Seguridad y Alta disponibilidad

Capitulo 1 Principios de Seguridad y alta disponibilidad.

Principales objetivos de la seguridad informática:

- Detectar los problemas y amenazas a la seguridad (minimizar y gestionar los riesgos)
- Garantizar la adecuada utilización de recursos y aplicaciones
- Limitar perdidas y conseguir la recuperación del sistema en caso de incidente de seguridad
- Cumplir con el marco legal y requisitos a nivel organizativo.

Es necesario estar al día en esta materia.

Webs de interés en Seguridad:
http://www.inteco.es/blogs/inteco/Seguridad/BlogSeguridad/ultimos_articulos/
http://www.securitybydefault.com/
http://www.hispasec.com/
http://www.elladodelmal.com/

la **Seguridad absoluta** no es posible, por seguridad se entiende las Técnicas encaminadas a obtener altos niveles de seguridad, por ello se habla de **Fiabilidad** (probabilidad de que un sistema se comporte tal y como se espera de el), consiste básicamente en garantizar tres aspectos:

- **Confidencialidad**: Cualidad de un mensaje, comunicación o datos por la que solo pueda ser entendido por la persona a la que es enviado.
- **Integridad**: Cualidad de un mensaje, comunicación o datos que permite comprobar que no ha sido alterado.
- **Disponibilidad**: capacidad de un servicio, sistema o datos par ser accesibles y utilizable por los usuarios o procesos cuando se requiera.

Tienen que existir estos tres aspectos para que haya seguridad

Estos tres conceptos se estudian junto con:

- **Autenticacion**: Verificar que un mensaje pertenece a quien el documento dice (usuario, login, contraseña).
- **No repudio o irrenunciabilidad**: Permite probar la participación de las partes en una comunicación.
  - No repudio en origen: El emisor no puede negar el envió, la prueba la crea el emisor y la recibe el destinatario.
  - No repudio en destino: El receptor no puede negar la recepción ya que el emisor tiene pruebas de la recepción, creadas por el receptor y recibidas por el emisor.

Autenticaion:

- Algo que se sabe — por ejemplo una contraseña de acceso
- Algo que se tiene — por ejemplo una tarjeta de acceso
- Algo que se es — por ejemplo la huella dactilar

Orden requisitos seguridad: Disponibilidad → Confidencialidad → Integridad → Autenticacion → No repudio

Confidencialidad, La confidencialidad se puede conseguir encriptando archivos y programas.

- En windows es posible encriptar carpetas y archivos mediante **EFS** (Encrypted File System), tras seleccionar un archivo o carpeta en propiedades y opciones avanzadas esta la opción “Cifrar contenido para proteger datos”
- Existe un programa llamado LockNote que es una especie de bloc de notas que al guardar encripta la información con contraseña, el archivo resultante es un ejecutable .exe que contiene el programa y el texto contenido (como puede ser datos de usuarios y contraseñas, datos bancarios, etc.).

Integridad: Existe un malware denominado **rootkit**, que es un programa que sustituye los ejecutables binarios del sistema para ocultarse mejor, pudiendo servir de puerta trasera o backdoor para la ejecución remota, en windows la utilidad **System File Checker** (**SFC**) comprueba la integridad de los archivos de sistema.

- En Windows, en una terminal (cmd) ejecutamos **sfc** /scannow y se comprobaran todos los archivos de sistema (requiere que este insertado el CD de instalación para la comparación).
- En Linux se pude comprobar el Cheksum de un archivo con el comando md5sum "fichero" y comparar el resultado con el cheksum original.
- **Rootkit hunter** es una herramienta mas completa bajo GNU/Linux para revisar permisos de los ejecutables, buscar rootkits conocidos y comprobación de la integridad de archivos de sistema.

Disponibilidad, Identificar y analizar la disponibilidad de servicios o servidores, puertos abiertos y versiones de sistemas operativos que lo soportan. Nmap se utiliza en auditorias de seguridad (y también se puede utilizar en un primer ataque). Búsqueda de posibles vulnerabilidades por medio de:

- www.securityfocus.com Facilita informes sobre vulnerabilidades en aplicaciones y sistemas operativos.
- Nessus4 (www.nessus.org) Aplicación que detecta vulnerabilidades, para windows y Linux.
- MBSA (Microsoft Baseline Security analyzer), herramienta diseñada para analizar el estado de seguridad según recomendaciones de Microsoft.
- Nmap (www.insecure.org/nmap/) aplicación en modo comando o gráfico (znmap) que proporciona, versiones de sistemas operativos instalados, direcciones MAC e IP, puertos abiertos o cerrados y versiones de aplicaciones.

Del estudio y análisis de las **vulnerabilidades** (agujeros de seguridad de un sistema) se aprovechan los desarrolladores de exploits. El fin del **exploit** puede ser violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio (introduciendo **payload**, que es como un malware que mete el exploit) o como origen de otros ataques a terceros, hay aplicaciones que poseen un conjunto de exploits para aprovecharse de las vulnerabilidades conocidas como "metasploits"

Recomendación

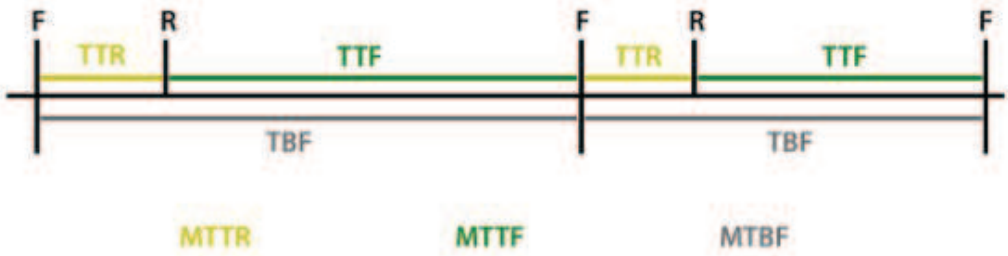
- ✔ Actualizar los sistemas.
- ✔ Aplicaciones configuradas con actualización automática.
- ✔ Activar la notificación de actualizaciones automáticas.
- ✔ Controlar la veracidad antes de instalar actualizaciones.

Actualmente existe software malicioso (malware) que sobrescribe las actualizaciones de aplicaciones conocidas.

Alta Disponibilidad, que es 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 critico, hay dos tipos de interrupciones:

- ➢ **Interrupciones previstas**, por ejemplo para realizar cambios o mejoras de hardware o software.
- ➢ **Interrupciones imprevistas**, son acontecimientos imprevistos (virus, desastres naturales, fallos hardware, etc.)

Las **métricas** utilizadas para medir la disponibilidad y fiabilidad de un sistema son **MTTF, MTTR y MTBF** Si F indica el momento en el que el dispositivo falla y R el momento en que está de nuevo disponible, gráficamente tenemos:



TTR (Time to repair), tiempo que se necesita para volver a poner en marcha el sistema
TTF (Time to failure), tiempo que pasa hasta que falla
TBF (Time between failures), tiempo entre fallos

- **MTTF** (Mean time to failure) Tiempo medio hasta que se produce un fallo.
  - MTTF = (Tiempo total de funcionamiento correcto) / (no fallos)
- **MTTR** (Mean time to repair) Tiempo medio que se tarda en poner de nuevo en marcha el sistema.
  - MTTR = (Tiempo total de inactividad) / (no fallos)
- **MTBF** (Mean time between failures) Tiempo medio entre fallos.
  - MTBF = (Tiempo total) / (no fallos)

Existen distintos niveles de disponibilidad, el mayor **nivel de exigencia** se obtiene **con los 5 nueves**: 99,999%, que acepta 5 minutos de inactividad al año.

Ejercicio de ejemplo:

1. Calcular el MTTR, MTTF y MTBF de un servidor que ha tenido 5 caídas en los últimos 3 meses. Las tres primeras se solucionaron en 5 minutos, pero las dos últimas supusieron un tiempo de inactividad de 30 y 40 minutos respectivamente.
   5 fallos en 3 meses

   3 meses -> 24 x 60 x 90 = 129600 minutos

   5 fallos -> 5 + 5 + 5 + 30 + 40 = 85 minutos

   129600 – 85 = 129515 minutos de funcionamiento correcto

   MTTR = 85 m / 5 = 17 m

   MTTF = 129515 / 5 = 25903 m

   MTBF = 129600 / 5 = 25920 m

2. ¿Qué porcentaje de disponibilidad ha tenido el servidor del caso anterior?
   25903 / 25920 = 0,9993 -> 99,93%

   otra forma quizás mas intuitiva:
   Tiempo funcionamiento/Tiempo total = 129515/129600= 0,9993 > 99,93%

3. ¿Cuánto tiempo puede estar inactivo al mes un equipo para conseguir la disponibilidad de 5 nueves?
   1 mes x 30 días/mes x 24 horas/mes x 60 min/hora = 43200 minutos tiene un mes

   100 -> 43200 m

   99,999 -> x

   x = 43200 x 99,999 / 100 = 43199,568 m que tiene que estar funcionando

   43200 – 43199,568 = 0,432 minutos (o sea, 25,92 s) de inactividad al mes, como máximo

Nota: si se deja instalando algo en Linux, se puede programar el apagado automático, ejecutando en otra terminal otro comando al de un tiempo, con: **sudo shutdown** -h +60 en este caso 60 indica al de 60 minutos se apagara.

Elementos vulnerables en el sistema informático y **que hay que proteger**:

- El software
- El hardware
- Los **Datos** es el elemento principal a proteger y el mas difícil de recuperar.

Las medidas de seguridad se contemplan a diferentes niveles: locales, personales/individuales y globales.

La seguridad informática desde diferentes perspectivas:

➢ Seguridad pasiva	Seguridad física, ambiental y copias de seguridad.
➢ Seguridad lógica	Control, usuarios, privilegios, contraseñas, software de seguridad antimalware y cifrado de la información.
➢ Seguridad en redes corporativas	Protocolos/aplicaciones seguras, SSH, TLS/SSL y VPN
➢ Configuraciones de alta disponibilidad	Redundancia RAID, balanceo de carga, virtualizacion.
➢ Normativa legal en materia de seguridad	LOPD y LSSICE

Las **amenazas** pueden ser provocadas por personas, condiciones físico-ambientales y software o lógicas.

➢ **Amenazas provocadas por personas**

➔ Dentro de una organización **el propio personal**.

➔ **Hacker**, que es un experto o guru en aspectos técnicos relacionados con la informática (White hat o Hacker y Black hat o Crackers)

- **Newbie** Hacker novato
- **Wannabe** Le interesa el haching pero al estar empezando no es reconocido por la elite.
- **Lammer** o Script-Kiddies Hacen hacking utilizando programas que buscan y descargan.
- **Luser** (looser + user) termino para referirse a los usuarios comunes despectivamente.

➔ **Pirata informático**, ciberdelincuente, personas dedicadas a realizar actos delictivos y perseguidos legalmente.

➢ **Amenazas físicas y lógicas**

➔ Las amenazas físicas y ambientales afectan a las instalaciones y/o el hardware que contienen.

- Robos, sabotajes, destrucción de sistemas
- Cortes, subidas y bajadas bruscas de suministro eléctrico.
- Condiciones atmosféricas adversas, humedad, temperatura extrema.
- Catástrofes naturales.
- Interferencias electromagnéticas.

➔ **Amenazas lógicas** (software o código que de una u otra forma afecta al sistema).

- **Herramientas de seguridad**, que detectan y solucionan fallos en los sistemas pero que también sirven para atacarlos.
- **Falsos programas de seguridad** (Rogueware), falsos antivirus y antiespias.
- **Puertas traseras** (backdoors), atajos que insertan los programadores en los programas.
- **Virus**, código que se adhiere o pega en un fichero ejecutable y lo infecta.
- **Gusanos** (Worm), programa que se ejecuta y propaga por si mismo generalmente en las redes.
- **Troyanos**, aplicaciones con instrucciones escondidas que parece que hace una cosa, pero realmente ejecuta otras funciones ocultas sin conocimiento del usuario.
- **Programas conejo** o bacterias, programas que no hacen nada util, solo se reproducen y dejan sin recursos el sistema.
- **Canales cubiertos**,

Técnicas de ataque, clasificación de las amenazas en función a la técnica empleada.

- **Malware** Se llama así a los programas malintencionados en general como virus, espías, gusanos, troyanos, etc.
- **Ingeniería social** Obtener información a través de la manipulación y confianza de usuarios legítimos, con el fin de obtener beneficios.
- **Scam** Estafa electrónica por medio del engaño como donaciones, transferencias, puede ser scam si hay perdida monetaria y hoax (bulo) si solo es engaño.
- **Spam** Correos o mensajes basura no solicitados.
- **Sniffing** Monitorar el trafico de una red para hacerse con información confidencial.
- **Spoofing** Suplantación de identidad o falsificación.
- **Pharming** Redireccion de un nombre de dominio a otra maquina falsificada y distinta.
- **Phishing** Estafa por suplantación de identidad e ingeniería social (acceso a cuentas bancarias)
- **Password cracking** descifrar contraseñas de sistemas y comunicaciones.
- **Botnet** Permite controlar los ordenadores infectados de forma remota.
- **Denegación de servicio** (DoS) Causar que un servicio o recurso sea inaccesible al usuario.
- **Tabnabbing** similar al **Phishing** se aprovecha del hábito de tener varias pestañas abiertas a la vez en el navegador, entonces cuando entramos a un sitio web aparentemente normal (pero que es parte de esta estafa), el mismo esperará a que cambiemos de pestaña para modificar su ícono, título y contenido, y hacerse pasar por alguno de los sitios que usamos habitualmente (como nuestro correo, redes sociales, bancos, etc). Al volver a esta pestaña, veremos una pantalla para ingresar los datos de acceso y creeremos que es porque nuestra sesión expiró, aunque obviamente se trata del sitio hostil que tomó la forma de uno conocido para nosotros.

Auditoria de seguridad de sistemas de información
Es el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades.

Objetivos de una auditoria:
- Revisar la seguridad de los entornos y sistemas.
- Verificar el cumplimiento de la normativa y legislación vigente (Ley de protección de datos).
- Elaborar un informe independiente

Estándares:
- ISO 27001 Define los requisitos de auditoria y sistemas de gestión de seguridad.
- ISO 27002 Código internacional de buenas practicas de seguridad de la información.

***Servicios de auditoria, fases**:

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

Tipos de auditoria

- Auditoria de seguridad interna — Nivel de seguridad de las redes locales y de carácter interno.
- Auditoria de seguridad perimetral — Perímetro de la red local, conectado a redes publicas.
- Test de intrusión — Se intenta acceder a los sistemas para comprobar el nivel de resistencia a la intrusión.
- Análisis forense — Análisis posterior de incidentes, mediante el cual se trata de reconstruir como se ha penetrado en el sistema.
- Auditoria de código de aplicaciones — Análisis del código independientemente del lenguaje empleado.

Las auditorias hay que realizarlas con cierta frecuencia.

Medidas de seguridad

- Según el sistema a proteger
  - Seguridad **física** — Trata de proteger el hardware.
  - Seguridad **lógica** — Protege el software.
- Según el momento en el que se pone en marcha las medidas de seguridad
  - Seguridad **activa** — son preventivas, de este tipo son la medidas de seguridad lógica.
  - Seguridad **pasiva** — son correctivas, posteriores a un ataque o incidente, de este tipo son las medidas de seguridad física y copias de seguridad.

Capitulo 2 Seguridad pasiva

Principios de la seguridad pasiva

La seguridad pasiva son las acciones o medidas posteriores a un ataque o incidente.

Amenazas	Medidas paliativas
Suministro eléctrico: cortes, variaciones del nivel medio de tensión (subidas y bajadas), distorsión y ruido añadido.	- Sistema de alimentación ininterrumpida (SAI o UPS). - Generadores eléctricos autónomos. - Fuentes de alimentación redundantes.
Robos o sabotajes: acceso físico no autorizado al hardware, software y copias de seguridad	- Control de acceso físico: armarios, llaves, blindaje, biometría. - Vigilancia mediante personal y circuitos cerrados de televisión (CCTV).
Condiciones atmosféricas y naturales adversas: temperaturas extremas, humedad excesiva, incendios, inundaciones, terremotos.	- Elegir la correcta ubicación de sistemas, teniendo en cuenta en la construcción la probabilidad de catástrofes naturales y ambientales. - Centro de respaldo en ubicación diferente al centro de producción. - Proporcionar mecanismos de control y regulación de temperatura, humedad, etc.

Las **consecuencias de las amenazas** son:

- Perdida o mal funcionamiento del hardware.
- Falta de disponibilidad de servicios.
- Perdida de información.

Copias de seguridad

Las copias de seguridad o backup son replicas de datos que nos permiten recuperar la información original en caso de ser necesario.

Modelos de almacenamiento:

- **DAS** (Direct Attached Storage) Método tradicional, el propio disco duro del ordenador.
- **NAS** (Network Attached Storage) Almacenamiento conectado en Red.
- **SAN** (Storage Area Network) Dispositivos de almacenamiento conectados a una red de alta velocidad.

Modelos de almacén de datos

- Desestruturados DVD, memorias USB, discos duros con una mínima información de que ha sido copiado y cuando.
- Estructurados Se dividen en tres tipos de copias
  - ✔ Completa, total o integra Copia total de todos los datos.
  - ✔ Incremental Copia de los archivos que han cambiado desde la ultima copia.
  - ✔ Diferencial Copia de los archivos que han cambiado desde la ultima copia total.

Recomendación sobre el tipo de copia a efectuar

- Si el volumen de datos de nuestra copia de seguridad no es muy elevado, lo mas practico es realizar **siempre copias totales**.
- Si el volumen de datos de nuestra copia de seguridad es muy elevado, pero el volumen de datos que se modifican no lo es, se hace copia total y posteriormente realizar **siempre copias diferenciales**.
- Si el volumen de datos de nuestra copia de seguridad es muy elevado y el volumen de datos que se modifican también lo es, las copias diferenciales ocuparan mucho espacio y lo mas practico es realizar una primera copia total y posteriormente realizar **siempre copias incrementales**.

Método de copia	Espacio de almacenamiento	Velocidad de copia	Restauración	Copia recomendada
Completo	Máximo	Muy lento	Muy simple	Pocos datos a copiar
Completo + Incremental	Mínimo	Rápido	Compleja	Muchos datos que cambian frecuentemente
Completo + diferencial	Intermedio	Lento	Sencilla	Datos cuya velocidad de cambio es moderada

Tipo de copia	Lee atributo de archivo (A)	Modifica atributo del archivo (A)
Total	NO	SI
Diferencial	SI	NO
Incremental	SI	SI
Diaria	NO	NO
Copia	NO	NO

Ejemplo de planificación de copia de seguridad:

- Todos los días 1 de cada mes, a las 23:00 horas: copia de seguridad total.
- Todos los viernes a las 23:00 horas: copia de seguridad diferencial desde la copia del día 1.
- Todos los días (excepto los viernes y el día 1) a las 23:00 horas: copia de seguridad incremental desde la copia del día anterior.

Regla 3 2 1 de copias de seguridad:

- ✔ Tener 3 copias de seguridad diferentes (original y 2 copias).
- ✔ Tener 2 soportes diferentes
- ✔ Tener 1 copia fuera de la empresa.

Copias de seguridad con Herramientas del sistema (opciones):

- **Compresión** disminuye el espacio ocupado.
- **Duplicación** copias de seguridad duplicadas en un segundo soporte.
- **Cifrado**
- **Nombre del archivo** suele incluir el tipo de copia y la fecha, ejemplos:
  - copiatotal_01En11.tar.bz2
  - copiadiferencial_2012Enero15.tar.bz2

GNU/Linux

Bajo Linux se usa el comando **tar** que es un empaquetador de archivos junto con **cron** para automatizar las tareas.

- **TAR**
  - empaquetado, opciones mas comunes:
    - tar -vcf nombre_archivo.tar nombre_carpeta_a_empaquetar
    - v: (verbose) permite obtener una descripción de los archivos empaquetados/desempaquetados
    - c: (create/vrear) crea un archivo tar
    - f: (file/archivo) indica que se dara un nombre al archivo tar
    - --newer=fecha: realiza un empaquetado incremental teniendo en cuenta que archivos han sido modificados, desde la fecha que se le indique.
  - Desempaquetado, opciones mas comunes:
    - tar -tvxf mi_archivo.tar
    - t: ver el contenido (sin extraer)
    - x: (extract/extraer) extrae los archivos en la carpeta que contiene el tar

- **CRONTAB**
  - La sintaxis es crontab [-e] -l [-r] [usuario]
    - el parámetro -e indica la edicion del cron
    - el parámetro -l ver las tareas programadas en el archivo cron
    - el parámetro -r borrar un archivo cron
    - si no se especifica el usuario, el comando se ejecutara para el usuario en sesión.
      crontab -e y dentro estas las lineas de texto con las programaciones:
      * * * * * comando_o_programa_a_ejecutar
      Cada asterisco en orden significa:
      Minuto (0 -59) **Hora** (0 – 23) **Día del mes** (1 – 31) **Mes** (1 – 12) **Día de la semana** (0 – 6) 0 domingo
      0 3 * * 5 /usr/bin/backup ejecuta el programa backup todos los días viernes a las 3 de la mañana

Ejemplo script para realizar una copia total de una carpeta determinada:

```
#!bin/bash
#Script de copia total
#variable con los directorios que se copian
directorio="/home/juan/carpeta"
#variable con el directorio  donde se guarda la fecha del ultimo backup
fechacopia="/home/juan/copia"
#variable con el directorio donde se guarda la copia
backup="/home/juan/copia"
fecha=`date +"%y%b%d"` #fecha de la copia con formato año mes dia
#El comando tar empaqueta los archivos de directorios contenidos en $directorio
#Con 2> redirigimos los mensajes de error al fichero errores_$fecha.txt
tar -vcf $backup/copiatotal_$fecha.tar $directorio 2> $backup/errores_$fecha.txt
#escribo en el fichero logscopias.txt las fechas de las copias totales hechas
echo Copia total realizada_$fecha >> $backup/logscopias.txt
#Se da permisos de ejecucion con: chmod u+x copiatotal.sh
#
#Se ejecuta en terminal con: sh copiatotal.sh
#
#Si en errores sale Removin leading '/' from member names indica que al
#descomprimir quita la primera / de tal manera que se descomprime a partir de
#donde este el fichero copia
#ahora se realiza una copia del backup en otro sitio remoto con scp
scp $backup/copiatotal_$fecha.tar usuario@IP:/home/usuario
#donde usuario es el nombre asignado y IP la direccion IP del servidor
```

Windows
En windows existe una utilidad para las copias de seguridad, bajo comando en terminal con: ntbackup o gráficamente en Inicio – Todos los programas – accesorios – Herramientas del sistema – 'Copia de seguridad'

Las opciones de copia de seguridad son:

- Total — Copia todos los datos seleccionados y marca el archivo como copiado, no tiene en cuenta el atributo A, pero si lo modifica una vez copiados.
- Diferencial — Copia todos los archivos modificados desde la ultima copia Tota o Incremental, no modifica el atributo A, pero si hace uso de el.
- Incremental — Copia todos los archivos que han cambiado desde la ultima copia total o incremental realizada, hace uso del atributo A y lo modifica una vez copiados.
- Diaria — Hace una copia de los archivos modificados en el día indicado.
- Copia — Copia los datos de un lugar a otro, no tiene en cuenta el atributo A ni lo modifica,

Ejemplo de script bach de copia de seguridad:

```
@ECHO OFF
REM Hace copia de seguridad total del contenido de la carpeta Mis documentos y lo guarda en el escritorio
ntbackup backup "C:\Documents and Settings\ral\Mis documentos" /m copy /f "C:\Documents and Settings\ral\Escritorio\total_1.bkf" /j "CopiasSAD total"
REM Hace copia de seguridad diferencial del contenido de la carpeta Mis documentos y lo guarda en el escritorio
ntbackup backup "C:\Documents and Settings\ral\Mis documentos" /m differential /f "C:\Documents and Settings\ral\Escritorio\diferencial_1.bkf" /j "CopiasSAD diferencial"
```

Ejemplo de script bach para subir un fichero por ejemplo de copia de seguridad a un servidor ftp.

```
ftp -s:Envio_a_FTP.txt 192.168.7.111
```

El archivo txt al que se hace referencia contiene lo siguiente:

```
sad
contraseña
bin
put Backup_completo.bkf
bye
```

Tanto el archivo txt como el archivo a subir (Backup_completo.bkf) han de estar en el mismo directorio desde el que se ejecuta el script.

Copias de seguridad mediante aplicaciones

- En windows tenemos:
  - Cobian Backup (http://www.cobiansoft.com/cobianbackup.htm). Aplicación de Backup para windows, con muchas opciones, incluida la compresión y encriptacion, tambien poder subir el archivo de copia a un servidor.
- En Linux
  - fwbackups (http://www.diffingo.com/oss/)

Recuperación de datos, es posible recuperar archivos borrados mediante una serie de aplicaciones:

- Windows
  - Recuva. (http://www.piriform.com/recuva) Aplicación de recuperación de archivos borrados.
- GNU/Linux
  - Testdisk
  - Foremost
  - Scalpel
  - SpinRite (de pago)

Centros de procesado de datos (CPD)
Se denomina procesamiento de datos o CPD a aquella ubicación donde se encuentran todos los recursos necesarios para el procesamiento de la información de una organización. Se conoce también como Centro de computo o Centro de calculo, en ingles **Data center**. Estos recursos consisten en unas dependencias acondicionadas, servidores y redes de comunicaciones.

El factor mas importante para la creación de los CPD es **garantizar la continuidad y alta disponibilidad**, los requisitos generales son:

- **Disponibilidad y monitorizacion** "24x 7x 365", disponibilidad, confianza y accesibilidad los 365 días del año.

- **Fiabilidad infalible** (5 nueves), 99,999% de disponibilidad.

- **Seguridad, redundancia y diversificación**. Almacenaje exterior de datos, tomas de alimentación independientes, SAIs y servicios de telecomunicaciones

- **Control ambiental/prevención de incendios**, Control de la calidad del aire, temperatura, humedad, electricidad, fuego, etc.

Según las recomendaciones la temperatura debe ser de 22'3ºC o en el margen de 15 a 23ºC y una humedad de entre 40% a 60%. Es necesario disponer de un **Plan de contingencia** corporativo con las actuaciones en caso de incidente.

Control de acceso físico, a las personas se las puede identificar por:

- **Algo que se posee** como una tarjeta de acceso, una llave, etc.
- **Algo que se sabe** como una contraseña, numero de identificación que se solicitar a su ingreso.
- **Algo que se es** como las huellas digitales, firma escrita, ojos, voz, etc.

Un rack normalizado para equipamiento informático tiene un ancho normalizado de 19 pulgadas.

Sistemas biometricos, son sistemas muy seguros:

- **Huella** digital
- Verificación de **voz**
- Verificación de patrones **oculares**
- Verificación Automatica de **Firmas** (VAF)

Circuito cerrado de televisión (CCTV) y Cámaras IP.

Sistemas de alimentación ininterrumpida (SAI)
Un SAI o UPS es un dispositivo que gracias a sus baterías puede proporcionar energía eléctrica tras un corte de suministro eléctrico.

Otra función de un SAI es mejorar la calidad de la energía eléctrica, filtrando subidas y bajadas de tensión así como eliminado armónicos de la red eléctrica.

Tipos de SAI:

- **SAI OffLine**, No estabilizan la corriente y solo generan la tensión cuando se produce un corte eléctrico

- **SAI InLine** o Interactive, Estabilizan la corriente incorporando un estabilizador de salida y solo generan la tensión de salida cuando se produce un corte eléctrico.

- **SAI OnLine**, Generan siempre la tensión de salida nueva independientemente de la entrada.

Los SAI disponen de funciones de conexión para monitorizacion y consulta del estado remoto, mediante puerto serie o USB y un software especifico.

Algunos de los eventos que muestra el software de un SAI son: Estado de la Batería, sobrecarga de salida, Fallo Red, Tiempo restante en caso de fallo, etc.

La potencia de los SAI o UPS viene definida en **VA** (Voltiamperio) que es la potencia aparente o efectiva consumida por el sistema.

En continua la potencia se mide en vatios (W) y es el resultado de multiplicar la tensión en voltios (V) por la intensidad en amperios (A), sin embargo en alterna para equiparar los vatios (w) a voltiamperios hay que multiplicar los vatios por 1,4 y así tener en cuenta el pico máximo de potencia que puede alcanzar el equipo, de esta manera se obtiene la potencia aparente (VA), así **W*1,4=VA**.

Así mismo se recomienda dejar un margen de potencia sin usar en el SAI, por lo que se recomienda que el consumo de todos los equipos conectados no sobrepase el **70% de la capacidad total del SAI**.

Ejercicio de ejemplo calculo SAI:
Calcular los VA de una SAI que debe tener conectados a tomas de batería los siguientes equipos:

- 3 torres de 180 w c/u
- 2 monitores LED de 10 w c/u
- 1 router de 0,2 A
- 2 switches de 0,1 A
- 1 impresora de 200 VA

Solución:

- 3 torres de 180 w c/u → 3 x 180 x 1,4 = 756 VA (VA = w x 1,4)
- 2 monitores LED de 10 w c/u → 2 x 10 x 1,4 = 28 VA
- 1 router de 0,2 A → P = V x I
  0,2 x 220 = 44 w
  44 x 1,4 = 61,6 VA
- 2 switches de 0,1 A → Todo lo anterior, pero en un paso
  2 x 0,1 x 220 x 1,4 = 61,6 VA
- 1 impresora de 200 VA → 200 VA

Suma Consumos calculados en VA: 756 + 28 + 61,6 + 61,6 + 200 = 1107,2 VA en total

Necesitamos una SAI que al 70% (p. ej) de capacidad nos de los 1107,2 VA calculados.

1107,2 – 70%
x – 100%

x = 1107,2 x 100 / 70 = **1581,71 VA** deberá tener, como mínimo, la SAI que buscamos.

Capitulo 8 Configuraciones de Alta disponibilidad.

Alta disponibilidad se refiere a la capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento, debido a su carácter critico, las **soluciones** adoptadas son:

- **Redundancia en dispositivos hardwar**e, de tal manera que ante un fallo continué el servicio, por ejemplo duplicados de equipos, servidores, fuentes de alimentación redundantes o dispositivos de red redundantes.
- **Redundancia, distribución y fiabilidad en la gestión de la información**, por ejemplo:
  - ✔ Sistemas RAID de almacenamiento.
  - ✔ Centros de procesamiento de datos de respaldo, garantizando copias de seguridad en distintas ubicaciones.
- **Redundancia en las comunicaciones**, por ejemplo dos salidas a internet con dos proveedores distintos de tal manera que si falla uno se mantenga la conexión con el otro (Balanceo de carga).
- Independencia en la administración y configuración de aplicaciones y servicios. Por ejemplo con la **virtualización** que ofrece servidores dedicados independientes bajo una misma maquina.

RAID (Redundant Array of Independent Disks), es un conjunto de discos independientes entre los que se distribuye o replica la información y que puede ser gestionado por:

- ✔ **Hardware**,: el control se realiza por medio de tarjetas controladoras RAID dedicadas que gestionan el control de los diferentes discos.
- ✔ **Software**: Es el sistema operativo el que gestiona los discos mediante una controladora de discos tipo IDE, SATA, SCSI, etc.
- ✔ **Híbridos**: son los que están basados en software y hardware, con controladoras RAID baratas.

Las configuraciones RAID estándar son:

- ✔ **RAID 0** o data striping: conjunto dividido, distribuye los datos equitativamente entre dos o mas discos sin información de paridad que proporcione redundancia, incrementa el rendimiento pero si falla un disco se pierden los datos.
- ✔ **RAID 1** o data mirroring: conjunto espejo, crea una copia exacta de los datos en dos o mas discos, si falla uno de los discos la información no se pierde al estar replicada en otro disco.
- ✔ **RAID 5**: conjunto dividido con paridad distribuida, requiere un mínimo de tres discos, consiste en una división a nivel de bloques distribuyendo la información de paridad entre los discos miembros del conjunto, gracias a la información de paridad si falla un disco la información no se pierde.

Balanceo de carga, consiste en un dispositivo hardware o software que reparte las peticiones de los clientes entre los diferentes servidores a los que se conecta dicho dispositivo, un ejemplo es cuando tenemos dos router distintos y cada un con un proveedor de internet diferente y hacemos que las peticiones que se hacen hacia internet por parte de los usuarios de la red salgan repartidas entre dichos router.

Virtualización, permite la ejecución simultanea de distintos sistemas operativos sobre una aplicación ejecutada y soportada bajo un equipo y sistema operativo determinado.