de los Estados Unidos y la policía de Guatemala. Después de las investigaciones y de seguir el rastro digital de los

acosadores, se procedió a la entrada y el registro del domicilio de los presuntos acosadores. En el registro de la vivienda se descubrió la existencia de varias decenas de víctimas en varios países del mundo. Finalmente se decretó su ingreso en prisión.

5.3.15. Abraham Abdallah

El caso de Abraham Abdallah tiene todos los ingredientes para ser uno de los más extravagantes dentro de los fraudes con tarjeta de crédito. Este ayudante de camarero cogió directamente la lista de las personas más ricas y con una combinación de búsquedas en Internet y de ingeniería social se dedicó a recopilar números de la Seguridad Social, fechas de nacimiento, direcciones e incluso números de tarjetas de crédito. Posteriormente, utilizó los números de las tarjetas de personas como Oprah Winfrey, Steven Spielberg y Warren Buffett. Lo increíble del asunto es que, hoy en día, todavía se desconocen todas las compras y los cargos que realmente pudo estar haciendo. Se conocen los que no pudo hacer, pero se habla incluso de la compra de propiedades con estas suplantaciones de personalidad.

5.3.16. El problema de ser famoso

Majerczyk y Ryan Collins se han declarado culpables de invasión de la intimidad y divulgación de contenido privado. Sin estar relacionados, ambos conseguían fotografías íntimas de actrices y cantantes famosos. Más de 1.000 celebridades vieron publicadas por toda la red imágenes privadas suyas desnudas o con muy poca ropa. El método consistía en acceder a las cuentas de Gmail y Apple iCloud de las víctimas. Para llevarlo a cabo, primero enviaban correos a sus objetivos en nombre de iCloud, pidiéndoles las contraseñas como parte de un proceso de seguridad. Una vez obtenidas, tenían vía libre para entrar en el sistema de almacenamiento en la nube.

Ahora, tanto Collins como Majerczyk harán frente a una posible condena por un delito que atenta contra la privacidad y la imagen de todas las víctimas. La privacidad está prevista en la Declaración Universal de los Derechos Humanos, en el artículo 12. Si bien el Departamento de Justicia de los Estados Unidos no encontró pruebas que los vincularan con la filtración de las imágenes íntimas, los dos *crackers* se declararon culpables.

5.3.17. Campaña política de Macron

Se dijo que la campaña presidencial de Emmanuel Macron del 2017 había sido «víctima de un ataque pirata masivo y coordinado». Se hicieron públicos más de 20.000 correos relativos a la campaña presidencial un día antes de que los votantes franceses fueran a las urnas.

Unos 9 *gigabytes* de datos fueron publicados por un usuario llamado EMLEAKS en Pastebin, un sitio web para compartir documentos que permite la publicación anónima. Nunca ha quedado claro quién era el responsable de publicar los datos o si los correos electrónicos eran genuinos. Nadie sabe tampoco el impacto que ha tenido este ataque en el resultado de las elecciones.

5.4. Nuevos delitos informáticos

En pleno 2020 ya se está avisando de los peligros de los nuevos dispositivos médicos conectados a la red o que se pueden comunicar con esta.

Marcapasos y monitores de ritmo cardíaco

El Departamento de Seguridad Nacional Americano, que supervisa la seguridad en infraestructuras críticas de los Estados Unidos, incluyendo dispositivos médicos, emitió una alerta porque hay 750.000 marcapasos Medtronic vulnerables a la piratería informática.

La primera vulnerabilidad, identificada como CVE-2019-6538, proviene del protocolo inalámbrico de Conexus que no requiere de autenticación ni de autorización, hecho que significa que cuando la radio del dispositivo está activada, los atacantes pueden tomar el control de la comunicación. Una vez hecho esto, no hay nada que les impida reconfigurar el dispositivo médico con configuraciones potencialmente mortales.

La segunda vulnerabilidad, identificada como CVE-2019-6540, proviene del protocolo Conexus que no utiliza ningún tipo de cifrado inalámbrico, de forma que los atacantes cercanos pueden extraer los datos sensibles durante la comunicación del dispositivo.

Bombas de infusión

En 2017, se identificaron problemas con varias bombas de infusión en los hospitales de EE. UU. Se encontraron un total de ocho vulnerabilidades de seguridad en la bomba de infusión Medfusion 4000, fabricada por el fabricante de dispositivos médicos Smiths Medical. Los dispositivos en cuestión se utilizan en todo el mundo para la entrega de pequeñas dosis de medicamentos en el contexto de una atención crítica aguda, incluidos los cuidados intensivos neonatales, los cuidados intensivos pediátricos y los procedimientos de quirófanos. La amenaza para la seguridad detectada podría permitir a un atacante remoto obtener acceso no autorizado y afectar a la operación prevista de la bomba, incluida la administración de sobredosis mortales. Los problemas de seguridad identificados son:

- Uso de usuarios y contraseñas codificados para establecer automáticamente una conexión inalámbrica si no se ha modificado la configuración por defecto.

- Un error de desbordamiento de la memoria intermedia que se podría explotar para la ejecución remota de código malicioso en el dispositivo médico de destino.

- Falta de autenticación cuando se configuró la bomba para permitir conexiones FTP.

- Presencia de credenciales codificadas para el servidor FTP de la bomba.

- La carencia de validación adecuada del certificado del anfitrión deja la bomba vulnerable a ataques del tipo Man-in-the-middle (MiTM).

Sistemas de resonancia magnética

Un sistema de resonancia magnética de Bayer Medrad ha sido el primer dispositivo a ser *hackeado* en Estados Unidos. El dispositivo en cuestión se utiliza para controlar lo que se conoce como inyector de potencia, que ayuda a dar un agente de contraste a los pacientes del hospital. Estos agentes químicos están diseñados para mejorar la calidad de las exploraciones de resonancia magnética (MRI), que se utilizan para detectar desde traumas hasta tumores del cerebro y de la columna vertebral. A pesar de que este ataque no amenaza necesariamente a la seguridad de los pacientes, provocó la parada de las máquinas durante un periodo prolongado. Este problema, indirectamente, podría desencadenar varios errores clínicos.

Redes informáticas de sistemas de salud (hospitales...)

La amenaza más grande para la seguridad médica está en las redes hospitalarias enteras. En lugar de centrarse en los pacientes individuales y sus dispositivos implantados, los piratas informáticos tienen más probabilidades de atacar a sistemas hospitalarios enteros. Durante los últimos años, se han producido numerosos ataques de virus *ransomware* a los proveedores de salud, incluyendo el ataque del *malware* WannaCry, que devastó el Servicio Nacional de Salud de Estados Unidos (NHS) y numerosos hospitales. Estos ataques, que aprovecharon agujeros de seguridad de los sistemas operativos de Microsoft, pusieron en evidencia el hecho de que los hospitales todavía no están preparados para resolver estos tipos de incidencias. Cuando las redes hospitalarias son atacadas, potencialmente también se podrían comprometer los historiales médicos de pacientes de toda la red. También se podrían llegar a modificar estos historiales con consecuencias mortales. Incluso el acceso a estas redes podría tener como objetivo el control de dispositivos médicos conectados a la red.

6. Marco normativo asociado a la informática y a los ciberdelitos

El marco normativo asociado a la informática, en general, es muy diverso. Hay que tener en cuenta que hay un marco civil destinado a proteger la información y las personas en el ámbito digital, y especialmente en Internet, que contiene sanciones en su incumplimiento. El marco penal se asocia a los delitos informáticos y puede llegar a comportar incluso penas privativas de libertad.

6.1. Legislación en el ámbito digital e Internet

Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE). Se aplica al comercio electrónico y a los otros servicios de Internet cuando sean parte de una actividad económica. También regula todo aquello que hace referencia a las obligaciones y responsabilidades de los prestadores de estos servicios. El concepto de servicios de la LSSICE es amplio y engloba otras cosas además de la contratación de bienes y servicios por vía electrónica.

Entre otros, y siempre que representen una actividad económica, se incluyen los siguientes:

- La contratación de bienes o servicios por vía electrónica.
- La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
- La gestión de compras en la red por grupos de personas.
- El envío de comunicaciones comerciales.
- El suministro de información por vía telemática.
- Las actividades de intermediación relativas a la provisión de acceso a la red.
- La realización de una copia temporal de las páginas de Internet solicitadas por los usuarios.
- El vídeo bajo demanda, como servicio en el que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

Ley 22/1987 de propiedad intelectual. Esta ley ha sufrido muchos cambios, el último, en febrero de 2019 (Ley 2/2019). A pesar de esto, el espíritu inicial se mantiene. Regula los derechos de autor y sus creaciones. Desde la vertiente tecnológica, el aumento progresivo del uso de Internet hace necesario un estudio de la regulación que protege las creaciones que se ponen a disposición de los usuarios en la red y que se transmiten por medio de esta. Si bien hace años era muy caro y complicado hacer una copia de una obra, hoy en día el panorama es muy diferente, puesto que es enormemente fácil y barato reproducir y distribuir contenidos. Este cambio (en las formas de reproducción y distribución de las obras) genera un desfase entre las vías de tutela de la propiedad intelectual (surgidas en un momento y en una realidad muy diferente del actual) y la necesidad de protección que demanda la propiedad intelectual

actualmente. En definitiva, este desfase ha hecho que la propiedad intelectual se convierta en un tema de controversia y objeto de un debate social muy intenso.

A grandes rasgos, desde la perspectiva informática, la información que se protege es la creación de una obra, incluida esta en formato digital, los programas de ordenador, las bases de datos, obras multimedia y lugares y páginas web.

Ley 59/2003 de firma electrónica. La imposibilidad de emplear el documento de papel y la firma manuscrita en las transacciones electrónicas determina que aparezcan instrumentos que cumplan las funciones tradicionales que los primeros ejercían. La firma manuscrita supone la identificación de la persona y su vinculación con el contenido del documento. La firma electrónica surge como técnica sustitutiva de la firma manuscrita, que pretende cubrir las mismas funciones:

- la determinación de la identidad del emisor del mensaje y
- la comprobación que los términos de los mensajes de datos enviados no han sido alterados.

Ley 3/2018 de protección de datos personales y garantía de los derechos digitales. Esta ley adapta la normativa europea del Reglamento General de Protección de Datos (GDPR). Se pretende «garantizar y proteger, en cuanto al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar». Por lo tanto, la ley trata de proteger la intimidad de las personas físicas frente al tratamiento de sus datos personales.

Nota

Técnicamente deroga la Ley de protección de datos 15/1999 y su Reglamento de desarrollo 1720/2007.

El Reglamento General de Protección de Datos (GDPR) (UE 2016/679) es un reglamento europeo mediante el cual la Eurocámara, el Consejo de la Unión Europea y la Comisión Europea pretenden fortalecer y unificar la protección de datos para todos los países de la Unión Europea (UE), y controlar también la transferencia de datos. Se publicó en mayo del 2016 y entró en vigor el pasado 25 de mayo de 2018.

6.2. Los delitos informáticos y el Código Penal

A continuación, veremos más detalladamente algunos artículos del Código Penal (CP), relacionados con los mal llamados delitos informáticos (como ya hemos visto, no existen definidos como tales):

- **Artículo 197 (delitos contra la intimidad)**
  1. Quien, para descubrir los secretos o vulnerar la intimidad de otros, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualquier otro documento 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, tiene que ser castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

3. Quien, por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte de un sistema informático o se mantenga dentro de este en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, tiene que ser castigado con pena de prisión de seis meses a dos años.

Por lo tanto, son constitutivas de delito las siguientes conductas (sin consentimiento de la persona afectada, ni autorización judicial motivada):

- El apoderamiento de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales.
- La interceptación de las comunicaciones.
- La intrusión en un sistema informático.

Por lo tanto, NO se puede abrir un correo que no sea el personal, sin autorización. Esta cuestión es, desde el punto de vista judicial, muy compleja, puesto que, incluso en aquellos casos en que el correo electrónico es considerado como una herramienta empresarial, abrir el contenido podría comportar problemas legales.

- **Artículo 248 (estafa)**

1. Cometen estafa quienes, con ánimo de lucro, utilicen engaño suficiente para producir error en otro, y lo induzcan a realizar un acto de disposición en perjuicio propio o de otro.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio parecido, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabriquen, introduzcan, posean o faciliten programas informáticos específicamente destinados a la comisión de las estafas que prevé este artículo.

c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos que constan en cualquiera de estos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

Artículo 248

Este artículo recoge, entre otros, los fraudes por *phising* informático.

- **Artículo 264 (delito de daños)**

1. Quien por cualquier medio, sin autorización y de manera grave borre, estropee, deteriore, altere, suprima, o haga inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido sea grave, tiene que ser castigado con la pena de prisión de seis meses a dos años.

2. Quien por cualquier medio, sin estar autorizado y de manera grave, obstaculice o interrumpa el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, estropeando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido sea grave, tiene que ser castigado, con la pena de prisión de seis meses a tres años.

Artículo 264

Este artículo contendría los ataques DoS, *defacements*, etc.

En definitiva, hay que recordar:

- No todo aquello que es técnicamente posible es legal.
- El desconocimiento de las normas no exonera de responsabilidad al informático.
- Si una prueba no se ha obtenido con suficientes garantías, puede ser invalidada.

La siguiente tabla resumen sigue la clasificación que hace el Consejo de Europa, en nuestro Código Penal, donde hay reflejadas las siguientes conductas delictivas (fuente: Guardia Civil):

1.º Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 197	Se tipifican en este artículo las conductas que llevan a apoderarse de mensajes de correo electrónico ajenos o que permitan el acceso a documentos privados sin la autorización de sus titulares.
	La instalación de *softwares* del tipo ***sniffer***, ***keylogger*** o **troyanos** que permitan el acceso a datos reservados de carácter personal, como por ejemplo mensajes de correo electrónico. El acceso no autorizado a sistemas informáticos aprovechando *bugs* (agujeros) de seguridad u otras técnicas de *hacking*. El apoderamiento de datos reservados a otras personas que se encuentren en cualquier soporte informático.
Artículo 264.2 Artículo 278.3	Destrucción, alteración o daño de programas o documentos contenidos en ordenadores.
	La remisión o instalación en un ordenador ajeno de virus, gusanos o *softwares* maliciosos que alteren contenidos u ocasionen daños. La destrucción de datos o producción de daños en sistemas informáticos después de accesos no autorizados.
Artículo 278.1	Apoderamiento o difusión de documentos o datos electrónicos de empresas.
	La instalación de *softwares* del tipo ***sniffer***, ***keylogger*** o **troyanos** que permitan el acceso a datos de empresas que permitan realizar competencia desleal. El acceso no autorizado a sistemas informáticos aprovechando *bugs* (agujeros) de seguridad u otras técnicas de *hacking* para descubrir secretos de empresa.

2.º Delitos informáticos

Artículo 248.2	Estafas como consecuencia de alguna manipulación informática.
	Compras fraudulentas a través de Internet. Ventas fraudulentas a través de Internet. Fraudes en banca electrónica usurpando la identidad de la víctima.
Artículo 256	Utilización no consentida de un ordenador (sin la autorización de su propietario) que le causa un perjuicio económico superior a 300,5 €.
	Comunicaciones en Internet desde el ordenador puente de otra persona, que ocasiona que a esta se le facturen por este hecho más de 300,5 €.

Hay que destacar que conductas tan habituales en esta Sociedad de la Información, como son los correos basura o el simple escaneo de puertos, difícilmente encuentran cabida

entre los delitos tipificados en nuestro Código Penal, por lo cual no son perseguibles por vía penal.

3.º Delitos relacionados con el contenido

Artículo 186	Distribución a menores de edad de material pornográfico.
	Engaños en chats específicamente destinados a menores, haciéndose pasar por uno de ellos, enviándoles fotografías pornográficas y proponiéndoles prácticas abusivas.
Artículo 189	Distribución de material de pornografía infantil a través de Internet.
	Intercambiar o enviar fotografías de pornografía infantil a través de correo electrónico, chat o cualquier otro programa que permita la distribución de ficheros. Tener este material para distribuirlo a través de Internet.

4.º Delitos relacionados con infracciones de la propiedad intelectual y derechos afines

Artículo 270	Copia no autorizada de programas de ordenador o de música.
	Venta a través de Internet de copias de *softwares* o de CD de películas o música.
Artículo 270	Fabricación, distribución o tenencia de programas que vulneran las medidas de protección antipirateria de los programas.
	Creación, distribución o tenencia de *cracks* que permiten saltarse las limitaciones con las que cuentan algunos programas.
Artículo 273	Comercio a través de Internet de productos patentados sin autorización del titular de la patente.
	Venta en Internet de copias ilegales o productos piratas.

7. Estándares ISO/UNE y organismos internacionales

El ámbito forense y la seguridad informática cuentan con un conjunto de normativas y de organismos internacionales con objeto de tener guías de buenas prácticas (cómo hacer las cosas), métodos y medidas comunes.

7.1. Seguridad informática

Familia ISO 27000. Es un conjunto de estándares internacionales sobre la Seguridad de la Información. La familia ISO 27000 contiene un conjunto de buenas prácticas para el establecimiento, la implementación, el mantenimiento y la mejora de Sistemas de Gestión de la Seguridad de la Información (SGSI). Están publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en inglés a las siglas de *Information Security Management System*.

La serie contiene las mejores prácticas recomendadas en Seguridad de la Información para desarrollar, implementar y mantener especificaciones para los SGSI. Las más relevantes para nosotros son:

- **ISO/IEC 27000**. Information security management systems - Overview and vocabulary[9]
- **ISO/IEC 27001**. Information technology - Security Techniques - Information security management Systems
- **ISO/IEC 27002**. Code of practice for information security controls - essentially a detailed catalog of information security controls that might be managed through the ISMS
- **ISO/IEC 27003**. Information security management system implementation guidance
- **ISO/IEC 27004**. Information security management - Monitoring, measurement, analysis and evaluation
- **ISO/IEC 27005**. Information security risk management
- **ISO/IEC 27006**. Requirements for bodies providing audit and certification of information security management systems
- **ISO/IEC 27017**. Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- **ISO/IEC 27031**. Guidelines for information and communication technology readiness for business continuity
- **ISO/IEC 27032**. Guideline for cybersecurity
- **ISO/IEC 27033-1**. Network security - Part 1: Overview and concepts
- **ISO/IEC 27033-2**. Network security - Part 2: Guidelines for the design and implementation of network security

- **ISO/IEC 27033-3**. Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
- **ISO/IEC 27039**. Intrusion prevention
- **ISO/IEC 27036-4**. Information security for supplier relationships - Part 4: Guidelines for security of cloud services

7.2. Análisis forense

La serie 27000 también contiene varias normas relacionadas con la gestión de las evidencias digitales (27037) y el análisis forense (27042).

ISO/IEC 27037. Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence

Gestión de las evidencias digitales (aparecen las etapas previas al análisis de las evidencias).

ISO/IEC 27040. Information technology - Security techniques - Storage security

Reúne guías y recomendaciones para que el almacenamiento de las evidencias digitales sea seguro. Nos presenta riesgos existentes en el almacenamiento y nos provee directrices o buenas prácticas incluyendo modelos de auditorías y revisiones para poder controlar el almacenamiento de las evidencias y garantizar que se haga de forma correcta y segura.

ISO/IEC 27041. Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative

ISO/IEC 27042. Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence

Indicaciones para el análisis e interpretación de la evidencia digital.

ISO/IEC 27043. Information technology - Security techniques - Incident investigation principles and processes

Además, de las normas anteriores, España dispone de normas UNE específicas que no son una mera traducción de las anteriores. Estas normas, relativas a la gestión de la evidencia digital, el análisis forense y los informes periciales, son las siguientes:

Familia UNE 71505

UNE 71505-1. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales

UNE 71505-2. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas

UNE 71505-3. Tecnologías de la Información (TI). Sistemas de Gestión de Evidencias Electrónicas (SGEE). Parte 3: Formatos y mecanismos técnicos

UNE 71506. Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas

UNE 197010. Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)

Finalmente, entre otras, también podemos disponer de las guías RFC:

RFC 3227. Manejo y recolección de evidencias. Este documento nos indica las principales guías para la recolección y el almacenamiento de evidencias digitales. Esta RFC se considera un estándar.

RFC 4810. Cómo preservar la información a largo plazo. Esta RFC nos define un estándar relacionado con la preservación de la información. Punto muy importante para los informes periciales y las investigaciones tecnológicas, puesto que el trabajo siempre tiene que poder ser comprobado para validar su autenticidad y su veracidad. En esta RFC, entre otras, se indica a los peritos cómo tienen que proceder para verificar una firma digital después de haber pasado un gran espacio de tiempo desde la generación de la misma.

7.3. Organismos internacionales

Los organismos internacionales son multidisciplinarios y están integrados por expertos de diferentes disciplinas, con el objetivo de avanzar en el conocimiento de la ciencia forense y su aplicación en el ámbito judicial, fomentando la colaboración para la consecución de acuerdos mutuos dentro del campo. Estos acuerdos son de vital importancia tanto en el contexto científico como en el del proceso judicial, contextos en los que surgen debates de diferente índole.

- International Association of Computer Investigative Specialist (IACIS). Esta asociación ofrece una certificación internacional (CFEC, Computer Forensic External Certification), dirigida a analistas que no formen parte de los cuerpos policiales o judiciales.

- International Organization on Computer Evidence (IOCE).

- Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas (esCERT).

- American Academy of Forensic Sciences (AAFS). http://www.aafs.org/

- European Network of Forensic Science Institutes (ENFSI). http://enfsi.eu/

Resumen

En este módulo didáctico hemos visto qué es la informática forense, sus orígenes y cómo se ha expandido mucho más allá de reunir evidencias con finalidades judiciales. La informática forense puede ser vista como una disciplina forense donde se analiza un caso, se extraen evidencias de este y se formula una posible explicación de qué ha pasado. Esta visión está muy ligada a una peritación judicial y, en consecuencia, al funcionamiento del sistema judicial.

Puesto que constituye una disciplina consolidada, su vinculación con estándares internacionales y con normativa legal es muy importante. La normativa vigente puede ser civil, como por ejemplo la Ley de protección de datos y la Ley de propiedad intelectual o penal como la tipificación y las penas asociadas a los ciberdelitos. En cuanto a los estándares, la encontramos con la seguridad de la información y con los métodos y la recogida de evidencias que hacen que toda la comunidad de informática forense trabaje del mismo modo.

A causa de que la informática forense ha ampliado mucho su campo de uso, se ha planteado también como elemento en las organizaciones dentro de la seguridad informática y en la gestión de incidentes. Así pues, puede ayudar a proteger la información, activo principal de las organizaciones.

La gestión de incidentes es muy importante, puesto que no es posible la seguridad absoluta. La informática forense se ha convertido en una herramienta fundamental para evaluar las anomalías en sistemas informáticos. Una correcta evaluación (informe forense) tiene que permitir el uso en sede judicial y a la vez un documento para corregir los fallos de un sistema informático, a fin de que no vuelva a suceder el incidente.

A pesar de que el análisis forense se puede aplicar a las organizaciones por motivos técnicos, de gestión del sistema, o para la implantación de políticas de seguridad, en las peritaciones también se tiene que ver su intersección con el sistema legal, es decir, que no se trata únicamente de ordenadores, redes y documentos electrónicos, sino también de procesos legales, garantías en la obtención de las pruebas, informes claros y concisos, y hechos que se tienen que presentar de manera conveniente y convincente.

La informática forense, por lo tanto, constituye la intersección entre la seguridad de la información, la gestión del incidente, la peritación y la normativa vigente.

Actividades

1. Buscad por la red información adicional sobre Locard y compartidla en el foro. Descubriréis que han cambiado muchos de los conceptos de la criminalística moderna. La ciencia forense actual sería diferente sin su trabajo.

2. Buscad una noticia vinculada a la delincuencia tecnológica y subidla al foro de la asignatura.

Ejercicios de autoevaluación

1. ¿Qué quieren decir los siguientes acrónimos?

LSSICE	
LPI	
CP	
GDPR / RGPD	
IDS	
LOPDGDD	
TIC	
ENFSI	
CID / CIA	

2. ¿Cuáles de estas frases respecto a las peritaciones son ciertas y cuáles falsas?

a) Las peritaciones se orientan a la evaluación de la eficacia y la eficiencia.
b) Su objetivo es la constitución de pruebas mediante la emisión de un dictamen sobre hechos concretos.
c) Solo se emiten conclusiones sobre puntos concretos.
d) Su periodicidad es planificada o periódica.
e) Se llevan a cabo por presunción de delito, daño o ineficacia.
f) El perito es libre de definir su ámbito de actuación.

3. Relacionad los siguientes términos:

Delito informático		SGSI
Delito de intrusión		Cualquier disciplina cuyos principios científicos se utilicen para ayudar a la justicia
ISO 27000		No está definido en el Código Penal
Ciencias forenses		197bis del Código Penal

4. ¿Cuáles son los principios de la informatica forense?

5. ¿Es cierto o falso que el principio de Locard dice que cualquier rastro tiene que provenir de dos o más contactos?

6. ¿Cuáles de estas frases son ciertas y cuáles falsas?

a) La preparación es una etapa muy importante para minimizar la cantidad e importancia de los ataques al sistema.
b) La metodología forense se tiene que aplicar una vez contenido el incidente, puesto que es cuando hay las evidencias digitales.
c) La informática forense y la recuperación del sistema se tienen que ponderar para evitar la pérdida de evidencia digital.
d) La contención del incidente se puede hacer de forma automática.
e) Con herramientas de gestión de incidentes no hace falta un equipo de respuesta de incidentes.

7. ¿Cuáles son los artículos del Código Penal vinculados a los ciberdelitos?

8. ¿Cómo se define la informática forense?

a) Como un conjunto de recursos interconectados para mejorar el rendimiento.
b) Como una ciencia forense que se encarga de la preservación, identificación, extracción, documentación e interpretación de la evidencia digital, de forma que esta sea aceptada en el protocolo de seguridad.
c) Como una ciencia forense que se encarga de asegurar, identificar, preservar, analizar y presentar la evidencia digital, de forma que esta sea aceptada en un proceso judicial.
d) Como una ciencia o especialidad científica donde los principios, métodos y técnicas se aplican a la justicia, en cualquiera de sus aspectos.

9. Relacionad los temas con sus descripciones:

Detectar intrusión		Anticiparse al incidente
Locard		Detección y análisis
Objetivo preventivo		Tener control sobre la evidencia
Principio de la informática forense		IDS
Etapa de gestión de incidentes		Cada contacto deja un rastro

10. ¿Cuáles de estas frases son ciertas y cuáles falsas?

a) La informática forense se inició en la Primera Guerra Mundial y como consecuencia de esta.
b) Los usos de las ciencias forenses, y la informática forense no es una excepción, están muy ligados a los procesos judiciales.
c) La informática forense permite mejorar la seguridad de la organización.
d) La evidencia digital, afortunadamente, no es volátil, de forma que su adquisición es un proceso factible.
e) La informática forense es un proceso científico y gracias a esto podemos asegurar que las pruebas son rigurosas.

Solucionario

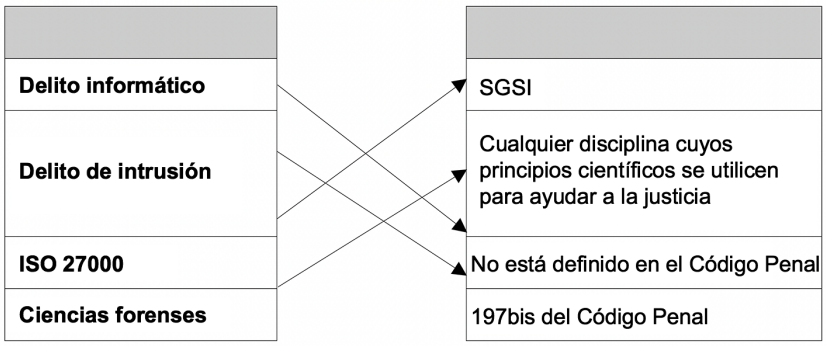
Ejercicios de autoevaluación

1.

LSSICE	Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.
LPI	Ley de propiedad intelectual.
CP	Código Penal.
GDPR / RGPD	Reglamento General de Protección de Datos (RGPD) o su equivalente inglés General Data Protection Rule (GDPR).
IDS	Intrusion Detection System. Sistema de detección de intrusos.
LOPDGDD	Ley orgánica de protección de datos personales y garantía de los derechos digitales.
TIC	Tecnologías de la Información y la Comunicación.
ENFSI	European Network of Forensic Science Institutes.
CID / CIA	Confidencialidad, Integridad y Disponibilidad (CID) o el equivalente en inglés Confidenciality, Integrity and Availability (CIA).

2. a) Falso
b) Cierto
c) Cierto
d) Falso
e) Cierto
f) Falso

3.



4.
- Evitar la contaminación.
- Actuar metódicamente.
- Tener control sobre la evidencia.

5. Falso.

6. a) Cierto
b) Cierto
c) Cierto
d) Falso
e) Falso

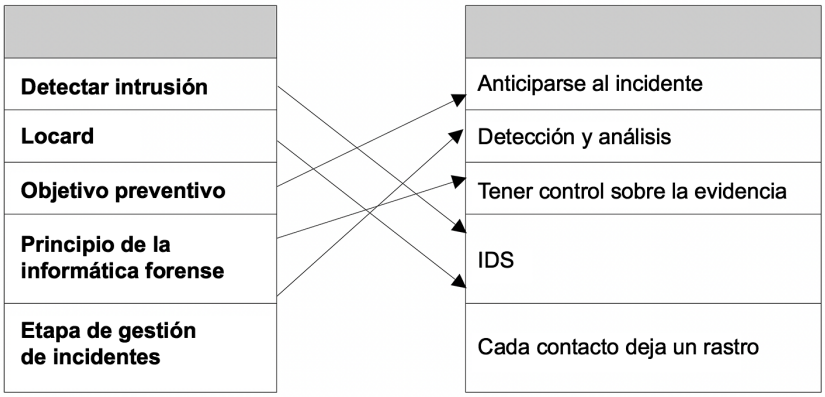
7. Artículos del Código Penal:

- 197
- 248

- 264

8. c

9.



10. a) Falso
b) Cierto
c) Cierto
d) Falso
e) Cierto

Glosario

activo *m* Son los componentes indispensables para el correcto funcionamiento de un sistema informático. En general, el *hardware*, el *software* y los datos.

CART Computer Analysis and Response Team. El equipo de respuesta de análisis de ordenadores del FBI ofrece ayuda en la investigación y adquisición de pruebas de ordenador, así como exámenes forenses y apoyo técnico para investigaciones.

ciencia forense *f* La aplicación de prácticas científicas dentro del proceso legal. La ciencia forense alcanza tanto la rama civil como la penal del derecho.

cracking Acceder de manera ilegal a datos almacenados en un ordenador o servidor.

datos *m pl* Conjunto discreto de factores objetivos sobre «alguna cosa». Puede ser un número, una letra...

delito de intrusión informática *m* Acceso a un sistema informático vulnerando la seguridad establecida. Aparece tipificado en el artículo 197bis del Código Penal.

demanda *f* Petición concreta, ante un órgano de una jurisdicción determinada, que inicia un procedimiento ante este. En esta demanda se narran los hechos, se adjuntan documentos y se expresan fundamentos de derecho.

denuncia *f* Acción de poner en conocimiento de la autoridad competente una infracción penal o administrativa. En general, es obligatoria para quien lo haya presenciado o tenga conocimiento de esta.

diligencia *f* Actuación del secretario judicial en un procedimiento criminal o civil.

elemento material probatorio *m* Objeto que sirve para probar unos hechos como, por ejemplo, una pistola que está en la escena del crimen.

evidencia *f* Cualquier elemento que proporcione información de la cual se pueda inferir alguna conclusión o bien que constituya un hallazgo relacionado con el hecho que se investiga.

firma electrónica *f* Procedimiento que permite comprobar la identidad del emisor de un mensaje electrónico y su autenticidad. Para que sea equiparable a la firma manuscrita tiene que ser avanzada, basada en un certificado reconocido y haber sido creada por un dispositivo seguro de creación de firma.

firma electrónica avanzada *f* Firma que permite identificar el signatario y que se puede vincular, de manera única, tanto al signatario como a los datos, y también permite detectar cambios posteriores de los datos.

FLECT Federal Law Enforcement Training Center. Centro de entrenamiento federal para el cumplimiento de la ley. Es una organización de formación de cumplimiento de la ley que entrena a más de 80 agencias federales. El centro también proporciona servicio a agencias estatales e internacionales. Tiene su sede en Glynco. http://www.fletc.gov

IACIS International Association of Computer Investigative Specialists. Organización internacional de especialistas en investigación informática. Es un voluntariado internacional sin ánimo de lucro compuesto por profesionales dedicados a la enseñanza en el campo de la informática forense. Los miembros del IACIS representan a profesionales de ámbito nacional e internacional. http://www.iacis.com/

incidente *m* Cualquier hecho anómalo que afecte al funcionamiento del sistema informático.

información *f* La reunificación y estructuración de los datos en un contexto que le da sentido.

informática forense *f* Ciencia forense que se ocupa del uso de los métodos científicos aplicables a los sistemas informáticos. Se encarga de la preservación, identificación, extracción, documentación e interpretación de la evidencia digital, de forma que esta sea aceptada en un proceso judicial.

insaculación *f* Selección del perito por sorteo entre los miembros de las listas de peritos o bien entre tres peritos (terna) que se hayan propuesto al juez.

IOCE International Organization on Computer Evidence. Organización internacional de especialistas en evidencia computacional. Su propósito es proveer un foro internacional para el intercambio de la información relacionada con la investigación computacional y la informática forense.

jurisdicción *f* Conjunto de órganos jurisdiccionales ordinarios o especiales. A los ordinarios, se les atribuye el conocimiento y la resolución de los conflictos en general, mientras que los especiales se ocupan de materias específicas como, por ejemplo, la militar.

jurisdicción ordinaria *f* Jurisdicción separada en cuatro órdenes: civil, penal, contencioso administrativo y laboral o social.

máxima *f* Regla, principio o proposición generalmente admitida por quienes profesan una facultad o ciencia.

ministerio fiscal *m* Órgano integrado dentro del poder judicial que actúa con autonomía en la realización de sus funciones, ejerce su misión por medio de órganos propios y actúa de manera coordinada y unitaria en todo el territorio del Estado.

organización *f* Cualquier entidad, institución o agrupación que necesite o utilice una infraestructura informática para llevar a cabo su objetivo.

política de seguridad *f* Conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la organización. Se trata de un plan realizado para combatir todos los riesgos a los que está expuesta la organización en el mundo digital.

provisión de fondos *f* Cantidad de dinero que la parte o las partes entregan por anticipado de los honorarios totales para efectuar las pruebas periciales solicitadas.

querella *f* Concepto similar a la denuncia, pero en este caso el querellante manifiesta la voluntad de formar parte de la causa y se tienen que cumplir algunos requisitos adicionales. Se dirige a la acción penal.

ransomware *m* *Software* malicioso que requiere a la víctima un pago para poder acceder a los ficheros que ha cifrado.

recurso de apelación *m* Recurso frente a la sentencia definitiva dictada por el juez penal.

sistema informático *m* Todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

Tecnologías de la Información *f pl* Conjunto de técnicas para procesar información en cualquier formato que pueda aparecer. Con esto también se incluye la informática.
sigla: **TI**

terna *f* Conjunto de tres personas para que se designe entre ellas la que tiene que ejercer un cargo o una ocupación.

TI Véase Tecnologías de la Información.

Bibliografía

Abel Lluch, X. (2006). *Empresa y prueba informática*. Barcelona: Bosch.

Agencia Estatal BOE (1882). Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (BOE núm. 260, de 17/09/1882). <http://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf>

Agencia Estatal BOE (1978). Constitución Española de 27 de diciembre de 1978 (BOE núm. 311, de 29 de diciembre de 1978). <http://www.parlament.cat/document/nom/ConstitucioConsolidat.pdf>

Agencia Estatal BOE (1995). Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (BOE núm. 281, de 24/11/1995). <http://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf>

Agencia Estatal BOE (1996). Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril (BOE núm. 53, de 2 de marzo de 2019). <http://www.boe.es/boe_catalan/dias/2019/03/02/pdfs/BOE-A-2019-2974-C.pdf>

Agencia Estatal BOE (2002). Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE núm. 166, de 12/07/2002). <http://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>

Agencia Estatal BOE (2003). Ley 59/2003, de 19 de diciembre, de firma electrónica (BOE núm. 304, de 20/12/2003). http://www.boe.es/buscar/act.php?id=BOE-A-2003-23399

Agencia Estatal BOE (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6 de diciembre de 2018, páginas 119.788 a 119.857). <http://www.boe.es/boe_catalan/dias/2018/12/06/pdfs/BOE-A-2018-16673-C.pdf>

Balagué Doménech, J. C. (2007). *La prueba pericial contable en las jurisdicciones civil, penal, contencioso-administrativa y laboral*. Barcelona: Bosch.

Colobran Huguet, M.; Arques Soldevila, J.; Marco Galindo, E. (2008). *Administració de sistemes operatius en xarxa*. Barcelona: Editorial UOC.

Colobran Huguet, M. (2015). *A General-Purpose Security Framework. PHD Thesis*. Universitat Autònoma de Barcelona. <http://www.tdx.cat/handle/10803/322814>

Colobran Huguet, M.; Arques Soldevila, J.; Guash Petit, A. (2012). *Anàlisi forense de sistemes d'informació. Investigació de la prova digital*. Barcelona: Editorial UOC.

Elias Baturones, J. J. (2008). *La prueba de documentos electrónicos en los tribunales de justicia*. Valencia: Tirant lo Blanch.

Flores Prada, I. (2006). *La prueba pericial de parte en el proceso civil*. Valencia: Tirant lo Blanch.

García Pañeda, X.; Melendi Palacio, D. (2008). *La peritación informática. Un enfoque práctico*. Oviedo: Colegio Oficial de Ingenieros en Informática del Principado de Asturias.

Guasch Petit, A. y otros (2008). *Auditoría, peritajes y aspectos legales para informáticos*. Barcelona: UOC.

Harris, S.; Harper A.; Eagle, C.; Ness, J.; Lester, M. (2005). *Hacking Etico / Gray Hat Hacking* (Hackers & Seguridad / Hackers and Security). Anaya Publishers.

Humero Martín, A. (2006). *Guía de actuación y responsabilidades del perito en los procedimientos: civiles, penales, contencioso-administrativos, tributarios, sancionadores de consumo, arbitrales*. Madrid: Dykinson.

Luzón Cuesta, J. M. (2000). *La prueba en el proceso penal derivada de la entrada y registro domiciliario*. Madrid: Cólex.

Scientific Working Group on Digital Evidence (2006). *Best Practices for Computer Forensics*. <http://www.swgde.org/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf>

Unión Europea (2016). *General Data Protection Regulation (EU)* 2016/679. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL>

U.S. Department of Justice. Federal Bureu of Investigation. Laboratory Division (2007). Handbook of Forensic Services. EUA. <http://www.fbi.gov/file-repository/handbook-of-forensic-services-pdf.pdf/view>