

# DOCUMENTO DE FUNDAMENTACIÓN CONCEPTUAL: Servicios Microsoft y Alta Disponibilidad

## MÓDULO 1: Fundamentos de Plataforma y Servicios de Infraestructura

### 1.1 Windows Server 2022: La Plataforma Operativa

Concepto	Fundamentación y Justificación
Rol de Servidor	Windows Server 2022 es la base del sistema operativo de red (NOS). Proporciona el <i>kernel</i> y el entorno de ejecución necesario para alojar y gestionar los servicios críticos de infraestructura (DNS, DHCP, AD, SQL). Se selecciona por su enfoque en la seguridad multicapa (especialmente <b>Secured-core server</b> ) y su compatibilidad nativa con arquitecturas híbridas (Azure).
Instalación Core vs. Desktop	La opción <b>Server Core</b> elimina la GUI (Interfaz Gráfica de Usuario), reduciendo significativamente la <b>superficie de ataque</b> del sistema y minimizando el consumo de recursos. Se prefiere para roles fijos y críticos como Controlador de Dominio. La <b>Desktop Experience</b> (con GUI) se utiliza cuando se requiere la instalación de aplicaciones con interfaz gráfica o para entornos de administración menos experimentados.
Direccionamiento IP Estático	Todo servidor que provee servicios de infraestructura ( <b>DNS, DHCP, AD, Gateway, Cluster</b> ) debe poseer una dirección IP estática. Esto asegura la <b>localización predecible</b> y constante del servicio. Si la dirección IP cambiara, los clientes perderían la capacidad de autenticarse o resolver nombres.

Exportar a Hojas de cálculo

### 1.2 DNS (Domain Name System): El Directorio de la Red

Concepto	Fundamentación y Justificación
Propósito y Funcionamiento	DNS es el servicio que traduce nombres de dominio legibles para humanos (ej., <b>servidor.miempresa.local</b> ) a direcciones IP numéricas (ej., <b>192.168.1.10</b> ). Funciona jerárquicamente. Es el protocolo fundamental para la usabilidad de Internet y las redes privadas modernas.

<b>Registros Críticos</b>	DNS almacena varios tipos de registros de recursos: <b>Registro A</b> (Name-to-IP), <b>Registro PTR</b> (IP-to-Name, para Búsqueda Inversa) y, crucialmente, los <b>Registros SRV</b> ( <i>Service Locator</i> ). Los Registros SRV son utilizados por los clientes de la red para localizar servicios específicos de Active Directory (Kerberos, LDAP, etc.).
<b>Integración con AD</b>	La integración de las zonas DNS en Active Directory (Zonas Integradas en AD) permite la <b>replicación de la base de datos DNS</b> junto con la base de datos de AD, asegurando que todos los Controladores de Dominio tengan información DNS consistente y actualizada, mejorando la tolerancia a fallos del servicio DNS.

Exportar a Hojas de cálculo

### 1.3 DHCP (Dynamic Host Configuration Protocol): Gestión Eficiente de IPs 🚀

<b>Concepto</b>	Fundamentación y Justificación
<b>Ciclo de Asignación (DORA)</b>	DHCP opera a través del proceso <b>DORA (Discover, Offer, Request, Acknowledge)</b> . Este proceso permite a un cliente obtener dinámicamente una configuración de red completa, eliminando la necesidad de configuración manual y evitando conflictos de IP.
<b>Ámbitos (Scopes) y Opciones</b>	Un <b>Ámbito</b> define un rango completo de direcciones IP disponibles para una subred específica. Las <b>Opciones de Ámbito</b> (ej., Opción 003: Router/Gateway; Opción 006: Servidores DNS) son las configuraciones adicionales que DHCP entrega al cliente, asegurando que todos los dispositivos apunten correctamente a los servicios de infraestructura.
<b>Autorización</b>	En un entorno de Active Directory, el servidor DHCP debe ser <b>Autorizado</b> en el directorio para poder operar. Esto previene la operación de servidores DHCP no autorizados ( <i>Rogue DHCP servers</i> ), que podrían asignar configuraciones incorrectas y causar un fallo total en la comunicación de red.

Exportar a Hojas de cálculo

## MÓDULO 2: Fundamentos de Directorio y Autenticación (Ruta A: Active Directory) 👑

### 2.1 Active Directory Domain Services (AD DS): La Identidad Central

<b>Concepto</b>	Fundamentación y Justificación
-----------------	--------------------------------

<b>Servicio de Directorio</b>	AD DS es una base de datos jerárquica y distribuida que almacena información sobre los objetos de la red (usuarios, equipos, servicios). Su propósito principal es proporcionar un punto centralizado para la <b>Autenticación (Kerberos)</b> y la <b>Autorización (ACLs)</b> .
<b>Estructura Lógica (Bosque, Dominio, OU)</b>	El <b>Bosque</b> es el límite de seguridad y replicación más alto, compartiendo el mismo esquema. El <b>Dominio</b> es la unidad de administración y replicación de la base de datos de AD. Las <b>OU (Unidades Organizacionales)</b> son contenedores dentro del dominio, utilizados para organizar objetos y delegar permisos o aplicar GPO de forma granular.
<b>Catálogo Global (Global Catalog)</b>	Un subconjunto de los datos de AD que se replica en todos los Controladores de Dominio designados. Permite a los usuarios buscar cualquier objeto en cualquier dominio dentro del Bosque sin necesidad de conocer o contactar el dominio del objeto.

Exportar a Hojas de cálculo

## 2.2 Controlador de Dominio (DC) y Promoción

<b>Concepto</b>	Fundamentación y Justificación
<b>Rol de DC</b>	Un DC es un servidor que aloja una copia escribible de la base de datos de AD y participa en la replicación. Maneja las peticiones de inicio de sesión y de búsqueda de directorio. El proceso de <b>Promoción</b> (mediante <code>Install-ADDSTForest</code> o <code>Install-ADDSDomain</code> ) convierte un servidor Windows estándar en un DC, instalando las bases de datos (NTDS.DIT) y ajustando la configuración de red.
<b>Requerimientos de DNS y SRV</b>	La promoción a DC automáticamente configura el DNS con los <b>Registros SRV</b> necesarios (ej., <code>_kerberos._tcp.dc._msdcs.miempresa.local</code> ). Si estos registros no están presentes o el DC no es su propio servidor DNS, los clientes fallarán al intentar autenticarse o localizar los servicios clave de AD.
<b>Modo de Restauración (DSRM)</b>	La contraseña de <b>DSRM (Directory Services Restore Mode)</b> es esencial. Permite iniciar el DC en un modo de aislamiento para realizar reparaciones o restauraciones de la base de datos de Active Directory sin que el servicio de directorio se inicie, manteniendo la estabilidad del Bosque.

Exportar a Hojas de cálculo

---

## MÓDULO 3: Fundamentos de Alta Disponibilidad (Ruta B: Cluster DB)

### 3.1 Alta Disponibilidad (HA) y Tolerancia a Fallos

Concepto	Fundamentación y Justificación
<b>Alta Disponibilidad (HA)</b>	El concepto de HA busca asegurar que una aplicación o servicio esté <b>accesible continuamente</b> , generalmente midiendo el tiempo de actividad ( <i>uptime</i> ) en términos de "nueves" (ej., "cinco nueves" o 99.999%). Un clúster de conmutación por error es una solución de HA porque, aunque ocurre una interrupción breve (tiempo de <i>failover</i> ), el servicio se recupera automáticamente.
<b>Tolerancia a Fallos</b>	Es la capacidad de un sistema para operar sin interrupción a pesar de un fallo en un componente (ej., un servidor completo). Los sistemas de tolerancia a fallos son más costosos y complejos, pero eliminan virtualmente todo tiempo de inactividad planificado o no planificado. Un WSFC se acerca a la tolerancia a fallos, pero técnicamente sigue siendo una solución de HA.
<b>Conmutación por Error (Failover)</b>	El proceso automático y controlado en el que un recurso o aplicación pasa del nodo primario (activo) a un nodo secundario (pasivo) tras detectar un fallo. Este proceso debe ser transparente para el cliente.

Exportar a Hojas de cálculo

### 3.2 WSFC (Windows Server Failover Clustering): La Capa del SO

Concepto	Fundamentación y Justificación
<b>WSFC</b>	Es una característica de Windows Server que permite que múltiples servidores (Nodos) trabajen juntos para proveer Alta Disponibilidad a roles específicos (como SQL Server, File Server, etc.). El clúster monitorea el estado de los recursos y gestiona el <i>failover</i> .
<b>Quórum</b>	El mecanismo de votación que previene el escenario de <b>Split-Brain</b> (donde los nodos se aíslan y cada uno intenta tomar el control de los recursos). El Quórum asegura que solo la mayoría de los votos pueda mantener el clúster en línea, obligando a que la minoría se apague. Los modos de Quórum incluyen <b>Node Majority</b> , <b>Node and Disk Majority</b> o <b>Node and File Share Majority</b> .
<b>CNO (Cluster Name Object)</b>	Es un objeto de equipo creado en Active Directory que representa el clúster. Proporciona el <b>Nombre Virtual</b> y la <b>IP de administración del Clúster</b> , permitiendo que los administradores se conecten a la capa de gestión del WSFC sin importar qué nodo esté activo.

Exportar a Hojas de cálculo

### 3.3 SQL Server Failover Cluster Instance (FCI)

Concepto	Fundamentación y Justificación
<b>FCI y SQL Server</b>	FCI es una instancia de SQL Server que se instala directamente en la estructura del WSFC. La instancia se ejecuta como un servicio de clúster, lo que significa que el servicio de SQL Server es el recurso monitoreado que se mueve entre los nodos.
<b>Uso de Almacenamiento Compartido</b>	La FCI requiere <b>almacenamiento compartido</b> (SAN, iSCSI, o Storage Spaces Direct). Los archivos de la base de datos ( <b>.mdf</b> , <b>.ldf</b> ) residen en este almacenamiento compartido. Solo el nodo activo tiene control y acceso a estos discos, garantizando la integridad de los datos.
<b>Conexión Transparente del Cliente</b>	El cliente (aplicación o usuario) se conecta al <b>Nombre de Red de SQL Virtual</b> (un recurso definido en el clúster, no al CNO). El clúster se encarga de dirigir esa conexión al nodo activo que actualmente posee el servicio de SQL y el disco compartido. Esto asegura que, después de un <i>failover</i> , la aplicación solo necesita reconectarse al mismo nombre virtual.