EXAMEN FUNDAMENTOS HARDWARE

1) Servidores DAS, NAS y SAN.

DAS

ventajas: costes de implantación bajos. Alto ancho de banda, no dependen de la velocidad de una red.

Inconvenientes: Dispersión del almacenamiento que implica una dificultad en la gestión de los Backups. Incapacidad para compartir datos o recursos no usados con otros servidores.

Utilidades: Equipos de sobremesa. Servidores de área local.

NAS

ventajas: Mejor TCO. Arquitectura fácilmente escalable.

Inconvenientes: La red LAN puede actuar de cuello de botella. Menor rendimiento y fiabilidad que DAS por el uso compartido de las comunicaciones.

Utilidades: Carpetas compartidas. Sirve de soporte para el compartimiento de los datos.

SAN

ventajas: Fácil escalabilidad. Mayor velocidad de acceso a los datos.

Inconvenientes: El coste. Cuello de botella de la red al acceso al disco.

Utilidades: Servidores de grandes empresas. Virtualización de sistemas.

2) Ley de protección de datos

Nivel Básico

Tipos de datos: Nombre. Apellidos. Direcciones de contacto

Medidas de seguridad obligatorias: Documento de seguridad. Régimen de funciones y obligaciones del personal. Registro de incidencias.

Nivel Medio

Tipos de datos: Comisión infracciones penales. Comisión infracciones administrativas.

Medidas de seguridad obligatorias: Medidas de seguridad de nivel básico. Responsable de Seguridad. Auditoría bianual

Nivel Alto

Tipos de datos: Ideología. Religión. Creencias

Medidas de seguridad obligatorias: Medidas de seguridad de nivel básico y medio. Seguridad en la distribución de soportes. Registro de accesos

3) Tipos de RAID

Raid 0

Array de discos con striping sin tolerancia a fallos. Minimo 2 discos

Ventajas: permite acceso a más de 1 disco a la vez. Tasa de transferencia mas elevada.

Desventajas: no tolera fallos. No dispone de información de paridad.

Raid 1

Array de discos en espejo sin striping ni paridad.

Ventajas: buena protección de la información en caso de fallos. Tasa de transferencia extremadamente alta.

Desventajas: ineficiencia debido a las tareas de escritura en el disco espejo.

Raid 3

Array de discos con striping a nivel de bygte (paridad dedicada)

Ventajas: elevada tasa de transferencia L/E. Alta disponibilidad

Desventajas: paridad dedicada = cuello de botella

Raid 4

Array de disco con striping a nivel de bloque (paridad dedicada)

Ventajas: Alta disponibilidad del array con elevada tasa de transferencia de datos.

Desventajas: Controladora compleja y costosa

Raid 5

Array de discos con striping a de bloque y paridad distribuida.

Ventajas: buen rendimiento mínima pérdida de capacidad de almacenamiento

Desventajas: menos prestaciones que un raid 1

Raid 6

Array de discos con striping a nivel bloque y doble paridad distribuida.

Ventajas: permite fallos hasta en 2 discos simultáneamente

Desventajas: Coste mayor

Raid 0+1 2xRaid0 espejados

Raid 1+0 2xRaid1 distribuidos

RAID 10 (1+0) Un RAID 0 de Espejos.
Primero se crea un espejo RAID 1 y luego, sobre los anteriores, se establece un RAID 0. El resultado es un array dotado de redundancia con una mejora de rendimiento al no precisar escritura de paridad. Para que no se pierdan datos cada RAID 1 deberá mantener al menos uno de sus discos sin fallos.

4) ¿Que es un CPD? Nivel físico y lógico

Un CPD es una ubicación donde se encuentran todos los recursos necesarios para el procesamiento de la información de una empresa.
Su objetivo es garantizar la continuidad del servicio.

A nivel físico la separación en varias áreas beneficia el control de acceso, reducción del riesgo y control ambiental. Es aconsejable además, dividir la sala principal en dos o más cuartos separados con lo que se reduce la probabilidad de desastres.

A Nivel organizativo proporciona acceso a las nuevas tecnologías de la empresa.

Seguridad Física y Lógica en un CPD

Suele existir, en grandes empresas, un documento denominado Plan de Continuidad Del Negocio.

Las 3 estrategias son: prevención, mitigación, recuperación.

Esto se puede conseguir copiando datos en centros diferentes, conexiones de alta velocidad entre ellos o tener una infraestructura paralela para absorber la actividad del sistema ante incidencias.

Los riesgos físicos pueden dividirse en: Riesgos naturales, Riesgos de vecindad procedentes del entorno creado por el hombre.
Para evitar estos riesgos lo mas sencillo es ir escogiendo una localidad apropiada. La medida más efectiva para prevenir la intervención humana es ubicar la tecnología en sitios seguros, bajo llave, para restringir el acceso solo al personal autorizado mediante cerrojos.
Es importante aplicar barreras que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas.