TEMA 2: SEGURIDAD PASIVA: HARDWARE Y ALMACENAMIENTO

1. UBICACIÓN Y PROTECCIÓN FÍSICA

Los equipos informáticos mas importantes de la empresa se sitúan en una sala especial llamada CPD – Centro de Proceso de Datos.

La empresa debe tener por escrito un plan de recuperación (plan de contingencia) ante cualquier problema que pueda ocurrir en el CPD o que afecte a los equipos que contiene.

Un Centro de Respaldo es un CPD similar al centro principal, alejado muchos kilómetros, sincronizado para poder asumir sus funciones en cualquier momento.

OBJETIVO:

Estudiar y documentar distintos dispositivos hardware de aseguramiento de sistemas informáticos.

Estudio sobre los mecanismos de seguridad física: características, proveedores, precio... y su diferenciación de mecanismos de seguridad lógica. Clasificación de los mecanismos en de seguridad física en activos y pasivos.

El primer paso para establecer la seguridad de un servidor o de un equipo es decidir adecuadamente donde vamos a instalarlo.

Los planes de seguridad física se basan en proteger el hardware de los posibles desastres naturales, de incendios, inundaciones, sobrecargas eléctricas, robos y otra serie de amenazas. Se trata de establecer barreras físicas y procedimientos de control como medidas de prevención y contramedidas para proteger los recursos y la información.

Factores para elegir la ubicación:

El edificio: espacio, acceso, suministro eléctrico, climatización, comunicaciones…
Preferentemente en las primeras plantas; sótanos no por las inundaciones, pisos altos no por los incendios.
Tratamiento acústico: ruido y vibración amortiguados.
Detectores de humo y extintores automáticos.
Climatización, control de temperatura.
Buenos pasillos para el acceso de los equipos. Falsos techos y suelos para el cableado.
Seguridad física del edificio.
Suministro eléctrico propio del CPD: sistema independiente del resto de la instalación y elementos de protección y seguridad específicos.
Condiciones ambientales e infraestructura de la zona. Alejada de posibles desastres naturales.
Alejado de empresas potencialmente peligrosas.

¿Dónde debe instalarse el CPD?

Evitar interferencias de radiofrecuencia.
Protegido de entornos peligrosos: maquinaria, inundaciones, fuego,…
El suministro eléctrico y de comunicaciones debe ser independiente al del resto de la empresa para aislar el CPD de los problemas en otras zonas del edificio.

Control de acceso.

Utilizar el control de acceso al edificio complementado con otros sistemas de control de acceso específicos al CPD. (***Sabes – Tienes – Eres***) El control de acceso debe ser mejor que el de el resto de zonas de trabajo.
Detectores de metales y escáneres de control de pertenencias.
Utilización de sistemas biométricos de identificación.
Alarmas, protección electrónica, monitorización de las actividades.
Videovigilancia…

Sistemas de climatización y protección en el CPD.

Además de instalar el CPD en la mejor localización posible, es imprescindible que se instalen en su interior, junto con los equipos propios de procesamiento de datos, sistemas de climatización, de protección contra incendios y sistemas de alarma apropiados.

Recuperación en caso de desastre.

Nuestro objetivo debe ser siempre evitar daños en el CPD, pero hay que ser realistas y tener preparado un ***plan de contingencia*** que debe ponerse en marcha en caso de desastre.
Una opción es tener un ***centro de backup independiente***, de modo que aunque los equipos del CPD queden fuera de servicio por una avería muy grave, la organización pueda seguir realizando su actividad con cierta normalidad.


Instalaciones
Cyberneticos
el centro de datos verde
SAI
Dpto. Técnico
Grupo Electrógeno
Centro de Datos
Sala de Reuniones
Area de descanso
Dpto. Comercial y Marketing
Presidencia
Dpto. Administración y Contabilidad

2. SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI/UPS)

Los equipos SAI (Sistema de Alimentación Interrumpida) disponen de baterías para alimentar un conjunto de máquinas en caso de que la corriente eléctrica general sufra un corte.

Sistemas auxiliares de alimentación eléctrica.

SAI: Sistema de Alimentación ininterrumpida: dispositivo electrónico que permite proteger a los equipos de picos o caídas de tensión. Protege al usuario de cambios en el suministro eléctrico y de cortes de luz.

UPS: Uninterruptible Power Supply

Dispone de baterías que alimentan el equipo en ausencia de electricidad en la línea. No están diseñados para conectar dispositivos de alto consumo de energía.

Permite al usuario el tiempo suficiente para guardar el trabajo en curso y apagar el equipo correctamente.

Aíslan al equipo de posibles subidas de tensión.

Podemos configurarlos para que apaguen el equipo ante un corte eléctrico (podemos configurar el tiempo que esperamos antes de apagar el equipo si se mantiene el corte eléctrico), parada ordenada si el suministro no se recupera en un tiempo prudencial.
Podemos conocer el estado de las baterías, conocer los cortes ocurridos recientemente, programar otro tipo de acciones en caso de corte, mensajes, alarmas,...

Características:

Número de ordenadores que podemos conectar (no olvidar conectar el monitor;)
Tiempo extra de trabajo: las baterías de un SAI se degradan con el tiempo, por lo que en algún momento necesitarán ser sustituidas.
Regulador de voltaje
Otros conectores: RS232C, RJ54, USB… para su gestión y configuración.
Tipos de SAI:

- Sistema de alimentación en estado de espera o **Stand-by Power Systems (SPS)**
- **SAI en línea (on-line)**

3. ALMACENAMIENTO DE LA INFORMACIÓN: RENDIMIENTO, DISPONIBILIDAD Y ACCESIBILIDAD

Un factor clave de la seguridad de cualquier sistema es cómo y donde se almacena la información.

Estrategia de almacenamiento

Los aspectos más importantes que tenemos que tener en cuenta a la hora de elegir el sistema de almacenamiento son el rendimiento, la disponibilidad y la accesibilidad a la información.

Objetivos:

Rendimiento: capacidad de cálculo de información de un ordenador.
Disponibilidad: capacidad de los sistemas de estar siempre en funcionamiento. **Alta disponibilidad**.
Accesibilidad a la información: facilidad de acceso a la información.

4. ALMACENAMIENTO REMOTO, DISTRIBUIDO Y REDUNDANTE

El objetivo es mejorar todas o algunas de las siguientes **características del sistema de almacenamiento**:

Capacidad
Tolerancia a fallos – Disponibilidad
Seguridad
Velocidad de lectura/escritura – Accesibilidad
Coste económico

Para ello tendremos que decidir entre las siguientes **opciones de almacenamiento**:

*Almacenamiento **remoto** – Almacenamiento **local***

*Almacenamiento **distribuido** – Almacenamiento **centralizado***

*Almacenamiento **redundante** – Almacenamiento **único***

4.1 RAID – CONJUNTO REDUNDANTE DE DISCOS INDEPENDIENTES – CONJUNTO REDUNDANTE DE DISCOS BARATOS

RAID Redundant Array of Inexpensive Disks

Los sistemas de almacenamiento RAID consisten en un conjunto de técnicas hardware y/o software que utilizan varios discos para guardar la información. Este sistema de almacenamiento nos ayudara a garantizar algunos objetivos de la Seguridad Informática, como la disponibilidad.

Este sistema de almacenamiento distribuye o duplica la información entre los discos que lo componen de forma que se consiguen algunas mejoras (en función de la configuración podemos mejorar todas o algunas de las siguientes características del almacenamiento):

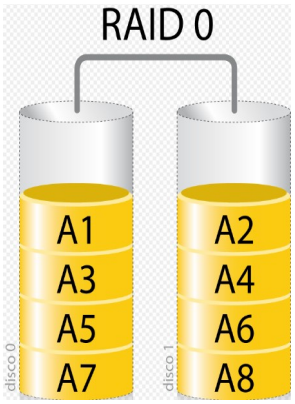
Mayor ***capacidad***	***crear unidades más grandes***
Mayor ***tolerancia a fallos – disponibilidad***	***crear unidades más fiables***
Mayor ***velocidad de lectura/escritura***	***crear unidades más rápidas***
Mayor ***seguridad***	
Mayor ***ahorro económico***	

Implementación: Se pueden implementar tanto por software (usando el sistema operativo) como por hardware (usando una tarjeta controladora raid)

Tipos de RAID

4.1.1 RAID DE NIVEL 0 (RAID 0)

Conjunto **dividido**



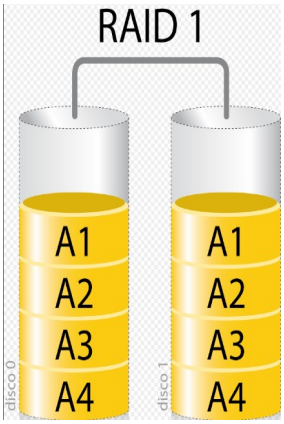
Los datos se distribuyen de forma equilibrada entre los 2 o mas discos del sistema de almacenamiento. Imaginémonos que tenemos una canción y un sistema RAID 0, cuando el SO va a guardar esa canción la parte en segmentos que suelen ser del mismo tamaño y los distribuye entre los dos discos duros, así una parte de la canción estará en un disco duro y la otra en el otro disco duro. Esta técnica favorece la velocidad pero hay que tener en cuenta que si uno de los dos discos duros falla la información es irrecuperable.

Spanning: Los bloques se escriben en el primer disco hasta que se llena, entonces continua escribiendo en el siguiente y así sucesivamente. Por tanto la lectura/escritura de cada bloque tiene que esperar a que termine la anterior.

Striping: Los bloques se escriben cada vez en un disco distinto. Es más rápido que el spanning porque hace trabajar a todos los discos a la vez.

4.1.2 RAID DE NIVEL 1 (RAID 1)

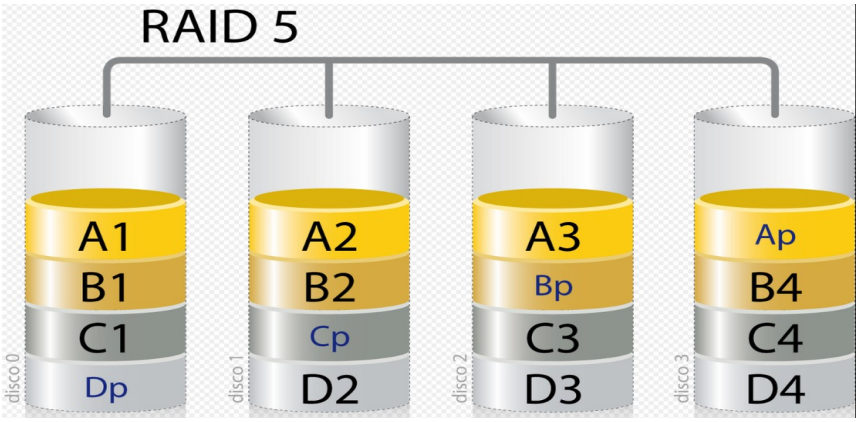
Conjunto en **espejo o mirror**



Los datos de un disco se duplican en todos los demás. Los datos están disponibles en dos o más discos al mismo tiempo. Es conocido también como **espejo**, la canción del ejemplo anterior ahora estará almacenada completamente (sin segmentarla) en todos los discos del RAID.

4.1.3 RAID DE NIVEL 5 (RAID 5)

Conjunto **dividido con paridad distribuida**



Los datos se almacenan en varios discos y se guarda paridad de ellos. En la lectura se leen los datos solamente, el bloque de paridad es leído cuando hay un fallo. Es parecido a RAID 0 pero en uno de los discos se guarda la paridad. Imaginémonos el siguiente caso:

Disco 1 ***Disco 2*** ***Disco 3*** ***Disco 4 (paridad par)***

11011011 01101011 00011101 **10101101**

Los 1 y 0 son fragmentos de un fichero distribuido entre 3 discos y en el cuarto se guarda su paridad. Para calcular la paridad se cuenta el numero de 1, **si el numero de 1 es par entonces el primer digito es 0 sino es 1**. Esquema: numero de 1 = par –> 0 || numero de 1 = impar –>1

4.1.4 RAID EN WINDOWS

Discos básicos: una unidad física (de disco) se corresponde con una o varias unidades lógicas (particiones).

Discos dinámicos: Nuevo tipo de almacenamiento (a partir de Windows 2000) que permite la creación de volúmenes dinámicos.

Existen 5 tipos de volúmenes dinámicos:

Simples: un volumen que utiliza espacio de un solo disco físico.
Distribuidos: volumen que se crea ocupando espacio de varios discos físicos. JBOD. Concatenación de discos.
Seccionados: corresponde al nivel 0 de RAID.
Reflejados: corresponde al nivel 1 de RAID.
RAID 5: corresponde al nivel 5 de RAID.

Windows 7:

Equipo/administrar/almacenamiento/administración de discos/

Windows 2012:

Administrador del servidor/almacenamiento/administración de discos/

4.1.4 RAID EN LINUX

Crear un software RAID (www.guia-ubuntu.com)

Ejemplo: Crear una configuración RAID 1 por software en Linux. Simular el fallo de un disco. Simular la sustitución de un disco.

I. Crear una máquina virtual Ubuntu Server con un solo disco de 5 GB.

II. Añadir a la máquina virtual (con Ubuntu Server ya instalado, pero parada) otros dos disco (disco1.vdi y disco2.vdi dinámicos) de 10GB. Montaremos el RAID 1 sobre estos discos.

III. Arrancamos la máquina y comprobamos que los discos están conectados:

 # fdisk -l (/dev/sda; /dev/sdb; /dev/sdc)
#**ls /dev/sd?**

IV. Instalamos el paquete mdadm

 # apt-get mdadm

V. Creamos el RAID 1

 # mdadm - -create /dev/sd0 - - level=1 - -raid-devices=2 /dev/sdb /dev/sdc
 # fdisk -l comprobamos que tenemos el nuevo dispositivo /dev/sd0

VI. Particionamos el nuevo disco /dev/sd0, creamos el sistema de ficheros y lo montamos.

 # fdisk /dev/sd0 (tipo p, numero 1 y todos los sectores disponibles)
 # mkfs -t ext4 /dev/sd0p1 creamos el sistema de ficheros y lo montamos
 # mkdir /mnt/raid1
 # mount -t ext4 /dev/sd0p1 /mnt/raid1

VII. Comprobamos el estado del RAID en el fichero ***/proc/mdstat***, en este fichero podemos comprobar el estado del raid, el tipo de raid y los discos que lo componen. (En nuestro caso activo, raid1 y sdb – sdc).

VIII. Si un disco falla, podemos desconectarlo y el raid sigue funcionando. Cuando dispongamos de otro disco, podemos conectarlo y el raid lo rellenará con los datos adecuados en función de la configuración.

 # mdadm /dev/sd0 - -fail /dev/sdb simulamos el fallo en el disco sdb
 # mdadm /dev/sd0 - -remove /dev/sdb quitamos el disco sdb del raid
Después de cada comando comprobamos el fichero ***/proc/mdstat***, en ambos casos la composición del raid aparece incompleta **[_U]**
 # mdadm - -zero-superblock /dev/sdb borramos la configuración disco sdb para poder simular despues que añadimos un disco nuevo.
 # mdadm /dev/sd0 - -add /dev/sdb añadimos el nuevo disco sdb
Después se inicia el proceso de sincronización del raid 1 ***recovery***, cuando termina el raid recupera el estado **[UU]**

IX. Si queremos que los sistemas de ficheros del raid estén disponibles al arrancar el sistema, debemos incluirlos en el ***fstat***

X. Desactivar y activar el raid temporalmente

 # mdadm /dev/sd0 - -stop desactivamos el raid temporalmente

 # mdadm /dev/sd0 - -assemble - -scan activamos el raid

4.2 CLUSTER DE SERVIDORES

Conjunto de varios servidores que se construyen e instalan para trabajar como si fuesen uno solo.

Unidos mediante una red de alta velocidad, el conjunto se ve como si fuese un único ordenador.

Objetivos:

Alta disponibilidad
Alto rendimiento
Balanceo de carga
Escalabilidad

Clasificación de los clusters:

Clusters de alto rendimiento (HC o High Performance Clusters) para solucionar problemas que requieren gran capacidad de calculo y grandes cantidades de memoria.
Clusters de alta disponibilidad (HA o High Availability) buscan dotar de alta disponibilidad y confiabilidad a los servicios que ofrecen. Utilizan hardware duplicado
Clusters de alta eficiencia (HT o Higy Throughput) diseñados para ejecutar el menor numero de tareas en el menor tiempo posible.

Clusters de infraestructuras comerciales – clusters científicos.

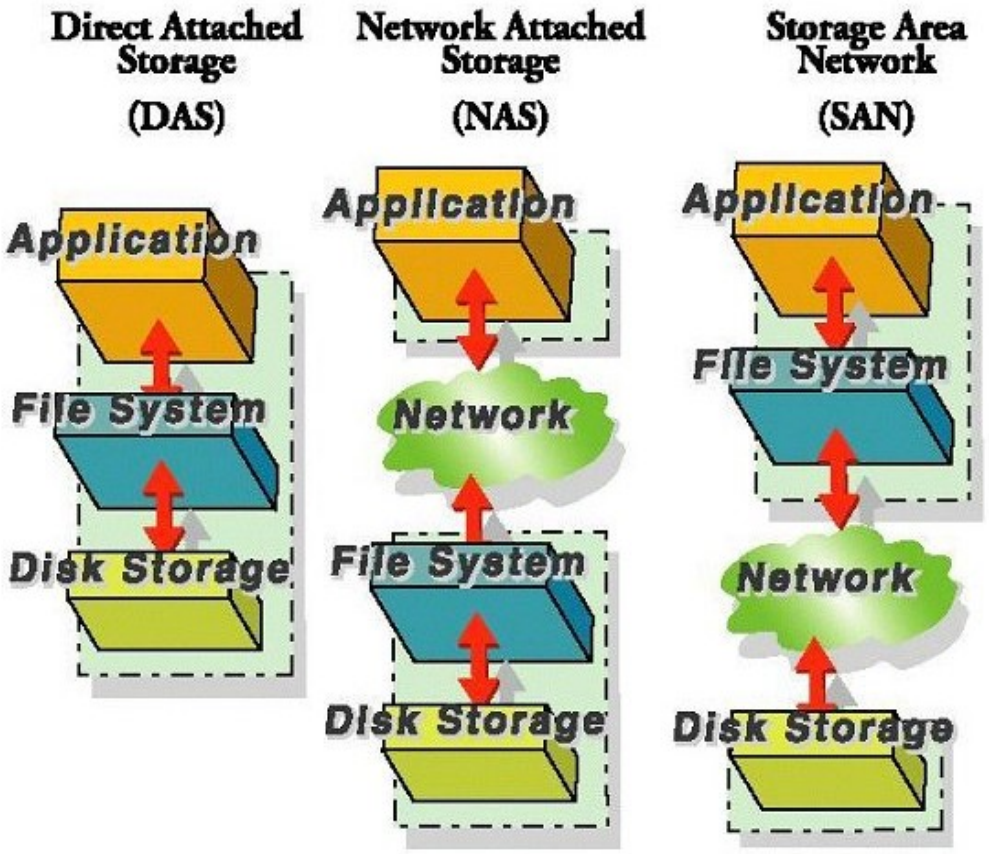
Componentes de los clusters:

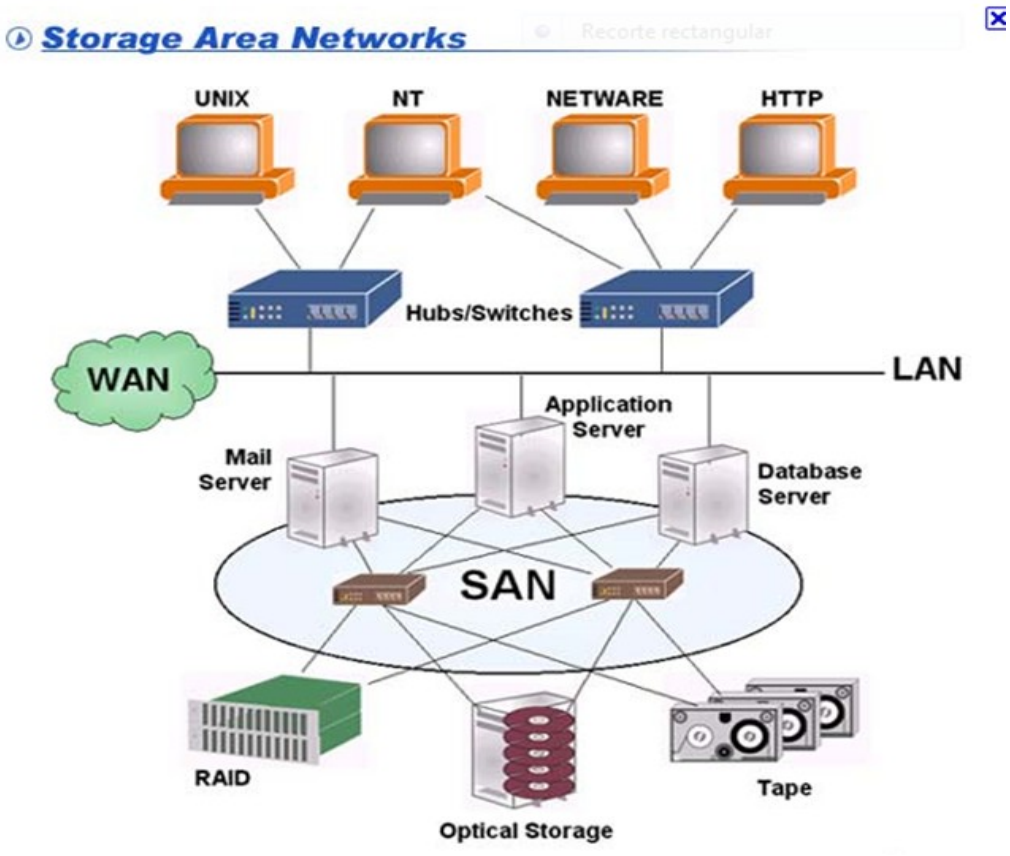
Nodos
Sistema operativo: (multiproceso y multiusuario)
Conexión de red: sistema de alta velocidad: Gigabit…
Milddleware: Software que se encuentra entre el sistema operativo y las aplicaciones para que el usuario tenga la sensación de que está trabajando con un solo equipo.
Sistema de almacenamiento:

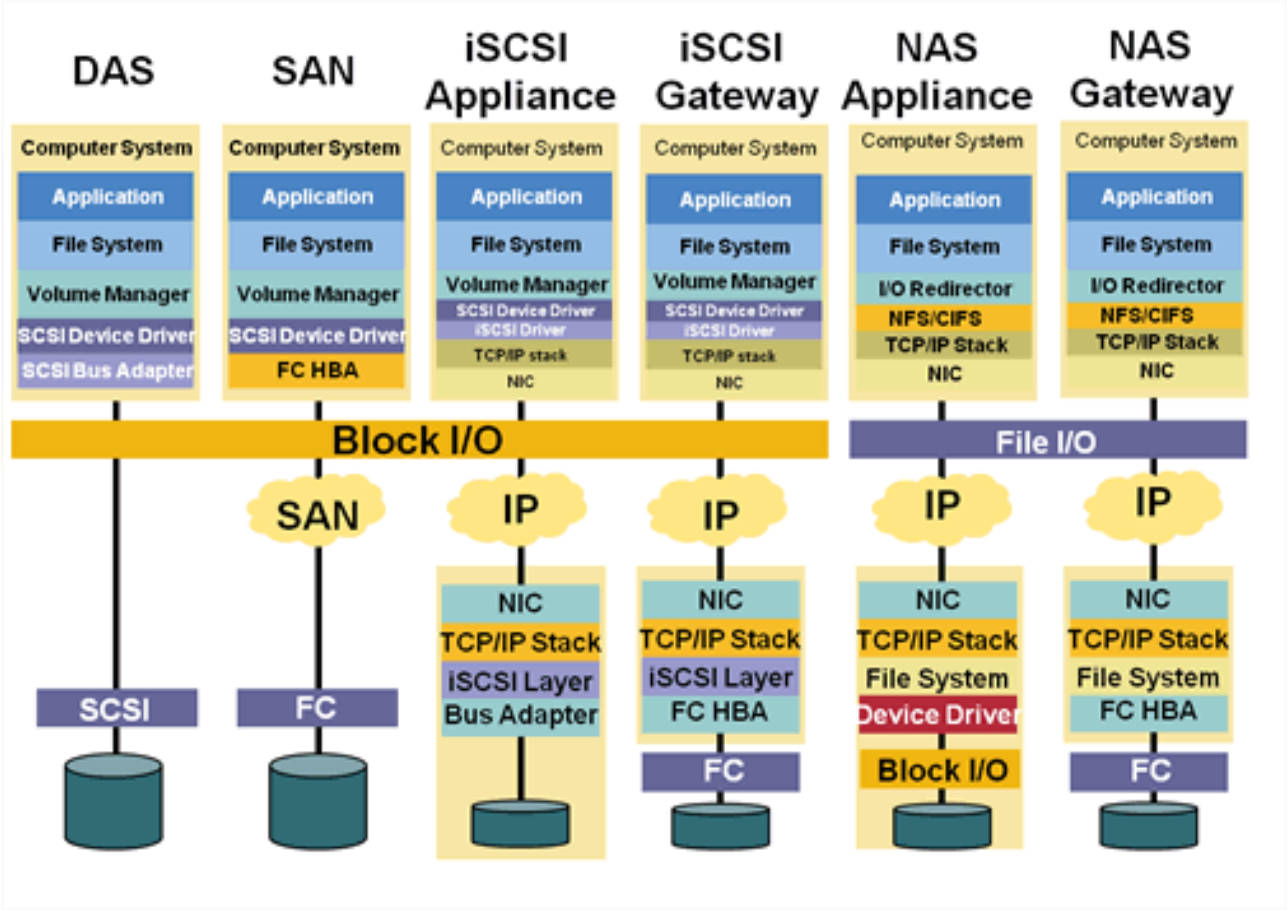
DAS: Almacenamiento local
NAS: Almacenamiento local en otro equipo que usamos a través de la red local.
SAN: Almacenamiento en red, hay una red de alta capacidad entre los discos y los procesadores.

Las tecnologías NAS y SAN nos permiten un control y gestión mucho mayores sobre los datos procesados.

Estas tecnologías son independientes de la existencia de un clúster, aunque son idóneas para trabajar con ellos.


Direct Attached Storage
(DAS)
Application
File System
Disk Storage
Network Attached Storage
(NAS)
Application
Network
File System
Disk Storage
Storage Area Network
(SAN)
Application
File System
Network
Disk Storage


Storage Area Networks
UNIX
NT
NETWARE
HTTP
Hubs/Switches
WAN
LAN
Application Server
Mail Server
Database Server
SAN
RAID
Optical Storage
Tape



4.3 GRANJA DE SERVIDORES

Una granja de servidores es un grupo de servidores, para ejecutar tareas que van más allá de la capacidad de un servidor dedicado.

Esto hace posible la distribución de tareas, de forma que el sistema gana una óptima tolerancia a fallos, ya que si uno de los servidores colapsa, el sistema continúa trabajando. El término usado en inglés es **server farm**.

4.4 VIRTUALIZACIÓN

Una máquina virtual nos permite tener varios ordenadores virtuales ejecutándose sobre el mismo ordenador físico.

Software de virtualización: **Oracle Virtual Box, ProxMox, Vmware, ...**

4.5 ALMACENAMIENTO EN LA NUBE Y P2P

Motivación:

Queremos disponer de información accesible desde Internet.
Queremos ofrecer servicios en Internet pero no disponemos de la tecnología necesaria en nuestra empresa.
Cuando estamos lejos de la oficina podemos necesitar algún fichero o que nuestros clientes accedan a determinada información.
Queremos una copia de seguridad alejada de nuestra oficina.

La solución es abrir en Internet el acceso a los discos de la empresa con los problemas de seguridad que esto conlleva o contratar **servicios de almacenamiento en la nube**.

La primera generación (Megaupload, Fileserver, …) consiste en que un usuario sube un fichero a la web para que otros usuarios lo descargen. Solo almacena ficheros estructurados en carpetas.

La segunda generación (**DropBox, iCloud, Box.net, Skydrive, GoogleDrive**,...) sincroniza carpetas de los dispositivos de los clientes con los servidores del proveedor en la nube.

Inconveniente: Nuestros datos están fuera de nuestras instalaciones. Puede que en otro país. Posiblemente sea conveniente cifrar la información que subimos. Perdemos el control de nuestra información.
Ventaja: La empresa proveedora del servicio en la nube se encarga de las copias de seguridad.
Ventaja: La empresa proveedora dispone de una conexión a Internet muy superior a la nuestra.

Las soluciones **P2P (peer to peer)** están más extendidas entre particulares (eMule, Torrent,...)
Si en el almacenamiento en la nube hay que desconfiar de un proveedor, aquí hay que desconfiar de muchos.
Este tipo de redes es muy interesante para la difusión de contenidos.

4.6 DFS

Sistema de ficheros distribuidos

Administración DFS (technet.microsoft.com)

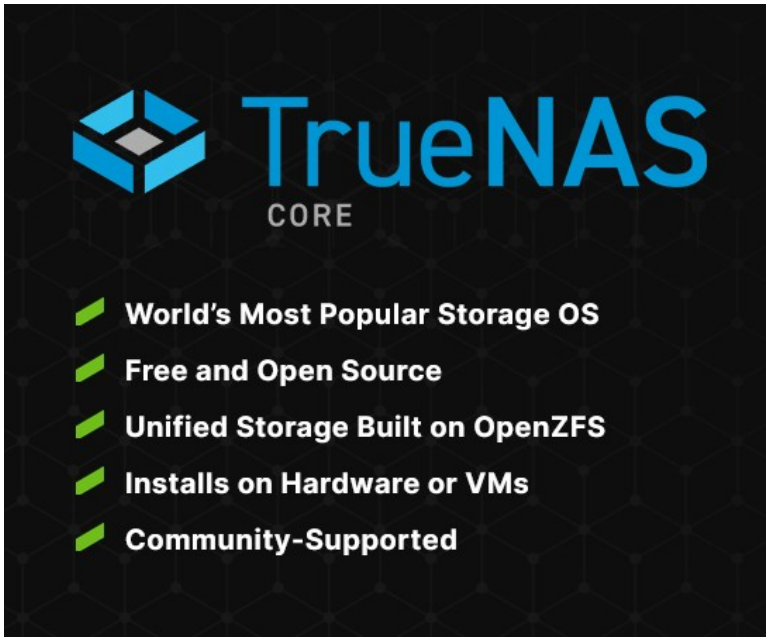
Espacio de nombres DFS
Replicación DFS

4.7 TrueNAS

Sistema operativo para implementar un NAS (Sistema de almacenamiento en red).

TrueNAS (Wikipedia)

TrueNAS



ENLACES INTERESANTES - BIBLIOGRAFÍA

Disco duro (Wikipedia)

Memoria RAM (Wikipedia)

Almacenamiento distribuido (Wikipedia)

Centro de respaldo (Wikipedia)

RAID (Wikipedia)

Cluster de servidores (Wikipedia)

NAS Network Attached Storage (Wikipedia)

SAN Storage Area Network (Wikipedia)

NFS Network File Sistem (Wikipedia)

Samba (Wikipedia) SMB Server Message Block CIFS Comon Internet File System (Wikipedia)

DFS Distributed File Sistem (Wikipedia)

Virtualización (Wikipedia)

TrueNAS (Wikipedia) TrueNAS

ProxMox

"Fundamentos de seguridad de redes" – Eric Maiwald – Editorial Mc Graw Hill – ISBN 970-10-4624-2

"El Tao de la monitorización de seguridad en redes – Richard Bejtlich – Editorial Pearson Educación – ISBN 84-205-4600-3

"Seguridad informática – Jose Fabián Roa Buendía – Editorial Mc Graw Hill – ISBN 978-84-481-8396-7

EJERCICIOS

SEGURIDAD PASIVA – SEGURIDAD FÍSICA

1. Define el concepto de "**seguridad pasiva de un sistema informático**"

Comenta tres técnicas o herramientas de seguridad pasiva y física.
Comenta tres técnicas o herramientas de seguridad pasiva y lógica.

2. Explica las características de un **CPD**.

3. Explica la diferencia entre **CPD** y **Centro de Respaldo**.

4. Explica el concepto, características y utilidad de un **SAI**.

5. Explica los conceptos de **almacenamiento**:

Local vs Remoto
Distribuido vs Centralizado
Redundante vs Único

6. Explica en que consiste el sistema **RAID**. Describe los tipos de RAID que conozcas.

7. Explica la técnica de almacenamiento en **RAID 0**. Concepto, características, ventajas e inconvenientes de utilizarla.

8. Explica la técnica de almacenamiento en **RAID 1**. Concepto, características, ventajas e inconvenientes de utilizarla.

9. Explica la técnica de almacenamiento en **RAID 5**. Concepto, características, ventajas e inconvenientes de utilizarla.

10. Explica el concepto, utilidad y diferencias entre los sistemas de almacenamiento y organización de disco(s) **Windows**: Simple, Distribuido o Seccionado.

11. Explica el concepto de **recurso compartido en Windows**, utilidad y características.

12. Explica en que consiste la **virtualización**. Ejemplos de software de virtualización que conoces.

13. Explica las diferencias entre los sistemas de almacenamiento **DAS**, **NAS** y **SAN**.

14. Explica cuáles son las principales características y tecnologías utilizadas en los sistemas de almacenamiento **SAN**.

15. Explica la diferencia entre **cluster**, **granja de servidores** y **servidor de virtualización**.

16. Localiza en Internet 3 ejemplos de instalaciones que potencien la **protección física** de los centros de procesos de datos de la empresa. Analiza comparativamente los tres casos estudiados.

17. Estudiar una propuesta como **centro de respaldo** para una pequeña empresa con un disco de datos que no supera los 500GB.

18. Propuesta de adquisición para una pequeña empresa de un disco duro (**IDE, SATA, USB, Disco en red, memoria flash,...**). Características y valoración de los dispositivos propuestos.

19. Prepara unos **presupuestos hardware y software para la adquisición de equipos**:

Equipo para un cliente en su casa con los periféricos adecuados.
Servidor para una pequeña empresa (25 trabajadores y usuarios de equipos clientes)
Equipo cliente para una pequeña empresa (25 trabajadores y usuarios de equipos clientes)

SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA

20. Describe las características técnicas y precio de, al menos, tres **Sistemas de Alimentación Ininterrumpida (SAI)**

21. **Conexión y configuración de un SAI** a un equipo del aula. Instalación del software de gestión del SAI.

SISTEMAS BIOMÉTRICOS DE IDENTIFICACIÓN

22. Cuantos tipos de **sistemas de identificación biométricos** conoces. De cada uno de ellos intenta localizar un dispositivo ejemplo, describir sus características, precio,…

Prueba un control de acceso por reconocimiento facial en el móvil.
Prueba un control de acceso por reconocimiento de voz en el móvil.

Avanzado

RAID

23. Probar distintas configuraciones **RAID en Windows.** (Utilizando máquinas y discos virtuales).

24. Probar distintas configuraciones **RAID en Ubuntu server**.

DFS

25. Montar un sistema **DFS** entre dos servidores Windows.

CLUSTER DE SERVIDORES – GRANJA DE SERVIORES – SERVIDOR DE VIRTUALIZACIÓN

26. Explica la diferencia entre **cluster**, **granja de servidores** y **servidor de virtualización**.

27. Configurar un **servidor de máquinas virtuales**. Software recomendado **ProxMox**.

28. Configurar un **cluster** utilizando varias máquinas.

29. Configurar una **granja de servidores** que nos permita alojar las máquinas virtuales que utilizan varios alumnos.

30. Localiza en Internet ejemplos de implementación de estos sistemas y webs donde podamos **contratar** estos servicios.

SAN - NAS

31. Explica la diferencia entre los sistemas de almacenamiento DAS, SAN y NAS.

32. Localiza en Internet ejemplos de implementación de estos sistemas.

33. Configura un servidor **TrueNAS**