Unidad 1

Introducción a la seguridad informática

Seguridad y alta disponibilidad

Índice

Introducción

La seguridad depende del dominio al que se desee aplicar. En el mundo de la informática, muchas facetas pueden estar en riesgo. La seguridad informática está directamente centrada en la protección de los elementos vulnerables: software, hardware y datos.

Las características que un sistema informático seguro tiene están relacionadas con la fiabilidad, la confidencialidad, la integridad y la disponibilidad.

Todos los sistemas informáticos deben protegerse instalando, configurando y actualizando el software de seguridad. Estos softwares presentan las propiedades de funcionalidad, usabilidad y seguridad. La paradoja de la seguridad muestra cómo estos factores están estrechamente relacionados, puesto que, si el sistema no es funcional y usable, este será menos seguro e incómodo.

Al finalizar esta unidad

- Descubriremos las diferentes facetas de la seguridad informática.
- Aprenderemos las principales amenazas a las que se enfrentan los sistemas informáticos.
- Conoceremos los tipos de medidas de seguridad.
- Estudiaremos las medidas de seguridad física y ambiental.
- Describiremos el concepto de análisis forense de sistemas informáticos.
- Definiremos las fases de un ataque y las medidas de seguridad lógicas.
- Conoceremos las diferentes políticas de seguridad de una empresa.
- Distinguiremos entre los distintos métodos y protocolos de autenticación y autorización.
- Aprenderemos la diferencia entre los distintos tipos de copia de seguridad.

1.1. Protección y características

Las principales características a los que un sistema informático debe tener son:

1. **Fiabilidad:** el sistema informático debe mantenerse en un nivel de funcionamiento, sin bajar su rendimiento, lo cual incluye la capacidad de superar adversidades, sin dejar de ofrecer sus servicios a los usuarios.
2. **Confidencialidad:** los datos que almacena el sistema solo deben ser accesibles por aquellas personas que tienen permisos para manejarlos.
3. **Integridad:** los datos deben permanecer sin pérdida o alteración.
4. **Disponibilidad:** los datos como el sistema informático debe estar siempre accesibles en cualquier momento.

1.1.1. Medidas de protección

Dependiendo del tipo de amenaza, adoptaremos las siguientes medidas de seguridad activas o pasivas:

- **Medidas activas:** son las que utilizamos para combatir daños en el sistema informático provocados por el factor humano. Requieren atención por parte de un profesional e implican la supervisión de este. Un ejemplo de este tipo es la instalación y configuración de un firewall.
- **Medidas pasivas:** son las que se aplican al sistema informático desde su instalación, para minimizar el impacto causado por accidentes y averías. Un ejemplo de este tipo es una alarma antincendios.

Existen medidas preventivas tanto en seguridad activa como pasiva, pero hay que aclarar que existe otra clasificación de las medidas de protección:

- **Medidas preventivas:** se adoptan para evitar el problema. Por ejemplo, una evaluación de vulnerabilidades.
- **Medidas correctivas:** se adoptan para solucionar los efectos una vez el problema se haya producido.

1.1.2. Amenazas

Son muchas las amenazas a las que está expuesto un sistema informático, entre las cuales se encuentran las siguientes:

Amenazas físicas

Aquellas que ponen en riesgo al hardware del sistema:

- **Desgracias sobrevenidas:** inundaciones, incendios, terremotos.
- **Situaciones de riesgo hardware:** exceso de temperatura, cortes en suministro eléctrico, picos de tensión.
- **Averías o fin de vida útil del hardware:** fallos en componentes electrónicos, dispositivos y sistemas de almacenamiento.
- **Robos:** accesos no permitidos al sistema para robarlo de forma total o parcial.
- **Acceso no autorizado a ficheros o dispositivos:** usuarios que acceden sin tener permiso.

Amenazas lógicas

Son aquellas amenazas que hacen referencia al software, especialmente a los datos:

- **Acceso ilegítimo:** personal externo intenta hacerse pasar por el administrador para tomar el control total del sistema.
- **Software malicioso:** virus, gusanos, troyanos..., en general todo tipo de software malintencionado. Se denomina malware, y sin que el usuario se percate, se introducen el sistema informático para utilizarlo con fines maliciosos.
- **Vulnerabilidad en la protección de los datos:** suplantación de identidad y captación de los datos con fines ilegales, etc.

1.2. Seguridad física y ambiental

Los componentes de los sistemas informáticos, el hardware, están formados por componentes electrónicos, los cuales están expuesto a una gran variedad de riesgos:

- Cortocircuitos provocados por el agua y la humedad.
- Bajo rendimiento por las altas temperaturas.
- Picos de tensión.
- Corte de suministro eléctrico que ocasione bases de datos inservibles.
- Componentes de elevado coste, lo cual puede atraer la intención de algunos ladrones, aunque lo normal, el verdadero interés son los datos que llevan.

1.2.1. Ubicación y protección de equipos y servidores

En una empresa, los servidos cuentan con un gran valor económico y estratégico, en ellos encontramos los activos más valiosos, como pueden ser datos. La información que se obtiene de los análisis de datos es fundamental y debe ser protegida:

- Evitar conducciones de gas, agua o calefacción.
- Disponer de un doble suelo para evitar cortocircuitos e inundaciones.
- Debe estar con una correcta climatización.
- Evitar los cortes de suministro eléctrico gracias a sistemas de alimentación ininterrumpida.
- En zonas con presencia electromagnética, será importante aislar el CPD, los armarios *rack* y el cableado.
- Proteger ante contratiempos naturales, como en las zonas de riesgo sísmico.

1.2.2. Protección ante fallos del cableado

Los cables pueden sufrir una deteriorización en su calidad o sufrir daños, por lo que se debe contar con herramientas que faciliten su arreglo, como conectores y bobinas.

En cuanto al cableado interno del CPD, en caso de fallo y necesitar una reparación, no se puede aceptar que el tiempo de parada (*downtime*) sea elevado, por lo que se suelen combinar métodos de varios cables que se comportan como un único cable virtual. Por ejemplo, esta metodología se aplica en enlaces de red inalámbrica. Las características de estos cables son:

- El protocolo de *link aggregation* de los cables es el mismo y todos deben trabajar a la misma velocidad de transmisión (1 Gbps). Es importante recalcar que un *bond*, formado por varios cables, no multiplica la velocidad, sino que la divide en cada uno de los cables que lo forman.

- El *bond* o agrupación de cables seguirá funcionando, aunque algunos fallen. Únicamente se reduciría la velocidad de transmisión.
- Los cables están unidos, por lo que el *bond* permanece oculto mostrando un único enlace o interfaz de red.

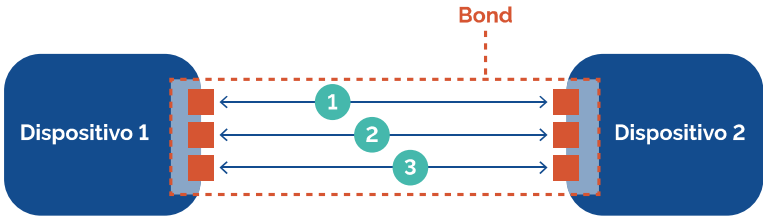

Imagen 1. Bond formado por tres cables

Podemos nombrar diferentes protocolos para enlaces redundantes. Por ejemplo, se suele utilizar el protocolo LACP (*Link Aggregation Control Protocol*) para redes Ethernet. Este comparte las características mencionadas anteriormente. Sin embargo, hay otros protocolos que proporcionan redundancia, en lugar de sumar el ancho de banda, por lo que únicamente funciona uno de los cables del *bond*. Por otro lado, otros protocolos hacen uso de todos los cables de forma alternativa través de un algoritmo *round-robin*.

Los *smartphones* ya utilizan el protocolo LACP y pueden combinar la conexión de datos 3G/4G (LTE) y una red wifi (WLAN). Por otro lado, también se puede dar el caso de un punto de acceso wifi Dual Band que divide el tráfico de datos según las frecuencias de 2.4 GHz y 5GHz. Dual Wan hace referencia a la utilización de dos conexiones a internet para evitar la incomunicación que se daría si una de las dos cayera, siendo el administrador el que establece los porcentajes, ya sea de forma manual o automática. Los modelos de routers más avanzados son Multi-Wan, por lo que se pueden utilizar varios enlaces WAN.

1.2.3. Protección ante humedades e inundaciones

Es muy habitual en los centros de procesamiento de datos (CPD) instalar sistemas y sensores de humedad. Esto nos evita los problemas derivados por condensación, humedades o roturas ocasionales.

Los equipos informáticos trabajan en un rango de humedad más restringido. Siempre que la humedad no descienda excesivamente, los sistemas podrán trabajar sin problema,

- El rango de humedad ideal estaría entre un 45-55% de humedad.
- Menos de 40% se considera no recomendable. Ni que suba del 60%.

Pero: ¿qué ocurre si se produce una inundación? El agua termina accediendo al CPD produciendo una catástrofe. Por ese motivo, los equipos nunca estarán al nivel del suelo. Es recomendable situar los equipos en un doble suelo, o utilizar armarios *rack* con patas o ruedas que los separen unos 10cm del suelo.

1.2.4. Protección ante incendios y altas temperaturas

Entre las que podemos adoptar el siguiente paquete de medidas:

- Instalación de un sistema de climatización que mantenga la sala refrigerada. La idea es que la temperatura esté entre los 15 y los 25ºC.
- Sistemas de ventilación potentes en todos los servidores y los armarios rack.
- Almacenamiento de copias de seguridad.
- Colocación de alarmas antincendios y detectores de humo.
- Colocación de extintores de CO2. Recuerda que no vale cualquier extintor cuando se trata de equipos informáticos.
- Uso de puertas cortafuegos.
- Utilización de material ignifugo en la estructura, paredes y suelos. La pintura a ser posible ignifuga y libre de elementos químicos tóxicos.

NOTA

- Los extintores deben ser de gas.
- Es recomendable una buena circulación del aire, ya que garantiza una temperatura ideal y menor consumo eléctrico.

Una mala combinación de temperaturas es perjudicial para los equipos informáticos y podrían incluso dejar de funcionar. Un buen sistema de climatización es una suma de factores que asegura una correcta refrigeración del CPD.

Así mismo, la temperatura también representa un problema para el usuario, a quien también le recomendamos una serie de medidas básicas:

- Colocar el portátil sobre una plataforma con rejilla, elevada y con ventiladores (alimentada por USB) mientras se trabaja con ellos.
- Utilizar siempre los portátiles sobre superficies planas. Estas, permiten la circulación del aire y evitan sobrecalentamiento.
- No colocar los ordenadores cerca de los radiadores de calefacción.

Una mala temperatura puede destrozar los equipos informáticos, por lo que se recomienda que la temperatura no varíe de 15º-25º, que la temperatura no supere nunca los 35% y que la humedad no supere el 90%.

Imagen 1 Ventilador para rack

Imagen 2 Ventilador para portátiles

1.2.5. Protección ante terremotos

Las instalaciones que protejan al sistema informático deben ser robustas con materiales y estructuras antisísmicas. También se pueden tomar medidas como la colocación de sistemas de amortiguación o aislamiento sísmico para los equipos informáticos, y la realización de simulaciones y planes de contingencia en caso de sismo.

En ciertos países o zonas de alto riesgo sísmico como Japón, los CPD se construyen sobre estructuras especialmente diseñadas y construidas, incluyendo también doble suelo en caso de tsunami. Otras empresas, prefieren utilizar un CPD prefabricado que se ubica en el exterior de los edificios.

1.2.6. Protección ante problemas de suministro eléctrico

Debemos de tener en cuenta el momento de elegir una buena ubicación e instalación desde el punto de vista del suministro eléctrico, pero solo se tratarán los relacionados con la seguridad. Lógicamente, debe ser una instalación acorde a la potencia requerida de los equipos que más consumen, por lo que solo vamos a tratar: cómo evitar riesgos en nuestro hardware:

SAI: tipos y características

Existen unos aparatos que sirven para proteger los dos principales problemas que nos vamos a encontrar: cortes del suministro y picos de tensión. Son los **Sistemas de Alimentación Ininterrumpida (SAI)**

Es un equipo previsto para trabajar conectado entre la red eléctrica y la carga que se necesite proteger, ofreciendo un suministro eléctrico de emergencia en caso de fallo o anomalía en la red. Según su topología (offline, inline u online) ofrecerá un nivel de protección eléctrica más o menos completo. Y según su capacidad y potencia, el SAI montará de una a varias baterías, que comenzarán a descargarse para para mantener una alimentación ininterrumpida durante cortes de suministro eléctrico.

Imagen 3: SAI

Por lo tanto, un SAI dispone de una toma de entrada y una o más de salida para proporcionar corriente ante un corte del suministro.

NOTA

Cuando hablamos de Ininterrumpida, no hay que confundir con interrumpida. La principal diferencia entre interrumpida e ininterrumpida es la forma en que manejan la transición de la alimentación eléctrica en caso de una interrupción del suministro eléctrico.

A la hora de elegir un SAI tendremos en cuenta las siguientes indicaciones:

- **Potencia máxima que proporciona.** Se mide en voltiamperios (VA). Se han de cubrir las potencias de los equipos conectados con un índice de tolerancia entre 15-20%.

  1 vatio(W) = 1 voltioamperio (VA)* F.P (factor de potencia)

  **El factor de potencia suele rondar 0.8-0.9 en todos los SAI*

- **Tipo de autonomía.** Dependerá del número de baterías, la carga de estas y la potencia del suministro. Los fabricantes deben aportar el tiempo de autonomía de estas según potencia requerida.

En cualquier caso, **algunos modelos** SAI disponen de una toma de salida maestra. Si detecta que el equipo conectado se apaga, también corta el suministro de las tomas controladas. Un ejemplo sería conectar el ordenador a la toma *master* y los demás periféricos a las tomas *controlled*, ya que:

- Al encender el equipo conectado a la toma *master*, les llegaría electricidad a los otros equipos conectados.
- Al apagar el equipo, cortaríamos el suministro de los otros tres dispositivos, suponiendo un ahorro energético.

Imagen 4: Diferentes tomas de salida programables

Por últimos, vamos a mencionar otra las características que tienen los SAI más avanzados: *la segmentación de carga*, que consiste en dividir en dos, las tomas de salida: *críticas y no críticas*.

Si el SAI entra en modo batería, igualmente sigue proporcionando energía, pero si desciende sus valores por debo de un nivel correcto, el SAI apaga las tomas no críticas para centrar su energía en los equipos críticos.

Esta función es especialmente útil en entornos empresariales, donde es común tener equipos críticos y no críticos, y se requiere una mayor precisión en el suministro de energía para garantizar la continuidad del negocio

Monitorización

Es muy importante que tengamos en cuenta que se debe actuar con rapidez cuando un SAI entra en modo batería para evitar la pérdida de datos y daños en los equipos conectados.

Ocurre que los cortes eléctricos pueden producirse en cualquier zona, no solo en poblaciones pequeñas o en zonas en obras. En las grandes ciudades suelen ser breves, y gracias a los SAI los sistemas siguen funcionando como si nada hubiera ocurrido. Alertado por el SAI, el trabajo del administrador será apagar los equipos conectados antes de que se agote la batería.

Existen tipos de SAI empresariales que pueden ser conectados mediante un puerto USB o en red para que un equipo supervise el estado del SAI y de los equipos conectados. Gracias a una aplicación, se puede configurar para que mande una señal por debajo de un umbral predefinido para apagar los equipos que lo controlan. De este modo, no es necesaria la intervención del administrador. Es fundamental para toda empresa que cuente con este tipo de SAI que se pueden auto apagar.

Los SAI más avanzados cuentan con una aplicación para controlar el sistema de manera centralizada. Todos los equipos conectados pueden recibir señales para monitorizar el estado de este si instalamos el software adecuado. El tiempo de autonomía dependerá no solo del número de equipos conectados, sino también de la potencia de estos y de la capacidad de las baterías del SAI.

Lo SAI más avanzados cuentan con lo siguiente:

1. Una aplicación para controlar el sistema de manera centralizada.
2. Todos los equipos conectados pueden recibir señales para monitorizar el estado de este si instalamos *software* adecuado.

Precauciones y mantenimiento

La batería de un SAI tiene una vida útil. Llegado a este punto, es un dato que debe venir reflejado en las especificaciones técnicas del SAI. Normalmente, los SAI más avanzados disponen de pantallas LED donde avisan del deterioro de la batería, para que esta sea reemplazada.

Es habitual también el remplazo de baterías, sobre todo si se hinchan o peor aún, expulsan parte de algún producto químico interno, que casi con toda seguridad, será necesario reemplazar el SAI por completo.

Hay que tener especial cuidado con el traslado con el fin de evitar graves lesiones en caso de descarga, pues son aparatos que acumulan energía. Incluso suelen ser *muy* pesados, por lo que se recomienda ser transportados por dos personas y con las debidas medidas preventivas.

PDU

Comúnmente se suele confundir un SAI con una PDU o Unidad de Distribución de Potencia (*Power Distribution Unit)*. Una PDU es lo que conocemos todos como regleta.

Imagen 5. PDU

Existen PDU de muchos tipos y tamaños, desde simples regletas hasta cabinas de gestión remota de la carga.

NOTA

Mientras que un SAI es un dispositivo de respaldo de energía que mantiene los equipos en funcionamiento durante una interrupción del suministro eléctrico, una PDU se utiliza para distribuir la energía eléctrica a varios equipos y puede proporcionar monitoreo y control adicionales de la energía eléctrica.

1.2.7. Protección ante accesos no autorizados y robos

Debemos tener especial cuidado a la hora de proteger y evitar los accesos no autorizados a nuestra empresa. Desde distintos tipos de alarmas hasta cadenas o candados, se han de valorar las siguientes protecciones específicas:

- Los equipos pueden ser protegidos por *candados antirrobo.* Destaca por ser el más estandarizado el de la marca Kensington. La mayoría de las cajas incluyen argollas que pueden ser utilizadas en otro tipo de *hardware.*
- El acceso debe ser limitado a un número de personas específico. Por lo tanto, el CPD debe estar siempre bajo llave, aunque lo más recomendable es otro sistema de control y acceso, tal como un acceso por código. También es posible utilizar accesos biométricos, doble contraseña, etc.
- Existe la posibilidad de instalar un sistema de videovigilancia en los accesos más importantes. Te en cuenta que el Reglamento General de Protección de Datos (RGPD), de 25 de mayo de 2018, obliga a colocar carteles de advertencia.

1.3. Análisis forense de sistemas informáticos

Las auditorías o peritajes de seguridad informática evalúan el sistema informático utilizando técnicas de pentesting y recomiendan medidas de seguridad para evitar puntos vulnerables. Los hackers éticos evalúan las amenazas y realizan pruebas de penetración para poner a prueba los sistemas.

El informe de la auditoría de seguridad se basa en la norma ISO 19011, conocida como Directrices para la auditoría de sistemas de gestión. Por otro lado, la Asociación Española de Normalización (UNE) también presenta normas orientadas al territorio nacional, recogidas en la UNE 197001:2011 en referencia a los Criterios generales para la elaboración de informes y dictámenes periciales. En cuanto a informes con validez legal en un proceso judicial, se pueden seguir el Sistema de Gestión de Evidencias Electrónicas (SGEE) UNE 71505:2015 y la Metodología para el análisis forense de las evidencias electrónicas UNE 71506:2016.

El informe debe contemplar:

- El objetivo de la auditoría, que puede ser periódico o de seguimiento.
- El alcance de la auditoría, haciendo referencia a los procesos, los departamentos y el tiempo.
- El equipo auditor.
- Las fechas y los lugares de la auditoría.
- Los criterios de la auditoría, señalando los procesos y los estándares que se han seguido.
- Los resultados de la auditoría, pudiendo diferenciar entre principales hallazgos (contando con fallos sistemáticos) y hallazgos menores (mencionando errores no genéricos y puntuales). También se pueden incluir los elementos probatorios de los hallazgos y los puntos positivos encontrados.
- Las conclusiones de la auditoría.

Otro tipo de información adicional que se puede incluir son:

- La planificación de la auditoría.
- El resumen del proceso de la auditoría.
- Los obstáculos y las limitaciones.
- Las áreas no cubiertas.
- Los acuerdos y desacuerdos entre el auditor y el cliente.
- Las recomendaciones de mejora.
- Los planes de seguimiento propuestos.

1.3.1. Fases del análisis forense

1. **Estudio previo:** se lleva a cabo un estudio y un análisis inicial a través de entrevistas y documentación para poder especificar el problema que se va a tratar.
2. **Adquisición de datos:** se recopila información y se duplican los dispositivos que se deben analizar, estableciendo un enlace firme para garantizar la integridad de las pruebas. Las distintas fuentes de información pueden ser:
   - Ficheros log del cortafuegos.
   - Ficheros log del sistema de control de incidencias.
   - Ficheros log del sistema operativo, del servidor y de los equipos, entre otros.
   - Ficheros log proporcionados por el proveedor de internet (IPS).
   - Correos electrónicos.
   - Historial del navegador.
   - Entrevistas con el administraros y los usuarios del sistema.
   - Listados de vulnerabilidad.
3. **Análisis e investigación:** en esta fase se realiza el análisis forense propiamente dicho. Se examina la información obtenida en la fase anterior y se procede a identificar y documentar las evidencias relevantes. Es importante mantener la cadena de custodia de las pruebas para que puedan ser utilizadas en un juicio en caso necesario. En esta fase también se lleva a cabo la reconstrucción de los hechos para entender lo que sucedió y cómo se llevó a cabo el ataque. En caso de que se haya encontrado algún malware, se analiza su comportamiento para entender su funcionalidad y posibles objetivos.
4. **Redacción del informe:** en esta fase se elabora un informe completo y detallado sobre todo lo analizado en las fases anteriores. Se describe en detalle el alcance y la metodología de la investigación, se presentan las evidencias encontradas y se explican los resultados del análisis. Además, se incluyen las conclusiones, recomendaciones y acciones para mejorar la seguridad y evitar que se repita el incidente. Es importante que el informe esté redactado de forma clara y precisa, y que contenga toda la información necesaria para que un juez o tribunal pueda entender lo sucedido.

1.3.2. Herramientas para el análisis forense

Las herramientas que se utilizan para el análisis forense de sistemas informáticos pueden utilizarse para clonar unidades de almacenamiento y para analizar dispositivos, ficheros log y conexiones de red, entre otros.

Las herramientas más utilizadas son:

- Digital Forensics Framework (DFF).
- Open Computer Forensics Architecture (OCFA).
- Computer Forensics Linux Live Distro o Computer Aided Investigative Environment (C.A.IN.E).
- SANS Investigative Forensic Toolkit (SIFT).
- The Sleuth Kit (TSK).
- Volatility Foundation, con Open Memory Forensics Workshop (OMFW).
- OpenSCAP.

Estas herramientas no deben confundirse con las herramientas empleadas para el pentesting que se ha mencionado con anterioridad. Mediante el análisis forense, se pretende recopilar información de un sistema dañado; mientras que el pentesting se centra en penetrar los sistemas. Sin embargo, algunas herramientas de pentesting cuentan con herramientas forenses, por ejemplo, Kali Linux.

1.3.3. Registro log centralizado

La sincronización del registro log centralizado es necesaria para el flujo de información y el envío de documentos entre dispositivos. Este proceso se conoce como ryslog. El término ryslog se utiliza para identificar al servidor y al protocolo utilizados para acceder al registro central.

Entornos Linux

El protocolo syslog está implementado en el paquete ryslog de Linux por defecto. El demonio ryslog recibe los eventos de las aplicaciones del sistema y los almacena en ficheros log, aunque también puede trabajar con equipos remotos y con múltiples formatos de almacenamiento de información. Esa información se puede almacenar redirigiéndola (*forward*) a otro equipo, de modo que se configura el equipo para compartir información con un servidor centralizado.

Entornos Windows

La redirección de eventos (WEF) y syslog comparten el mismo funcionamiento: el servidor central o recopilador recibe la información del resto de equipo o fuentes. Se emplea el protocolo WinRM para compartir esta información de forma remota (Administración remota de Windows o WS-Management). El servicio para recopilar eventos de Windows debe estar habilitado para realizar el proceso. Estos envíos de información son llamados suscripciones de eventos.

1.4. Fases de un ataque

Según el certificado CEH (Certified Ethical Hacker), los ataques a un sistema informático siguen las siguientes fases:

Reconocimiento » Escaneo » Obtención de acceso » Mantenimiento del acceso » Borrado de huellas

Imagen 6. Fases de un ataque informático

1. **Reconocimiento o reconnaissance:** es la fase preparatoria en la que el atacante recopila la información sobre su objetivo, realizando un escaneo no autorizado de la red. también se pueden utilizar técnicas de social engineering para obtener información de la víctima de manera indirecta, como, por ejemplo, engañando a un empleado para que revele información confidencial. No se debe olvidar que se puede encontrar información útil en la basura de la víctima (dumster diving). Entonces, se diseña la estrategia de ataque. Las técnicas de reconocimiento pueden ser activas (cuando se interactúa con el sistema informático de la víctima) o pasivas (cuando reúnen información obtenido de fuentes públicas).
2. **Escaneo o scanning:** utiliza la información recopilada para detectar las vulnerabilidades del sistema. Se utilizan herramientas utilizadas para recopilar la información de la red a través de comandos simples como *traceroute*. También se pueden utilizar herramientas de penetración (penetration testing tools) para probar las vulnerabilidades detectadas y determinar si se pueden explotar para obtener acceso. Un administrador debe controlar que no hay agujeros para que los hackers accedan, puesto que podrían buscar las vulnerabilidades de su software específico (vulnerability scanners).
3. **Obtención de acceso o gaining access:** no se necesita obligatoriamente conseguir acceso para dañar el sistema. La efectividad del atacante depende de la arquitectura y la configuración del sistema y de su propia destreza.
4. **Mantenimiento del acceso o maintaining Access:** se pueden utilizar los recursos del sistema o continuar explotando el sistema con un perfil bajo que evite ser detectado. Se instala una puerta trasera (backdoor) para poder volver a acceder sin ser detectado y se puede inocular en forma de troyano, por ejemplo.
5. **Borrado de huellas o covering tracks:** para mantener el acceso al sistema y para evitar tener consecuencias penales, los atacantes destruyen las evidencias que los puedan delatar. Hay huellas que se deben borrar en muchos ficheros log. Para esto, es necesario haber creado anteriormente la puerta trasera, así podrá eliminar sus datos y restaurar los ficheros alterados.

Las medidas de seguridad que hay que adoptar para proteger un sistema son:

- Política de contraseñas.
- Listas de control de acceso.
- Criptografía.
- Política de almacenamiento.
- Política de copia de seguridad.
- Protección ante el software malicioso (malware).
- Securización del software utilizado.
- Seguridad perimetral.
- Alta disponibilidad.
- La monitorización y detección de intrusiones (Intrusion Detection System - IDS)

Estas recomendaciones serán tratadas a lo largo de los temas.

1.5. Política de contraseñas

La autenticación es el proceso por el cual un entorno informático confirma la identidad de la persona que lo utiliza, es decir, es quien dice ser. Así mismo, no tiene por qué ser una persona ya que todo sistema informático se pone a disposición de otros procesos y servicios.

Este proceso requiere un uso de *credenciales*, las cuales debe conocer solo la persona identificada. Existen así mismo, muchos tipos de sistemas de autenticación: contraseñas, escáneres biométricos, tarjetas magnéticas, etc., e incluso algunos que son una combinación de dos o más criterios.

El uso de este proceso puede derivar en dos situaciones:

- Ser la persona correcta al identificarse
- No ser la persona correcta al identificarse

La segunda posibilidad deriva en otras dos posibilidades. Que no sea la persona correcta, o que sí sea la persona indicada pero no esté en funciones de identificarse, ya sea porque le ha sido retirado el permiso de acceso o ingreso al sistema (usuario bloqueado).

Cuando una persona se identifica en el sistema como usuario, la decisión de si puede o no realizar alguna operación, depende de los *permisos* que tenga asignados.

Llamamos *login* o acceso al sistema, al proceso por el cual una persona inicia la sesión en el sistema mediante una contraseña que autorice el ingreso. Por el contrario, llamamos *logout* o cierre de sesión cuando el usuario termina haciendo lo contrario.

La autenticación se basa en dos conceptos importantes:

- Las contraseñas son personales e intransferibles.
- Cada persona que vaya a utilizar un sistema informático necesita un usuario y contraseña personal.

Aparte de estos conceptos, existen recomendaciones dentro la seguridad al administrar un sistema: nunca se debe abrir sesión como usuario administrador, excepto para tareas que así lo requieran. Eso significa que la persona encargada dispone de *dos* usuarios para llevar a cabo las tareas del sistema.

Con esto garantizamos la seguridad de que, si una persona ajena al sistema o un *hacker* aprovecha y entra por los agujeros de seguridad del sistema, podrá hacer poco daño si no cuenta con los privilegios de administrador.

Cabe destacar que, si el servicio se está ejecutando con permisos de administrador, toda intrusión en el sistema se hace a través de esos permisos, con lo cual podrá hacer cualquier cosa, incluso borrar el rastro de su actividad.

Esta es la razón por la que nunca debemos iniciar sesión como usuario administrador. De hecho, muchos de los sistemas operativos modernos, permiten realizar diferentes tipos de tareas desde cuentas de usuarios limitados, tan solo solicitando lo que se conoce como *credencial de administrador*.

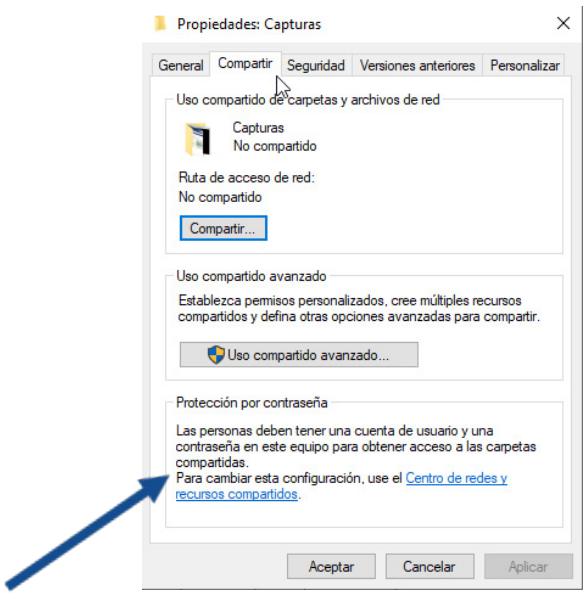

Imagen 7 Símbolo usado para especificar que esa operación requiere permisos del administrador.

En el caso de Linux, el usuario administrador recibe el nombre de *root*. Si queremos convertirnos en administrador, debemos ejecutar el siguiente comando en la consola:

```
Loading...

Welcome to JS/Linux (riscv64)

Use 'vflogin username' to connect to your account.
You can create a new account at https://vfsync.org/signup .
Use 'export_file filename' to export a file to your computer.
Imported files are written to the home directory.

[root@localhost ~]# su
[root@localhost ~]#
```

Imagen 8 Ejemplo de usuario root en una consola de comandos en Linux

Sin embargo, algunas distribuciones como Ubuntu modifican la forma del comando y utilizan otro diferente, con el fin de tener la misma validez, pero sin tener que entrar al sistema con el usuario administrador. Se trata de *sudo*, el cual solicita la contraseña del administrador para ejecutar el comando que hemos solicitado. Sin embargo:

No todos los usuarios pueden utilizar ese comando, tan solo los que pertenecen al grupo *sudoers*. De esta forma, se puede controlar que usuario puede usarlo y asignar los usuarios de confianza para ello.

El propósito de este método es buscar que no haya posibilidad de introducir la contraseña de root, evitando que ningún *malware* pueda capturarla.

1.5.1. Verificación en dos pasos

Es un nivel de seguridad superior que los sistemas suelen implementar. Se conoce también como *de doble factor*. Implica la introducción, además de la propia contraseña, de una prueba de identidad enviada al teléfono móvil del usuario. Lo más común, es que sea un código que se genera sobre la marcha y permite el acceso final al servicio. Suele ser un enlace sobre el que el usuario debe pulsar.

Imagen 9: Verificación de doble factor

La llamada *banca online* es un ejemplo de aplicación que utiliza este mecanismo de autenticación para la autorización de pagos y transferencias. *Software* como Drupal WordPress, que al fin y al cabo son CMS (Content Management System), suele disponer de *plugins* para incorporar al sistema un paso más ante la verificación, muchos de ellos basados en Google Authenticator, el sistema de Google capaz de verificar en dos pasos.

1.6. Listas de control de accesos (ACL)

Las listas de control de acceso (ACL) es la herramienta que utiliza el sistema operativo para gestionar los permisos de acceso. Estas listas especifican qué usuarios y grupos tienen acceso a un recurso determinado y con qué nivel de permisos. También pueden incluir excepciones o reglas especiales para ciertos usuarios o grupos. En general, las ACL se definen a nivel de sistema de archivos, pero también se pueden aplicar a otros recursos como impresoras, bases de datos o servidores de red.

El sistema debe darle acceso solo a los recursos a los que el usuario ha sido autorizado. Se consigue de la siguiente manera:

- Grupos de usuarios
- Listas de control de acceso

El administrador es el que, mediante *grupos* de usuarios, define en el sistema la jerarquía a la que pertenecen los usuarios. Un grupo no es más que un rol dentro del propio sistema, por ejemplo, "marketing", "dirección", "recursos humanos", etc. De la misma manera, un mismo usuario puede pertenecer a más de un grupo.

Normalmente, el sistema operativo contiene un grupo de usuarios que viene predefinido y es conocido como "Todos los usuarios". Es el grupo al que pertenecen todos los usuarios del sistema de manera automática. Existe otro grupo llamado "Usuarios conectados", al cual pertenecen todos los usuarios conectados al sistema. Encontramos más grupos dentro del sistema tales como "Usuarios del dominio" y "Administradores", al que pertenece, al menos, el usuario administrador de dicho sistema.

Es el administrador el que asigna los permisos a cada grupo, basándose en la cantidad de usuarios y grupos que existen. Por ejemplo, el administrador puede dar acceso a la carpeta *C:\Datos\Marketing* para que los usuarios que pertenezcan a los grupos "marketing" y "dirección" puedan trabajar en ella, mientras que el resto de los usuarios reciben un mensaje de error al intentar acceder.

Se recomienda asignar directamente los permisos a los grupos, nunca a los propios usuarios, hasta tal punto que se recomienda incluso crear un grupo nuevo, aunque sea un solo usuario el que tenga acceso a un recurso determinado.

1.6.1. Tipos de permisos

Los diferentes tipos de permisos dependerán del tipo de recurso (fichero, puerto, dispositivo, etc.). En el caso de que sea un fichero o una carpeta en concreto, va a depender del sistema de ficheros y del propio sistema operativo en los que se trabaje. Por ello, uno de los mejores sistemas de ficheros respecto al tema de permisos es Windows (con su sistema de ficheros NTFS). Pudiendo controlar las siguientes características:

- **Lectura**
  - Entrar en carpeta / ejecución del propio archivo
  - Listar carpetas / leer archivos
  - Leer atributos
  - Leer permisos
- **Escritura**
  - Crear archivos en carpeta / escribir datos
  - Crear carpetas / anexar datos
  - Escribir atributos
  - Eliminar subcarpetas y archivos
  - Eliminar carpeta / archivo
- **Administración**
  - Tomar control
  - Cambiar permisos
- **Control absoluto:** todo lo anterior

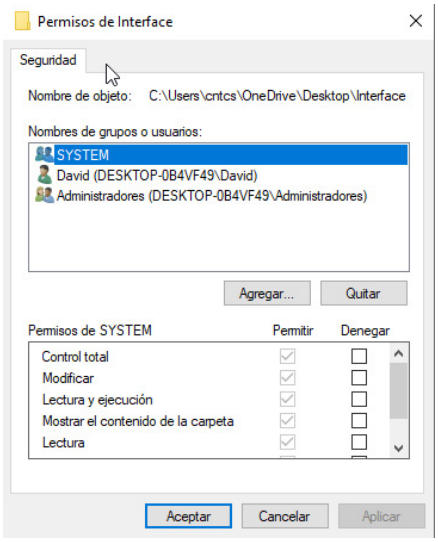

Imagen 10. Permisos de una carpeta en Windows

1.6.2. ACL

En un enrutado, las ACL son las listas con las condiciones que van a hacer que el tráfico que pasa por ese *router* tome un camino u otro también.

Las ACL toman valores como la dirección de origen y destino, los números de puerto y el protocolo superior para decidir si un paquete es aceptado o rechazado por un *router*.

En cada paquete que llega al *router* se realiza una serie de comprobaciones en las que el orden importa, ya que, si la primera condición ya se cumple, se sale de la ACL, sin comprobar el resto de las condiciones.

A modo de resumen, podríamos decir que las ACL son normas que se usan para el procesamiento de los paquetes que entran y salen del *router*.

Cada una de las interfaces de un *router* puede servir para salida y para entrada de paquetes, pero su ACL no tiene por qué ser el mismo para ambos, de hecho, suele ser diferente.

Lógicamente, si no hay ACL configuradas, se permite el paso de todos y cada uno de los paquetes por nuestro *router*.

Si queremos modificar una ACL, lo preferible es eliminarla y crearla de cero.

Por último, cabe destacar que en general la última línea de una ACL no se suele poner explícitamente y siempre es *denegar cualquiera*.

Hay varios tipos de ACL:

- **Estándar:** solo se comprueba la dirección de origen del paquete.
- **Extendidas:** se comprueba la dirección de origen, la dirección de destino, el protocolo y los puertos.
- **Dinámicas:** en este caso, se exige que haya autenticación en el *router* por parte del usuario vía *Telnet*.
- **Reflexivas:** en este tipo, se permite el tráfico saliente, pero se limita el tráfico de regreso a modo de respuestas al tráfico que se inicia en el *router*.
- **Basadas en tiempo:** se define un intervalo de tiempo real, donde se valida el tráfico de paquetes que pasa por nuestro enrutador.

Cada vez que llega un paquete al *router*, se valida si cumple las sentencias de la ACL en el orden en el que se han creado.

En cuanto cumpla con alguna de las sentencias, se para la comprobación.

```
Router(config)#
Router(config)#access-list 1 permit any
Router(config)#
```

Imagen 11. Creación de ACL en router Cisco

Siempre se suele colocar al final de la lista, por defecto, la sentencia implícita ***deny any***, que indica que, si ninguna regla anterior se ha cumplido, se deniega el paquete.

Para cada una de las tramas que se registran, el proceso con las ACL es el siguiente:

Si la trama se acepta, se procede a des encapsularla y se comprueba si hay alguna ACL funcionando en esa interfaz de entrada.

Si existe una ACL y además el paquete es denegado, se descarta.

Si no existe ninguna ACL o, aunque existente, el paquete es aceptado, se busca cual es la interfaz de salida en la tabla de enrutamiento.

Vemos si la interfaz que va a dar salida al paquete tiene asociada alguna ACL.

Si existe una ACL y además el paquete es denegado, se descarta.

Si no existe ACL, o se acepta el paquete con las sentencias, se da salida al paquete de datos.

El siguiente diagrama resume este proceso:

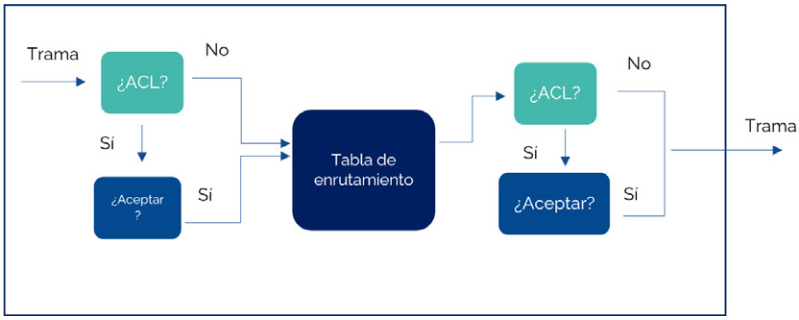

Imagen 11. Procesamiento de tablas con ACL

Los permisos que se pueden conceder o denegar dependen del sistema operativo. Ten en cuenta que la propia ACL es una información que se guarda junto con el archivo o carpeta en cuestión, ya que se trata de un conjunto de datos del mismo nivel que ponen a disposición del usuario sus fechas de creación, de actualización, tamaño, etc.

Permisos en Linux			
-	rwx	rwx	rwx
Tipo de archivo	Permisos de usuario	Permisos de grupo	Permisos de Otros

En el caso de los sistemas Unix (Linux), se utiliza el sistema de ficheros ext4, que solo dispone de los permisos de lectura, escritura y ejecución (rwx). Se pueden asignar dentro del propio fichero al dueño de este, al grupo y al resto de usuarios.

Esto correspondería a una ACL donde solo aparece el usuario dueño del archivo, el grupo al que pertenece y un grupo adicional llamado "Resto de usuarios". De manera que, para conseguir la misma singularidad que caracteriza a Windows, un administrador Unix (Linux) tiene que recurrir a la creación de varios grupos, asignando a cada usuario a varios de ellos. Es una tarea tediosa ya que requiere la entrada de todos los usuarios ya existentes si se desea crear un grupo nuevo.

Por fortuna, Linux permite permisos avanzados y ACL tal y como lo hace Windows. Basta con montar un sistema de ficheros con las opciones *acl* y *user_xattr*, y luego utilizar los siguientes comandos: *getfacl* y *setfacl*. Para leer y modificar respectivamente. Como hemos comentado sobre los sistemas empresariales, algunas distribuciones, como es el caso de Red Hat, han desarrollado sistemas más avanzados destinados únicamente al mundo empresarial.

Predominio de la denegación

La denegación prevalece sobre la *concesión*. Imagina un archivo con la siguiente configuración de permisos:

Grupo "marketing": permitir lectura.

Grupo "recursos humanos": denegar lectura.

Si se diese el caso de que un usuario pertenece a estos dos grupos, no podría leer el archivo, pues la denegación tiene preferencia. En inglés se conoce como *deny-first*.

Herencia de permisos

En cuanto a la herencia de permisos, es importante señalar que los permisos pueden ser heredados tanto de la carpeta padre como de otros objetos de seguridad (como grupos o usuarios), dependiendo de cómo se configuren las ACL.

Los permisos son *heredados* en las carpetas y archivos que incluyen. Cuenta con varias ventajas:

El propio administrador no tiene que asignar permisos a subcarpetas, a excepción de si van a diferenciarse de los de la carpeta superior.

Los nuevos ficheros y subcarpetas incluidas en la carpeta actual recibirán dichos permisos sin la actuación previa del administrador.

Incluso es posible *añadir* permisos a los permisos heredados ya existentes.

Permisos del administrador

El rol de administrador o el propio usuario reconocido en el sistema como administrador, no se ve afectado por ningún cambio en las ACL. De esta manera, si un archivo tuviera el permiso de lectura denegado para el grupo "Todos", aun así, el administrador podría leer dicho archivo.

Permiso en otro tipo de recursos

Las ACL se pueden utilizar para controlar el acceso a cualquier otro tipo de recursos, como son los *pendrives,* impresoras, puertos externos, etc.

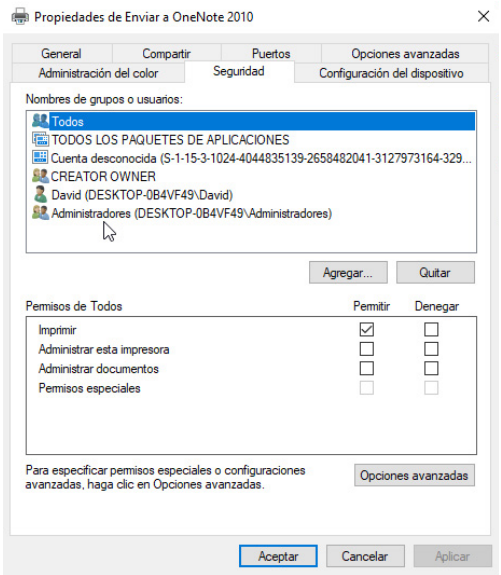

Imagen 12. Permisos y ACL de una impresora

Es responsabilidad directa del administrador del sistema asignar los permisos a todos los recursos, carpetas y archivos del sistema.

En los sistemas Linux, existe una manera de definir permisos a otros tipos de recursos, pero lo hace utilizando el directorio */dev*, donde todos los recursos están simbolizados en forma de ficheros virtuales.

1.7. Autenticación centralizada

Desde sus inicios, las redes de ordenadores (LAN), estudiaron el problema de la administración de usuarios. De entrada, los administradores debían reproducir la base de datos en todos los equipos por varios motivos:

- Un usuario podría requerir o necesitar iniciar sesión en cualquiera de los equipos.

  Para poder asignar los permisos correctos, el almacenamiento compartido debía conocer todos los usuarios que solicitan el acceso a los datos.

  Esto suponía una serie de problemas en cuanto al mantenimiento: altas y bajas de usuarios, cambios de contraseñas, etc. Por ese mismo motivo, de manera temprana se empezaron a implementar métodos de gestión centralizada entre los usuarios. De modo que:

  El administrador gestionaba únicamente una base de datos de usuarios y grupos.

- Todos los equipos cotejaban las credenciales del usuario que intentaba iniciar sesión.

1.7.1. Autenticación centralizada en Windows

Desde las primeras versiones de Windows Server (aun cuando se llamaba Windows NT), la gestión de usuarios del mismo *dominio* se regía a través de *Active Directory*. Un *dominio* es, un grupo de ordenadores conectados en red y con gestión centralizada cuya base de datos de usuarios se almacena junto con otra enorme cantidad de información. Todo este conjunto de datos se almacena en los denominados *controladores de dominio*. Debe estar disponible para sus equipos, por eso está en constante replicación, independientemente de que falle alguno de sus controladores.

La aplicación que permite la gestión de los usuarios se llama Usuarios y Equipos de Active Directory. Nos permite, a la misma vez, crear y eliminar usuarios, equipos y grupos.

Windows Server 2003 y sistemas anteriores, solo permitían una *política de contraseñas* lineal, ya que afectaba a todos los usuarios del dominio por igual. Windows 2012 y posteriores corrigen esta política y permiten definir diversas políticas de contraseñas y asignarlas a cualquier usuario o grupo.

1.7.2. Autenticación centralizada en Linux

Gracias al sistema llamado PAM (Pluggable Authentication Modules), que consiste en un conjunto de librerías destinadas a que el administrador elija el modo que usará el sistema y las aplicaciones para autenticar a los usuarios. PAM permite cambiar incluso la autenticación por contraseñas a otra por reconocimiento facial, por ejemplo. Esto se hace asignando a PAM una librería diferente, ya que el método reside en la forma de cifrar las contraseñas.

La forma de conseguir una gestión centralizada entre los usuarios de un sistema Linux, consiste en configurar PAM de manera que, pueda acceder a una base de datos en red a través de una librería especializada para ello. Destaca LDAP, sucesor de NIS, que nació mejorando las prestaciones de esta última.

1.7.3. Single sign-on

Este concepto hace referencia a la manera por la cual un usuario introduce sus credenciales una única vez, pero accede a diferentes aplicaciones que, normalmente, solicitan un inicio de sesión independiente. Un ejemplo de SSO puede verse en las aplicaciones *online* de Google. Si por ejemplo iniciamos sesión en Gmail, sería posible abrir otras aplicaciones sin volver a tener que introducir la contraseña, ya que pertenecen al mismo grupo. De igual manera, si cerramos la sesión en una de ellas, el resto queda totalmente inaccesible.

Este método exige la existencia de un servidor de identidades. Este servidor debe ser *accesible por todas las aplicaciones relacionadas*, las cuales almacenan las credenciales de los usuarios que acceden a ellas. Los datos que cada aplicación maneja son encapsulados en lo que se denomina *token de usuario*. Es lo que hace que puedas acceder a otra aplicación sin tener que volver a introducir la contraseña.

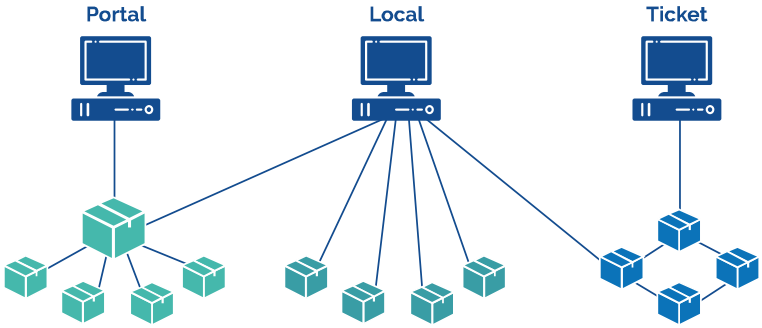

Imagen 13. Funcionamiento básico del sistema Single Sign-On

Dichas aplicaciones deben estar preparadas para que funcionen bajo este método, de modo que cuando reciben un inicio de sesión de cualquier usuario, deleguen esta tarea al servidor de identidades SSO.

Existen otro tipo de tecnologías como OpenID y AuthO, ambas diseñadas para simplificar la vida al usuario en el empleo de contraseñas. Cabe destacar que AuthO es una API, mientras que OpenID es un protocolo.

Single Sign-On (SSO) puede ser implementado tanto en sistemas Windows como Linux, y que existen diferentes proveedores de servicios de SSO, como Okta, OneLogin, Ping Identity, entre otros, además de los mencionados OpenID y AuthO.

1.7.4. Protocolos de autenticación

Existen numerosos protocolos de autenticación que garantizan los procesos de autenticación en la red. Se pueden identificar personas, equipos y procesos.

Podemos distinguir entre:

- **Protocolos de autenticación:** hace referencia a protocolos empleados por otros protocolos superiores, por ejemplo, certificados digitales o contraseñas de un solo uso.
- **Protocolos AAA (Authentication, Authorization and Accounting):** hace referencia a los protocolos que cuentan con un intercambio de mensajes y recopilación de información para autorizar el acceso.

El segundo protocolo hace uso de los primeros mencionados. Internamente, muchos protocolos cuentan con otros métodos de protocolo.

EAP (Extensible Authentication protocol)

Se trata de un sistema que transporta los métodos de autenticación por la red. PEAP (Protected EAP) transmite los protocolos EAP por un túnel cifrado.

Kerberos

Kerberos es un protocolo de autenticación que se utiliza para verificar la identidad de los usuarios en una red. Se basa en un sistema de tickets, donde un usuario se autentica ante un servidor de autenticación (AS) para obtener un ticket de sesión (TGT), que se utiliza para obtener tickets de servicio (TGS) de los servidores de recursos. El servidor de autenticación y el servidor de tickets suelen estar en la misma máquina, conocida como Centro de Distribución de Claves (KDC). Para asegurar que los tickets no sean falsificados o reutilizados, se utilizan claves criptográficas compartidas entre el usuario y los servidores. También es importante que los relojes de los servidores estén sincronizados para evitar problemas de expiración de tickets. En resumen, Kerberos es un protocolo seguro y escalable para la autenticación de usuarios en redes de computadoras.

El proceso que sigue este procedimiento es:

1. El cliente (usuario) solicita un Ticket Granting Ticket (TGT) al Servidor de Autenticación (AS).
2. El Servidor de Autenticación verifica la identidad del cliente y, si es correcta, envía un TGT al cliente.
3. El cliente cifra el TGT usando su propia clave y lo envía de vuelta al Servidor de Autenticación para su verificación.
4. Si el Servidor de Autenticación verifica que el TGT es auténtico, envía un Ticket Granting Server (TGS) al cliente.
5. El cliente envía una solicitud de acceso a un recurso específico al Servidor de Tickets (TGS) junto con el TGS recibido anteriormente.
6. El Servidor de Tickets verifica la autenticidad del TGS y, si es auténtico, envía un ticket de servicio (ST) al cliente.
7. El cliente envía el ST al servidor de recursos para acceder al recurso deseado.
8. El servidor de recursos verifica la autenticidad del ST y, si es auténtico, concede acceso al recurso.

Cada uno de estos pasos se realiza mediante el intercambio de mensajes entre los diferentes componentes de Kerberos.

Radius (Remote Authentication Dial-In User Service)

Es un protocolo que almacena los usuarios en una base de datos. El servidor comprueba que cierto usuario puede iniciar sesión con cierta contraseña a través de mensajes encapsulados en tramas UDP. Este proceso se utiliza, por ejemplo, con los routers domésticos. RADIUS es ampliamente utilizado en redes de telecomunicaciones y proveedores de servicios de internet para autenticar y autorizar el acceso de usuarios remotos a través de marcación telefónica, DSL, cable y otros medios de acceso.

Otros protocolos AAA (Authentication, Authorization and Accounting)

A lo largo del tiempo, se han necesitado la mejora de los protocolos de autenticación de los sistemas informáticos. Nuevas versionas han aparecido e, incluso, nuevos protocolos han surgido.

1.8. Política de almacenamiento

1.8.1. Redundancia

El almacenamiento redundante es aquel que utiliza dos o más unidades de almacenamiento. Una de sus características es que se replica la misma información, de forma que, si ocurre algún problema en una de ellas, seguimos teniendo acceso a los datos en las otras unidades disponibles.

Estos sistemas son los denominados RAID, y los podemos ver implementados tanto en la parte *software* como en la parte *hardware*.

Según la forma en la que realicemos la replicación de los datos entre ellos, existen varios niveles de RAID:

- **RAID 0:** distribuye equitativamente los datos entre los discos. En caso de avería, no se pierde toda la información, tan solo la mitad. Se utiliza con el fin de mejorar el rendimiento, ya que cuantos más discos, más velocidad de acceso.
- **RAID 1:** también conocido como *disco espejo*. Se copian los datos de forma idéntica en los discos ya que, si un disco falla, la información la seguimos teniendo disponible en el otro. Es el tipo más utilizado en las pequeñas y **medianas empresas.**
- **RAID 5:** también denominado *distribución con paridad*. En este caso, los datos se van a distribuir uniformemente, teniendo en cuenta que debe haber un mínimo de 3 discos. En caso de avería, los bloques perdidos son recalculados a partir de los otros discos.

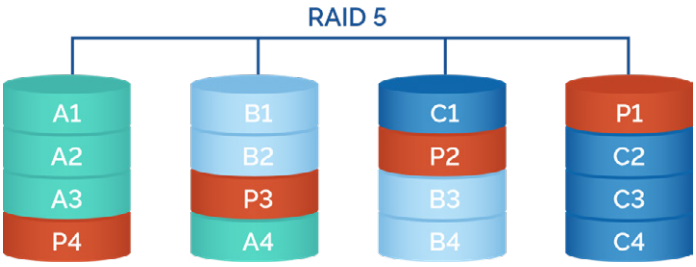

Imagen 14. Distribución de los ficheros en un sistema RAID 5

Por ejemplo, cuando falla un disco en un RAID 5, los datos los seguimos teniendo disponibles. Eso sí, el administrador debe sustituir el disco con la avería por otro nuevo. De esta manera, el sistema de manera automática reconoce el disco e inicia el proceso de réplica de datos, para reestablecer la situación de seguridad.

Ejemplos de RAID		
RAID 0: Un ejemplo de esto es cuando se usan dos discos duros en un ordenador para ejecutar juegos o aplicaciones que requieren de alta velocidad de lectura y escritura de datos.	**RAID 1:** Un ejemplo de esto es cuando se usan dos discos duros idénticos en un servidor web para almacenar información crítica de la empresa, de modo que si uno de los discos falla, se puede continuar trabajando con el otro sin pérdida de datos.	**RAID 5:** Un ejemplo de esto es cuando se usan tres o más discos duros en una empresa para almacenar grandes cantidades de información, como archivos de clientes o transacciones financieras. Si uno de los discos falla, los datos perdidos pueden ser reconstruidos a partir de los otros discos.

Casi siempre, el sistema RAID permite *la extracción en caliente* y suelen advertir de fallos en las unidades. Así que es recomendable la rápida actuación del administrador para sustituir los discos defectuosos, ya que algunos sistemas no permiten varios fallos al mismo tiempo.

Hot Spare

En términos de informática, es un disco "de repuesto". Se encuentra instalado en el sistema RAID, pero no se utiliza hasta que otro disco muestre síntomas de avería. Cuando el propio sistema detecta dicha avería, se replica la información en el *hot spare* y lo incluye en el RAID, dejando inutilizado el disco averiado.

La ventaja de este sistema es que el sistema RAID sigue funcionando de forma *degradada* hasta que el administrador sustituya el disco averiado por otro nuevo.

1.8.2. Disponibilidad

Se refiere a la capacidad de tener acceso a los datos en todo momento siempre y cuando sean necesarios y sin un horario preestablecido.

Con el fin de evitar averías en las unidades de almacenamiento, utilizamos métodos de almacenamiento redundante o almacenamiento distribuido, que permiten que el sistema informático seguir funcionando perfectamente y sin pérdida de datos.

Son los llamados sistemas de alta disponibilidad.

A través de un protocolo conocido como iSCSI, nos permite manipular discos remotos como si se tratase de una unidad física, particionarlos e incluso formatearlos. Es un protocolo comúnmente utilizado en sistemas virtualizados.

Necesitaremos una red de cableado óptico y de gran velocidad orientadas al almacenamiento iSCSI. Estas redes reciben el nombre de redes SAN, cuyos principales conceptos son los siguientes.

- **Iniciador iSCSI.** Es el equivalente al bus SCSI. Hacemos el control a través de la red.
- **Destino iSCSI.** Es un identificador para que pueda ser utilizado por los sistemas cliente.
- **iSCSI LUN.** Es la unidad que el servidor pone a disposición de los clientes

Imagen 15. Distribución red SAN

Todos los servidores NAS que podemos montar, permite la creación de este sistema pudiendo ocupar un disco completo o parte de él, de manera que, los demás equipos pueden crear un enlace para que puedan acceder simultáneamente y verlo todo como un disco local.

Para crear dicho destino, es necesario realizar lo siguiente:

1. Iniciaremos el servicio llamado *Iniciador de iSCSI de Microsoft*.
2. Abrimos la aplicación, definimos un *target* y automáticamente los destinos creados serán montados como si de un disco local se tratara, pudiendo tras cada arranque del sistema, acceder a él.

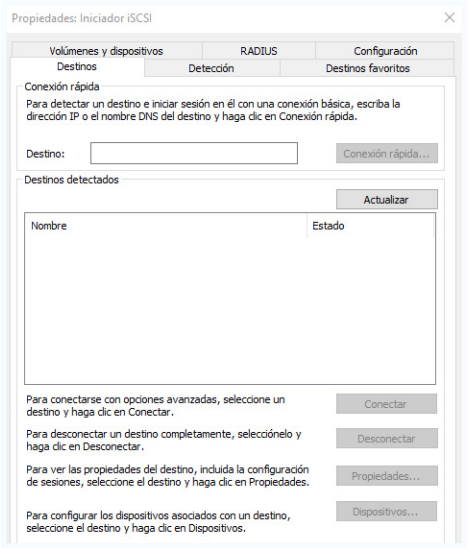

Imagen 16. Iniciador iSCSI de Windows.

Alta disponibilidad con NAS

NAS hace referencia a Network Attached Storage o almacenamiento conectado a la red. Estos servidores están diseñados para funcionar como clúster, proporcionando un servicio ininterrumpido (High Availability o HA). Uno de los NAS que forma el clúster actúa como servidor activo sirviendo los datos a la red; el otro NAS actúa como servidor pasivo esperando un fallo del primero para poder trabajar. La conexión de estos dos NAS se conoce como heartbeat connection.

Almacenamiento en la nube

El almacenamiento en la nube hace referencia a un tipo de almacenamiento que se encuentra alojado en servidores externos, ubicados en cualquier parte del mundo y solamente accesibles a través de internet. Este tipo de almacenamiento lo ofrecen compañías como Amazon, Dropbox, Google, etc.

Es un servicio de almacenamiento de datos remoto, pero no sabemos dónde se encuentran los servidores físicos que alojan los datos. Suelen tratarse de CPD enormes, continuamente procesando sus datos para garantizar rendimiento, disponibilidad y accesibilidad a todo aquel que tenga acceso. Debido a esto, se recomienda a las empresas ser metódicas con qué datos trabajan y en qué condiciones.

1.9. Política de copias de seguridad

Las copias de seguridad o *backups* son herramientas que se usan en la informática para respaldar la información de modo que si ocurre un incidente que suponga la perdida de información esta esté replicada en algún sitio y se pueda recuperar.

Cuando se hace una restauración de una copia de seguridad esto implica que se recupera toda la información contenida en la copia.

1.9.1. Tipos de copia de seguridad

Hay veces en las que no es posible realizar copias de seguridad completas de toda la información almacenada, ya sea por falta de recursos o porque no es lo deseado y por eso tenemos tres tipos de copias de seguridad:

- **Completas o totales:** este tipo de copias almacenan en el backup toda la información que albergamos. Además, activan el atributo o flag de modificado para todos los archivos.
- **Incrementales:** en este tipo de copias solo se copia lo que ha sido cambiado o modificar y desactivan el *flag* de modificar de los archivos que se copian.
- **Diferenciales:** solo se copian los archivos modificados.

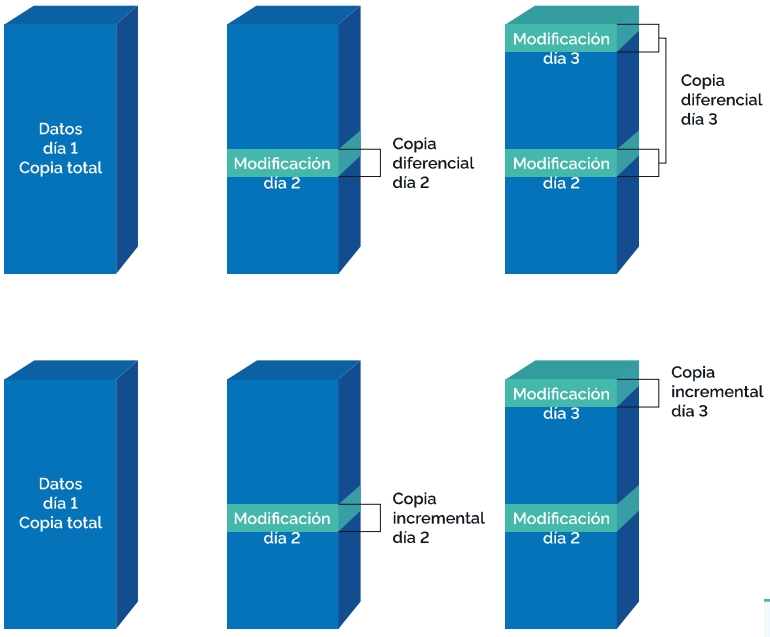

Imagen 17. Tipos de copia de seguridad.

La diferencia real entre una copia de seguridad incremental y una diferencial es que en la segunda nunca se desactiva el *flag* de modificado.

Es conveniente que las copias de seguridad no se espacien mucho en el tiempo, porque si por ejemplo realizamos una copia el lunes y los datos los perdemos jueves, los de martes y miércoles no se podrán recuperar.

¿SABÍAS QUÉ?

La diferencia real entre una copia de seguridad incremental y una diferencial es que en la segunda nunca se desactiva el flag de modificado.

Es conveniente que las copias de seguridad no se espacien mucho en el tiempo, porque si por ejemplo realizamos una copia el lunes y los datos los perdemos jueves, los de martes y miércoles no se podrán recuperar.

1.9.2. Elementos de la política de copias de seguridad

Esta política de seguridad se conoce como estrategia BCDR (Business Continuity and Disaster Recovery),

La política de copias de seguridad bien sea de usuarios particulares como de empresas, deben incluir los siguientes factores:

- Los datos que se desean salvaguardar y su origen.
- La frecuencia con la que se desea realizar una copia de seguridad y la temporalización de esta.
- El destino de las copias de seguridad, donde se almacenará la información.
- El tipo de copia, compresión y cifrado de datos que se quiere realizar.
- Quién custodiará las copias de seguridad.

El software de buckup permite la creación de diversos trabajos o tareas (Jobs o tasks) con distintas propiedades. Algunas empresas suelen combinar los planes de copias de seguridad, almacenando algunas tareas en el almacenamiento local y guardando otras en la nube. En caso de contener datos personales, se debe realizar un inventario del almacenamiento del backup, según el reglamento general de Protección de Datos.

1.9.3. Aplicaciones de copia de seguridad

A la hora de realizar copias de seguridad debemos de tener en cuenta los siguientes aspectos de manera fundamental:

- **Orden y claridad:** el nombre que le pongamos a la copia debe de ofrecernos una buena descripción de que contiene y de cuando es la copia.
- **Comprobación de las copias:** debemos de comprobar habitualmente si las copias de seguridad se realizan y si se encuentran en buen estado.
- **Localización:** debemos de intentar que las copias se almacenen en un lugar distinto al de la realización, porque en caso de fallo físico perderíamos ambas informaciones.
- **Automatización:** es conveniente que esta tarea se automatice para ahorrar costes.
- **Calendario:** todos los *backups* deben de estar planificados además de su tipo.
- **Simulacros:** es conveniente que se realicen simulacros de perdida de datos para poder comprobar que la restauración funcionaria.
- **Protección:** los *backups* deben de tener una protección igual a la del sistema cuando no superior para evitar ataques y filtraciones.

1.9.4. Restauración de copias de seguridad

Para restaurar una copia de seguridad solo tenemos que seguir los siguientes tres pasos:

1. **Paso 1.** Se restaura la última copia de seguridad total.
2. **Paso 2.** Si tenemos copias de seguridad incrementales se restauran de la más antigua a la más moderna siempre que sean posteriores a la copia de seguridad total.
3. **Paso 3.** Si tenemos copias de seguridad diferenciales y no haya ninguna total o incremental posterior, se restaura la más moderna de estas.

www.universae.com