PROFUNDIZACIÓN CONCEPTUAL Y ESTRUCTURA ORGANIZACIONAL EN AD

1. La Organización Digital: Estructura y Límites de Active Directory 👑

Para un entorno Microsoft, **la organización** se define por los límites que establece Active Directory (AD). Estos límites no son físicos, sino **límites de seguridad, administración y replicación**.

1.1 El Bosque (Forest): El Límite de Seguridad Máximo

El **Bosque** es el nivel jerárquico más alto de Active Directory y representa el **límite de seguridad, el límite de replicación del Esquema y el límite de confianza**.

- **Límite de Seguridad:** Si un administrador tiene privilegios a nivel de Bosque, tiene control sobre **todos** los dominios dentro de ese Bosque. Ninguna relación de confianza externa (trust) es implícita a nivel de Bosque.
- **Esquema (Schema):** El Bosque comparte un **Esquema único** para todos sus dominios. El Esquema es el *blueprint* o diccionario que define los tipos de objetos (usuario, equipo) y los atributos (nombre, email) que pueden existir en el directorio. Cualquier cambio en el Esquema afecta a toda la organización.
- **Catálogo Global (Global Catalog):** El Bosque define el ámbito del Catálogo Global. Este servicio permite a los usuarios **buscar cualquier objeto** (usuario, grupo) en cualquier dominio del Bosque sin necesidad de conocer o contactar ese dominio directamente, esencial para la funcionalidad de Outlook y la búsqueda de recursos.

1.2 El Dominio: El Límite Administrativo y de Identidad

El **Dominio** es la unidad lógica donde reside la base de datos de AD (**NTDS.DIT**) y donde se centraliza la **Autenticación (Kerberos)**.

- **Identidad Centralizada:** Un usuario que pertenece al dominio (`usuario@miempresa.local`) puede autenticarse contra cualquier recurso dentro del dominio o del Bosque a través de confianzas.
- **Límite de GPO y Seguridad:** Las políticas de contraseñas y las configuraciones de auditoría más estrictas se aplican típicamente a nivel de Dominio, forzando una base de seguridad uniforme para toda la organización.
- **Replicación:** Los datos de la base de datos de AD se replican entre todos los **Controladores de Dominio (DCs)** que pertenecen a ese Dominio.

---

2. Unidades Organizacionales (OU): Mapeando el Organigrama 📊

La **Unidad Organizacional (OU)** es el elemento de AD que **mapea directamente la estructura de la organización**. No son límites de seguridad como tal (ya que las GPO se heredan), pero son límites de **administración delegada** y de **aplicación granular de políticas**.

2.1 La OU como Reflejo de la Organización

Una organización puede estructurar sus OUs de tres formas principales:

1. **Por Geografía:** `OU_Montevideo`, `OU_Maldonado`. (Útil para políticas de red basadas en ubicación).
2. **Por Función/Departamento:** `OU_Ventas`, `OU_IT`, `OU_Contabilidad`. (El modelo más común, ideal para la **delegación de tareas** y aplicación de GPO basadas en el rol del usuario).
3. **Por Tipo de Objeto:** `OU_Usuarios`, `OU_Grupos`, `OU_Equipos`. (Usado para simplificar el filtrado y la vinculación de GPO).

2.2 Principios de Diseño con OUs

- **Delegación de Control:** Es la función principal de la OU. Permite que un administrador de nivel bajo (ej., un técnico de soporte) gestione recursos **solo** dentro de esa OU (ej., solo restablecer contraseñas de `OU_Ventas`) sin tener privilegios de administrador de Dominio.
- **Aplicación de GPO Granular:** Las OUs son el nivel más bajo en el proceso de aplicación de políticas **LSDOU**. Vincular una GPO a una OU garantiza que la política sea aplicada con la máxima especificidad (ej., solo bloquear el CMD para los PCs de `OU_Atención_al_Cliente`).

---

3. Gestión de Identidades: El Modelo AGDLP y el Mínimo Privilegio 🔑

La clave para una organización segura y auditable es gestionar el acceso a través de grupos, nunca a través de usuarios individuales.

3.1 Cuentas (Accounts): La Identidad Digital

- **Usuarios:** La identidad individual de un empleado o estudiante. Es el **sujeto** que solicita el acceso a un recurso.

- **Cuentas de Servicio:** Cuentas sin interacción humana creadas para ejecutar aplicaciones (ej., SQL Server, IIS, un *script* de backup). Estas cuentas deben estar sujetas al **Principio de Mínimo Privilegio** y nunca deben ser administradores de dominio.

3.2 El Modelo AGDLP: Auditoría y Escalabilidad

El modelo **AGDLP (Accounts, Global Groups, Domain Local Groups, Permissions)** es la arquitectura de oro para la asignación de permisos:

Acrónimo	Tipo de Objeto	Contenido	Aplicación	Justificación Organizacional
Accounts	Usuarios	Personas o Cuentas de Servicio.	Se añaden a GG.	**Individualidad:** Control preciso sobre quién es quién.
Global Groups (GG)	Grupo	Usuarios con el mismo **rol funcional** (ej., `GG-Ventas`).	Se anidan en DLG.	**Funcionalidad:** Simplifica la administración de la identidad. Si Ana se mueve a Marketing, se saca de `GG-Ventas` y se añade a `GG-Marketing`.
Domain **L**ocal Groups (DLG)	Grupo	Grupos Globales y Universal.	Se asignan **Permisos** a un recurso.	**Recurso/Permiso:** El nombre del DLG describe el permiso (`DL-RW_CarpetasVentas`).
Permissions	Permisos	Las reglas NTFS/Compartidas.	Se asignan al DLG.	**Seguridad y Auditoría:** Solo se audita el DLG. Se sabe que cualquier miembro de ese DLG tiene esos permisos.

Exportar a Hojas de cálculo

Beneficio Organizacional: Cuando un permiso cambia (ej., la carpeta Ventas ahora solo requiere Lectura), solo se modifica el permiso en el DLG. Si un usuario cambia de rol, solo se modifica su pertenencia al GG. La administración se vuelve ágil y centralizada.

---

4. Control de Acceso: Las Capas de Permisos (NTFS) 🔒

4.1 Principio de Mínimo Privilegio (PoLP)

El PoLP dicta que el acceso debe ser el **mínimo estrictamente necesario** para que un usuario complete su trabajo. Esto significa que si un usuario solo necesita ver un archivo, se le asigna permiso de **Lectura**, no **Modificación** o **Control Total**. La asignación excesiva de permisos es la principal causa de fugas de información y malware en la red.

4.2 Permisos de Compartición vs. Permisos NTFS

El acceso a un recurso compartido (`\\servidor\carpeta`) siempre pasa por dos filtros de seguridad:

1. **Permisos de Compartición (Share Permissions):** Controlan si se puede **establecer una conexión** con el recurso a través de la red. Son la primera capa.
2. **Permisos NTFS:** Controlan si se puede **hacer algo** (Leer, Escribir, Modificar) una vez que la conexión está establecida. Son el filtro de seguridad definitivo.

Regla de Oro: Para que un usuario acceda a un archivo, debe tener **el permiso más restrictivo** de las dos capas. En la práctica organizacional, se recomienda:

- **Permiso de Compartición:** Asignar **Control Total** al Grupo de Dominio Local (DLG).
- **Permiso NTFS:** Asignar el permiso **Modificar** o **Leer** al mismo DLG. (NTFS define el acceso real y estricto).

---

5. Automatización y Eficiencia (PowerShell) 🚀

En una organización moderna, la administración manual no es escalable. La creación de 100 usuarios manualmente es inviable. **PowerShell** es el lenguaje de *scripting* que permite la automatización y la gestión remota.

5.1 Justificación de PowerShell en la Organización

- **Escalabilidad:** Crear, modificar o auditar 500 cuentas de usuario se realiza en segundos con un *script*, no en horas con el ADUC.
- **Consistencia:** Un *script* siempre ejecuta los comandos en el mismo orden y con los mismos parámetros, garantizando que todos los objetos creados (usuarios, VMs, etc.) cumplan con los mismos estándares de la organización.
- **Gestión Remota:** Permite administrar servidores sin GUI (Server Core) y ejecutar comandos en múltiples equipos simultáneamente.

5.2 Estructura y Sintaxis (Verbo-Nombre)

El lenguaje PowerShell se basa en el formato **Verbo-Nombre** (ej., `Get-Service`, `New-ADUser`). Esto facilita la memorización y la predicción de comandos:

- **`Get-`:** Obtener o recuperar datos (auditoría/lectura).

- **`Set-`:** Modificar o cambiar propiedades.
- **`New-`:** Crear un nuevo recurso.
- **`Remove-`:** Eliminar un recurso.

Dominar el módulo **`ActiveDirectory`** y la sintaxis de **filtrado** (`-Filter`) es el objetivo central para la gestión eficiente y la automatización de informes en el entorno organizacional.