

Seguridad y Alta Disponibilidad

CFGS Administración de Sistemas Informáticos en Red
2.º curso

TEMA 1

Principios de seguridad informática

Sumario

I Conceptos básicos.....	4
1 CID.....	4
2 Autenticación – AAA.....	6
II Seguridad física y seguridad lógica.....	7
1 Seguridad física.....	7
1.1 Acceso de personas no autorizadas.....	7
1.2 Protección frente a otras amenazas.....	7
2 Seguridad lógica.....	8
III Vulnerabilidades.....	9
1 Vulnerabilidad de día cero (<i>zero-day</i> o <i>0-day</i>).....	9
2 Ingeniería social.....	10
IV Amenazas.....	11
V Seguridad activa y seguridad pasiva.....	12
VI Seguridad física y ambiental.....	13
1 Centro de Proceso de Datos.....	13
1.1 Localización del CPD.....	14
1.2 Fuentes de alimentación redundantes.....	14
VII Listas de control de acceso.....	17
VIII Autenticación de usuarios.....	18
1 Contraseñas.....	18
1.1 Gestión de contraseñas.....	18
1.2 Ataques a contraseñas.....	19
2 Biometría.....	19
3 Autenticación en dos pasos.....	20
IX Seguridad en el almacenamiento.....	21
1 Almacenamiento redundante.....	21
2 Almacenamiento en red: NAS y SAN.....	21
3 Copias de seguridad e imágenes de respaldo.....	22
3.1 Métodos de copia de seguridad.....	22
3.2 Medios de almacenamiento.....	24
3.3 Otras consideraciones sobre las copias de seguridad.....	25
X Auditorías de seguridad.....	26
1 Objetivos de una auditoría de seguridad informática.....	26
2 Tipos de auditorías de seguridad informática.....	26
2.1 Análisis forense en sistemas informáticos.....	28
XI Centros de información y respuesta.....	32
1 Qué es un CSIRT.....	32
2 CSIRT de nuestro ámbito.....	33
2.1 Comunidad Valenciana.....	33
2.2 España.....	33
2.3 Unión Europea.....	33
2.4 Otros.....	33
3 Organismos de ciberseguridad.....	34
3.1 INCIBE.....	34
3.2 ENISA.....	34
XII Bibliografía.....	35

v1.03



Julio Garay
IES Poeta Paco Mollá
Petrer (Alicante), 2021

Estos apuntes están sujetos a una licencia
Creative Commons Reconocimiento-NoComercial-CompartirIgual 3.0.

Para ver una copia de esta licencia, por favor visite la página web
<http://creativecommons.org/licenses/by-nc-sa/3.0/deed.es>

En resumen, usted es libre de:

Compartir — copiar y redistribuir el material en cualquier medio o formato

Adaptar — remezclar, transformar y construir a partir del material

Bajo los siguientes términos:

Atribución — Usted debe dar crédito de manera adecuada, brindar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo del licenciente.

NoComercial — Usted no puede hacer uso del material con propósitos comerciales.

CompartirIgual — Si remezcla, transforma o crea a partir del material, debe distribuir su contribución bajo la misma licencia del original.

No hay restricciones adicionales — No puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras a hacer cualquier uso permitido por la licencia.

I Conceptos básicos

La **seguridad informática** es la práctica de proteger la información mitigando los riesgos a que puede verse sometida. Se suele considerar que incluye la prevención (o al menos la reducción de la probabilidad) de que la información se vea afectada por:

- el acceso no autorizado o inapropiado
- Uso ilegal
- Divulgación (revelación, inspección, copia)
- Alteraciones (disrupción, borrado, corrupción, modificación)

La seguridad informática involucra acciones y procedimientos definidos para garantizar la **prevención, detección y represión** de cualquiera de los incidentes mencionados, si tuviesen lugar. Además, debe planear acciones **correctivas**, para los casos en que las medidas anteriores no hayan sido suficientes para impedir un incidente.

Aunque en Seguridad Informática nos ocupamos de la protección de la información digital, debemos tener en cuenta que la información puede tomar cualquier forma, y no sólo **electrónica**: también se encuentra en forma **física o tangible** (p. ej. documentos de papel), o **intangible** (conocimiento por parte de seres humanos).

1 CID

La seguridad informática busca una protección equilibrada de la **confidencialidad**, la **integridad** y la **disponibilidad** (CID), centrándose en una implementación de normas y protocolos eficaces, pero que no afecten negativamente la productividad organizacional.

Confidencialidad

Consiste en garantizar **que la información sea accesible solamente para un grupo de personas autorizadas**, determinado por el propietario de dicha información. En otras palabras, consiste en «**guardar el secreto**» de esa información, fuera de las personas que tienen derecho a acceder a ella.

Integridad

Se define como el mantenimiento y garantía de la **exactitud** y **consistencia** de la información durante su ciclo de vida. En otras palabras, consiste en «**mantener los datos de forma que sean correctos y completos**».

Disponibilidad

Es la cualidad de los datos de ser **accesibles** por parte de los usuarios que los necesiten. En otras palabras, significa «**hacer que los datos sean accesibles para los usuarios en todo momento**». Debe tenerse en cuenta que el concepto «en todo momento» es utópico.

co: hasta los sistemas más fiables tienen algún porcentaje de tiempo, por pequeño que sea, de inaccesibilidad. El porcentaje de tiempo de accesibilidad requerido depende de las necesidades del sistema y sus usuarios: para algunos sistemas, una disponibilidad del 95% puede ser suficiente. En otros, se puede requerir el 99% o más. Algunas medidas convencionales de alta disponibilidad son las de «los nueves»:

- «Dos nueves», 99% de disponibilidad. los datos pueden permanecer inaccesibles hasta 3,65 días al año.
- «Tres nueves», 99,9% de disponibilidad. los datos pueden permanecer inaccesibles hasta 8¾ horas al año.
- «Cuatro nueves», 99,99% de disponibilidad. los datos no pueden permanecer inaccesibles más de **52,56 minutos al año**.
- «Cinco nueves», 99,999% de disponibilidad. los datos no pueden permanecer inaccesibles más de **5,26 minutos al año**. Se considera un estándar de excelencia. Muy costoso y muy difícil de alcanzar.

Cada «nueve» que añadimos incrementa enormemente los requerimientos para poder cumplir con la disponibilidad comprometida. Por poner un ejemplo real, Amazon se compromete a una disponibilidad del 99,95% en sus sistemas, a medio camino entre los «tres nueves» y los «cuatro nueves». Y no siempre ha sido capaz de cumplir con dicho compromiso.

A los conceptos anteriores se suelen añadir la **Autenticación** (o Autenticación) que, por su importancia, veremos en más detalle en el siguiente punto (p. 6), y el **No repudio**, formando el acrónimo *CIDAN*.

No repudio

Aunque ha tenido diferentes definiciones, algunas de ellas un tanto crípticas, en términos generales el concepto **No repudio** se puede interpretar, en una definición relativamente accesible, como:

Una propiedad lograda por medios criptográficos que impide que un individuo o entidad niegue haber realizado una acción particular relacionada con ciertos datos (como mecanismos de no-rechazo o autoridad (origen); de prueba de obligación, intención o compromiso; o de prueba de pertenencia).

Es decir, el *no repudio* se centra en ofrecer una garantía de que «alguien» ha hecho «algo» con ciertos datos (por ejemplo, que los ha recibido o leído, o creado, o modificado), sin que ese «alguien» pueda negarlo.

2 Autenticación – AAA

Como todos intuimos, la **Autenticación** es una parte básica de la seguridad informática. Consiste en el **conjunto de medidas tomadas para garantizar que una persona que accede a un sistema es quien dice ser**.

Ampliando un poco el concepto, llegamos a la tríada AAA: Autenticación, Autorización, y Registro (en inglés *Authentication, Authorization, Accounting*, de ahí las tres aes).

Autenticación

Como hemos dicho, consiste en garantizar que una persona es quien dice ser. Yendo un poco más allá, se puede ampliar a sistemas (cuando se intenta establecer una conexión, asegurarse de que el sistema que la inicia y el que la recibe son los sistemas que se quiere conectar).

Autorización

Establece los **privilegios** de un usuario autenticado: una vez que hemos garantizado que la persona que se conecta es quien dice ser, los mecanismos de autorización determinan qué puede hacer dicha persona en nuestro sistema: a qué datos puede acceder, y con qué «poderes»: ¿puede leerlos? ¿Puede también modificarlos, añadir datos nuevos, eliminar datos existentes? ¿Puede incluso alterar la estructura de los datos, añadiendo campos nuevos en una base de datos, por ejemplo?

Registro

El registro es un sistema de recopilación de información con respecto a qué usuario(s) ha(n) accedido a qué datos, y qué ha(n) hecho con ellos. El nivel de detalle puede variar según los requerimientos de seguridad que tengamos: puede ser suficiente que el sistema anote que el usuario *X* accedió a la BD *Y* en tal fecha y hora, o puede ser necesario que se recoja también a qué tablas accedió, qué datos leyó, o qué datos creó, modificó o eliminó.

II Seguridad física y seguridad lógica

Una de las clasificaciones más habituales de tipos de seguridad es la que distingue entre seguridad física y seguridad lógica.

1 Seguridad física

La **seguridad física** de un sistema informático consiste en la aplicación de barreras físicas y procedimientos de control frente a **amenazas físicas al hardware**.

1.1 Acceso de personas no autorizadas

En seguridad informática hay un dicho según el cual «si alguien tiene acceso físico a tu sistema, ya no es tu sistema». Esto es así porque, cuando dispone de acceso físico a un ordenador, puede extraer la información que contiene, puede eliminarla, puede instalar herramientas de malware, etc. Es posible tomar medidas para reducir el riesgo o retrasar la labor de alguien que acceda con intenciones oscuras a nuestro sistema, pero su efectividad puede ser limitada. Por eso la seguridad física es clave: si impides el acceso físico al sistema, la única posibilidad de ataque es a través de las redes y del software, y ahí es más fácil proteger nuestro equipo.

A parte de los **ataques dirigidos** expresamente contra la información almacenada o transmitida, debemos considerar también amenazas como **robos o sabotajes**.

1.2 Protección frente a otras amenazas

La seguridad física también debe proteger nuestros sistemas frente a otras amenazas, tanto ocasionadas por el hombre como por la naturaleza del medio físico en que se encuentran ubicados los sistemas. Las principales amenazas que hay que tener en cuenta son:

- Desastres naturales, incendios accidentales, inundaciones... y cualquier variación producida por las condiciones ambientales (fundamentalmente exceso de calor y/o humedad);
- Cortes en el suministro eléctrico;
- Cortes en el acceso a red y/o Internet;
- Disturbios internos y externos (aunque causados por personas, no los consideramos aquí como específicamente dirigidos contra nuestros sistemas, aunque pueden afectarlos, como es lógico).

Evaluar y controlar permanentemente la seguridad física del sistema es la base para comenzar a integrar la seguridad como función primordial del mismo. Tener controlado el ambiente y acceso físico permite disminuir siniestros y tener los medios para luchar contra accidentes.

2 Seguridad lógica

La **seguridad lógica** de un sistema informático consiste en la aplicación de barreras y procedimientos que protejan el acceso a los datos y a la información contenida en dicho sistema.

El activo más importante de un sistema informático es la información, lo que convierte su protección en un objetivo vital. La seguridad lógica, por tanto, es un elemento clave de todo sistema informático.

La seguridad lógica trata de conseguir los siguientes objetivos:

- Restringir el acceso a los programas y archivos.
- Asegurar que los usuarios puedan trabajar sin supervisión y no puedan modificar los programas ni los archivos que no correspondan a su autorización.
- Garantizar que se estén utilizados los datos, archivos y programas correctos en y según el procedimiento correcto.
- Verificar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada (confidencialidad) y que la información recibida sea la misma que la transmitida (integridad).
- Disponer de métodos alternativos de emergencia para la transmisión de información.

III Vulnerabilidades

Definimos **vulnerabilidad** como una **debilidad de cualquier tipo que compromete la seguridad del sistema informático**.

Podemos clasificar las vulnerabilidades de los sistemas informáticos (SI) en función de diversos criterios:

- Vulnerabilidades de **diseño**
 - Debilidad en el diseño de protocolos utilizados en las redes.
 - Políticas de seguridad deficientes e inexistentes.
- Vulnerabilidades de **implementación**
 - Errores de programación.
 - Existencia de *puertas traseras* en los sistemas informáticos.
 - Descuido de los fabricantes.
- Vulnerabilidades en el **uso**
 - Configuración inadecuada de los sistemas informáticos.
 - Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
 - Disponibilidad de herramientas que facilitan los ataques.
 - Limitación gubernamental de tecnologías de seguridad.

1 Vulnerabilidad de día cero (*zero-day* o *0-day*)

Una vulnerabilidad de día cero (en inglés *zero-day* o *0-day*) es aquella que es desconocida por quien debería estar interesado/a en mitigarla (incluido/a quien haya creado el software vulnerable), pero de la que se sabe cómo explotarla. En tanto la vulnerabilidad no sea mitigada, puede ser explotada por hackers para afectar al software, los datos, o quizá para acceder a otros dispositivos conectados a la misma red. Un *exploit*¹ dirigido a obtener ventaja de una vulnerabilidad de este tipo, se llama, lógicamente, *exploit zero-day*, o ataque *zero-day*.

El término «día cero» se refería, originalmente, al número de días desde que un desarrollo de software se publicaba. El software «día cero» era el que se había obtenido hackeando los ordenadores de la persona o compañía creadora del software (PoCCS), antes de su publicación.

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

Más adelante se aplicó a las vulnerabilidades que permitían este tipo de ataque, y al número de días que la PoCCS había tenido para fijarlo, desde que lo conoce (por tanto, «día cero» se refiere a vulnerabilidades que la PoCCS aún no conoce; a partir del momento en que es consciente de la vulnerabilidad, comienzan a contar los días hasta la publicación de una solución para mitigar la vulnerabilidad).

2 Ingeniería social

El mayor riesgo de un sistema informático suele estar entre el teclado y la silla. Suele ser mucho más fácil engañar a una persona que a una máquina.

Ingeniería social

Conjunto de técnicas usadas por los (ciber)criminales para engañar a los usuarios incautos con el fin de manipular sus sistemas informáticos u obtener datos confidenciales.

Generalmente se aprovecha la falta de conocimiento de los usuarios; debido a la velocidad a la que avanza la tecnología, la mayoría de los usuarios de sistemas informáticos no son conscientes del valor real de los datos personales ni saben muy bien cómo proteger dicha información. Además, puesto que la Ingeniería social no se basa en atacar a la máquina, sino al ser humano, no requiere conocimientos técnicos; más bien se centra en el uso de habilidades tan humanas y omnipresentes como la empatía, el engaño, el uso de medias verdades, el abuso de la confianza del prójimo, etc.

La Oficina de Seguridad del Internauta tiene una página bastante completa dedicada a la Ingeniería social: www.osi.es/es/campanas/ingenieria-social

IV Amenazas

En el punto anterior hemos visto los diferentes tipos de vulnerabilidades de un sistema informático. Ahora vamos a relacionar el concepto de vulnerabilidad con el de amenaza.

Amenaza

Una amenaza es un elemento o acción que puede perjudicar la seguridad de la información. Su existencia depende de la presencia de vulnerabilidades de las que se puedan aprovechar.

Cuando en un sistema informático se detecta una vulnerabilidad y existe una amenaza asociada a dicha vulnerabilidad, puede ocurrir que la amenaza se haga realidad, poniendo en riesgo el sistema.

Evento

En este contexto, un evento es un suceso en el que una amenaza se pone en práctica, como un ataque.

Si dicho evento se produce y el riesgo que era probable ahora es real, el sistema informático sufrirá daños que habrá que valorar cualitativa y cuantitativamente:

Impacto

Daños sufridos por un sistema informático que ha sido víctima de un evento de seguridad.

Resumiéndolo en una frase, **un evento producido en el sistema informático por una amenaza asociada a una vulnerabilidad del sistema, produce un impacto sobre él.**

Si queremos eliminar las vulnerabilidades del sistema informático o queremos disminuir el impacto que puedan producir sobre él, hemos de proteger el sistema mediante una serie de medidas que podemos llamar defensas o salvaguardas. Toda la idea de Seguridad Informática gira en torno a estos conceptos.

V Seguridad activa y seguridad pasiva

El otro gran criterio para clasificar las medidas de seguridad consiste en el momento en que las medidas se activan ante un evento de seguridad.

Seguridad activa

La seguridad activa incluye todas las medidas de seguridad que tratan de impedir que un evento de seguridad tenga lugar. Su objetivo es eliminar las vulnerabilidades y/o limitar las amenazas.

Medidas de seguridad activa son, por ejemplo, el uso de cortafuegos, la limitación de acceso a los sistemas con medidas de acreditación, el uso de unidades de almacenamiento redundantes, la limitación de uso de dispositivos externos, etc.

Seguridad pasiva

La seguridad pasiva agrupa todas las medidas de seguridad que, **una vez producido un evento de seguridad** (es decir, cuando la seguridad activa ha fallado), permiten que el sistema se recupere con el menor impacto posible.

El ejemplo más obvio de medidas de seguridad pasiva es el uso de copias de seguridad (*back-up*). Si algún evento ha afectado a nuestros sistemas, bases de datos, etcétera, siempre podremos usar copias de seguridad recientes para restaurar el sistema a un estado correcto de funcionamiento reciente.

VI Seguridad física y ambiental

En este tema vamos a examinar algunos conceptos relativos a la seguridad física, ya que no se desarrollan tan en profundidad como la seguridad lógica en el resto del temario de este módulo.

Ya hemos visto que la seguridad física tiene como objetivo proteger el hardware de todo tipo de amenazas físicas.

Ante todo, la primera medida de seguridad física consiste en agrupar los equipos informáticos (particularmente los servidores) en un sitio donde se puedan aplicar todas las medidas de seguridad física fácilmente: el CPD.

1 Centro de Proceso de Datos

Un centro de proceso de datos (CPD, aunque es frecuente que se le den otros nombres, como *centro de cálculo*, *datacenter*, etc.) es un edificio o sala especialmente acondicionados para mantener protegidos y en estado óptimo de funcionamiento nuestros equipos. El tener nuestros equipos centralizados nos ofrece las siguientes ventajas:

Ahorrar en costes de protección y mantenimiento. La vigilancia, la refrigeración, etcétera, se aplican en un único sitio.

Optimizar las comunicaciones entre servidores. La cercanía entre sistemas permite usar cableado más corto y reducir la necesidad de equipos de red intermedios que pueden reducir la velocidad de transferencia.

Aprovechar mejor el personal del departamento de informática. No hace falta desplazarse a distintas plantas o edificios para realizar instalaciones, reparar hardware, etc.

Un CPD debe tener su propio plan de seguridad pasiva. Un **plan de recuperación de desastres** debe especificar, muy detalladamente (porque en caso de crisis no suele haber tiempo para pensar), qué hacer ante una caída de cualquiera de los servicios prestados por el CPD. Cualquier cambio efectuado en el CPD debería incluir la actualización de este plan, que debe incluir:

Hardware. Qué modelos de máquinas hay instalados (tanto servidores como equipos de red), qué modelos alternativos es posible utilizar y cómo se instalarían (conexiones, configuración).

Software. Qué sistema(s) operativo(s) y aplicaciones están instalados, con el número de versión actualizado y sus opciones de configuración correspondientes (permisos, usuarios, etc.)

Datos. Qué sistemas de almacenamiento se están usando (discos locales, NAS, SAN...), con qué configuración y cómo se hacen las copias de seguridad.

1.1 Localización del CPD

El CPD debe estar protegido al máximo, porque contiene uno de los principales recursos de cualquier organización: su información. Para ello:

- Se optará por instalarlo en un edificio en una zona con baja probabilidad de accidentes naturales (terremotos, huracanes, inundaciones).
- También se evitará la proximidad de elementos de riesgo como ríos, playas, presas, aeropuertos, autopistas, bases militares, centrales nucleares, etc.
- Hay que tener en cuenta que no haya edificios vecinos al nuestro pertenecientes a empresas dedicadas a actividades potencialmente peligrosas: gases inflamables, explosivos, etc.
- Preferentemente se seleccionarán las primeras plantas del edificio.
 - No la planta baja, que está expuesta a ataques desde el exterior (impacto de vehículos, asaltos, etcétera).
 - Tampoco las plantas subterráneas, que serían las mas afectadas en caso de inundación.
 - Las plantas más altas, por otra parte, están sometidas al riesgo de incendios en cualquier otra planta, y a accidentes aéreos.
- El acceso a la sala debe estar muy controlado y limitado al personal del CPD.
- En un CPD se suele usar falso suelo y falso techo, para facilita la instalación de cableado de alimentación y red y para mejorar la ventilación.
- Normalmente habrá equipos de detección de humos y sistemas automáticos de extinción de incendios que no usen agua, sino [halón](#).
- Habrá equipos de aire acondicionado, porque los CPD se suelen calentar mucho, debido al trabajo de los equipos instalados en él. Se suele buscar una temperatura de trabajo ideal de 22 °C, especialmente acomodada a los trabajadores que tengan que entrar en la sala.

1.2 Fuentes de alimentación redundantes

Uno de los puntos clave de un CPD es la alimentación eléctrica. Un fallo en el suministro eléctrico puede suponer la parada de todo el CPD, y daños en archivos, sistemas o bases de datos que estuviesen en uso en el momento del evento.

Por ello, los CPD generalmente cuentan con fuentes de alimentación redundante, que permitan sortear este tipo de problemas. Los principales son dos: los SAI y los grupos electrógenos.

1.2.1 Sistemas de alimentación ininterrumpida (SAI)

Un SAI (en inglés *UPS: Uninterruptible Power Supply*) es un dispositivo que cuenta con una batería o conjunto de baterías con el que se alimenta uno o varios sistemas.

En caso de fallo del suministro eléctrico, los equipos conectados al SAI siguen funcionando porque consiguen electricidad de la(s) batería(s). La capacidad de suministro depende del SAI y del consumo de los equipos, pero es habitual que garanticen un suministro de al menos diez minutos.

El factor más importante para elegir un SAI es la **potencia consumida** (en vatios) por los equipos que debe proteger, y **cuánto tiempo** necesitamos que los proteja.

Si es posible, conviene aplicar redundancia e instalar un doble juego de equipos SAI, para estar cubiertos en caso de que uno fallara. Esto es posible porque la mayoría de los servidores vienen con doble fuente de alimentación, lo que nos permite conectar una fuente a cada grupo de SAI.

En caso de fallo de suministro eléctrico, el SAI:

1. Espera unos minutos por si el corte ha sido puntual y vuelve el suministro en poco tiempo.
2. Si el suministro no vuelve, ejecuta una parada ordenada de los equipos conectados al SAI.

Un SAI tiene otra importante ventaja: suele llevar un **estabilizador de corriente** que quita los picos de tensión que nos llegan por el cableado, que también pueden ser muy perjudiciales.

Los SAI suelen incorporar algún sistema de **monitorización** de los mismos, que se aprovecha gracias a su conexión a algún ordenador. Esto nos permite ver el estado de las baterías, así como una lista de incidentes que el SAI guarda, en la que podemos ver cuándo ha habido problemas de suministro, y cuánto han durado (y si el sistema ha tenido que apagar equipos o no).

Los SAI avanzados nos permiten configurar **disparadores (triggers, en inglés)**, que responden a determinadas circunstancias con los comandos que deseemos: por ejemplo, que en caso de fallo eléctrico, se apaguen determinados equipos, o se suspendan, cuánto esperar antes de hacerlo, etc.

En cuanto al **mantenimiento**, es importante comprobar regularmente el estado de las baterías, que con el tiempo y el uso tienden a degradarse y funcionar cada vez peor... o no funcionar. En caso necesario, suelen ser sencillas de sustituir.

1.2.2 Grupos electrógenos

Un grupo electrógeno (GE) puede proporcionar alimentación eléctrica a todo un CPD (o sólo a los equipos que consideremos clave). No es más que un generador eléctrico movido por un

motor, generalmente de gas o diésel. Al igual que el SAI, entran en funcionamiento en caso de fallo del suministro eléctrico.

El GE puede mantener la alimentación durante mucho más tiempo que un SAI, y se puede mantener indefinidamente, mientras haya carburante disponible.

Normalmente, cuando el suministro eléctrico falla, el SAI se hace cargo del suministro a los equipos que lo necesiten. El GE puede tardar un tiempo en empezar a funcionar y alcanzar un régimen estable, y durante este tiempo es el SAI el que salva la situación. Una vez que el GE esté funcionando de forma estable, el SAI vuelve a actuar como si el suministro eléctrico se hubiese restaurado.

En el momento en que el suministro eléctrico se restaure, se puede detener el GE, sustituyendo su suministro por el de la línea, mientras el SAI mantiene de nuevo a los equipos funcionando. Pero es posible que se decida seguir trabajando con el GE, si el suministro externo no es estable y hay varios cortes seguidos en un periodo corto de tiempo.

VII Listas de control de acceso

Las listas de control de acceso son una de las formas básicas de **autorización**, y forman parte de la seguridad lógica activa. Una **lista de control de acceso** (en inglés **ACL**, *Access-control list*) es una lista de permisos aplicada a un objeto que especifica qué usuarios tienen permiso para acceder a dicho objeto, y las operaciones que pueden ejecutar sobre él.

Cada entrada de una ACL de un objeto dado especifica un sujeto y una operación asociada permitida para dicho sujeto sobre el objeto en cuestión.

Una ACL en un sistema informático es una estructura que almacena entradas referidas a usuarios o grupos de usuarios específicos, otorgándoles derechos concretos de acceso a objetos del sistema, como procesos, archivos o programas. Cada entrada de la lista es una **entidad de control de acceso**. Cada objeto del sistema está asociado con un atributo de seguridad que identifica la lista de control de acceso que se le aplica.

Cuando un usuario solicita acceso a un objeto en un modelo de seguridad basado en ACL, el sistema operativo comprueba la ACL para ver si hay alguna entrada que se le aplique a un usuario en concreto (o a algún grupo al que pertenezca). Normalmente se le aplicará al usuario los derechos de acceso más amplios posibles, si hay varias entradas que autoricen su acceso.

VIII Autenticación de usuarios

La autenticación de usuarios suele hacerse en base a uno de los factores siguientes:

- Algo que sabes (por ejemplo, una contraseña, un PIN, un patrón de puntos...)
- Algo que tienes (por ejemplo, una tarjeta de identidad con chip o banda magnética, un [token SecurID](#)...)
- Algo que eres (sistemas biométricos: una huella dactilar, un escáner de iris, reconocimiento facial...)

1 Contraseñas

El sistema más usado, más económico y sencillo es basado en contraseñas.

En todo sistema informático se suele establecer una política de contraseñas, que determina:

1. La longitud mínima de la contraseña
2. Los tipos de caracteres que tiene que incorporar obligatoriamente (caracteres alfabéticos en mayúscula/minúscula, numéricos, símbolos...)
3. Cada cuánto tiempo es obligatorio cambiarla
4. Cuántas contraseñas recordará el sistema, para prohibir reusar alguna de las X últimas contraseñas usadas por el usuario.

En definitiva es siempre importante encontrar un equilibrio entre una política segura, y la facilidad de uso. Una política de contraseñas que obligue a usar 20 caracteres, con varios caracteres alfanuméricos, mayúsculas minúsculas, cifras y símbolos, y que obligue a cambiarla cada tres meses... generará contraseñas muy seguras, y seguramente provocará que la mayoría de los usuarios la apunten en algún papel (el clásico *Post-It*) para tenerlas a mano.

Lo normal es que un técnico (superior) en informática tenga una idea muy razonable del grado de seguridad de una contraseña, pero podemos aconsejar a los usuarios de nuestros sistemas que comprueben la fortaleza de sus contraseñas en la página web howsecureismypassword.net

1.1 Gestión de contraseñas

Lo ideal es usar contraseñas complejas, abstractas, ilegibles y difíciles de teclear... y dejar que sean los dispositivos los que las recuerden. Hoy en día, todos los navegadores web (p. ej. *Firefox*, *Chromium*, *Brave*) permiten recordar las contraseñas por el usuario. Si sólo accedemos a navegadores en equipos seguros (o con cuentas seguras), es una opción muy práctica y segura. Los navegadores suelen permitir usar una única contraseña central para proteger todas las contraseñas que memoricen, lo cual aumenta aún más la seguridad de este sistema.

Otra forma de gestionar las contraseñas es usar un **gestor de contraseñas**: un programa que nos permite almacenar todas nuestras contraseñas en una base de datos cifrada; sería el equivalente seguro y responsable del temido *Post-It*. Entre otros ejemplos, se puede recomendar el uso de KeepassX, libre, gratuito y multiplataforma.

1.2 Ataques a contraseñas

¿Qué formas tiene un ciberdelincuente de obtener nuestra contraseña?

La más obvia, peligrosa, y que mejores resultados da, suele ser la **ingeniería social**: hacerse pasar por alguien a quien concedemos cierta autoridad, o alguien de quien nos fiamos, para averiguarla.

Aparte de la ingeniería social, hay dos formas básicas de obtener una contraseña:

- **Ataque de fuerza bruta.** Consiste en probar todas las contraseñas posibles: «a», «b», «c»... «z», «0», «1»... «9», «aa», «ab», «ac»... Dependiendo del sistema en la práctica no es efectivo, salvo que usemos contraseñas muy cortas. Por eso se suele recomendar una longitud mínima, y el uso de diversos tipos de caracteres (multiplican las combinaciones que habría que probar).
- **Ataque de diccionario.** En lugar de probar todas las contraseñas posibles, se prueban todas las contraseñas existentes en un archivo denominado *diccionario*. Generalmente incluirá la mayoría de las palabras de un idioma dado, y/o combinaciones de las que se sabe que se suelen usar mucho como contraseñas. También es fácil hacer esta prueba cambiando en dichas palabras las vocales por números según el [esquema l33t](#), o añadiendo una o dos cifras al final.

Estas son las razones por las que se establecen las políticas de contraseñas que hemos visto más arriba.

Existe una última forma de obtener nuestra contraseña: **atacar el sitio donde se almacena**, si tiene alguna vulnerabilidad que lo permita. Muchos sitios web, a lo largo de las últimas décadas, han sufrido ataques en los que ciberdelincuentes se han hecho hasta con **cientos de millones** de combinaciones *nombre de usuario/contraseña*. El problema se agrava enormemente por la tendencia de la gente a usar **la misma contraseña en varios sitios**, de forma que si atacando uno de ellos un ciberdelincuente obtiene nuestra contraseña, la puede usar en muchos otros sitios, y acceder a nuestras redes sociales, sitios de trabajo, etc. Por eso es siempre **muy importante usar una contraseña diferente en cada sitio**, y dejar que el gestor de contraseñas las recuerde por nosotros.

2 Biometría

La identificación con *algo que eres* es cada día más popular. La mayoría de los móviles modernos incorporan lectores de huellas dactilares, y algunos se aventuran incluso con reconocimiento facial.

Conviene ser muy cauto con estos sistemas, que dan una falsa sensación de seguridad a sus usuarios. Suele ser mucho más sencillo de lo que parece hacerse pasar por nosotros con estos sistemas:

- Los sistemas de reconocimiento facial han sido comprometidos con una simple foto del usuario.
- Los sistemas de huella dactilar se pueden comprometer con huellas dactilares del propietario, obtenidas de cualquier sitio (incluso del propio móvil, si la superficie es apta; y suele serlo). En Internet hay multitud de tutoriales para obtener una huella dactilar utilizable con estos sistemas.
- Los escáneres de iris han sido comprometidos con fotografías de muy alta resolución de los usuarios, sacadas a corta distancia.

3 Autenticación en dos pasos

Consiste en combinar dos tipos de autenticación. Por ejemplo, una contraseña y una huella dactilar. O un PIN y una tarjeta física.

En las páginas web modernas es cada vez más común combinar una contraseña (algo que sabes) con un SMS enviado al móvil del usuario (algo que tienes). Conviene utilizar este tipo de autenticación para todos los sitios cuya seguridad sea relevante (particularmente, sitios de comercio electrónico, viajes, banca electrónica... cualquier sitio donde se almacene información sobre nuestros medios de pago).

IX Seguridad en el almacenamiento

Para cualquier organización, la parte más importante de la informática son los datos. El hardware, el personal, los sistemas y aplicaciones... Todo se puede remplazar fácilmente, excepto los datos, que no se pueden adquirir ni contratar fuera de la organización: si se pierden, no hay de dónde recuperarlos.

Para reforzar la integridad y disponibilidad de los datos, se pueden aplicar varias estrategias.

1 Almacenamiento redundante

Los mecanismos más comunes en la actualidad para proporcionar redundancia en el almacenamiento son los esquemas RAID.

RAID define varios niveles, pero los más usados son:

- RAID 0: no ofrece redundancia. Sólo agrupar varios discos en una unidad, repartiendo los datos entre ellos, aumentando la capacidad y el rendimiento.
- RAID 1: discos en espejo. Se usan dos discos, manteniendo copias idénticas de los datos en ambos. El 50% de la capacidad total se pierde en redundancia.
- RAID 5: Discos agrupados en bandas con paridad. Se pueden agrupar 3 o más discos iguales, y el espacio equivalente a uno de ellos se pierde en redundancia (por ejemplo, con 4 discos se pierde el 25% del espacio total; con 10 discos, se pierde el 10%).
- RAID 6: Similar al RAID 5, pero con doble paridad. Se pierde el equivalente a dos discos en redundancia, pero se aumenta la seguridad.
- RAID 10 (o RAID 1+0): Consiste en crear dos (o más) espejos RAID 1, y luego asociarlos en un RAID 0 de nivel superior. Ofrece la misma seguridad y redundancia que RAID 1, pero aumenta el rendimiento por el uso de RAID 0.

Puedes leer más información sobre los niveles RAID 5 y 6 en [este enlace](#).

2 Almacenamiento en red: NAS y SAN

Una opción muy interesante es el almacenamiento en red. Esto nos permite trabajar con espacio de almacenamiento instalado en el CPD, donde están especialmente protegidos, y donde podemos usar técnicas de redundancia y balanceo de carga para hacer el servicio más eficiente.

Las dos formas básicas son **NAS** y **SAN**, y las veremos en detalle en el tema dedicado a la alta disponibilidad.

3 Copias de seguridad e imágenes de respaldo

Una **copia de seguridad** o (en inglés, aunque el término también se usa habitualmente en castellano) **back-up** es una copia de los datos contenidos en un dispositivo de almacenamiento, efectuada con el objetivo de recuperarlos si el dispositivo de almacenamiento sufre alguna pérdida de datos.

Aunque el término se suele considerar asociado al almacenamiento masivo en ordenadores (discos duros), también tiene sentido en relación con otros dispositivos como una tarjeta SIM, con el almacenamiento de bases de datos (que puede estar distribuido en varios discos duros, por ejemplo), etc.

En caso de necesidad, los datos contenidos en la copia de seguridad se pueden **restaurar** sobre el dispositivo que contenía los datos originalmente, o sobre uno que lo sustituya.

Dependiendo del tipo de incidente del que se quiera proteger los datos, los métodos de copia de seguridad pueden variar:

- El riesgo de que un usuario borre o dañe un archivo inintencionadamente se puede mitigar simplemente manteniendo una copia de los archivos importantes en otro directorio del mismo disco duro.
- Una avería del disco duro se puede mitigar manteniendo una copia de seguridad en otro disco de la misma máquina, o en otra máquina.
- Ante el riesgo de robo de un ordenador o de un dispositivo de almacenamiento, será necesario hacer una copia de seguridad en un medio externo.
- Para el caso de riesgo de grandes calamidades, como incendios, inundaciones, etcétera, habrá que hacer copias de seguridad en una localidad remota.

A la hora de definir una estrategia de copias de seguridad, debemos considerar los riesgos que enfrentamos. Además es necesario considerar que, **frecuentemente, los daños sufridos por archivos de datos no son advertidos inmediatamente**, por lo que **es probable que las copias de seguridad más recientes incluyan ya los datos dañados**, y será necesario acudir a copias más antiguas para recuperar (lo que se pueda de) los datos. Por ello es clave conservar varios *back-ups* realizados a lo largo del tiempo, para poder acudir a versiones anteriores de archivos que queramos recuperar.

3.1 Métodos de copia de seguridad

Hay diversas maneras de abordar la realización de copias de seguridad. En primer lugar, podemos clasificarlos en dos métodos básicos:

1. Copia de seguridad del dispositivo completo, a menudo llamadas **imágenes**, en referencia a que la copia sería una imagen perfecta del estado del dispositivo en el momento en que se hace;

2. Copias de seguridad a nivel de archivos.

Las imágenes de dispositivos del primer método se suelen usar en caso de fallos catastróficos de los medios de almacenamiento: un disco duro averiado, por ejemplo, se sustituye por uno igual, y se **vuelca** en él la imagen almacenada. Es usado fundamentalmente en unidades cuyo contenido no cambia habitualmente (de lo contrario sería necesario crear una imagen ante cada modificación, lo que no sería práctico).

En las copias de seguridad a nivel de archivos, el objetivo es restaurar un archivo o grupo de archivos cuando estos han sido dañados o borrados, y se desea recuperarlos. En ocasiones también puede ser necesario examinar versiones anteriores de un archivo, para comprobar su estado en un momento dado del tiempo, y comprobar los cambios que se han efectuado en él, si estos han tenido consecuencias no deseadas. Por ejemplo, si una aplicación comienza a dar fallos inexplicables a partir de una fecha dada, se suele examinar los archivos que forman la aplicación (o sus archivos de configuración) de fechas anteriores, para ver cómo han cambiado, e intentar averiguar la razón de los problemas.

Las copias de seguridad a nivel de archivos se pueden realizar según los siguientes esquemas:

3.1.1 *Copia completa (full back-up)*

Dado un conjunto de datos, **una copia completa crea una copia de los datos completos en un momento dado** (como da a entender su nombre). Una copia completa puede ser trabajosa de hacer, porque la cantidad de datos que se copia puede ser enorme, por lo que sólo se realizan cada cierto tiempo (por ejemplo, cada semana, cada dos semanas, o cada mes). Es habitual conservar varias copias, eliminando sólo las más antiguas.

3.1.2 *Back-up diferencial*

Hemos visto que las copias completas se realizan sólo cada cierto tiempo. Sin otra solución, eso supondría que, en caso de fallo, sólo podemos recuperar los datos del último *back-up*, que quizá se haya hecho hace varios días, o incluso semanas.

Para prevenir esto, se realizan los *back-ups* diferenciales. **Un *back-up* diferencial es una copia de todos los datos que se han modificado desde la última copia completa.** Para recuperar un archivo o conjunto de archivos, sería necesario recuperar primero los de la copia completa, y luego los de la copia diferencial.

Los *back-ups* diferenciales se efectúan, como es lógico, con cierta regularidad entre un *back-up* completo y el siguiente.

3.1.3 *Back-up incremental*

Otra solución para abordar el problema del espaciado entre *back-ups* completos es el *back-up* incremental. **Un *back-up* incremental es una copia de todos los datos que se han modificado desde la última copia, sea del tipo que sea.** Por tanto, un *back-up* incremental no almacena datos repetidos. Para recuperar un archivo o conjunto de archivos, sería necesario recuperar

primero los de la copia completa, y luego los de la última copia diferencial (si la hay), y luego los de todas las copias incrementales posteriores, una por una.

3.1.4 Back-up incremental inverso

Un *back-up* incremental inverso almacena una copia completa reciente de los datos completos, y una serie de diferencias entre la copia completa actual y las copias anteriores. La primera copia que se efectúa con este esquema es una copia completa. Una vez hecha esta copia, el sistema sincroniza periódicamente la copia completa con los datos actuales, manteniendo suficiente información con respecto a las modificaciones como para reconstruir versiones anteriores. Esto se puede hacer con *diffs*² binarios o con enlaces duros, como hace **Back-in-time**.

3.2 Medios de almacenamiento

A la hora de realizar copias de seguridad, un elemento clave es el **medio** en el que se hacen dichas copias. Hasta hace unos años, lo más común era usar cintas magnéticas: eran muy económicas con relación a su capacidad, y fáciles de almacenar. Las soluciones más potentes incluían verdaderos armarios robotizados que eran capaces de gestionar multitud de cintas, cargar la cinta que se requiriese en cada momento en la unidad lectora y, en definitiva, automatizar todo el proceso. Sin embargo, lo más común es que la gestión de las cintas fuese manual, lo que era bastante molesto y poco fiable.

Hoy en día, con los precios descendentes de los medios de almacenamiento, se suelen usar **disco duros**, **discos ópticos** (aunque su capacidad se ha ido quedando corta en los últimos años), **discos de estado sólido**, etc.

Otra opción es el **back-up «en la nube»**: los servicios de copia de seguridad remota o *en la nube* se usan para protegerse ante la eventualidad de catástrofes como incendios, inundaciones, terremotos o similares, que podrían destruir las copias de seguridad almacenadas localmente. El *back-up en la nube*, como el ofrecido por *iDrive*, *Backblaze* y similares, ofrece una capa adicional de protección de datos. La contrapartida es que nos vemos obligados a confiar en un proveedor externo para mantener la confidencialidad e integridad de los datos. Por otra parte, es fundamental tener en cuenta la **localización** de los servidores (la *nube* no es una «nube», es un servidor o grupo de servidores físicos, que están en algún sitio). Si los datos que manejamos son delicados, o están sometidos a una protección especial por la legislación de nuestro país o región, **es posible que estemos cometiendo algún tipo de falta o delito** si los almacenamos en un servicio que no ofrezca garantías aceptadas por nuestro país o región. Además, los servicios en nube dependen de nuestra conexión a Internet, cuya velocidad puede limitar las posibilidades de usarlo.

2 Un *diff* es un archivo en el que se recogen las diferencias entre dos archivos dados. Normalmente en el *diff* se indican qué filas o partes de uno de los archivos faltan o sobran con respecto al otro.

3.3 Otras consideraciones sobre las copias de seguridad

Una solución de copias de seguridad suele requerir algún sistema efectivo de **gestión de las copias**. Generalmente estaremos hablando de alguna aplicación que nos permita ver y acceder eficientemente a las copias hechas, los tipos, las fechas, las incidencias (por ejemplo, si algunos archivos no se han podido copiar por estar bloqueados), etc.

X Auditorías de seguridad

Una **auditoría³ de seguridad de la información** es un examen independiente de la capacidad y nivel de seguridad de la información en una organización.

Los pasos para desarrollar una auditoría de seguridad informática son los siguientes:

1. Enumeración de los servicios que se vayan a auditar.
2. Verificación del cumplimiento de estándares de calidad y normas de control.
3. Identificación del software, hardware y sistemas operativos instalados.
4. Análisis de los servicios y aplicaciones instalados.
5. Comprobación y evaluación de las vulnerabilidades detectadas.

Como consecuencia de la auditoría, y teniendo en cuenta las vulnerabilidades encontradas en ella, se desarrollan los siguientes pasos:

1. Corrección con medidas específicas.
2. Implantación de medidas preventivas.

1 Objetivos de una auditoría de seguridad informática

Las auditorías de ciberseguridad permiten detectar debilidades y vulnerabilidades de seguridad que podrían ser explotadas por usuarios malintencionados o atacantes, ocasionando perjuicios importantes para la organización. Además, sirven para evitar el robo de información y la competencia desleal.

Las auditorías de seguridad son básicas para todas las empresas —independientemente de su tamaño—, ya que permiten detectar posibles puntos débiles que sirvan de referencia para implementar un plan de mejora.

2 Tipos de auditorías de seguridad informática

En función de quién las realice, podemos dividir las en dos clases:

1. **Internas:** son realizadas por personal propio de la organización con o sin apoyo de personal externo.
2. **Externas:** son realizadas por personal externo e independiente a la organización.

3 Originalmente, las auditorías eran un examen realizado por una entidad externa sobre la información financiera de una entidad dada. El concepto se ha ido ampliando a medida que nuevos ámbitos requerían este tipo de exámenes externos.

En función de la metodología seguida en la auditoría, podemos distinguir:

1. **De cumplimiento:** auditorías que verifican el cumplimiento de un determinado estándar de seguridad (p. ej. ISO27001) o de las propias políticas y procedimientos internos de seguridad de la organización.
2. **Técnicas:** auditorías o revisiones de seguridad técnica cuyo alcance está acotado a un sistema o sistemas informáticos objeto de la revisión.

En función de su objetivo:

1. **Forense:** una vez que se produce un incidente de seguridad informática, este tipo de auditorías pretende recopilar toda la información relacionada para determinar las causas que lo han producido, el alcance del mismo (sistemas y/o información afectada), así como las evidencias digitales del mismo.
2. **Aplicaciones Web:** tratan de identificar potenciales vulnerabilidades en este tipo de aplicaciones que podrían ser explotadas por atacantes. Dentro de este tipo de auditorías se diferencian: el análisis dinámico de la aplicación (*DAST – Dynamic Application Security Testing*, que consiste en una revisión en tiempo de ejecución de la aplicación sobre la propia web) y el análisis estático de la aplicación (*SAST – Static Application Security Testing*, donde se buscan posibles vulnerabilidades en el código).
3. **Hacking ético o test de intrusión:** se trata de una auditoría en la que se ponen a prueba las medidas de seguridad técnicas de una organización (por ejemplo: cortafuegos, sistemas IDS/IPS, etc.) de la misma manera que lo haría un potencial atacante para identificar debilidades o vulnerabilidades explotables que deben ser corregidas.
4. **Control de acceso físico:** se auditan las plataformas y medidas de seguridad que componen el sistema de seguridad perimetral físico de una organización (cámaras, mecanismos de apertura de puertas, software de control de acceso...) para verificar su correcto funcionamiento.
5. **Red:** se revisan todos los dispositivos conectados a la red y se verifica la seguridad de los mismos (actualización de su *firmware*, firmas de antivirus, reglas de cortafuegos, control de acceso a la red, segmentación de la red en VLANs, seguridad de las redes *wifi*, etc.)

Toda auditoría de seguridad debe finalizar con la elaboración de un informe detallado que debería recoger los siguientes aspectos: alcance de la auditoría, metodología seguida, resultados de la evaluación de los objetivos de control, hallazgos detectados, riesgos asociados a los hallazgos y recomendaciones para su subsanación mediante la definición e implementación de un plan de acción correctivo.

2.1 Análisis forense en sistemas informáticos

Ya hemos visto que el análisis forense es uno de los tipos de auditorías de seguridad informática. La necesidad del análisis forense informático surge a partir del incremento de los diferentes incidentes de seguridad. En el análisis forense se realiza un análisis posterior de los incidentes de seguridad, con el objetivo de reconstruir la forma en que se han desarrollado. Las preguntas que el análisis forense pretende responder son las siguientes:

- ¿Quién ha realizado el ataque?
- ¿Cómo se ha realizado?
- ¿Qué vulnerabilidades se han explotado?
- ¿Qué hizo el intruso una vez que accedió al sistema?
- ¿Qué datos han sido comprometidos, y cómo?

El análisis forense consta de 3 fases claramente diferenciadas:

1. Recogida de datos
2. Análisis e investigación
3. Redacción de un informe

2.1.1 Contexto

El **Informe Anual de Seguridad Nacional 2019**, publicado por el **Departamento de Seguridad Nacional**,⁴ incluye un apartado relacionado con la ciberseguridad. En él se refleja que el CCN⁵ gestionó 42 997 incidentes de ciberseguridad, de los cuales el 7,46% fueron de **peligrosidad alta o muy alta**. Asimismo, el CERT⁶ de INCIBE⁷ se ocupó de 107 397 incidentes, de los cuales 72 858 correspondieron a ciudadanos y empresas y 33 743 a la red académica. Además, realizaron más de 83 000 notificaciones a proveedores de servicios y operadores de red. Finalmente, la Secretaría de Estado para el Avance Digital atendió más de 8000 consultas re-

4 El **Departamento de Seguridad Nacional (DSN)** es el órgano de asesoramiento al Presidente del Gobierno en materia de Seguridad Nacional. Depende del Gabinete de la Presidencia del Gobierno. Mantiene el Centro de Situación del Departamento de Seguridad Nacional para el ejercicio de las funciones de seguimiento y gestión de crisis, es responsable de impulsar el desarrollo e integración del Sistema de Seguridad Nacional y gestiona y asegura las comunicaciones especiales de la Presidencia del Gobierno.

5 El **Centro Criptológico Nacional (CCN)** es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

6 Un **Equipo de Respuesta ante Emergencias Informáticas (CERT)**, del inglés **Computer Emergency Response Team**) es un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

7 El **Instituto Nacional de Ciberseguridad de España (INCIBE)**, que depende del Ministerio de Asuntos Económicos y Transformación Digital, es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

lacionadas con la ciberseguridad. Cabe destacar que los ciberataques más recurrentes en 2019 fueron las intrusiones, que representaron el 38% del total de los incidentes registrados.

2.1.2 Recogida y análisis de evidencias

La **recogida o adquisición de datos es la actividad más crítica del análisis forense**. Esto es así porque, si se realiza mal, todo el análisis e investigación posterior perderían su validez, debido a que la información analizada no es la información pura del origen que deseamos analizar, sino que puede contener impurezas generadas por un proceso de recogida defectuoso.

Una vez que se ha detectado un incidente de seguridad, uno de los primeros problemas del analista en la recogida de datos se centra en decidir si **hay que apagar el equipo afectado o no**. Apagar o no el equipo afectado puede tener consecuencias variadas y severas: perder evidencias que estén en la memoria volátil, ver los usuarios conectados, ver los procesos en ejecución, conocer las conexiones existentes, etc. No hay una regla general, y **el analista deberá tomar la decisión** en función de múltiples factores, como los riesgos sospechados en caso de dejarlo encendido, la información que considere vital obtener, etc.

El siguiente paso es **localizar los dispositivos de almacenamiento** que están siendo utilizados por el sistema: discos duros, memorias (USB, RAM, etcétera). Una vez localizados, se detallará información como marca, modelo, número de serie, tipo de conexión (IDE, SCSI, USB, etc.), conexión al sistema (interfaz, orden de conexión, configuración como primario o secundario si es un dispositivo IDE, etcétera). A continuación se efectúa una **clonación bit a bit** de los dispositivos de almacenamiento del sistema. Debe ser realizada en un dispositivo cuyo contenido haya sido borrado por completo, para garantizar que no queden impurezas de otro análisis anterior. Generalmente, para evitar contaminaciones de datos, la clonación se efectúa mediante un LIVECD.

Una vez realizada la clonación, es recomendable realizar una **verificación de la copia**, para asegurarse de que el dispositivo de almacenamiento de origen y destino son idénticos, garantizándonos la integridad de los datos. Para ello se utilizan funciones HASH (como SHA1 o MD5).

A partir de este momento, el análisis se realiza sobre la copia, o sobre copias posteriores creadas a partir de esta primera. De esta manera no se corre el riesgo de dañar los datos analizados.

En todo momento, durante la recogida de evidencias y durante el análisis, hay que tener en cuenta la legislación vigente, puesto que los datos analizados pueden contener información personal.

2.1.3 Análisis e investigación

La fase de análisis e investigación de las evidencias informáticas exige un conocimiento profundo de los sistemas estudiados. Las fuentes de adquisición de información en esta fase son varias:

- Registros de los sistemas analizados;
- registro de los detectores de intrusión;
- registro de los cortafuegos;
- ficheros del sistema analizado.

En el caso de los ficheros del sistema analizado, hay que ser precavidos con las carpetas personales de los usuarios. Eso sí, hay que tener en cuenta que no se consideran personales los directorios creados por defecto durante la instalación del sistema operativo, como la cuenta de administrador o *root*. En todo caso conviene asesorarse con un jurista ante la realización de un análisis forense para prevenir posibles situaciones desagradables (como que seamos nosotros los denunciados por incumplir la legislación).

Cuando se accede a la información podemos encontrar **dos tipos de análisis**:

- **Físico**: información que no es interpretada por el sistema operativo ni por el de ficheros. La información en bruto, por decirlo así.
- **Lógico**: información que sí que es interpretada por el sistema operativo. En este nivel, por tanto, obtendremos la estructura de directorios, los ficheros existentes así como los que han sido eliminados (si sólo se han marcado como eliminados, pero no sobrescrito), horas y fechas de creación y modificación de los ficheros, tamaños, contenido en los sectores libres, etc.

Por otra parte, al analizar el contenido lógico de un disco, podemos encontrarnos datos de tres formas posibles:

- *Allocated*: inodo y nombre del fichero intactos, con lo que dispondremos del contenido íntegro.
- *Deleted/Reallocated*: inodo y nombre del fichero intactos (aunque recuperados, porque habían sido borrados), con lo que dispondremos del contenido íntegro.
- *Unallocated*: inodo y nombre de fichero no disponibles, con lo que no tendremos el contenido íntegro del archivo aunque sí algunos fragmentos. A veces, realizando una labor ímproba, se puede obtener parte de la información e incluso unir las partes y obtener casi toda la información del archivo (o al menos partes significativas).

Un paso importante es cerciorarnos de la hora que estaba usando el sistema original, para saber si las fechas de acceso marcadas en el dispositivo de almacenamiento son fiables, o si de-

ben ser corregidas. Una vez hecho esto, se puede establecer una línea de tiempo con las operaciones realizadas sobre el dispositivo.

Para facilitar el análisis, existen diversas **herramientas especializadas de análisis forense**. Estas son algunas:

- **EnCase**, una aplicación propietaria para la realización de análisis forense;
- **Autopsy** es un programa de entorno gráfico sencillo de usar, que permite analizar eficientemente discos duros y teléfonos móviles. Incorpora una arquitectura basada en *plug-ins*, lo que permite encontrar y añadirle módulos adicionales para obtener nuevas funciones, o desarrollar módulos propios en Java o Python.
- **The Sleuth Kit (TSK)**, una colección de herramientas de línea de comandos y una librería de C que permite analizar imágenes de discos y recuperar archivos de ellas. El programa anterior (Autopsy) y muchas otras herramientas libres y comerciales de análisis forense usan TSK para realizar sus funciones.

2.1.4 Redacción del informe

El último paso de un análisis forense, la redacción del informe, es una tarea ardua y compleja, porque debe combinar dos características:

- Debe recoger todas las evidencias, indicios y pruebas recabados, junto con el resultado del análisis realizado;
- Debe explicar su contenido de una manera clara y sencilla, teniendo en cuenta que muchas veces va a ser leído por personas sin conocimientos técnicos.

Por ello, el informe debe ser completamente riguroso pero absolutamente comprensible, por lo que cada punto deberá ser explicado minuciosamente.

XI Centros de información y respuesta

Los centros de información y respuesta son organizaciones especializadas en proveer información y ayuda ante amenazas informáticas.

1 Qué es un CSIRT

En 1988, el [gusano Morris](#), creado por un estudiante de 23 años de Harvard, afectó a casi 1 de cada 10 sistemas conectados a ARPANET —red antecesora de la actual Internet que contaba, por entonces, con unos 60 000 equipos conectados—. El gusano usaba un defecto de la versión Berkeley de Unix para reproducirse hasta bloquear el ordenador. Las estimaciones de los daños causados por *Morris* van de los 15 a los 96 millones de dólares. Este incidente puso de manifiesto la necesidad de coordinar el trabajo de administradores de sistemas y de gestores TIC de una manera ágil y eficiente, a partir de estructuras organizativas que no tuvieran sólo en cuenta los propios sistemas conectados a Internet.

A raíz de este caso, la DARPA⁸ consideró necesario un enfoque más organizado y estructurado para este tipo de situaciones, y patrocinó la creación del primer Equipo de Respuesta ante Incidentes, el **CERT/CC** (*Computer Emergency Response Team – Coordination Center*), ubicado en la Universidad Carnegie Mellon, en Pittsburgh (Pensilvania, Estados Unidos).

Un **CERT™** o **CSIRT**⁹ es un **centro de respuesta a incidentes de seguridad** en tecnologías de la información. Está constituido por un grupo de expertos responsable del desarrollo de medidas de prevención y reactivas ante incidentes de seguridad en sistemas de información. Un CSIRT vigila el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas.

Un CSIRT tiene definido un ámbito de actuación¹⁰, una comunidad a la que sirve (por ejemplo, una empresa, una comunidad autónoma, un país, etcétera). Su función es recibir, analizar y responder a informes de incidentes recibidos desde miembros de dicha comunidad, desde otros CSIRT, o terceras personas, coordinando la respuesta entre las partes.

En caso de incidente de seguridad informática, podemos acudir siempre a algún CSIRT en cuyo ámbito nos encontremos.

8 DARPA: [Defense Advanced Research Projects Agency](#), la agencia de desarrollo de proyectos de investigación del [Pentágono](#) que creó [ARPANET](#) y, a la larga, Internet.

9 **CSIRT** (*Computer Security Incident Response Team*, o sea, **Equipo de Respuesta ante Incidentes de Seguridad Informática**) es un **sinónimo de CERT**. El nombre «CERT» es una marca registrada de la Universidad Carnegie-Mellon, que permite el uso bajo licencia a diferentes organizaciones que ejercen funciones de CERT/CSIRT. De todos modos, en todos los sentidos CERT y CSIRT son sinónimos.

10 El término inglés específico para el **ámbito de actuación** de un CSIRT es **constituency**. Lo encontrarás a menudo en todo tipo de documentación relativa a cualquier CSIRT.

2 CSIRT de nuestro ámbito

2.1 Comunidad Valenciana

La Comunidad Valenciana cuenta con su propio CSIRT: [CSIRT-CV](#). Depende de la *Generalitat* Valenciana, y ofrece su servicio a ciudadanos y empresas de la comunidad autónoma.

2.2 España

A nivel nacional, en España contamos con varios CSIRT públicos:

- [CCN-CERT](#), el CERT del [Centro Criptológico Nacional](#), dependiente del [CNI](#)
- [INCIBE-CERT](#), el CERT del [Instituto Nacional de Ciberseguridad](#)
- [IRIS-CERT](#), el CERT de [RedIRIS](#)

Además de estos, otras comunidades autónomas, muchas grandes compañías, los diversos cuerpos y fuerzas de seguridad del Estado, así como el Ejército, disponen de sus propios CSIRT. Puedes encontrar una lista completa de los CSIRT de España en [CSIRT.es](#).

2.3 Unión Europea

La Unión Europea también cuenta con varios CERT:

- [CERT-EU](#), el CERT de la Unión Europea cuyo ámbito son las instituciones, agencias y cuerpos de la Unión
- [GSC-NDC-OC](#), el CERT del Consejo de la Unión Europea, cuyo ámbito son los países miembros e instituciones de la UE

La UE cuenta con dos CSIRT más, encargados únicamente de la protección de la [Comisión Europea](#) y del [Banco Central Europeo](#).

2.4 Otros

Además de estos, existen múltiples CSIRT más, tanto a nivel europeo como internacional.

la red [Géant](#), la red digital paneuropea para la comunidad científica y educativa, tiene un grupo de trabajo llamado TF-CSIRT que coordina CSIRT de todas las comunidades investigadoras y educativas de Europa (aunque también de sectores de fuerzas armadas y cuerpos policiales). Este cuerpo realiza un registro de CSIRT de toda Europa, manteniéndolos conectados a través del programa [Trusted Introducer](#).

3 Organismos de ciberseguridad

3.1 INCIBE

Aunque probablemente ya lo conozcas (lo hemos citado en las páginas anteriores), en España contamos con el **Instituto Nacional de Ciberseguridad (INCIBE)**, una institución pública centrada en la seguridad informática.

Su web ofrece una cantidad enorme de información, cursos, eventos, etc. Algunas de sus iniciativas más conocidas son:

- [CyberCamp](#), un evento anual de ciberseguridad, con charlas, debates, competiciones, etc. Dentro de [CyberCamp](#) destaca la competición de ciberseguridad CyberOlympics, para centros educativos de toda España, en la que tan buenos resultados suele obtener el IES Poeta Paco Mollá.
- [OSI](#): Oficina de Seguridad del Internauta, una página de información con un teléfono de ayuda (017), campañas de concienciación y múltiples recursos para ciudadanos preocupados por su seguridad informática.
- [Internet Segura for Kids](#), similar a la anterior, pero orientada al público infantil, con información sobre el uso de redes sociales, el ciberacoso, etc.

3.2 ENISA

A nivel europeo, contamos con [ENISA](#), la **Agencia de la UE para la Ciberseguridad**. Su objetivo es asistir a la Comisión Europea, los estados miembros y, por tanto, a las empresas de la UE para que estos satisfagan sus necesidades a nivel de red y seguridad de la información que manejan, incluyendo la legislación actual y futura de la UE.

XII Bibliografía

AULA MENTOR. [*Curso de seguridad Informática*](#). Ministerio de Educación y Formación Profesional.

UNIR (2020) [*Auditorías de seguridad informática: en qué consisten y qué tipos hay*](#). UNIR Revista.

RIFÀ POUS, H.; SERRA RUIZ, J.; RIVAS LÓPEZ, J. L. (2009) [*Análisis forense de sistemas informáticos. 1.ª ed.*](#). Fundació per a la Universitat Oberta de Catalunya.

JONES, N. (2015) [*Can You Create a Secure Password?*](#) GrownUpTech.