

# Conceptos/Posibles preguntas ADSI

## Tema 1: Sistemas de computación

### ¿Qué es un CPD?

Un Centro de Procesamiento de Datos o Data Center es un espacio físico que alberga los servidores, equipos informáticos, los sistemas de red y los sistemas de almacenamiento. Su objetivo es el procesamiento de la información una empresa. Un aspecto importante para cada organización es contar con al menos un CPD.

Deben de estar dotados de grandes medidas, tanto físicas como lógicas, de seguridad y acceso, ya que debe cumplir todos los aspectos y normativas establecidas.

Los aspectos más importantes en su diseño son:

- Climatización
- Medidas antincendios e inundación
- Acometidas eléctricas y de comunicaciones.

### ¿Qué es la virtualización?

Los servidores se administran con mayor facilidad si estos se encuentran implementados sobre máquinas virtuales, estas reducen el coste del hardware, su mantenimiento y el soporte del entorno.

Estas máquinas virtuales no son emuladores o simuladores, se tratan de equipos reales que ofrecen incluso mayor funcionalidad que un equipo físico. En cualquier centro de datos tradicional, existe una fuerte relación entre los distintos equipos y sus respectivos espacios de almacenamiento sus puertos de red o las aplicaciones que estos soportan. Mediante la infraestructura virtual, es posible romper estas barreras.

Las máquinas virtuales no tienen dependencia del Hardware sobre el cual se ejecutan, y protegen a los sistemas operativos que corren en las mismas de las peculiaridades hardware.

## ¿Qué es el cloud?

La nube permite a los usuarios almacenar la información en servidores de terceros, de tal forma que pueden ser accesibles desde cualquier terminal que posea acceso a internet, sin la necesidad, por lo general, de instalar SW adicional.

Debido a la gestión remota, casi toda la tecnología que existe en el modelo de computación en la nube se basa en la virtualización de navegadores de internet.

Es un servicio bajo demanda a través de la red, caracterizado por su adaptación, flexibilidad, escalabilidad, rapidez, optimización, eficiencia ...etc.

Se basa en la gestión remota de la información que los usuarios le han transmitido previamente. Todo eso conlleva que se vuelque gran cantidad de información relevante, tanto de carácter personal como de negocios.

SGSI está basado en el principio de mejora continua, que también se puede aplicar en la nube.

Las características del cloud son:

- Autoservicio a la carta
- Amplio acceso a la red
- Reserva de recursos en común
- Rapidez y elasticidad
- Servicio supervisado

¿amenazas?

## Modelos de negocio

- RGPD: Determina aspectos importantes respecto a la responsabilidad de la seguridad de los datos, no hay diferencia en la aplicación de la normativa en función del tipo de despliegue en la nube.
- IaaS: Proveedor proporciona a los usuarios acceso a recursos de cálculo como servidores, almacenamiento y redes. Las empresas utilizan sus propias aplicaciones y plataformas en una infraestructura de proveedor de servicios. El responsable del fichero no gestiona ni controla la infraestructura de nube

subyacente, pero tiene control sobre los sistemas operativos, almacenamiento, aplicaciones desplegadas y un control limitado de red.

- PaaS: Oferta de Cloud Computing que proporciona a los usuarios un entorno en cloud en el que se pueden desarrollar, gestionar y distribuir aplicaciones. Además del almacenamiento, los usuarios pueden utilizar un conjunto de herramientas prediseñadas para desarrollar, personalizar y probar sus propias aplicaciones. En este tipo se utilizan las herramientas del proveedor para la programación de aplicaciones y servicios
- SaaS: Oferta de Cloud Computing que proporciona a los usuarios el acceso al software basado en cloud de un proveedor. Los usuarios no instalan aplicaciones en dispositivos locales, todo se hace mediante la web o API.

## Tema 3: Integración de sistemas y seguridad

### Tipos de pruebas

Existen cuatro tipos de pruebas: Unitarias, de integración, de sistemas, de aceptación.

- Unitarias: Verifican el correcto funcionamiento de componentes o módulos individuales de un sistema. Prueba piezas de código individuales
- Integración: Verifican la correcta interacción y comunicación entre los diferentes componentes de un sistema. Validan la interacción entre distintos módulos. Estas pruebas se centran en asegurar que las distintas partes del sistema funcionen correctamente juntas
- Sistemas: Estas pruebas se centran en verificar que el sistema cumpla con todos los requisitos y funcionalidades establecidas, y que sea capaz de realizar sus tareas correctamente en un entorno similar al de producción. Verifican el buen funcionamiento de las interfaces entre sistemas que los componen y con el resto de los sistemas de información con los que se comunica.
- Aceptación: Las pruebas de aceptación se realizan para evaluar si el sistema cumple con los requisitos y criterios definidos por los usuarios finales o clientes. Evalúan si se puede ejecutar y administrar un sistema de software. Las hace el usuario cuando el sistema y funciona bien.

## Tipos de arquitecturas

- Arquitectura cliente/servidor: Determina que rol juega cada uno de los procesos en la arquitectura.
- Arquitectura peer to peer: Descarga música, procesamiento de imágenes, call center... etc.
- Arquitectura N-tier: Aisla el servicio de la base de datos.
  - Capa de presentación: Inicializa el perfil del usuario.
  - Capa de negocio: Acceso a la base de datos. Operaciones de aplicación.
  - Capa de integración (middleware): Gestor de acceso a datos.
  - Capa de datos (otra asignatura)

## ¿Qué son las credenciales?

Conjunto de usuario y contraseña (u otra forma de autenticación) que se utiliza para otorgar acceso y validar una identidad. Una de las funciones del administrador de sistemas será administrar las cuentas de usuarios y de equipos. Estas cuentas se utilizan para permitir que los usuarios inicien sesión en la red y obtengan acceso a todos los recursos compartidos. La cuenta de usuario es un objeto que contiene toda la información que define a un usuario, incluye nombre de usuario y contraseña, con los que el usuario inicia la sesión y los grupos de los que la cuenta es miembro.

Se puede utilizar para permitir que el usuario inicie sesión, permitir que los procesos y servicios se ejecuten dentro de un contexto de seguridad específico, y administrar el acceso de un usuario a los recursos.

## ¿Qué es una carpeta compartida?

Aquella carpeta a la que pueden tener acceso varios usuarios a través de la red. Una vez se comparte los usuarios pueden obtener acceso a todos sus archivos y subcarpetas, siempre que se les hayan concedido permisos.

## Perfiles

Proyectos:

- Gestión de proyecto
- Alcance del proyecto
- Implantación

Dirección de proyectos:

- Director de la informática
- Director de proyecto
- Jefe de proyecto: Dirige el equipo de trabajo compuesto por
  - Analistas funcionales
  - Analistas de aplicaciones
  - Programadores

Sistemas y redes:

- Jefe de sistemas
- Jefe de redes
- Administrador de Red/Sistemas
- Técnico de redes
- Operador redes/sistemas

Base de datos:

- Administrador de la base de datos

## Tema 4: Servicio de directorios

### ¿Qué es Active Directory?

Active Directory almacena información acerca de los usuarios, equipos y recursos de red y permite el acceso a los recursos por parte de usuarios y aplicaciones.

Sus funciones son:

- Centralizar el control de recursos de red: Solo los usuarios autorizados pueden obtener acceso
- Centralizar y descentralizar la administración de recursos: Los administradores pueden administrar equipos cliente distribuidos, servidores de red o aplicaciones.
- Almacenar objetos de forma segura en una estructura lógica: Jerárquica y segura
- Optimizar el tráfico de red: Permite usar el ancho de banda de una forma más efectiva. Reduce la cantidad de tráfico en la red.

### Estructura lógica del Active Directory

Se compone de Objetos, unidades organizativas, dominios, árboles de dominio y bosques de dominio.

- Objeto: Componente más básicos de la estructura lógica. Las clases de objeto son plantillas para los tipos de objeto que se pueden crear en el Active Directory.

Cada clase de objetos se define por un grupo de atributos, y cada objeto posee una única combinación de estos atributos.

- Unidades Organizativas: Se pueden utilizar estos objetos contenedores para estructurar otros objetos de modo que admitan los propósitos administrativos. Se facilita su localización y administración.
- Dominios: Conjunto de objetos definidos de forma administrativa y que comparten una base de datos, directivas de seguridad y relaciones de confianza comunes con otros dominios.
- Árboles de dominio: Son dominios agrupados en estructuras jerárquicas, al agregar un segundo dominio al árbol, se convierte en secundario del dominio raíz del árbol. El nombre del dominio secundario se combina con el de dominio primario para formar su propio nombre único. Ejemplo EPS.UFV.ES
- Bosques: Es una instancia completa del AD. Consta de uno o varios árboles. El primer dominio del bosque se considera dominio raíz del bosque. De forma predeterminada la información del AD solo se comparte dentro del bosque.

### Estructura física del Active Directory

Los elementos de la estructura física del AD son los siguientes:

- Controlador de dominio: Realiza funciones de almacenamiento y de replicación. Un CD solo puede admitir un dominio, y para asegurarse de la disponibilidad continua del AD, un dominio debe de tener más de un CD. Este controlador de dominio tiene unas particiones.
- Sitios: Son grupos de equipos conectados correctamente. Al establecer sitios, los controladores de dominio de un único sitio se comunican con frecuencia. Esta comunicación minimiza la latencia dentro del sitio, y se pueden crear sitios para disminuir el uso del ancho de banda entre los controladores de dominio que están en ubicaciones diferentes.
- WLAN: Los sitios y el establecimiento de WLAN facilitan varias actividades, replicación y autenticación.

## ¿Qué es GPO?

El Active Directory utiliza la directiva de grupo para administrar los usuarios y equipos de la red. Se puede definir el estado del entorno de trabajo de un usuario una sola vez y, a continuación, dejar que la familia Windows Server aplique de manera continua la configuración de Directiva de grupo definida. Se puede aplicar a toda la organización o a todo el grupo de equipos/usuarios específicos.

- Para usuarios: Personaliza el entorno de escritorio del usuario, o aplica directivas de bloqueo a los usuarios.
- De equipo: Personaliza el entorno de escritorio de todos los usuarios de un equipo, o que aplica directivas de seguridad a los equipos de una red

## Tema 5: DRP

### PCN y sus Fases

El plan de continuidad de negocio está pensado y organizado para que el impacto que puede producir la interrupción del servicio informático sobre el resto de la compañía sea mínimo, restaurando sistemas y comunicaciones en el menor tiempo posible con todos nuestros empleados y colaboradores.

Las fases del PCN son:

1. Determinación del alcance: Se incluyen los archivos de más criticidad
2. Análisis de la organización: Reuniones, análisis de impacto y de riesgo
3. Definición estrategia de continuidad: Se establece la información sobre los procesos afectados y riesgos de la estructura IT.
4. Funcionamiento en caso de contingencia:
  - a. Activación
  - b. Comunicación
  - c. Actuaciones
  - d. Planes operativos
5. Prueba, mantenimiento y revisión: Es primordial

## Niveles de criticidad

- Críticos: Sus funciones no pueden ser ejecutadas a menos que sean reemplazadas por recursos idénticos. El coste de interrupción es muy alto.
- Vitales: Sus funciones puede ser ejecutadas manualmente durante un perdido corto de tiempo. Tiene mayor tolerancia a las interrupciones, y el costo de interrupción es menor.
- Sensitivos: Sus funciones pueden ser ejecutadas manualmente durante un periodo relativamente largo. Mientras se hace manualmente requiere una plantilla adicional, el coste de interrupción es medio.
- No críticos: Sus funciones pueden estar interrumpidas durante un periodo relativamente largo, con poco o ningún coste.

## Parámetros DRP

- RTO: Recovery Time Objective es el tiempo máximo durante el cual es aceptable que se interrumpa la actividad de la empresa, es decir, el tiempo que podemos soportar que dure una interrupción antes de que empiece a perturbar la actividad normal del negocio.
- RPO: Recovery Point Objective es el punto previo en el tiempo al que podemos permitirnos volver para recuperar los datos y funcionalidades de la empresa. Representa la cantidad de datos que la empresa está dispuesta a perder entre la última copia de seguridad y una contingencia.
- ROL: Revised Operating Level es el nivel mínimo de recuperación que debe tener una actividad para que se considere recuperada. Dependencias con otros procesos, ya sean internos o con proveedores externos.



