El Mito de la Jerarquía en Active Directory

En el organigrama de una empresa, el CEO está en la cima. Sin embargo, en la arquitectura de **Active Directory (AD)**, la jerarquía corporativa es irrelevante. En el mundo técnico, el poder no es un estatus, es un riesgo.

El Privilegio como Responsabilidad, no como Rango

A menudo se comete el error de pensar que los privilegios de "Domain Admin" son una extensión del cargo directivo. Nada más lejos de la realidad. Cada cuenta con privilegios elevados expande la **superficie de ataque** de la organización. Si un atacante compromete la cuenta de un directivo que tiene permisos innecesarios, tiene las llaves de todo el reino.

El Filtro de Acceso: ¿Quién sí y quién no?

La asignación de permisos debe basarse exclusivamente en la **necesidad operativa**:

- **El Círculo de Confianza:** Solo administradores de sistemas designados, personal de IT con roles específicos en AD y equipos de seguridad auditables deben poseer estas credenciales.
- **La Zona de Exclusión:** Bajo ninguna circunstancia deben tener privilegios por defecto los perfiles directivos, los usuarios "avanzados" o las cuentas que se usan para tareas cotidianas (leer correo, navegar por internet).

Los Pilares de la Protección

Para blindar un entorno de identidad, no basta con reducir el número de administradores; hay que cambiar la metodología de trabajo:

1. **Principio de Mínimo Privilegio (PoLP):** Otorgar solo los permisos necesarios para realizar una tarea específica, ni uno más.
2. **Cuentas Separadas:** Un administrador debe tener una cuenta para su trabajo diario (sin privilegios) y otra distinta para tareas de gestión.
3. **Acceso Just-In-Time (JIT):** Los privilegios no son permanentes; se activan solo cuando se necesitan y por un tiempo limitado.

4. **MFA y Auditoría:** El doble factor de autenticación es innegociable, acompañado de un registro constante de quién hizo qué y cuándo.

Conclusión: La seguridad de una red no se mide por cuántas personas mandan, sino por cuántas personas están capacitadas (y limitadas) para protegerla. **Menos administradores equivalen a más seguridad.**

Ejercicio de Clase: "El Dilema del Administrador"

Contexto:

Eres el nuevo Responsable de Seguridad (CISO) de una empresa tecnológica de 200 empleados. Al revisar el grupo de "Administradores del Dominio", encuentras la siguiente lista de personas con acceso total:

Nombre	**Puesto**	**Justificación actual**
Carlos G.	CEO	"Necesito instalar programas cuando quiera."
Laura M.	SysAdmin Senior	Gestiona los servidores y el AD.
Pedro J.	Desarrollador Senior	"A veces necesito reiniciar servicios en el servidor de pruebas."
Marta R.	Soporte Técnico	"Para ayudar a los usuarios de forma remota más rápido."
Admin_Backup	Cuenta de Servicio	Ejecuta las copias de seguridad cada noche.

Tarea para el alumno:

1. **Evaluación de Riesgos:** Identifica qué cuentas representan un riesgo innecesario según el texto anterior y por qué.
2. **Propuesta de Reestructuración:** Para cada persona de la lista, decide si mantienes sus privilegios, si los eliminas o si propones una solución alternativa (ej. delegación de permisos específicos, cuenta separada, entorno de pruebas aislado).

3. **Protocolo de Emergencia:** Diseña un flujo breve de 3 pasos que debería seguir un empleado si necesita privilegios elevados de forma puntual (Aplicando el concepto **JIT - Just In Time**).