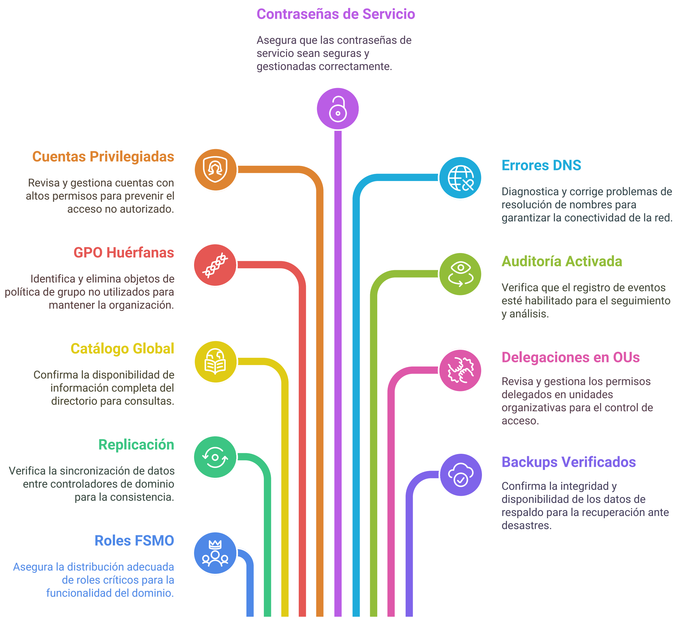
Cheq-AD 15: Tu Auditoría Rápida de Active Directory

Este documento presenta una guía concisa para realizar una auditoría rápida de Active Directory utilizando comandos de PowerShell y CMD. La auditoría se centra en diez áreas clave que son fundamentales para garantizar la salud y seguridad de un entorno Active Directory. Cada sección incluye comandos específicos y criterios de evaluación que permiten identificar el estado de los componentes críticos.

¿Qué área de Active Directory debe auditarse?



1. FSMO roles

```
(Get-ADForest).SchemaMaster
(Get-ADForest).DomainNamingMaster
```

→ ✅ ambos en DC redundante
→ ❌ si caen en un mismo DC viejo

2. Replicación

```
repadmin /replsummary
```

Fails = 0 → ✅

3. Catálogo global

```
Get-ADForest | select GlobalCatalogs
```

≥ 2 GC por site → ✅

4. GPO huérfanas

```
Get-GPO -All | ?{ -not $_.GpoStatus }
```

Resultado vacío = ✅

5. Cuentas privilegiadas

```
Get-ADGroupMember "Administrators"
```

Solo grupos/SDDL esperados → ✅

6. Contraseñas de servicio

```
Get-ADUser -Filter * -Properties PasswordLastSet | ?{ $_.ServicePrincipalName }
```

≥ 2 años sin cambio = ❌

7. DNS errores

```
dnscmd /statistics /errors
```

0 errores → ✅

8. Auditoría activada

```
auditpol /get /category:*
```

Subcategorías críticas en Success+Failure → ✅

9. Delegaciones en OUs

```
Get-ADOrganizationalUnit -LDAPFilter "(gPLink=*)" -Properties ManagedBy
```

Lista vacía = revisar → ⚠!!

10. Backups verificados

```
wbadmin get versions
```

Restore test < 90 días → ✅