Tema 3: Seguridad Pasiva

¿Qué aprenderás?

- Qué medidas se pueden tomar antes accidentes
- Qué medidas de acceso a un sistema basadas en algo física existen
- Qué es una copia de seguridad
- Qué es un CPD
- Qué es un NAS

¿Sabías que…?

- La temperatura en la sala de servidores es un parámetro básico para su buen funcionamiento

2.1. INTRODUCCIÓN

Ya tenemos clara la parte legal de toda la información que tenemos entre manos. Ahora lo que vamos a trabajar en ver cómo podemos hacer que esta información esté "segura".

Empezaremos por una parte interesante de la seguridad respondiendo a las siguientes preguntas:

"¿Qué pasa si se va la luz? ¿Qué pasa si un usuario se encuentra un disco USB en el suelo y lo inserta en el ordenador de la empresa, infectando el sistema y corrompiendo información? ¿Qué pasa si hay un incendio en el edificio?"

Cosas como estas y otras no podemos considerarlas como un ataque al sistema, sino que por causas "ambientales", hemos tenido un problema, es lo que vamos a trabajar en la **Seguridad Pasiva**.

Por lo tanto, podemos definir como Seguridad Pasiva como la parte de la seguridad informática que entra en acción para minimizar los daños causados por un usuario, un accidente o un programa maligno (**Malware**) en los sistemas.

2.2. AMENAZAS Y MEDIDAS

En la siguiente tabla tienen un listado de amenazas y medidas paliativas:

AMENAZAS	MEDIDAS
Suministro eléctrico: cortes, subidas y bajadas de tensión, distorsión y ruido en la señal	**Sistemas de alimentación ininterrumpida (SAI)** **Generadores eléctricos autónomos** **Fuentes de alimentación**
Robos o sabotajes: acceso físico no autorizado al hardware, software y copias de seguridad	**Control de acceso físico: armario, llaves, blindaje, biometría** **Vigilancia guardias y CCTV**
Condiciones atmosféricas y naturales adversas: temperaturas extremas, humedad excesiva, incendios, inundaciones, terremotos	**Elección adecuada de la ubicación de la sala de sistemas** **Centro de respaldo** **Mecanismos de regulación de temperatura y humedad**

Tabla: Amenazas y medidas paliativas

A continuación, vamos a desgranar algunos de las medidas que considero que debemos conocer:

2.2.1. EXTINTORES

Vamos a hablar poco sobre ellos, solo que sepáis los diferentes tipos que hay:

- Tipo A: Fuego provocado por material sólido: madera, papel o plástico
- Tipo B: Fuego provocado por líquido inflamable como alcohol y gasolina
- Tipo C: Fuego provocado por gas como butano
- Tipo D: Fuego provocado por metales como el sodio, magnesio o potasio
- Tipo E: Si hay riesgo de electrocución por conductores, baterías, etc.

Para el equipamiento informático se recomiendan los de CO2, anhídrido carbónico o un extintor polvo ABC.

2.2.2. SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI)

El **SAI** es un conjunto de baterías que alimentan una instalación eléctrica. Tiene una toma para conectarlo a la corriente y ofrece una serie de enchufes para conectar los equipos electrónicos.

Lleva un estabilizador de señal para evitar los picos de corriente que puedan dañar los equipos.

Su función es sencilla, en caso de fallo eléctrico los ordenadores conectados al SAI siguen funcionando porque consiguen electricidad de sus baterías. Como comprenderás, la vida de estas baterías no es eterna, por lo que, pasados unos minutos, si el corte no ha sido puntual y no se recupera inmediatamente el suministro, deberás ejecutar una parada ordenada de los equipos.

Dentro de la variedad que hay en el mercado los podemos clasificar como:

- SAI en estado de espera (**off-line**): este SAI se encuentra en paralelo con la toma de corriente, o sea, los equipos se alimentan del suministro principal. Cuando se produce el corte, el SAI activa sus baterías. Una vez finalizado el corte, se desactiva y las baterías empiezan a recargarse. Protegen ante fallos de suministro, subidas y bajadas de tensión. Su uso más común es el doméstico.

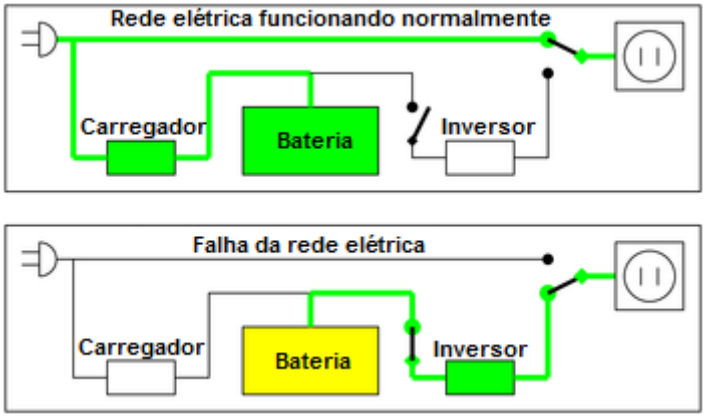


Imagen: Funcionamiento SAI Off Line
Fuente: Desconocida

- SAI Interactivo (**in-line**): es como el off-line, pero incorpora filtros activos para mejorar la tensión eléctrica. Su uso más común es en oficinas, equipos de clase media y baja, pequeños servidores.

- SAI en línea (**on-line**): este SAI se encuentra en serie con la toma de corriente, o sea, los equipos se alimentan de las baterías del SAI, por lo que ante un corte del suministro los equipos no tienen constancia de ello. Además de filtrar, convierte la señal eléctrica. Se destina a proteger servidores, clúster de equipos, instalaciones informáticas críticas, …

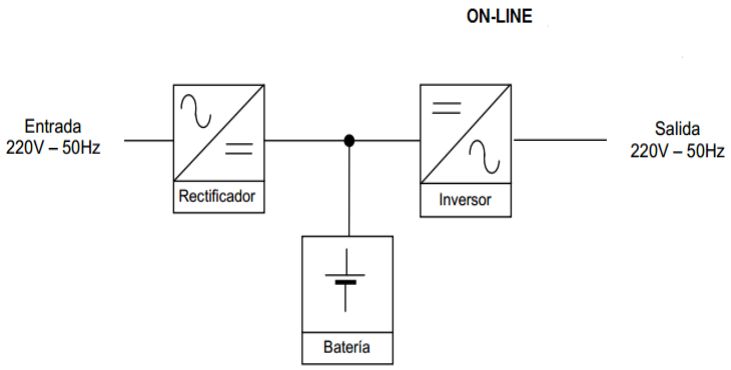


DIAGRAMA EN BLOQUES DE UN SAI

El problema para poder elegir un SAI es que tenemos que estimar el consumo de los equipos que vamos a conectarle. Como aproximación nos podemos guiar por las características de potencia que cada equipo tiene pegadas en la etiqueta de fabricante. Estos datos nos aparecerán en Wattios. Por ejemplo, un ordenador puede tener instalada una fuente de alimentación de entre 500 a 600 W. Un servidor NAS suele consumir entre 30 a 100 W, y un router, sobre 25 W. A la suma de toda esta potencia, ser recomienda redimensionarlo un 20%.

En base a lo que hemos hablado, hay tres características importantes más a la hora de seleccionar un SAI:

- El tamaño. Ocupa un volumen parecido al de un ordenador pequeño y el peso es superior.
- El tipo y cantidad de conexiones eléctricas con las que cuenta.
- La autonomía debe ser suficiente para poder guardar los datos y apagar el equipo informático o mantenerlo encendido. Lo normal es que oscile entre 3 y 4 minutos y los 30 o 40 minutos

2.2.3. EL CENTRO DE PROCESO DE DATOS O CPD

Es una sala especial que alberga los servidores manteniéndolos todos centralizados.

EL CPD tiene las siguientes **ventajas**:

- Un solo espacio para proteger y mantener
- No necesitamos cables largos o elementos intermedios que reducen el rendimiento
- Los técnicos no tienen que desplazarse a diferentes partes del edificio para realizar instalaciones, reparaciones y mantenimientos de los equipos

El CPD debe estar **protegido** al máximo:

- Elegiremos un edificio en una zona con baja probabilidad de accidentes naturales.
- También evitaremos la proximidad de ríos, playas, presas, aeropuertos, autopistas, bases militares, centrales nucleares, etc.
- Evitaremos ubicaciones donde los edificios vecinos al nuestro pertenezcan a empresas dedicadas a actividades potencialmente peligrosas: gases inflamables, explosivos, etc.
- Preferentemente seleccionaremos las primeras plantas del edificio.
- Se recomienda que el edificio tenga dos accesos y por calles diferentes.

- Es recomendable evitar señalizar la ubicación del CPD para dificultar su localización a posibles atacantes. La lista de empleados que entran a esa sala es muy reducida y saben perfectamente dónde está.
- Los pasillos que llevan hasta el CPD deben ser anchos porque algunos equipos son bastante voluminosos.
- El acceso a la sala debe estar muy controlado. Los servidores solo interesan al personal del CPD.
- En las paredes de la sala se deberá utilizar pintura plástica porque facilita su limpieza y se evita la generación de polvo.
- En la sala se utilizará falso suelo y techo porque facilita la distribución del cableado (para electricidad y comunicaciones) y la ventilación.
- La altura de la sala será elevada tanto para permitir el despliegue de falso suelo y techo como para acumular muchos equipos en vertical, porque el espacio de esta sala es muy valioso.
- En empresas de alta seguridad, la sala del CPD se recubre con un cofre de hormigón para protegerla de intrusiones desde el exterior.
- Instalaremos equipos de detección de humos y sistemas automáticos de extinción de incendios.
- El mobiliario de la sala debe utilizar materiales ignífugos.

Las máquinas del CPD hay que **protegerlas** ante:

- Temperatura. La temperatura del aire y los circuitos de los equipos generan mucho calor. Temperatura recomendable alrededor de los 22 grados.
- Humedad. Para evitarlo utilizaremos deshumidificadores.
- Interferencias electromagnéticas. El CPD debe estar alejado de equipos que generen estas interferencias.
- Ruido. Los ventiladores de las máquinas del CPD generan mucho ruido por lo que conviene introducir aislamiento acústico para no afectar a los trabajadores de las salas adyacentes.

En los CPD grandes se adopta la configuración de pasillos calientes y pasillos fríos**.** Las filas de equipos se colocan en bloques formando pasillos:

- **Pasillos calientes**: donde apuntan todos los ventiladores que extraen el calor de la máquina. En este pasillo se colocan los extractores de calor del equipo de climatización.
- **Pasillos fríos**: parte delantera de los equipos donde se introduce aire frío, generalmente a través del falso suelo utilizando baldosas perforadas

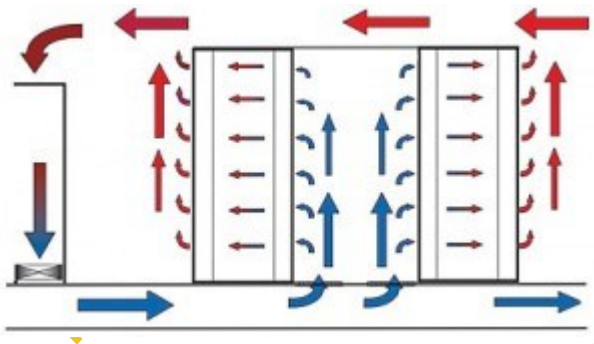


Imagen: Pasillos CPD

Fuente: http://blog.aodbc.es/2012/04/17/haz-tu-cpd-mas-verde-en-7-pasos/

El CPD necesita servicios de suministro eléctrico y comunicaciones. Es recomendable contratar con dos empresas distintas, de manera que un fallo en una compañía suministradora no nos impida seguir trabajando.

Suministro eléctrico

- El suministro eléctrico del CPD debería estar separado del que alimenta al resto de la empresa.
- Para los sistemas críticos, en los que la empresa no puede permitirse ninguna interrupción del servicio, deberemos instalar generadores eléctricos alimentados por combustible.

Comunicaciones

- Conviene que el segundo suministrador utilice una tecnología diferente al primero. Por ejemplo, si tenemos una conexión ADSL, el segundo no debería ser ADSL también, porque comparten el mismo cable hasta llegar a la central: un fallo en ese cable nos desconectaría de los dos suministradores.

Acceso

El acceso a la sala del CPD debe de estar especialmente controlado.

- Las máquinas solo necesitan ser utilizadas por un reducido grupo de especialistas.
- Las identificaciones habituales (contraseñas, tarjetas de acceso) se complementan con medidas más seguras, como la biometría.
- En instalaciones importantes, el CPD puede tener su propio equipo de vigilantes de seguridad.
- Se suele instalar también una red de sensores de presencia y cámaras de vídeo para detectar visitas inesperadas.

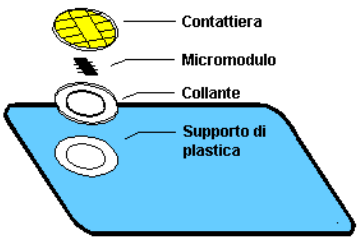
2.2.4. CREDENCIALES DE IDENTIFICACIÓN

Son medios físicos y/o lógicos que permiten nuestra identificación ante el sistema.

Los tenemos de tres tipos:

a) Credenciales físicas que posemos: las SmartCard

- **SMARTCARD**



Es una tarjeta de un tamaño variable que incorpora circuitos electrónicos integrados, que permiten almacenar un programa informático.

Contienen memoria no volátil y algún sistema de seguridad.

Nos encontraremos de diferentes tipos según su capacidad:

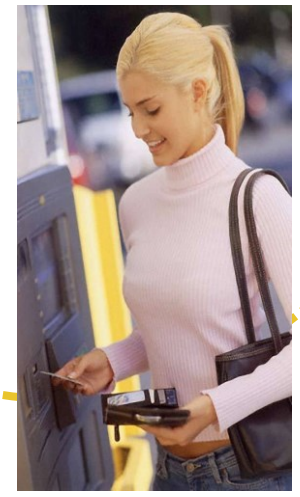
- Memoria. Solo contienen ficheros de información, no ejecutables. Son las tarjetas de identificación y control de acceso
- Micro procesadas. Tarjetas con estructura parecida a la de un ordenador y que contienen ficheros y aplicaciones de seguridad. Son las tarjetas de crédito
- Criptográfica. Contienen módulos de hardware que ejecutan algoritmos de cifrado y firmas digitales. Almacenan un certificado digital y su clave privada.

Las aplicaciones más comunes de estas tarjetas son:

- Identificación digital
- Control de acceso
- Monedero electrónico
- Firma digital
- Fidelización de clientes mediante descuentos o servicios especiales
- Sistema de prepago
- Tarjetas sanitarias

b) Credenciales lógicas que conocemos: el PIN

- **EL CÓDIGO PIN**



Esta foto de Autor desconocido está bajo licencia CC BY-SA-NC

Es un simple número que nos permite acceder con cierta seguridad a alguna operación cotidiana importante. El problema es que no es muy seguro. ¿Por qué? Por culpa del usuario. Solemos elegir números que no se nos olviden: años de nacimiento, combinaciones sencillas, mes/año… por lo que combinándolo con que suelen ser de cuatro cifras, un ataque de fuerza bruta o un poco de ingeniería social permite averiguarlo.

Como muestra, aquí tenéis los resultados de las pruebas de una empresa que recolectó un buen conjunto de contraseñas tras filtrase bases de datos con usuarios y contraseñas robadas en hackeos.

Aquí tenéis los más usados y con qué frecuencia se habían usado, ¿os suenan?

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

Imagen 1 PIN más usados

Fuente: Xataka

c) Credenciales fisiológicas que nos definen: la Biometría

- **BIOMETRIA**

La Biometría es una tecnología de identificación basada en el reconomiento de una característica física e intransferible de las personas: la huella digital o el reconocimiento facial.

Tiene dos características esenciales, es seguro y cómodo.

Entre sus aplicaciones teneos el control de acceso biométrico, el control de presencia biométrico, el login biométrico para aplicaciones informáticas o para cualquier otra que incorpore un lector biométrico para su integración.

De las tecnologías biométricas de la actualidad tenemos:

- Iris. Es la que da los resultados óptimos, pero es bastante incómoda
- Voz. Es práctica, pero está sujeta a cambios de voz debidos a enfermedad, ronquera y edad.
- Palma de la mano. Ocupa mucho espacio y alta tasa de error
- Firma. Es lo mismo que la voz, está condicionado por diferentes factores.
- Huella dactilar: es de las más usadas dentro de las aplicaciones móviles, donde la identificación debe de ser segura y cómoda para el usuario
- Vasculares del dedo. Utiliza el esquema de venas del dedo como patrón. No le afecta que el dedo esté dañado o erosionado.
- Facial. Permite identificación sin contacto, muy rápido y seguro.

2.4.5. ALMACENAR LA INFORMACIÓN

No podemos permitirnos una pérdida de información. Siempre puede producirse un fallo de hardware, humano o que se corrompa el sistema. Ante estas situaciones debemos poder recuperar la información lo más rápido posible. Esta es la base de la integridad y disponibilidad del sistema.

Para ello deberemos preocuparnos en:

- Comprar los mejores discos del mercado (el tiempo medio entre fallos del sistema deberá ser adecuado MTBF) y velocidad
- Almacenarlos en Servidores de Almacenamiento (NAS y SAN)
- Tener la información replicada en varios CPD
- Disponer de copias de seguridad

- **Almacenamiento en Red (NAS)**

Está orientada PYMES y usuarios profesionales. Se suele utilizar un equipo de la red con grandes prestaciones y que ofrezca discos para almacenar información al resto de usuarios de la red. Este equipo dispone de un software servidor con su propio protocolo. Los usuarios utilizarán un software cliente para conectarse al mismo. Actualmente se utiliza **CIFS** como evolución de **SMB**.

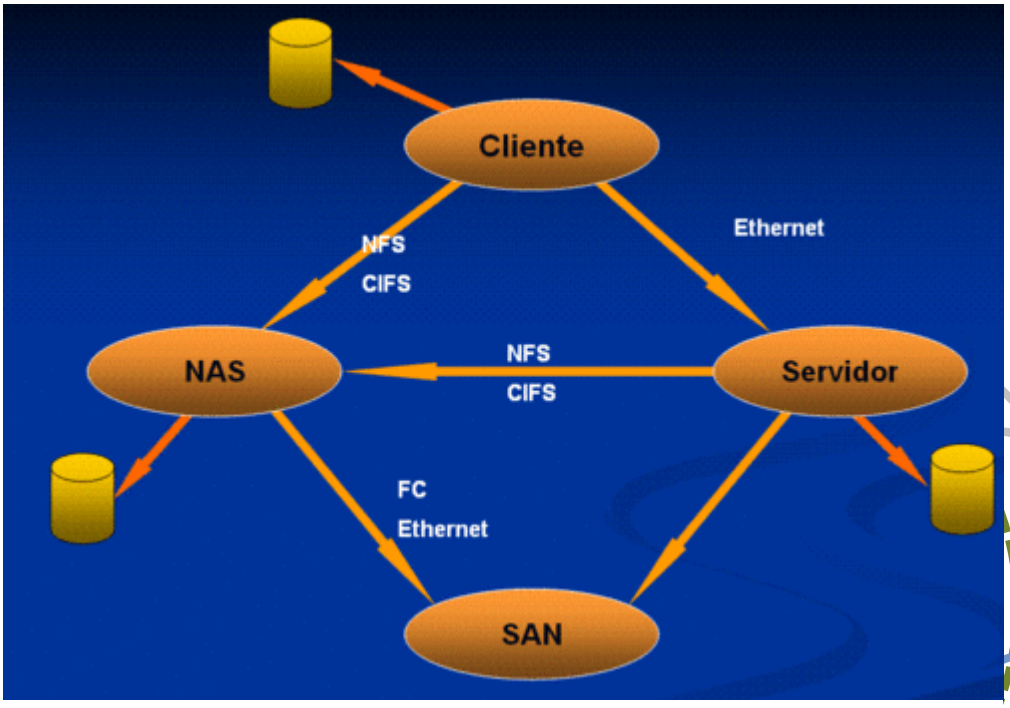
Este equipo, al disponer de varios discos, aplica técnicas RAID para aumentar el rendimiento y redundancia del sistema.

- **Área de almacenamiento en Red (SAN)**

En grandes entornos empresariales, con servidores, arrays de discos y equipos de respaldo, se opta por agrupar todos los discos en un único entorno centralizado, y organizar una estructura de red que permita un acceso más rápido a toda la información.

Habitualmente, la conexión son las SAM se realizan a través de redes dedicadas de alta velocidad, generalmente fibra óptica, y el protocolo iSCSI. Su tiempo de respuesta es muy bajo (prácticamente 0).

Actualmente se utilizan para almacenar grandes bases de datos y para virtualización de sistemas.



- **Almacenamiento en la nube (Cloud)**

Muchas empresas multinacionales (IBM, Apple, Microsoft, VMware) disponen de sus propios CPD y nos ofrecen el servicio de poder utilizar un espacio para nuestras necesidades de almacenamiento.

Normalmente los utilizamos cuando:

- Necesitamos compartir información con clientes
- Necesitamos acceder a información desde un equipo fuera de la empresa
- Deseamos realizar copias de seguridad de ficheros en otro lugar diferente

Este sistema nos proporciona una serie de ventajas:

- Podemos acceder a estos datos en cualquier lugar y hora (alta disponibilidad)
- La empresa proveedora se responsabiliza de su seguridad (copias de seguridad y control de versiones)

Pero tiene sus desventajas:

- Perderemos el control de acceso a nuestra información
- Debemos confiar a una empresa externa nuestra información
- Debemos confiar que aplican legislación y políticas de seguridad

Proveedores de estos servicios de almacenamiento tenemos:

- iCloud de Apple
- OneDrive de Microsoft
- Google Drive de Google
- Dropbox
- Box.net

El modelo es similar de venta es similar en todos los casos: te ofrecen un espacio gratuito de almacenamiento (aproximadamente 5 GB) y te presentan un plan de precios cuando necesitas aumentar tu espacio y/o servicios.

- **COPIAS DE SEGURIDAD (BACKUPS)**

Esta suele ser la primera medida de recuperación ante fallos de la información que se utiliza. El hacer copias de seguridad de los datos es un proceso que se puede automatizar y que se debe combinar con otras medidas como el RAID.

Primero de todo vamos a decidir dónde almacenaremos la copia de la información. Podemos hacerlo en una partición del disco duro. Esto no es una buena idea, pues si falla el disco se pierde todo, información y copia. Esto se suele utilizar más cuando queremos separar el sistema operativo de los datos. Realizamos una partición de sistema y otra de datos, así ante una nueva instalación no perderemos los datos. También podemos utilizar otro disco duro de la misma máquina o de otra máquina, o utilizar un disco duro de un NAS para almacenar las copias. Un sistema bastante extendido a nivel usuario y oficina es el disco duro extraíble. Es fácil de almacenar y de transportar.

Cuando hemos elegido el lugar de realización de la copia, vamos a ver de qué hacemos la copia. Tenemos la copia **completa**, que incluye toda la información que buscamos almacenar. Todo el disco con archivos y carpetas o toda la base de datos, por ejemplo.

Podemos incluir solo la información que ha cambiado desde la última vez que hicimos la copia completa. A esto lo llamamos copia **diferencial**

Y, por último, podemos almacenar la información que ha cambiado desde la última copia completa o diferencial. A esta copia la llamamos copia **incremental**.

Como puedes deducir, debemos realizar una combinación de la completa más una diferencial o incremental. Sin completa no podemos trabajar. Por lo tanto, tenemos que planificar una estrategia de copias de seguridad.

Una posible opción para una PYME sería:

- Una copia completa cada mes
- Una copia incremental cada dia
- Una copia diferencia cada semana

MÉTODO	ESPACIO	VELOCIDAD	PROCESO DE RESTAURACIÓN	TIPO DE COPIA
COMPLETA	MÁXIMO	MUY LENTO	MUY SIMPLE	POCOS DATOS PARA COPIAR
COMP + INCREMENTAL	MÍNIMO	RÁPIDO	COMPLEJO	MUCHOS DATOS QUE CAMBIAN FRECUENTEMENTE
COMP + DIFERENCIAL	INTERMEDIO	LENTO	SENCILLO	DATOS CUYA VELODAD DE CAMBIO ES MODERADA

Tabla: Políticas de Copias de Seguridad

- **EL PUNTO DE RESTAURACIÓN**

Los sistemas operativos Windows ofrecen una funcionalidad que consiste en generar un punto de restauración.

Este punto de restauración consiste en almacenar el estado del de los ejecutables y la configuración del sistema operativo, para que, en caso de fallo del sistema, poder volver a esa situación. Lo que no almacena es cambios en los documentos de los usuarios.

Si solo queremos proteger la configuración del sistema ante una instalación equivocada que nos produce fallos, podemos realizar una copia del Registro de Windows.

Recursos y enlaces

Backup con Linux. RSync:

Objetivo: En esta práctica vamos a realizar copias de seguridad de archivos de Linux, con la herramienta RSync, en un servidor remoto.

Después trabajaremos el empaquetar y comprimir con los comandos de Linux.

- https://youtu.be/VT6JQeio0sg
- https://youtu.be/-dBWFSzN3ac

Backup con Windows. Cobian Backup

Objetivo: En esta práctica vamos a realizar una copia de seguridad de una carpeta con un software llamado Cobian Backup.

- https://youtu.be/-aKQNCNu0D0

Copia de Seguridad en Linux. FWBackup

Objetivo: Aprenderás a configurar el programa FWBackup para realizar copias de seguridad de archivos y carpetas en entorno Linux.

- https://youtu.be/jkYSQnI9_iU

Recuperar Sistema Windows. Puntos de Restauración

Objetivo: Es esta práctica vamos a crear un Punto de Restauración del Windows 10 y probar su funcionamiento.

- https://youtu.be/D4g9digbuosSuper Computador Mare Nostrum https://www.bsc.es/

- Empresa de SAI https://www.saisempresas.com/

- Qnap https://www.qnap.com/es-es/

- Synology https://www.synology.com/es-es

- iCloud https://www.icloud.com/

- OneDrive https://onedrive.live.com/about/es-419/

- Google Drive https://www.google.es/drive

  HACER EL QR DE NUEVO

- Dropbox https://www.dropbox.com/

Test de autoevaluación

Cuando queremos realizar una copia de seguridad de toda la información del sistema, elegimos la opción

a) Integral
b) Completa
c) Diferencial
d) Total

Cuando queremos realizar una copia de seguridad de la información que se ha producido durante el dia, elegimos la opción:

a) Integral
b) Completa
c) Diferencial
d) Total

Indica qué almacenamiento de los siguientes tendrás físicamente en tu casa:

a) SAN
b) CPD
c) NAS
d) Cloud

Indica que tipo de SAI es el más frecuente que te puedes encontrar en un domicilio particular:

a) In-Line
b) On-Line
c) Off-line
d) Nadie tiene un SAI en su casa, es solo para empresas

SOLUCIONARIOS

Test de autoevaluación tema 3

Cuando queremos realizar una copia de seguridad de toda la información del sistema, elegimos la opción

a) Integral
b) Completa
c) Diferencial
d) Total

Cuando queremos realizar una copia de seguridad de la información que se ha producido durante el dia, elegimos la opción:

a) Integral
b) Completa
c) **Diferencial**
d) Total

Indica qué almacenamiento de los siguientes tendrás físicamente en tu casa:

a) SAN
b) CPD
c) **NAS**
d) Cloud

Indica que tipo de SAI es el más frecuente que te puedes encontrar en un domicilio particular:

a) In-Line
b) On-Line
c) **Off-line**
d) Nadie tiene un SAI en su casa, es solo para empresas

TEMA

Tema 3. Seguridad Pasiva

Administración de sistemas informáticos en Red

Seguridad y alta disponibilidad

Autor/a: Joaquín Erencia

Linkia FP