TEMA 1. Principios de seguridad y alta disponibilidad

Se supone que en las sociedades modernas, la mayor parte de los empleos ya no estarán asociados a las fábricas de productos tangibles, sino a la generación, almacenamiento y procesamiento de todo tipo de información y esa información debe estar segura y disponible.

1. Introducción

Con la proliferación de la informática en todos los ámbitos de la vida, el número de usuarios y profesionales de informática ha crecido exponencialmente en los últimos años, del mismo modo que las necesidades de comunicación y compartición de recursos en red.

Las dos nuevas problemáticas que subyacen de esta nueva realidad son, por un lado asegurar los sistemas y la información que disponemos, y por otro poder tener acceso a los servicios el mayor tiempo posible, sin interrupciones y con un cierto nivel de calidad, siendo la base para el estudio de la **seguridad informática** y la **alta disponibilidad** respectivamente.

2. Seguridad informática

Las tecnologías de la información y la comunicación (TIC), y concretamente la informática, se ha instalado en todos los ámbitos de la sociedad: sanidad, educación, finanzas, prensa, etc., siendo cada vez más útil e imprescindible para el desarrollo de sus actividades cotidianas. Del mismo modo que se extiende el uso de la informática, la seguridad informática debe tener una importancia cada vez mayor, teniendo en cuenta que el funcionamiento correcto de sus sistemas depende en gran medida, de protegerlos como el mayor de sus tesoros.

La seguridad informática consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Los principales objetivos de la seguridad informática por tanto son:

- **Detectar** los posibles **problemas y amenazas a la seguridad**, minimizando y gestionando los riesgos.
- Garantizar la **adecuada utilización de los recursos** y de las aplicaciones de los sistemas.
- **Limitar las pérdidas** y conseguir la adecuada **recuperación del sistema** en caso de un incidente de seguridad.
- Cumplir con el **marco legal** y con los requisitos impuestos a nivel organizativo.

Durante el desarrollo del curso, veremos que el conjunto de vulnerabilidades, amenazas, ataques y medidas de seguridad han ido aumentando y modificándose con el tiempo, siendo **necesario estar al día en esta materia**. Para ello haremos uso de diversas noticias de actualidad y reflexiones sobre las mismas.

La comunidad de usuarios y profesionales en materia de seguridad informática mantienen al día al resto de usuarios mediante noticias y post en blogs y webs especializadas. Como ejemplo podemos

consultar el blog y repositorio de blogs de seguridad informática disponible en la web del Instituto Nacional de Tecnologías de la comunicación S.A. (INTECO), sociedad anónima estatal adscrita a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información:

Ver web

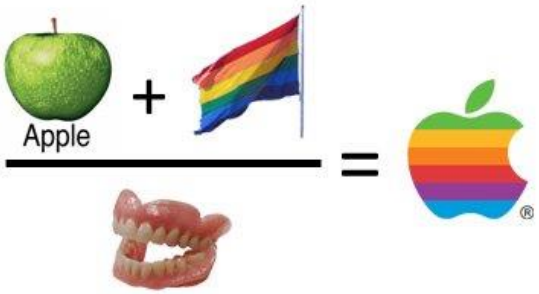
La seguridad informática lleva asociada un conjunto de palabras, en muchos casos nuevos términos en inglés. A lo largo del curso y en los artículos de actualidad se irán repitiendo, por lo que es recomendable ir construyendo nuestro glosario de términos con palabras como pharming, tabnabbing, malware, sniffing, spoofing, phishing, scam, spam, botnet, spyware, keylogger, etc.

Vamos a intentar entender gran parte de ellas a través de la lectura de un artículo que tienes en la web indicada en el aula virtual (origen y evolución del fraude)

- En el artículo anterior, identifica las palabras que no conozcas y busca su significado
- ¿Has recibido alguna vez un intento de phishing mediante correo electrónico de tipo spam? ¿Podrías indicar algún ejemplo?

3. Fiabilidad, confidencialidad, integridad y disponibilidad

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independientemente de las medidas que tomemos, por lo que debemos hablar de **niveles de seguridad**. La seguridad absoluta no es posible y en adelante entenderemos que la **seguridad** informática es un conjunto de técnicas encaminadas a obtener **altos niveles de seguridad en los sistemas informáticos**.



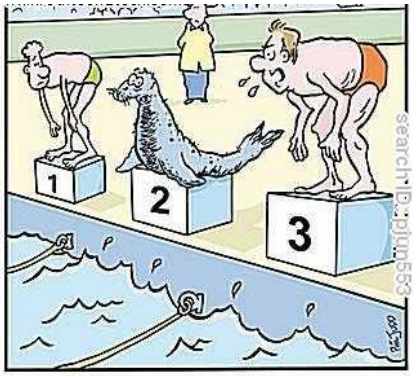
Podemos entender como seguridad una característica de cualquier sistema que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas informáticos, sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad, probabilidad de que un sistema se comporte tal y como se espera de él. Por tanto, se habla de tener **sistemas fiables** en lugar de sistemas seguros.

El experto Eugene H. Spafford cita en su frase célebre: "**el único sistema que es totalmente seguro es aquel que se encuentra apagado y desconectado, guardado en una caja fuerte de titanio que está enterrada en cemento, rodeada de gas nervioso y de un grupo de guardias fuertemente armados. Aún así, no apostaría mi vida en ello**".

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos:

- **Confidencialidad**: cualidad de un mensaje, comunicación o datos, para que solo se entiendan de manera comprensible o sean leídos, por la persona o sistema que esté autorizado. Comprende por tanto la privacidad o protección de dicho mensaje y datos que contiene.

"These documents are highly sensitive. Have them shredded, then burned."



"Are you sure this guy from Alaska is in a speed suit?"

- **Integridad**: cualidad de mensaje, comunicación o datos, que permite comprobar que no se ha producido manipulación alguna en el original, es decir, que no ha sido alterado.

- **Disponibilidad**: capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran. Supone que la información pueda ser recuperada en el momento que se necesite, evitando su pérdida o bloqueo.

"We back up our data on sticky notes because sticky notes never crash."

Hay que tener en cuenta que, tanto las amenazas como los mecanismos para contrarrestarlas, suelen afectar a estas tres características de forma conjunta. Así por ejemplo, fallos del sistema que hace en que la información no sea accesible pueden llevar consigo una pérdida de integridad. **Generalmente tienen que existir los tres aspectos descritos para que haya seguridad**.

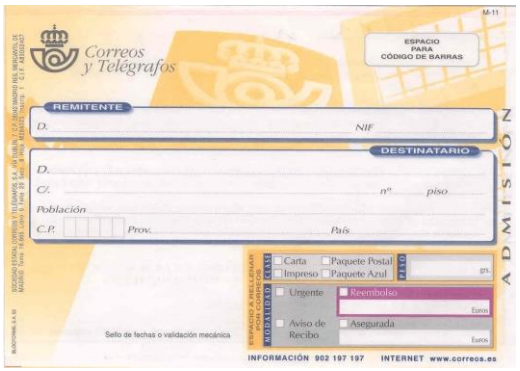
Dependiendo del entorno en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad. Por ejemplo, en un sistema **militar** se antepondrá la **confidencialidad** de los datos almacenados o transmitidos sobre su **disponibilidad**. En cambio, en

un servidor de archivos en red, se priorizará la **disponibilidad** frente a la **confidencialidad**. En un entorno bancario, la faceta que más ha de preocupar a los responsables del sistema es la **integridad** de los datos, frente a su **disponibilidad** o su **confidencialidad**: es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

Junto a estos tres conceptos fundamentales se suelen estudiar conjuntamente la **autenticación** y el **no repudio**.

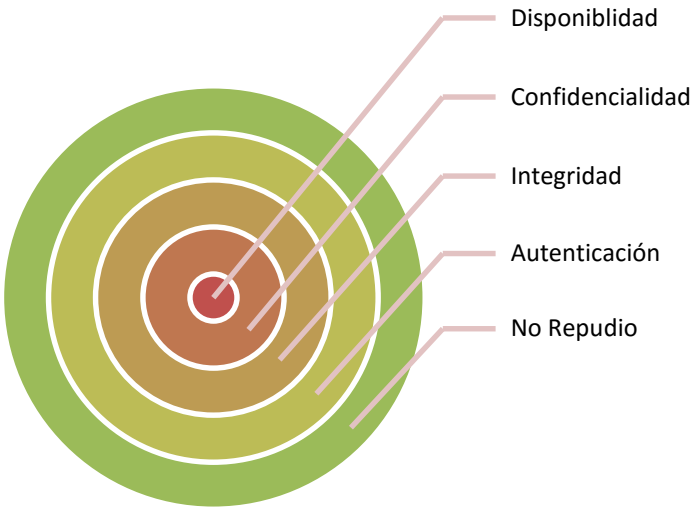
- **Autenticación**: verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice. Aplicado a la verificación de la identidad de un usuario en informática, cuando el usuario puede aportar algún modo que permita verificar que es quien dice ser, se suele realizar mediante un **usuario** o **login** y una contraseña o **password**.
- **No repudio o irrenunciabilidad**: estrechamente relacionado con la autenticación y permite probar la participación de las partes en una comunicación. Existen dos posibilidades:
  - **No repudio en origen**: el emisor no puede negar el envío. La prueba la crea el propio emisor y la recibe el destinatario.

  - **No repudio en destino**: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.



Si la autenticidad prueba quién es el autor o el propietario de un documento y cuál es su destinatario, el no repudio prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

Al grupo de estas características y objetivos de la seguridad se les conoce como CIDAN, nombre sacado de la inicial de cada característica. La relación de los mismos se presenta en la figura siguiente.



En la imagen superior se ilustra cómo se relacionan los diferentes servicios de seguridad, unos dependen de otros jerárquicamente, así si no existe el de nivel interior, no puede aplicarse el exterior. De esta manera, la disponibilidad se convierte en el primer requisito de seguridad, cuando existe ésta, se puede disponer de confidencialidad, que es imprescindible para conseguir integridad, imprescindible para poder obtener autenticación y, por último, el no repudio, que solo se obtiene si se produce previamente la autenticación.

A continuación veremos tres casos prácticos a modo de ejemplo sobre confidencialidad, integridad y disponibilidad.

Práctica 1.1. Práctica de confidencialidad.

En esta práctica guiada estudiaremos cómo se puede asegurar la confidencialidad de los datos en sistema Windows. Para todo ello usaremos encriptación sobre de archivos y carpetas usando EFS. Por último practicaremos con la herramienta de Microsoft que nos permite realizar encriptados sobre toda una unidad (bitlocker).

Práctica 1.1 Cara B, Desconfidencialidad sobre Sistemas Operativos.

En esta otra cara de la práctica 1.1 realizaremos un breve estudio de herramientas forenses que nos permiten atacar a unidades cifradas, tanto con EFS como con Bitlocker

Práctica de integridad.

Comprobaremos la integridad de los ficheros del sistema, intentando encontrar algún rootkit. Posteriormente practicaremos con la huella digital de un fichero, con el fin de encontrar posibles soluciones a ficheros falsos.

Práctica de disponibilidad.

Probaremos a escanear nuestra red, viendo los dispositivos que la componen y la disponibilidad de estos.

Alta Disponibilidad

La **alta disponibilidad** (HighAvailability) se refiere a la capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento y sin interrupciones, debido principalmente a su carácter crítico. El objetivo de la misma es mantener nuestros sistemas funcionando las 24 horas del día, 7 días a la semana, 365 días al año, manteniéndolos a salvo de interrupciones, teniendo en cuenta que se diferencian dos tipos de interrupciones:

- Las **interrupciones previstas**, que se realizan cuando paralizamos el sistema para realizar cambios o mejoras en nuestro hardware o software.
- Las **interrupciones imprevistas**, que suceden

por acontecimientos imprevistos (como un apagón, un error del hardware o del software, problemas de seguridad, un desastre natural, virus, accidentes, caídas involuntarias del sistema).

Las métricas comúnmente utilizadas para medir la disponibilidad y fiabilidad de un sistema son el tiempo medio entre fallos o **MTTF** (Mean Time To Failure) que mide el tiempo medio transcurrido hasta que un dispositivo falla, y el tiempo medio de recuperación o **MTTR** (Mean Time To Recover) mide el tiempo medio tomado en restablecerse la situación normal una vez que se ha producido el fallo. El **tiempo en el que un sistema está fuera de servicio** se mide a menudo como el cociente **MTTR/MTTF**. Lógicamente, nuestro principal objetivo es aumentar el MTTF y reducir el MTTR de forma que minimicemos el tiempo de no disponibilidad del servicio.

Existen distintos niveles de disponibilidad del sistema, según el tiempo aproximado de tiempo en inactividad por año se determina el porcentaje de disponibilidad. El mayor nivel de exigencia de alta disponibilidad acepta **5 minutos de inactividad al año**, con lo que se obtiene una **disponibilidad de 5 nueves: 99,999%**.

Como ejemplos de sistemas y servicios de alta disponibilidad podemos mencionar sistemas sanitarios, control aéreo, de comercio electrónico, bancarios, transporte marítimo, militares, etc., donde la pérdida o interrupción de conectividad pueden suponer graves consecuencias personales y económicas. En el tema 8 profundizaremos en algunas de las técnicas que permiten mejorar la disponibilidad de los sistemas y servicios ofrecidos por estos.

4. Elementos vulnerables en el sistema informático: Hardware, software y datos

La seguridad es un problema integral: los problemas de seguridad informática no pueden ser tratados aisladamente ya que **la seguridad de todo el sistema es igual a la de su punto más débil**. Al asegurar nuestra casa no sirve de nada ponerle una puerta blindada con sofisticada cerradura si dejamos las ventanas sin protección.

La educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar. Es evidente que por mucha tecnología de seguridad que se implante en una organización, si no existe una clara disposición por parte de los directivos de la empresa y una cultura a nivel de usuarios, no se conseguirán los objetivos perseguidos con la implantación de un sistema de seguridad. Por tanto, la seguridad informática precisa de **un nivel organizativo**, que posibilite unas normas y pautas comunes por parte de los usuarios de sistemas dentro de una empresa, por lo que diremos que:

Sistema de Seguridad = TECNOLOGÍA + ORGANIZACIÓN

Los tres elementos principales a proteger en cualquier sistema informático son el **software**, el **hardware** y los **datos**. En las auditorías de seguridad se habla de un cuarto elemento a proteger, de menor importancia desde el punto de vista de la seguridad informática, los **fungibles** (elementos que se gastan o desgastan con el uso continuo, como papel de impresora, tóner,...).

Habitualmente los **datos** constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar: con toda seguridad un servidor estará ubicado en un lugar de acceso físico restringido, o al menos controlado, y además en caso de pérdida de una aplicación (o un programa de sistema, o el propio núcleo del sistema operativo) este software se puede restaurar sin problemas desde su medio original (por ejemplo, el CD o DVD con el sistema operativo que se utilizó para su instalación). Sin embargo, en caso de **pérdida de una base de datos** o de un proyecto de un usuario, no tenemos un medio "original" desde el que restaurar, hemos de pasar obligatoriamente por un **sistema de copias de seguridad,** y a menos que la política de copias sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la pérdida.

También debemos ser conscientes de que las medidas de seguridad que deberán establecerse se deben contemplar a diferentes niveles, desde aspectos más locales, personales o individuales hasta los globales que afectan a una organización, o incluso la ciudadanía y empresas en su conjunto, como son las leyes. Por tanto la seguridad **informática comprenden** el **hardware** y el **sistema operativo**, las **comunicaciones** (por ejemplo, protocolos y medios de transmisión seguros), medidas de **seguridad físicas** (ubicación de los equipos, suministro eléctrico, etc.), los **controles organizativos** (políticas de seguridad de usuarios, niveles de acceso, contraseñas, normas, procedimientos, etc.) y **legales** (por ejemplo, la Ley Orgánica de Protección de Datos, LOPD).

Este esquema sirve de base para el desarrollo del curso analizando la seguridad informática desde distintas perspectivas, completando una visión global de la materia:

- **Seguridad pasiva**: Seguridad física y ambiental y copias de seguridad en los sistemas informáticos. Tema 2.
- **Seguridad lógica**: control de acceso a los sistemas, gestión de sistemas operativos: usuarios, privilegios, contraseñas en el tema 3, software de seguridad antimalware en el tema 4 y cifrado en la información y comunicaciones mediante el estudio de la criptografía en el tema 5.
- **Seguridad en redes corporativas**: estudiando protocolos y aplicaciones seguras como SSH, TLS/SSL y VPN, configuraciones seguras en inalámbricas en el tema 6 y protegiendo especialmente la seguridad perimetral mediante cortafuegos y proxy en el tema 7.
- **Configuraciones de alta disponibilidad**: mediante redundancia en el almacenamiento RAID, balanceo de carga, virtualización de servidores. Tema 8.
- **Normativa legal en materia de seguridad informática**: LOPD y LSSICE. Tema 9.

5. Amenazas

Las amenazas a un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema con un troyano, pasando por un programa descargado gratuito que nos ayuda a gestionar nuestras fotos, pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espías, hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad. Las amenazas pueden ser provocadas por: personas, condiciones físicas-ambientales y software, o lógicas.

Amenazas provocadas por personas

La mayoría de ataques a nuestro sistema provienen de personas que, intencionadamente o no, pueden causarnos enormes pérdidas. Generalmente se tratará de piratas informáticos, ciberdelincuentes, hackers o crackers, que intentan conseguir el máximo nivel de privilegio posible aprovechando algunas vulnerabilidades del software. Se dividen en dos grandes grupos: los atacantes pasivos que fisgonean el sistema pero no lo modifican o destruyen, y los activos que dañan el objetivo atacado o lo modifican en su favor.

Dentro de una organización: El propio personal puede producir un ataque intencionado, nadie mejor conoce los sistemas y sus debilidades, o un accidente causados por un error o por desconocimiento de las normas básicas de seguridad. Por otro lado ex empleados o personas descontentas con la organización pueden aprovechar debilidades que conocen o incluso realizar chantajes.

- **Hacker**: Experto o gurú en aspectos técnicos relacionados con la informática. Personas que les apasionan el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas. Suele distinguirse entre aquellos cuyas acciones son de carácter constructivo, informativo o solo intrusivo, o que además lo son de tipo destructivo, catalogados respectivamente de hackers y crackers, o white hat y black hat. Recientemente ha aparecido el término, más neutro, grey hat (sombrero gris), que ocasionalmente traspasan los límites entre ambas categorías. Otros términos y categorías son:
- **Newbie**: Hacker novato.
- **Wannaber**: Les interesa el tema de hacking pero que por estar empezando no son reconocidos por la élite.
- **Lammer** o **Script-Kiddies**: Pretenden hacer hacking sin tener conocimientos de informática. Solo se dedican a buscar y descargar programas de hacking para luego ejecutarlos.
- **Luser (looser + user)**: Es un término utilizado por hackers para referirse a los usuarios comunes, de manera despectiva y como burla.
- **Pirata informático, ciberdelincuente o delincuente informático**: Personas dedicadas a realizar actos delictivos y perseguidos legalmente: como la copia y distribución de software, música o películas de forma ilegal, fraudes bancarios o estafas económicas.

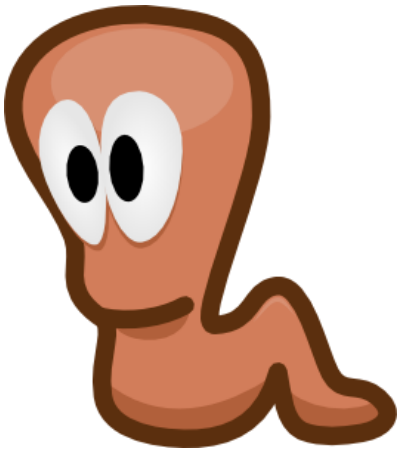
Amenazas físicas y lógicas

Las **amenazas físicas y ambientales** afectan a las instalaciones y/o el hardware contenido en ellas y suponen el primer nivel de seguridad a proteger para garantizar la disponibilidad de los sistemas. En el tema siguiente veremos con más profundidad los aspectos asociados a:

- **Robos**, **sabotajes**, destrucción de sistemas.
- Cortes, subidas y bajadas bruscas de **suministro eléctrico**.
- **Condiciones atmosféricas** adversas. Humedad relativa excesiva o temperaturas extremas.
- **Catástrofes** (naturales o artificiales) terremotos, inundaciones, incendios, humo o atentados de baja magnitud, etc
- **Interferencias electromagnéticas** que afecten al normal comportamiento de circuitos y comunicaciones.

Una **amenaza lógica** es software o código que de una forma u otra pueden afectar o dañar a nuestro sistema, creados de forma intencionada para ello (el software malicioso, también conocido como malware, se analizará a fondo en el tema 4) o simplemente por error (bugs o agujeros). Entre otros encontramos:

- **Herramientas de seguridad**: Existen herramientas para detectar y solucionar fallos en los sistemas, pero se pueden utilizar para detectar esos mismos fallos y aprovecharlos para atacarlos.
- **Rogueware o falsos programas de seguridad**: También denominados Rogue, FakeAVs, Badware, Scareware, son falsos antivirus o antiespías.
- **Puertas traseras o backdoors**: Los programadores insertan "atajos" de acceso o administración, en ocasiones con poco nivel de seguridad.
- **Virus:** Secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace. Detrás de la palabra virus existe todo un conjunto de términos que analizaremos con más detalle en el Capítulo 4, dentro de lo que se conoce como malware.



- **Gusano o Worm**: Programa capaz de ejecutarse y propagarse por sí mismo a través de redes, normalmente mediante correo electrónico basura o spam.
- **Troyanos** o Caballos de Troya: Aplicaciones con instrucciones escondidas de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario.
- **Programas conejo o bacterias**: Programas que no hacen nada útil, simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco...), produciendo una negación de servicio.
- **Canales cubiertos**: Canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; un proceso transmite información a otros que no están autorizados a leer dicha información.

Del mismo modo que hemos analizados las amenazas de los sistemas informáticos desde un punto de vista de quién o qué la genera, los tipos de amenazas pueden clasificarse en función de la técnica que se emplean para realizar el ataque. Las técnicas más usuales son las que se indican en la tabla siguiente.

Malware	Programas malintencionados (virus, espías, gusanos, troyanos, etc.) que afectan a los sistemas con pretensiones como: controlarlo o realizar acciones remotas, dejarlo inutilizable, reenvío de spam, etc.
Ingeniería social	Obtener información confidencial como credenciales (usuario-contraseña), a través de la manipulación y la confianza de usuarios legítimos. El uso de dichas credenciales o información confidencial servirá para la obtención de beneficios económicos mediante robo de cuentas bancarias, reventa de información o chantaje.
Scam	Estafa electrónica por medio del engaño como donaciones, transferencias, compra de productos fraudulentos, etc. Las cadenas de mail engañosas pueden ser **scam** si hay pérdida monetaria y **hoax** (bulo) cuando solo hay engaño.
Spam	Correo o mensaje basura, no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor. Suele ser una de las técnicas de ingeniería social basada en la confianza depositada en el remitente, empleadas para la difusión de scam, phishing, hoax, malware, etc.
Sniffing	Rastrear monitorizando el tráfico de una red para hacerse con información confidencial.
Spoofing	Suplantación de identidad o falsificación, por ejemplo encontramos IP, MAC, tabla ARP, web o mail Spoofing.
Pharming	Redirigir un nombre de dominio (domain ñame) a otra máquina distinta falsificada'-y fraudulenta.
Phishing	Estafa basada en la suplantación de identidad y la ingeniería social para adquirir acceso a cuentas bancarias o comercio electrónico ilícito.
Password cracking	Descifrar contraseñas de sistemas y comunicaciones. Los métodos más comunes son mediante sniffing, observando directamente la introducción de credenciales (shoulder surfing), ataques de fuerza bruta, probando todas las combinaciones posibles, y de diccionario, con un conjunto de palabras comúnmente empleadas en contraseñas.

Botnet	Conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática, en multitud de host, normalmente infectados, permite controlar todos los ordenadores/servidores infectados de forma remota. Sus fines normalmente son rastrear información confidencial o incluso cometer actos delictivos.
Denegación	Causar que un servicio o recurso sea inaccesible a los usuarios legítimos. Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, o también llamado ataque DDoS, a través de una botnet, siendo esta técnica el ciberataque más usual y eficaz.

6. Protección

Hasta ahora hemos hablado de los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del origen de tales amenazas; parece claro que, para completar nuestra visión de la seguridad, hemos de hablar de las **formas de protección de nuestros sistemas**.

Para proteger nuestro sistema hemos de realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrían generar y la probabilidad de su ocurrencia. Este análisis convencionalmente se realizará mediante auditorías de seguridad.

Auditoría de seguridad de sistemas de información

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad. Los objetivos de una auditoría de seguridad de los sistemas de información son:

- Revisar la seguridad de los **entornos y sistemas**.
- Verificar el cumplimiento de la **normativa** y legislación vigentes
- Elaborar un **informe** independiente.

Una auditoría se realiza con base a un patrón o conjunto de directrices o buenas prácticas sugeridas. Existen estándares orientados a servir como base para auditorías de informática. Uno de ellos es COBIT (Objetivos de Control de las Tecnologías de la Información), y adicional a éste podemos encontrar el estándar ISO 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, éste puede constituirse como una directriz de

auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27001.

Los servicios de auditoría constan de las siguientes fases:

- **Enumeración de sistemas operativos**, servicios, aplicaciones, topologías y protocolos de red.
- **Detección, comprobación y evaluación** de vulnerabilidades.
- **Medidas** específicas de **corrección**.
- Recomendaciones sobre implantación de **medidas preventivas**.

Tipos de auditoría

Los servicios de auditoría pueden ser de distinta índole:

- Auditoría de **seguridad interna**: se contrasta el nivel de seguridad de las redes locales y corporativas de carácter interno.
- Auditoría de **seguridad perimetral**: se estudia el perímetro de la red local o corporativa, conectado a redes públicas.
- **Test de intrusión**: se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada.
- **Análisis forense**: análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, se denomina análisis post mórtem.
- Auditoría de **código de aplicaciones**: análisis del código independientemente del lenguaje empleado, un ejemplo concreto y frecuente se realiza con los sitios web, mediante el análisis externo de la web, comprobando vulnerabilidades como la inyección de código SQL, Cross Site Scripting (XSS), etc.

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización del software y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

Algunas de las auditorías que trabajaremos a lo largo del libro son empleadas en ocasiones para acceder a sistemas y conexiones remotas no autorizadas, aunque en nuestro caso deben servir para ver el nivel de seguridad que disponemos en nuestros sistemas. Entre las más comunes son las auditorías de contraseñas de acceso a sistemas y de conexiones inalámbricas o wireless.

Medidas de seguridad

A partir de los análisis realizados mediante auditorías, hemos de diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso, de que se produzcan. A los mecanismos utilizados para implementar esta política de seguridad se les denomina mecanismos de seguridad, son la parte más visible de nuestro sistema de seguridad y se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red. Se distinguirán y estudiarán en los próximos temas las medidas de seguridad:

- **Según el recurso a proteger**:
    - Seguridad **física**: trata de proteger el hardware, teniendo en cuenta entre otros aspectos la ubicación y las amenazas de tipo físico: robos, catástrofes naturales o artificiales, etc. Algunas medidas son el estudio de la ubicación correcta, medidas preventivas contra incidentes como incendios o inundaciones o el control de acceso físico.

  - Seguridad **lógica**: protege el software tanto a nivel de sistema operativo como de aplicación, sin perder nunca de vista el elemento fundamental a proteger, la información o datos de usuario. Dentro de sus medidas se encuentran: copias de seguridad, contraseñas, permisos de usuario, cifrado de datos y comunicaciones, software específico antimalware, actualizaciones o filtrado de conexiones en aplicaciones de red.

- Según el **momento** en el que se ponen en marcha las medidas de seguridad:
  - Seguridad **activa**: son **preventivas** y evitan grandes daños en los sistemas informáticos, por tanto se consideran acciones previas a un ataque. Son de este tipo todas las medidas de seguridad lógica.
  - Seguridad **pasiva**: son **correctivas**, minimizan el impacto y los efectos causados por accidentes, es decir se consideran medidas o acciones posteriores a un ataque o incidente. Son de este tipo todas las medidas de seguridad física y las copias de seguridad que permiten minimizar el efecto de un incidente producido.

0. Índice