Diseño e implementación de un proyecto de migración y unificación de dominios corporativos entre sedes internacionales de una compañía multinacional

Juan Pablo Atehortúa Arenas

Trabajo de grado presentado como requisito para optar al título de Ingeniero en Telecomunicaciones

Universidad Nacional Abierta y a Distancia – UNAD

Facultad de Ingeniería

Programa de Ingeniería en Telecomunicaciones

Medellín, Colombia

Julio de 2025

Dedicatoria

Este trabajo está dedicado, en primer lugar, a Dios, por brindarme la fortaleza, la disciplina y la constancia necesarias para culminar esta etapa fundamental de mi formación profesional.

A mi familia, por su apoyo incondicional, comprensión y motivación permanente a lo largo de este proceso académico. Su respaldo fue un pilar esencial para superar los retos y exigencias que implicó el desarrollo de este proyecto.

A mis docentes de la Universidad Nacional Abierta y a Distancia (UNAD), quienes con sus conocimientos, orientación y acompañamiento contribuyeron de manera significativa a mi crecimiento académico y profesional.

Finalmente, dedico este trabajo a todas las personas que, de una u otra forma, aportaron a la construcción de este proyecto y al fortalecimiento de mi vocación como futuro ingeniero en telecomunicaciones.

Agradecimientos

Expreso mi sincero agradecimiento a la Universidad Nacional Abierta y a Distancia (UNAD) por brindar las herramientas académicas, metodológicas y tecnológicas que hicieron posible el desarrollo de este trabajo de grado, así como por fomentar una formación integral orientada a las necesidades del entorno profesional actual.

A los docentes del programa de Ingeniería en Telecomunicaciones, quienes a través de su acompañamiento, conocimientos y orientación contribuyeron significativamente al fortalecimiento de mis competencias técnicas y al adecuado desarrollo de este proyecto.

Agradezco de manera especial a mi familia, cuyo apoyo constante, comprensión y motivación fueron fundamentales durante todo el proceso académico, permitiéndome afrontar con responsabilidad y compromiso los desafíos presentados.

De igual forma, extiendo mi agradecimiento a las personas y equipos de trabajo que facilitaron información, brindaron asesoría técnica y aportaron su experiencia para la realización del análisis, diseño e implementación de la solución planteada en este proyecto.

Finalmente, agradezco a todas aquellas personas que, de manera directa o indirecta, contribuyeron al cumplimiento de los objetivos propuestos y al cierre exitoso de esta etapa de formación profesional.

Resumen

Este proyecto aborda el diseño e implementación de una estrategia de migración y unificación de dominios corporativos distribuidos en múltiples ubicaciones internacionales, específicamente en Colombia, Guatemala, El Salvador y Panamá. Actualmente, la organización opera dominios independientes de Active Directory en cada sede, lo que ha generado fragmentación administrativa, inconsistencias en la seguridad, incremento de los costos operativos y una interoperabilidad limitada entre los servicios. La metodología adoptada sigue un enfoque cuantitativo-descriptivo y aplicado, estructurado en fases secuenciales que incluyen la evaluación de la infraestructura, el diseño de una arquitectura de dominio unificada, la definición de políticas de seguridad y replicación, pruebas piloto de migración y la implementación final. Para apoyar el proceso de migración y garantizar la integridad de los datos, la disponibilidad y la continuidad de las operaciones, se emplearon herramientas como Active Directory Migration Tool (ADMT), PowerShell, así como los servicios de DNS y DHCP. La solución propuesta consolida los dominios existentes en un dominio corporativo centralizado, permitiendo una gestión unificada de identidades, la estandarización de políticas de seguridad y la optimización de la replicación entre sedes. Los resultados evidencian una mejora en la eficiencia administrativa, un fortalecimiento de la postura de seguridad, un aumento en la disponibilidad de los servicios y una reducción en la complejidad de la gestión de dominios. Este proyecto aporta tanto a nivel técnico como académico, al aplicar conocimientos teóricos de ingeniería de telecomunicaciones, servicios de red y ciberseguridad en un escenario organizacional real. La arquitectura de dominio unificado establece una base escalable y resiliente, capaz de soportar el crecimiento futuro, la integración con entornos de nube híbrida y los procesos continuos de transformación digital.

Palabras clave: Active Directory, migración de dominios, infraestructura de red, ciberseguridad, replicación, redes corporativas.

Abstract

This project addresses the design and implementation of a migration and unification strategy for corporate domains distributed across multiple international locations, specifically Colombia, Guatemala, El Salvador, and Panama. The organization currently operates independent Active Directory domains at each site, which has led to administrative fragmentation, security inconsistencies, increased operational costs, and limited interoperability among services. The adopted methodology follows a quantitative-descriptive and applied approach, structured into sequential phases that include infrastructure assessment, unified domain architecture design, security and replication policy definition, pilot migration testing, and final implementation. Tools such as Active Directory Migration Tool (ADMT), PowerShell, DNS, and DHCP services were used to support the migration process and ensure data integrity, availability, and continuity of operations. The proposed solution consolidates the existing domains into a centralized corporate domain, enabling unified identity management, standardized security policies, and optimized replication between sites. The results demonstrate improved administrative efficiency, enhanced security posture, increased service availability, and reduced complexity in domain management. This project contributes both technically and academically by applying theoretical knowledge of telecommunications engineering, network services, and cybersecurity to a real-world organizational scenario. The unified domain architecture establishes a scalable and resilient foundation capable of supporting future growth, hybrid cloud integration, and ongoing digital transformation initiatives.

Keywords**:** Active Directory, domain migration, network infrastructure, cybersecurity, replication, corporate networks.

Tabla de Contenido

Listas de Figuras

Lista de Tablas

Glosario

Active Directory (AD): Servicio de directorio desarrollado por Microsoft que permite almacenar información sobre objetos en una red y facilita la administración centralizada de usuarios, equipos, grupos, políticas y recursos. Utiliza protocolos como LDAP, Kerberos y DNS para autenticación, autorización y localización de servicios.

AD Connect: Herramienta de Microsoft que permite sincronizar identidades, usuarios y atributos entre un Active Directory local y Azure AD (Entra ID).

ADMT (Active Directory Migration Tool): Herramienta oficial de Microsoft que permite migrar objetos como usuarios, grupos y equipos entre dominios de Active Directory, facilitando procesos de consolidación o reestructuración de dominios.

Azure AD: Servicio de directorio en la nube de Microsoft para la gestión de identidades, autenticación y control de acceso a aplicaciones y servicios en la nube (actualmente denominado Entra ID).

BlueCat: Plataforma de gestión de DNS, DHCP e IPAM utilizada para la administración centralizada de direcciones IP y servicios de red, comúnmente empleada en entornos TELCO.

Bosque (Forest): Nivel jerárquico más alto de una implementación de Active Directory. Puede contener múltiples dominios y representa una frontera de seguridad y confianza.

Controlador de Dominio (Domain Controller – DC): Servidor que almacena una copia del directorio de Active Directory y proporciona servicios de autenticación y autorización a usuarios y equipos del dominio.

DHCP (Dynamic Host Configuration Protocol): Protocolo que asigna automáticamente direcciones IP y otros parámetros de red a los dispositivos. Aunque no es parte directa de Active Directory, es fundamental para la conectividad de los clientes al dominio.

DNS (Domain Name System): Sistema que traduce nombres de dominio legibles por humanos en direcciones IP. En entornos de Active Directory, es esencial para localizar controladores de dominio y servicios de red.

EDR/XDR (Endpoint/Extended Detection and Response): Soluciones de seguridad que permiten detectar, analizar y responder a amenazas avanzadas en endpoints y entornos corporativos.

ENTRA ID: Servicio de identidad en la nube de Microsoft que reemplaza Azure AD, proporcionando gestión de identidades, autenticación y control de acceso.

FSMO (Flexible Single Master Operations): Conjunto de cinco roles críticos en Active Directory que deben ser únicos dentro del dominio o bosque. Incluyen Schema Master, Domain Naming Master, RID Master, PDC Emulator e Infrastructure Master.

GPO (Group Policy Object): Conjunto de configuraciones que permiten a los administradores definir políticas de seguridad, scripts, instalación de software y configuraciones del entorno de usuario y equipo dentro de un dominio.

Kerberos: Protocolo de autenticación basado en tickets que permite la comunicación segura entre usuarios y servicios dentro de una red.

LDAP (Lightweight Directory Access Protocol): Protocolo estándar utilizado por Active Directory para consultar y modificar objetos dentro del directorio, siendo la base de los procesos de autenticación y búsqueda.

MFA (Multi-Factor Authentication): Método de autenticación que requiere más de un factor de verificación para confirmar la identidad de un usuario.

MPLS (Multiprotocol Label Switching): Tecnología de red que optimiza el tráfico mediante la conmutación de etiquetas, utilizada para mejorar el rendimiento y la calidad del servicio.

NTLM (NT LAN Manager): Protocolo de autenticación de Microsoft basado en un mecanismo de desafío y respuesta, considerado menos seguro que Kerberos.

OU (Organizational Unit): Contenedor lógico dentro de Active Directory que permite organizar usuarios, grupos y equipos, facilitando la delegación administrativa y la aplicación de GPOs específicas.

Replicación de Active Directory: Proceso mediante el cual los controladores de dominio sincronizan su información para mantener la coherencia de los datos en toda la infraestructura.

SD-WAN (Software-Defined Wide Area Network): Tecnología de red que permite gestionar y optimizar la conectividad entre sedes mediante software.

VPN (Virtual Private Network): Red privada virtual que permite establecer conexiones seguras a través de internet mediante cifrado de datos.

Introducción

Este anteproyecto propone el diseño de una solución técnica para la migración y unificación de dominios corporativos entre las sedes de una compañía multinacional ubicadas en Colombia, Guatemala, El Salvador y Panamá. Actualmente, cada sede opera con su propio dominio, lo cual genera dificultades en la administración centralizada de usuarios, políticas de seguridad y recursos compartidos. El objetivo es consolidar todos los dominios bajo una única estructura centralizada en Colombia, optimizando la gestión de TI y fortaleciendo la seguridad corporativa. La metodología incluye análisis de infraestructura, diseño de arquitectura de dominio, planificación de migración y pruebas piloto. Se espera como resultado una infraestructura unificada, Segura y escalable. Diseñar e implementar una solución técnica integral para la migración y unificación de dominios corporativos en una compañía multinacional con sedes en Colombia, Guatemala, El Salvador y Panamá. Actualmente, cada sede opera con un dominio independiente, lo que genera fragmentación en la administración de usuarios, políticas de seguridad, recursos compartidos y servicios de red. La propuesta busca consolidar todos los dominios bajo una infraestructura centralizada en Colombia, que funcionará como el dominio corporativo principal, permitiendo una administración más eficiente, segura y escalable. Para lograrlo, se plantea una serie de tareas técnicas que incluyen:

Análisis detallado de la infraestructura actual en cada sede, identificando controladores de dominio, servicios activos, políticas aplicadas y dependencias locales.

Diseño de la arquitectura del nuevo dominio corporativo, incluyendo la definición de Unidades Organizativas (OU), políticas de grupo (GPO), roles FSMO, y replicación entre controladores.

Configuración de túneles VPN seguros entre las sedes para garantizar la conectividad y replicación de Active Directory.

Migración de objetos de directorio (usuarios, grupos, equipos) utilizando herramientas como ADMT y scripts en PowerShell, asegurando la integridad de los datos y la continuidad operativa.

Implementación de políticas de seguridad unificadas, incluyendo autenticación, auditoría, control de acceso y cifrado de comunicaciones.

Pruebas piloto de migración, validando la funcionalidad del nuevo dominio, la replicación entre sedes y la correcta aplicación de políticas.

Documentación técnica completa, que incluirá diagramas de arquitectura, procedimientos de migración, manuales de administración y resultados de pruebas.

Este proyecto no solo representa una solución tecnológica para la empresa, sino también una aplicación práctica de los conocimientos adquiridos en la carrera de Ingeniería en Telecomunicaciones, abarcando áreas como redes, seguridad informática, administración de sistemas, virtualización y gestión de servicios corporativos. Se espera como resultado una infraestructura de dominio unificada, robusta y alineada con las mejores prácticas de administración de TI, que permita a la organización operar de manera más eficiente, segura y preparada para futuras expansiones.

Planteamiento del problema

La compañía actualmente administra múltiples dominios independientes en sus sedes de Colombia, Guatemala, El Salvador y Panamá. Esta fragmentación dificulta la administración centralizada de usuarios, políticas de seguridad, recursos compartidos y mantenimiento de infraestructura. Además, genera redundancia en procesos administrativos y técnicos, aumentando los costos operativos y reduciendo la eficiencia. Es necesario diseñar una solución que permita la migración y unificación de estos dominios bajo una única estructura corporativa centralizada en Colombia.

Actualmente, la compañía multinacional objeto de este estudio opera con infraestructuras de dominio independientes en sus sedes de Colombia, Guatemala, El Salvador y Panamá. Cada una de estas sedes mantiene su propio controlador de dominio, políticas de grupo (GPO), usuarios, equipos y servicios de red, lo que ha generado una serie de problemas técnicos, administrativos y de seguridad que afectan la eficiencia operativa de la organización.
Entre los principales problemas identificados se encuentran:

Falta de centralización en la administración de usuarios y recursos, lo que implica duplicidad de esfuerzos, inconsistencias en las políticas de seguridad y dificultades en la gestión de accesos.

Ausencia de una política de replicación y respaldo unificada, lo que pone en riesgo la integridad de los datos y la continuidad del negocio ante fallos o ataques.

Dificultades en la implementación de políticas corporativas homogéneas, debido a la dispersión de dominios y la autonomía técnica de cada sede.

Incremento en los costos operativos y de licenciamiento, al mantener múltiples infraestructuras paralelas sin una estrategia de consolidación.

Limitaciones en la movilidad y autenticación de usuarios entre sedes, lo que afecta la colaboración y el acceso a recursos compartidos.

Ante este panorama, se hace necesario diseñar e implementar un proyecto de migración y unificación de dominios, que permita consolidar todas las sedes bajo un único dominio corporativo centralizado en Colombia, con replicación segura y políticas estandarizadas.

Este proceso implica una serie de tareas técnicas críticas, entre las que se destacan:

Evaluación de la infraestructura actual en cada país, incluyendo hardware, software, servicios activos y dependencias.

Diseño de una arquitectura de dominio escalable y segura, que contemple roles FSMO, estructura de OUs, políticas de replicación y redundancia.

Establecimiento de canales de comunicación seguros (VPN) entre las sedes para garantizar la replicación de Active Directory y la autenticación remota.

Migración controlada de objetos de directorio mediante herramientas como ADMT, asegurando la integridad de los datos y la continuidad operativa.

Pruebas de validación funcional y de rendimiento, para garantizar que el nuevo dominio cumpla con los requisitos técnicos y de negocio.

Este planteamiento del problema justifica la necesidad de una solución integral que no solo resuelva los desafíos actuales, sino que también prepare a la organización para una gestión de TI más eficiente, segura y alineada con las mejores prácticas internacionales.

Justificación

La unificación de dominios permitirá una administración más eficiente de los recursos tecnológicos, mejorando la seguridad, la escalabilidad y la interoperabilidad entre sedes. Desde el punto de vista académico, este proyecto representa una aplicación práctica de los conocimientos adquiridos en la carrera de Ingeniería en Telecomunicaciones, especialmente en áreas como redes, seguridad informática, administración de sistemas y servicios de directorio.

La necesidad de migrar y unificar los dominios corporativos de una compañía con presencia en Colombia, Guatemala, El Salvador y Panamá surge como respuesta a los desafíos técnicos, operativos y de seguridad que implica mantener infraestructuras de TI fragmentadas. Cada sede opera actualmente con un dominio independiente, lo que genera duplicidad de esfuerzos administrativos, inconsistencias en políticas de seguridad y dificultades en la interoperabilidad de servicios.

Desde una perspectiva técnica, la unificación de dominios permite centralizar la administración de usuarios, grupos y equipos, reduciendo la carga operativa del personal de TI en cada sede. Asimismo, facilita la aplicación uniforme de políticas de grupo (GPO), garantizando que todos los usuarios operen bajo los mismos estándares de seguridad y configuración. De igual manera, optimiza la replicación de servicios críticos como la autenticación, el acceso a recursos compartidos y la auditoría de eventos. Además, reduce la superficie de ataque al consolidar la infraestructura bajo un esquema de seguridad corporativa más robusto y controlado, y permite la implementación de soluciones de alta disponibilidad y recuperación ante desastres, al contar con una arquitectura más coherente y predecible.

Desde el punto de vista académico y formativo, este proyecto representa una oportunidad para aplicar conocimientos adquiridos en áreas clave como el diseño de redes corporativas y

servicios de directorio (Active Directory), la configuración de servicios de red como DNS, DHCP y VPN, la migración de objetos entre dominios mediante herramientas como ADMT y PowerShell, la gestión de roles FSMO y la replicación entre controladores de dominio, así como la documentación técnica y la planificación de proyectos de TI.

En síntesis, la implementación de este proyecto no solo beneficiará a la organización al mejorar su eficiencia operativa y su postura de seguridad, sino que también permitirá al estudiante demostrar competencias profesionales en un entorno real, fortaleciendo su perfil como futuro ingeniero en telecomunicaciones.

Objetivos

Objetivo general

Diseñar e implementar una solución técnica integral para la migración, consolidación y administración centralizada de los dominios corporativos de las sedes internacionales de la compañía, estableciendo un dominio único y robusto en la sede principal ubicada en Colombia, que garantice la interoperabilidad, seguridad, escalabilidad y eficiencia operativa entre todas las sedes.

Objetivos Específicos

Analizar la infraestructura tecnológica y los dominios de Active Directory existentes en las sedes internacionales de Colombia, Guatemala, El Salvador y Panamá, con el fin de identificar el estado actual, las dependencias críticas y las posibles incompatibilidades para el proceso de migración.

Diseñar una arquitectura de dominio unificado basada en Active Directory que permita la integración segura y escalable de las sedes internacionales, garantizando una gestión centralizada de identidades, políticas y servicios de red.

Establecer políticas estandarizadas de seguridad y replicación que aseguren la confidencialidad, integridad y disponibilidad de la información, alineadas con buenas prácticas y estándares internacionales de seguridad de la información.

Ejecutar y validar pruebas piloto de migración del dominio unificado, evaluando el desempeño, la continuidad del servicio y la correcta operación de los mecanismos de autenticación, replicación y control de acceso antes del despliegue final.

Marco Teórico

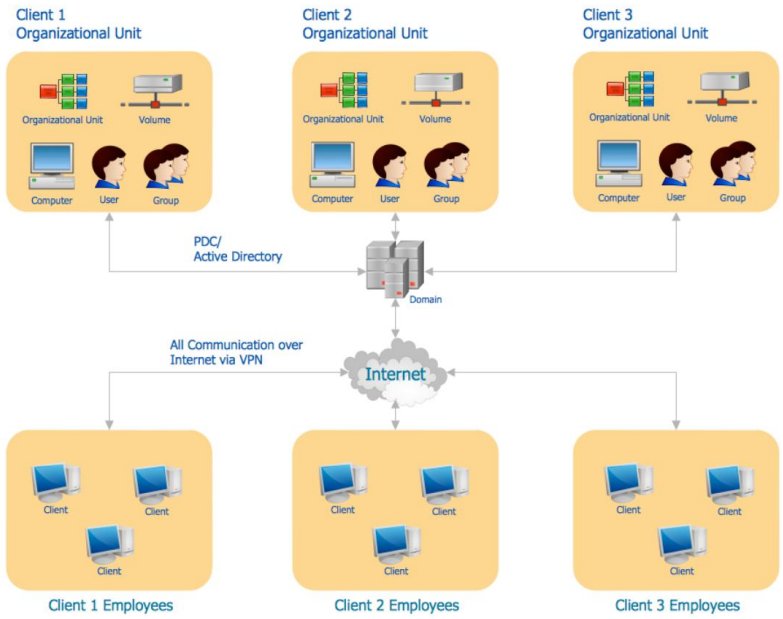
Este proyecto se fundamenta en conceptos clave como Active Directory, DNS, DHCP, políticas de grupo (GPO), replicación de controladores de dominio y herramientas de migración como ADMT. Active Directory permite la administración centralizada de usuarios y recursos. Las políticas de grupo permiten aplicar configuraciones de seguridad y operativas. La replicación entre controladores de dominio garantiza la disponibilidad y consistencia de los datos. Las herramientas como ADMT y PowerShell facilitan la migración de objetos entre dominios.

El presente proyecto se fundamenta en una serie de conceptos técnicos y arquitectónicos que son esenciales para comprender la complejidad y el alcance de una migración y unificación de dominios en un entorno corporativo distribuido. A continuación, se describen los principales elementos conceptuales que sustentan el desarrollo del anteproyecto.

Active Directory (AD)

Figura 0

Estructura de Active Directory con Unidades Organizativas

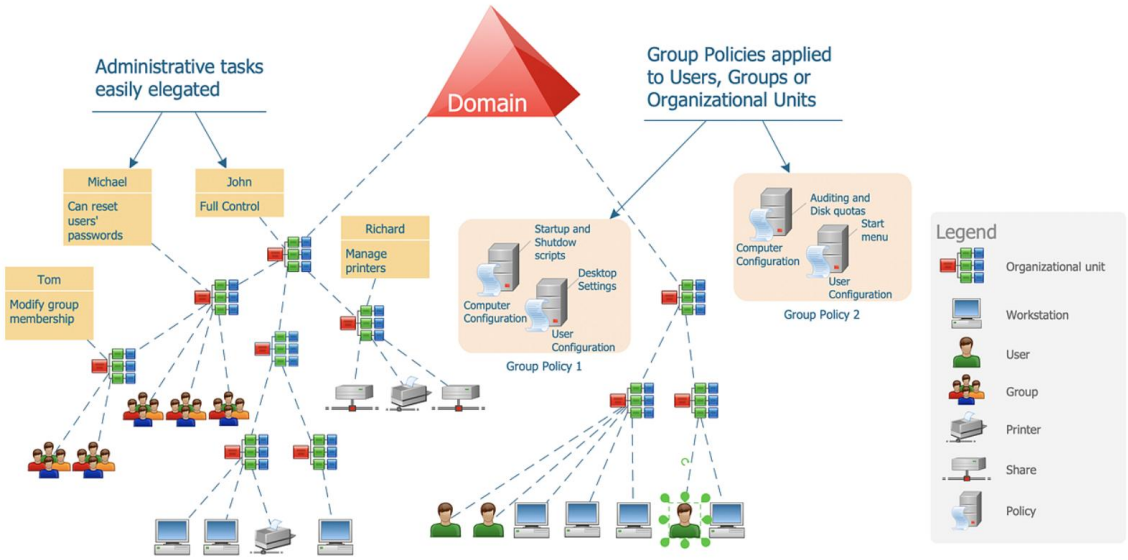


Fuente: https://www.conceptdraw.com/examples/active-directory-structure

Un directorio es una estructura jerárquica que almacena información sobre objetos en la red. Un servicio de directorio, como Active Directory Domain Services (AD DS), proporciona los métodos para almacenar datos de directorio y poner dichos datos a disposición de los usuarios y administradores de la red. Por ejemplo, AD DS almacena información acerca de las cuentas de usuario, como nombres, contraseñas, números de teléfono, etc., y permite que otros usuarios autorizados de la misma red tengan acceso a dicha información. (Microsoft Corporation, 2025).

Figura 1

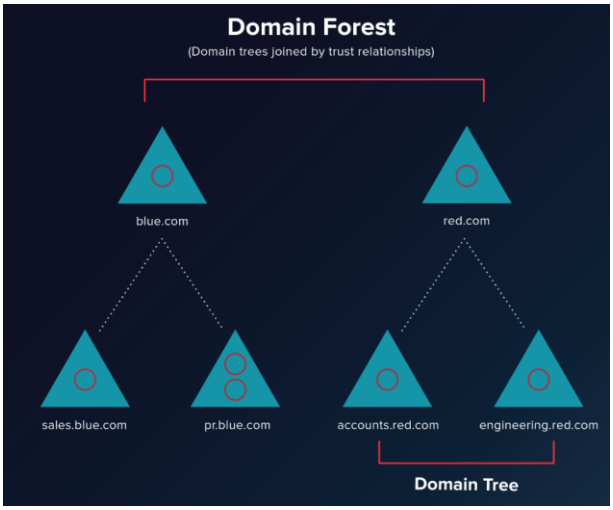
Diagrama de servicios de dominio de Active Directory



Nota. El diagrama muestra una infraestructura segura, gestionable y escalable para la administración de dominios. *Fuente*: https://www.conceptdraw.com/examples/active-directory-architecture-diagram

Figura 2

Estructura de bosque y árboles de dominios en Active Directory

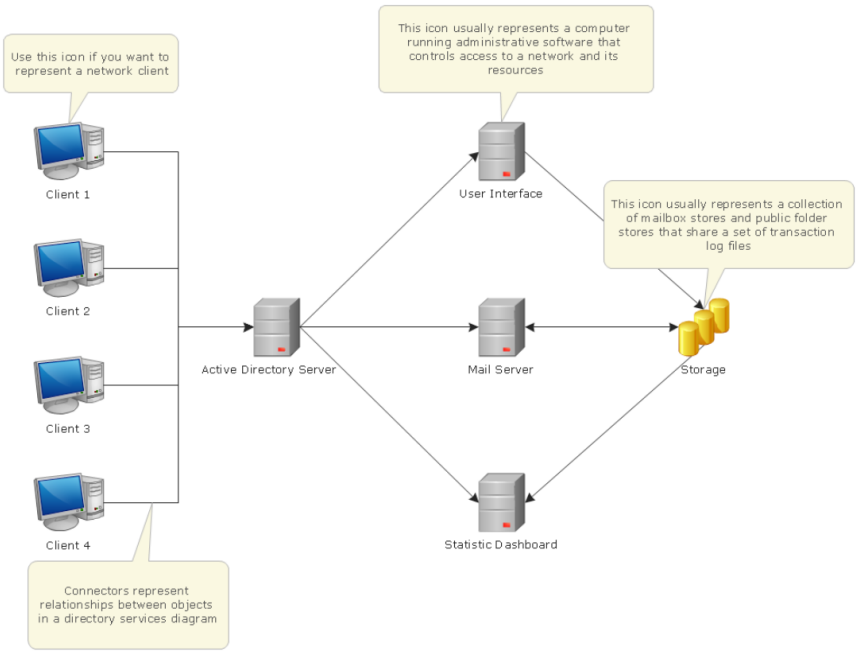


Fuente. https://www.varonis.com/blog/active-directory-forest

Active Directory almacena información acerca de los objetos de una red y facilita su búsqueda y uso por parte de los usuarios y administradores. Active Directory usa un almacén de datos estructurado como base para una organización jerárquica lógica de la información del directorio.

Figura 1

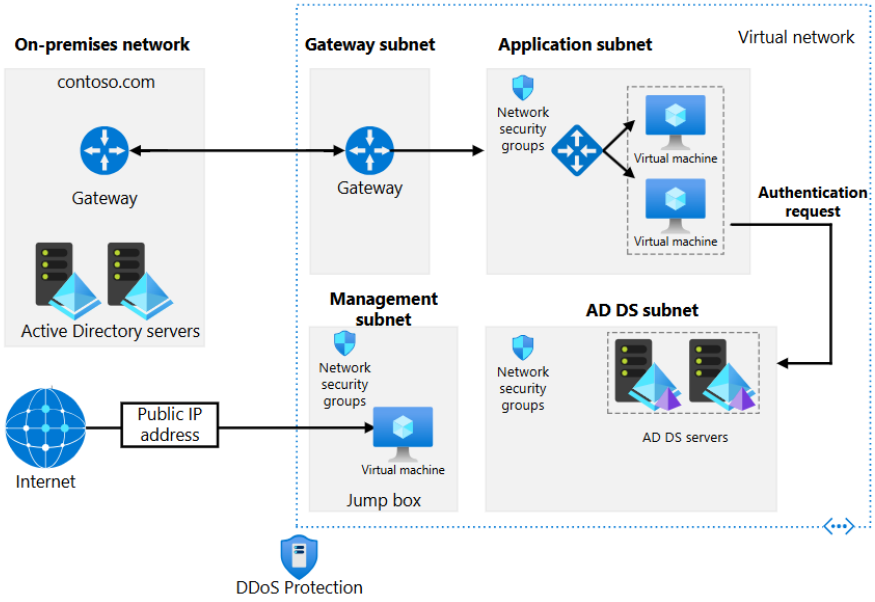
Integración de Active Directory con servicios corporativos



Nota. Diagrama que muestra la interacción de Active Directory con servicios empresariales como correo electrónico, almacenamiento y paneles de gestión. Active Directory actúa como núcleo de autenticación y autorización para el acceso a recursos corporativos. *Fuente* https://www.conceptdraw.com/examples/active-directory-architecture-diagram

Figura 2

Integración de Active Directory local con entornos en la nube (AD híbrido)



Fuente. https://learn.microsoft.com/es-es/azure/architecture/reference-architectures/identity/adds-forest

Este almacén de datos, también conocido como directorio, contiene información sobre los objetos de Active Directory. Estos objetos suelen incluir recursos compartidos como servidores, volúmenes, impresoras y cuentas de usuario y equipo de red. Para obtener más información sobre el almacén de datos de Active Directory, consulte Almacén de datos de directorio (Microsoft Corporation, 2025).

La seguridad se integra en Active Directory mediante la autenticación de inicio de sesión y el control de acceso a los objetos del directorio. Con un único inicio de sesión de red, los administradores pueden administrar los datos del directorio y la organización a través de su red, y los usuarios de red autorizados pueden tener acceso a los recursos en cualquier parte de la red (Varonis, 2022).

La administración basada en directiva facilita la administración de incluso las redes más complejas. Para obtener más información sobre la seguridad de Active Directory, consulte Introducción a la seguridad.

Figura 3

Integración de Active Directory con servicios de autenticación externa

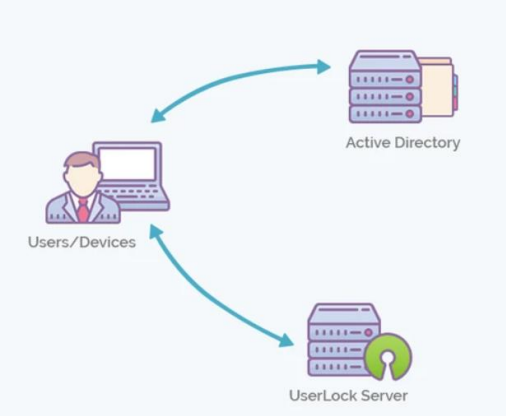
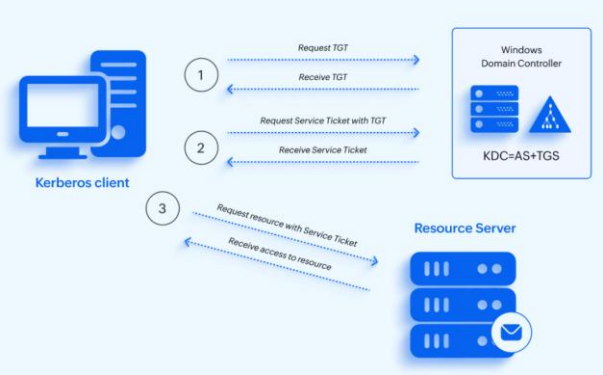


Figura 4

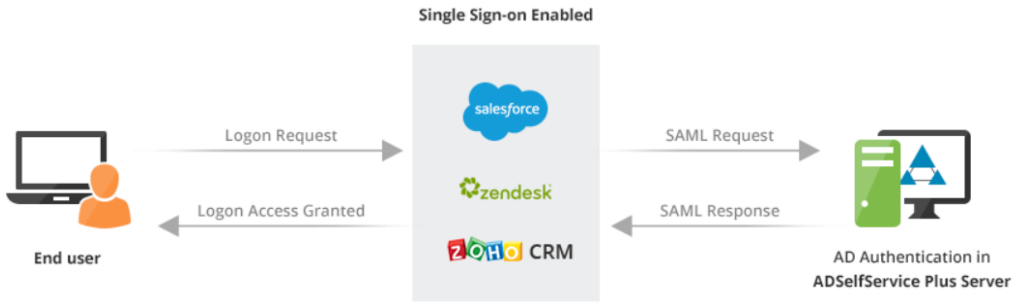
Proceso de autenticación Kerberos en Active Directory



Fuente. https://books.spartan-cybersec.com/cpad/introduccion-a-directorio-activo-ad/como-funciona-kerberos

Figura 5

Autenticación de usuarios mediante Single Sign-On (SSO)

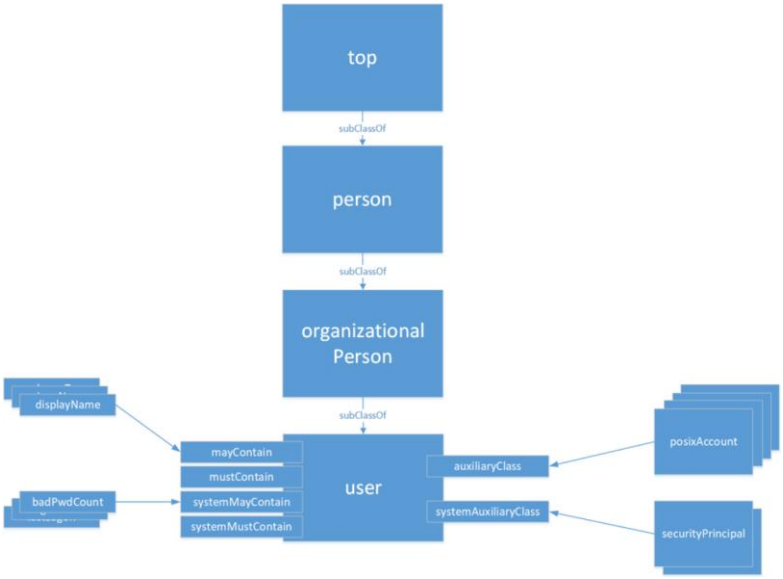


Fuente. https://www.manageengine.com/es/self-service-password/autenticación-sso-de-active-directory-de-windows.html

Active Directory también incluye un conjunto de reglas, el esquema, que define las clases de objetos y atributos contenidos en el directorio, las restricciones y los límites en las instancias de estos objetos y el formato de sus nombres. Para obtener más información acerca del esquema, consulte Esquema (IONOS, 2023).

Figura 6

Esquema lógico del modelo de objetos en Active Directory



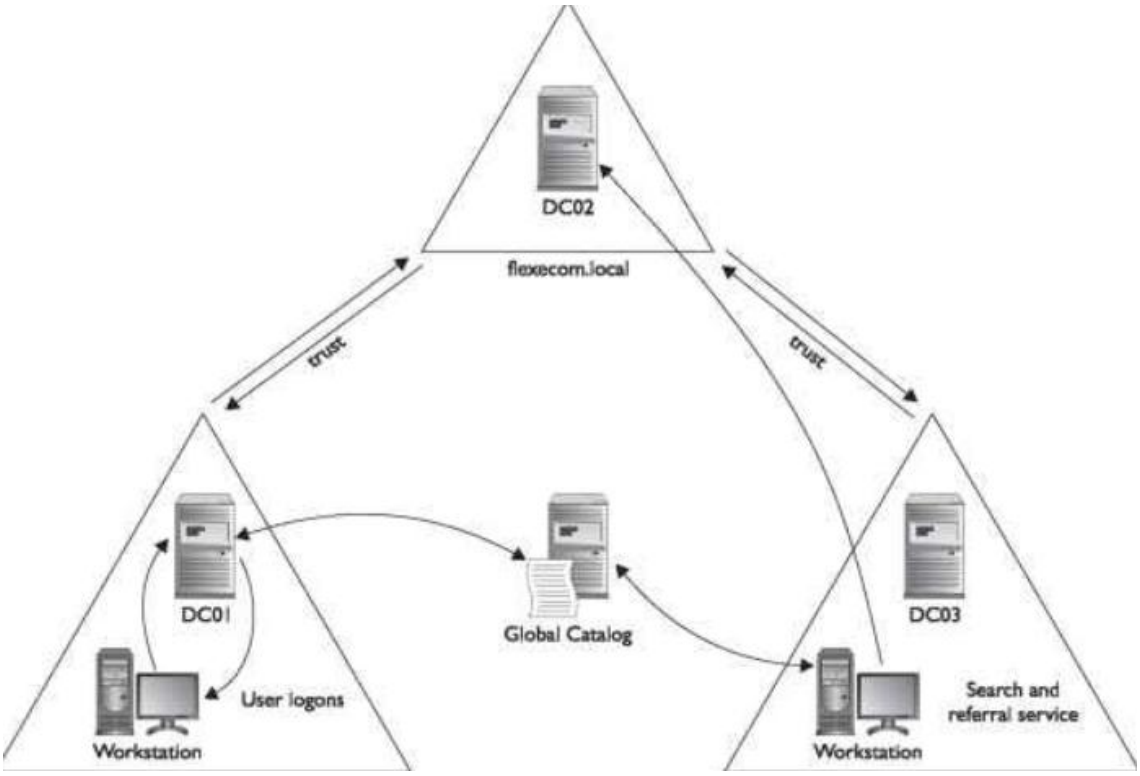
Fuente. https://www.easy365manager.com/how-to-get-all-active-directory-user-object-attributes/

Adicionalmente, el servicio incluye el Catálogo Global, que almacena información parcial de todos los objetos del bosque, permitiendo búsquedas eficientes entre dominios sin

importar su ubicación. Este componente resulta crítico en entornos multinacionales, donde la localización rápida de recursos y usuarios es un requisito operativo esencial.

Figura 7

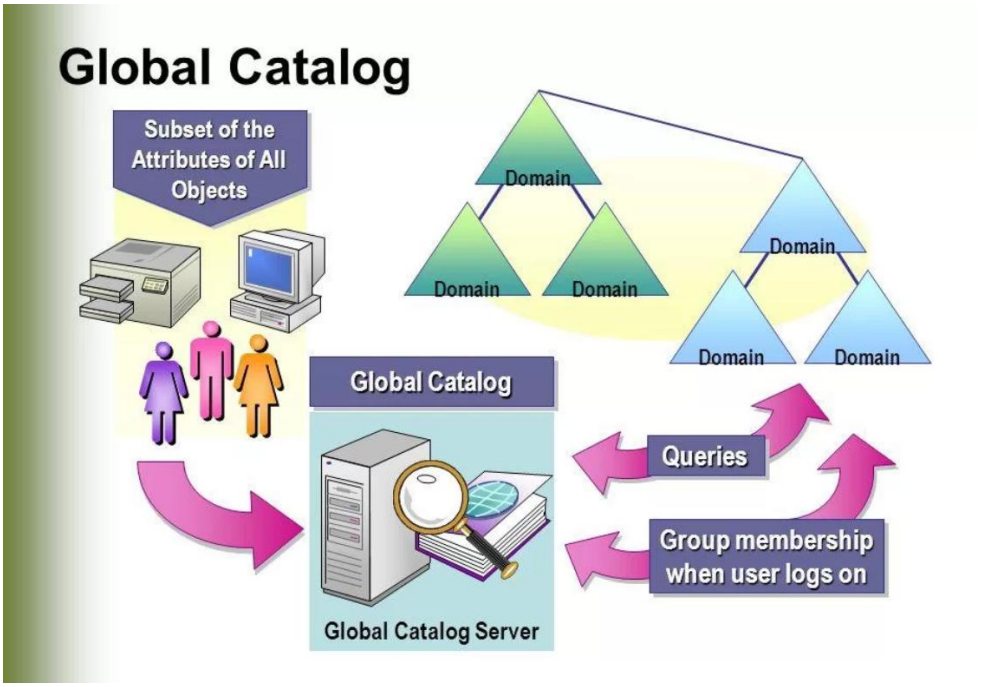
Función del Catálogo Global en Active Directory



Nota. Diagrama que muestra el rol del Catálogo Global dentro de Active Directory, evidenciando cómo los controladores de dominio almacenan información parcial de los objetos del directorio para facilitar búsquedas y autenticación de usuarios en entornos con múltiples dominios. *Fuente*. https://networkencyclopedia.com/global-catalog/

Figura 8

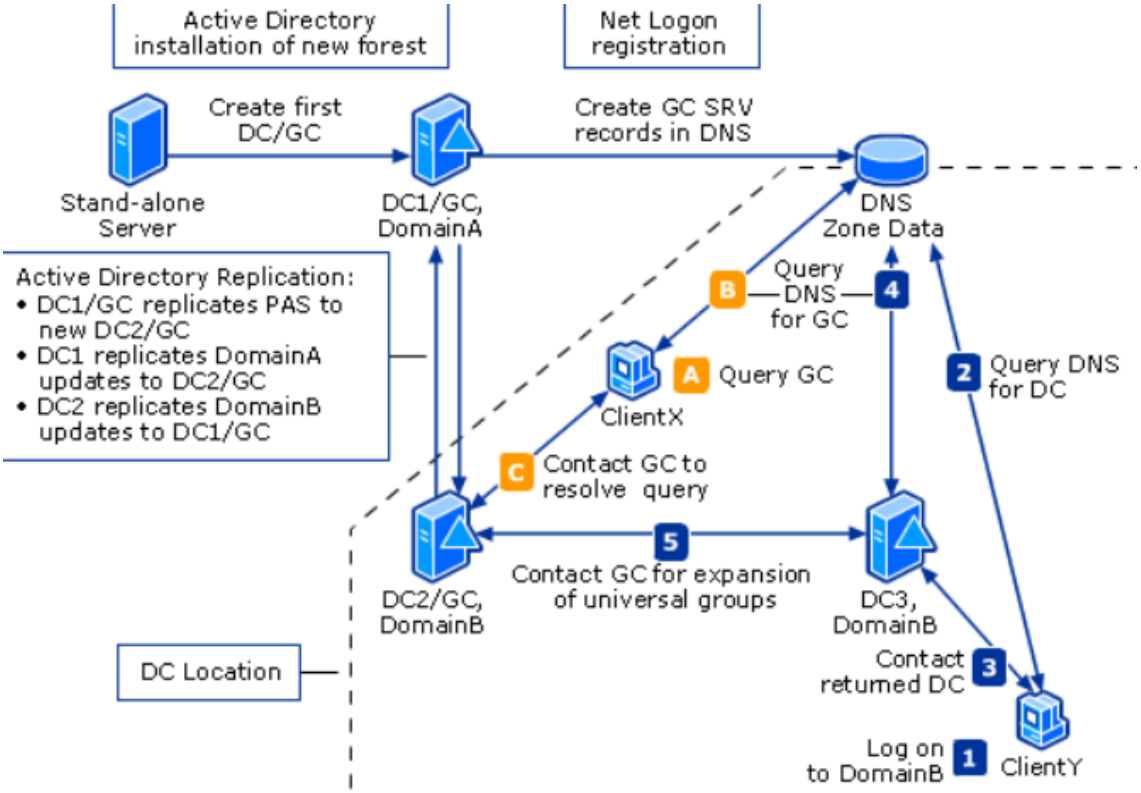
Funcionamiento del Catálogo Global en bosques de Active Directory



Fuente. https://windowstechno.com/what-is-global-catalog/

Figura 9

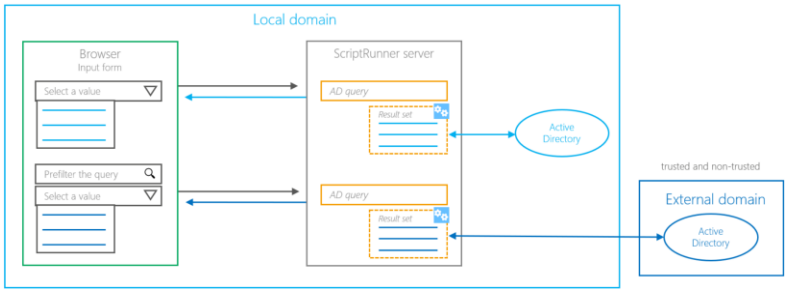
Proceso de consulta al Catálogo Global durante la autenticación



Nota. Flujo de autenticación de un usuario en un entorno multidominio, donde se muestra la interacción entre DNS, controladores de dominio y el Catálogo Global para resolver consultas y validar credenciales. *Fuente.* https://mikewu.org/powershell/search-users-across-active-directory-domains-powershell/

Figura 10

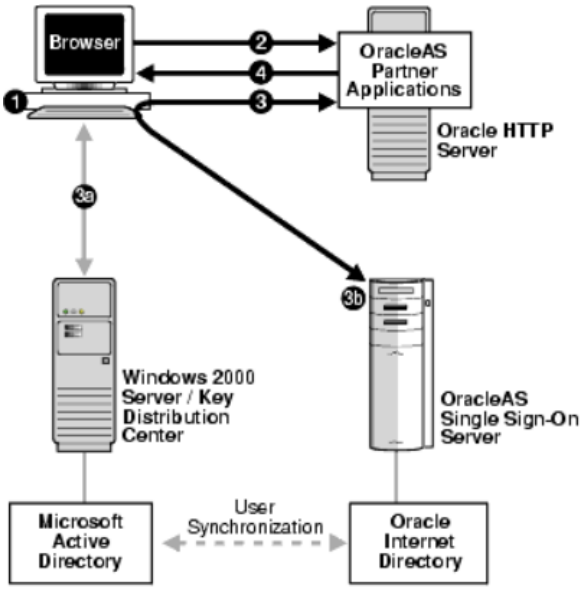
Consultas LDAP entre dominios confiables y no confiables



Nota. Diagrama que ilustra el flujo de consultas LDAP desde un dominio local hacia dominios externos, mostrando escenarios con relaciones de confianza y su impacto en la autenticación y búsqueda de objetos. *Fuente*. https://support.scriptrunner.com/articles/#!concepts/ad-queries

Figura 11

Integración de Active Directory con servicios externos mediante SSO

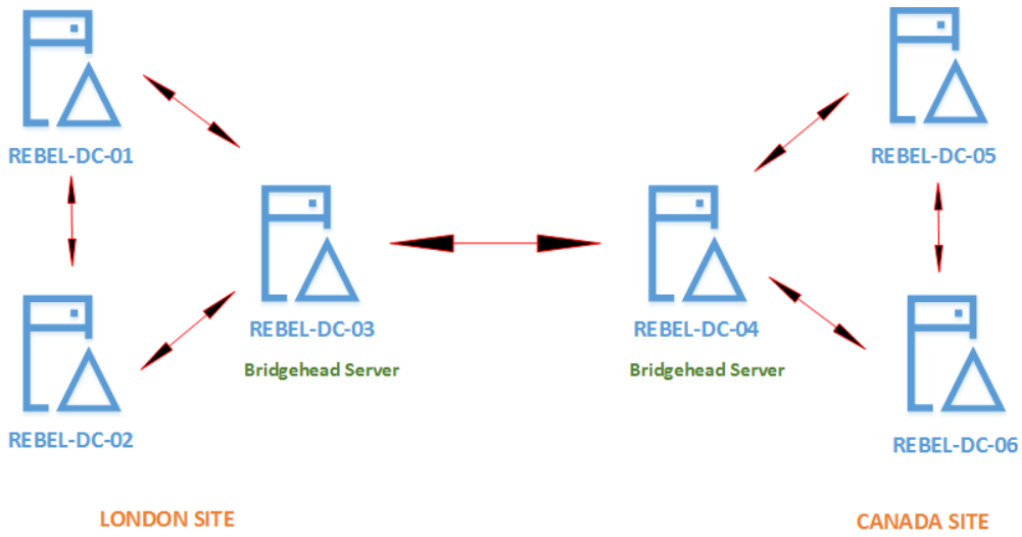


Nota. Arquitectura de integración entre Active Directory y servicios externos mediante mecanismos de autenticación centralizada y sincronización de identidades, permitiendo Single Sign-On (SSO) en aplicaciones empresariales. *Fuente.* https://docs.oracle.com/cd/F25597_01/document/products/cs/904/general/B15727-01/ch3_native.htm

La replicación es otro elemento clave de Active Directory. Todos los controladores de dominio mantienen copias sincronizadas del directorio, lo que garantiza la disponibilidad y consistencia de la información. Cualquier cambio realizado en un controlador se replica automáticamente a los demás, permitiendo tolerancia a fallos y continuidad del servicio incluso ante caídas parciales de la infraestructura (IONOS, 2023).

Figura 12

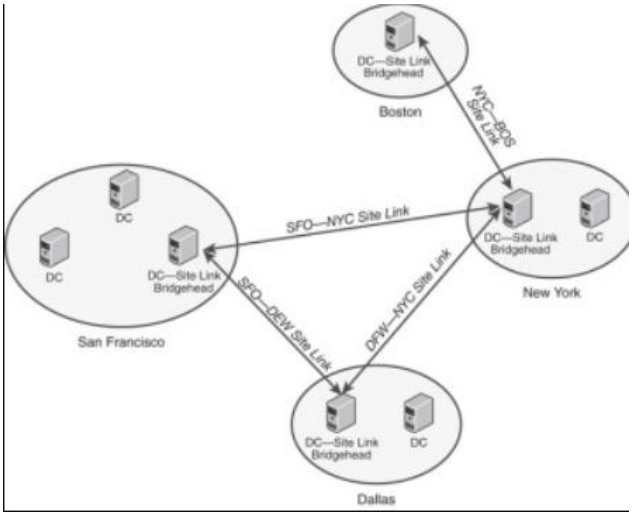
Replicación entre controladores de dominio en múltiples sedes



Nota. Diagrama de replicación entre controladores de dominio ubicados en distintas sedes geográficas, utilizando servidores puente (Bridgehead Servers) para optimizar el tráfico de replicación intersede. *Fuente.* https://pandorafms.com/es/it-topics/controladores-de-dominio-y-active-directory/

Figura 13

Topología de replicación intersede mediante Site Links

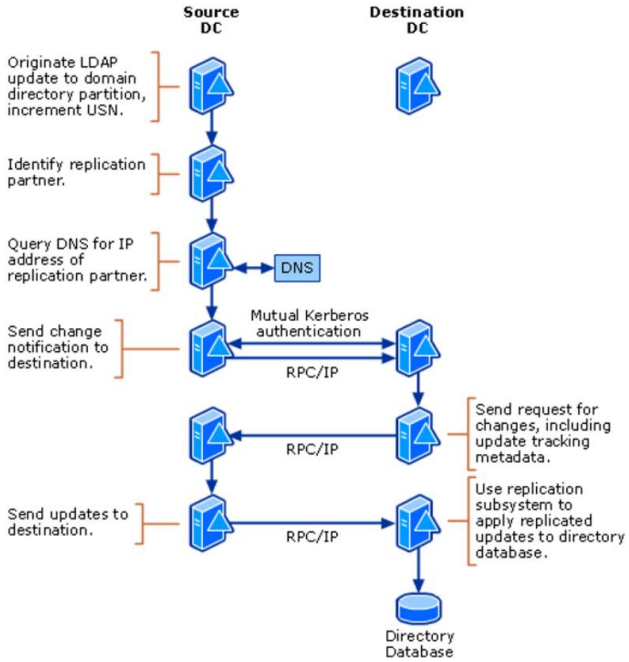


Nota. Representación de la topología de replicación entre sitios de Active Directory utilizando enlaces de sitio (Site Links), lo que permite controlar costos, horarios y rutas de replicación.

Fuente. https://flylib.com/books/en/4.34.1.58/1/

Figura 14

Flujo del proceso de replicación de Active Directory



Nota. Flujo detallado del proceso de replicación entre controladores de dominio, incluyendo autenticación Kerberos, resolución DNS y transferencia de cambios mediante RPC/IP. *Fuente*. https://www.systemconf.com/2020/06/11/what-is-active-directory-site-structure/

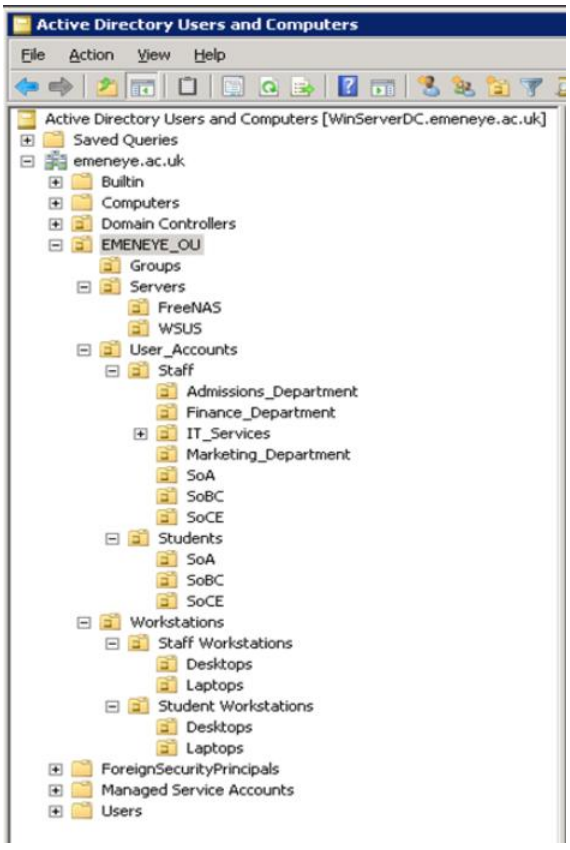
Tareas asociadas:

Dentro del proceso de migración y unificación de dominios, se contemplan tareas técnicas directamente relacionadas con Active Directory, tales como:

- Diseño de la estructura de Unidades Organizativas (OU) por país, área funcional o departamento.
- Configuración y distribución de los roles FSMO para garantizar equilibrio de carga y redundancia.

Figura 15

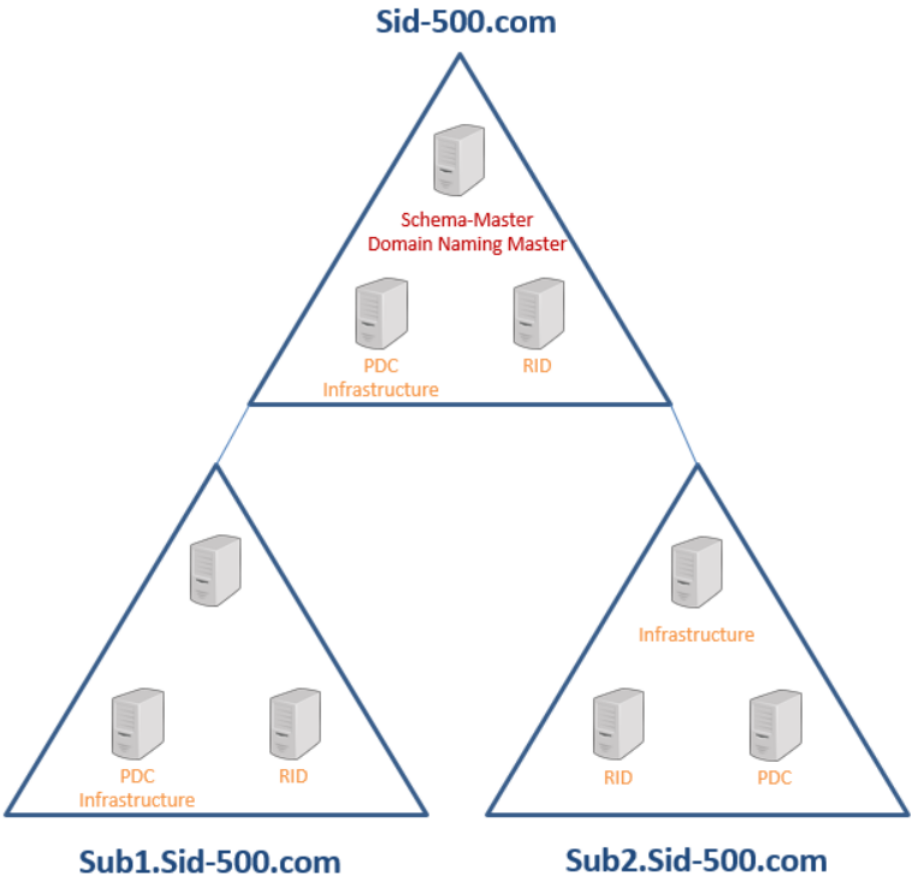
Estructura de Unidades Organizativas en Active Directory



Nota. Ejemplo de estructura jerárquica de Unidades Organizativas (OU) dentro de Active Directory, utilizada para organizar usuarios, equipos y recursos por áreas funcionales y aplicar políticas de grupo de forma granular. *Fuente.* https://emeneye.wordpress.com/2013/02/22/the-ou-structure-for-emeneye-ac-uk/

Figura 16

Distribución de roles FSMO en dominios y subdominios



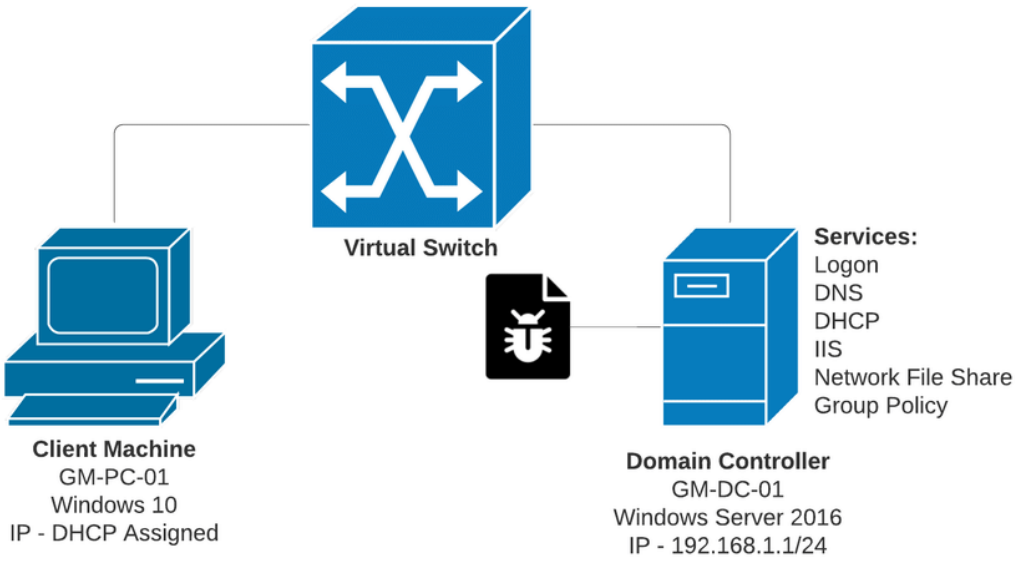
Nota. Diagrama que muestra la asignación de los roles FSMO dentro de un bosque y sus dominios hijos, destacando la función de cada rol en la operación y consistencia de Active Directory. *Fuente.* https://sid-500.com/2017/11/19/active-directory-flexible-single-master-fsmo-in-action/

Controladores de Dominio (Domain Controllers)

Para entender qué es un controlador de dominio, primero entendamos qué es dominio. Un dominio es simplemente una red de dispositivos (PC, ordenador portátil, impresoras, cámaras de seguridad, etc.) unidos mediante una infraestructura de conexión (cableada o Wi-fi) a un equipo servidor (que será el controlador de dominio). Es decir, un controlador de dominio es un servidor desde el cual se controla un conjunto de funciones de un dominio. Los dispositivos conectados a un dominio son principalmente servidores y estaciones de trabajo de Microsoft Windows (en sus diferentes versiones).

Figura 17

Arquitectura básica de un dominio con controlador de dominio



Nota. Diagrama que muestra la arquitectura básica de un dominio de Active Directory, donde un controlador de dominio centraliza servicios como autenticación, DNS, DHCP y aplicación de políticas de grupo a los equipos clientes del dominio. *Fuente*. https://www.researchgate.net/figure/Diagram-of-virtual-network-environment-The-domain-controller-was-assigned-a-static-IP_fig2_358422868

Funciones principales de un controlador de dominio

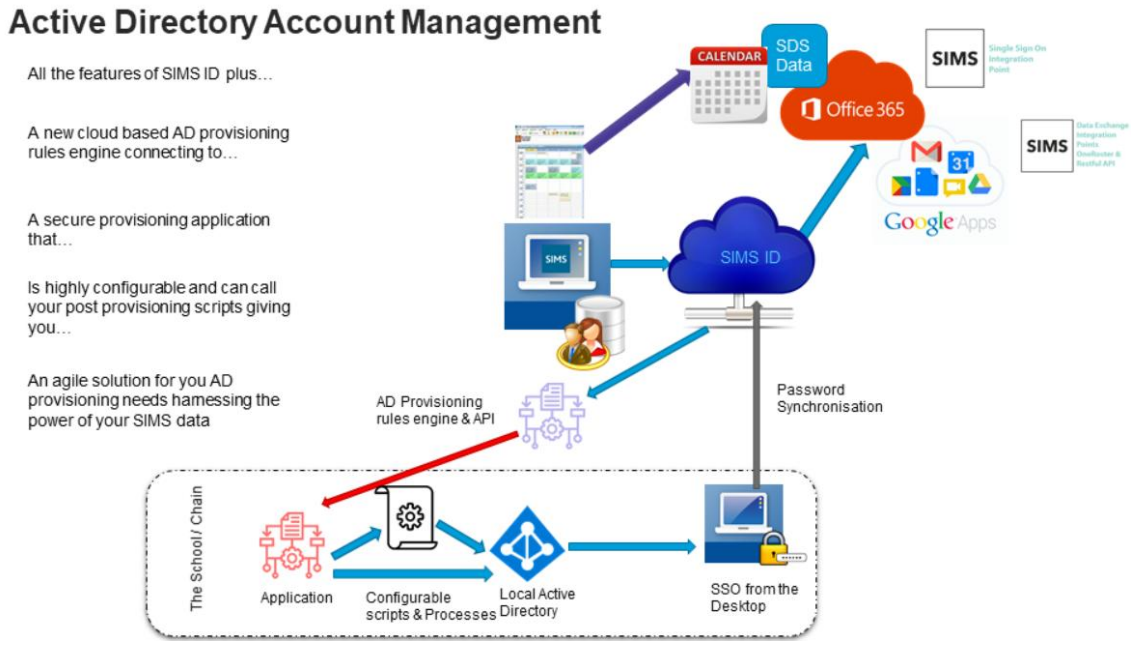
Albergar información de usuarios, gestión de contraseñas y accesos.

Distribuir software mediante directivas de grupo.

Gestionar políticas de usuarios y equipos. Cada usuario que esté dentro de un dominio tendrá asociada una cuenta de usuario única, mediante la cual podrá acceder a los recursos dentro del dominio siempre y cuando tenga derecho de acceso.

Figura 18

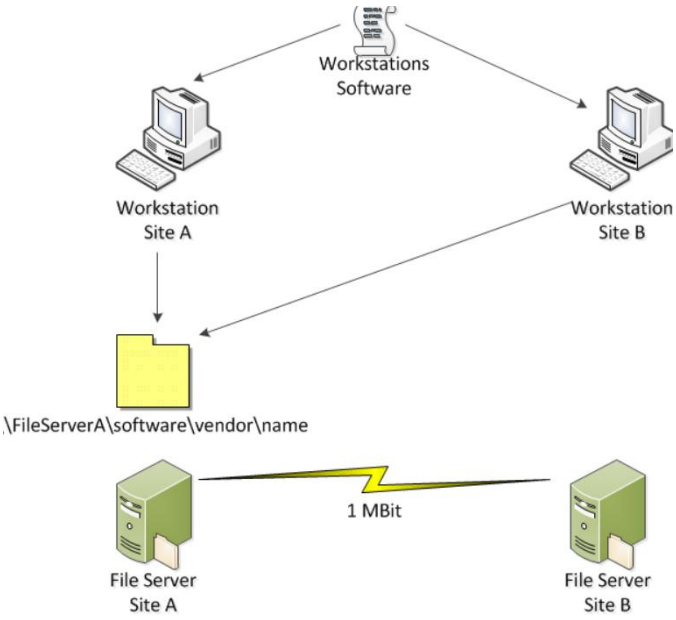
Gestión centralizada de identidades mediante Active Directory



Nota. Arquitectura de gestión de identidades que integra Active Directory con servicios en la nube y aplicaciones empresariales, permitiendo aprovisionamiento de cuentas, sincronización de contraseñas y autenticación mediante Single Sign-On (SSO). *Fuente*. https://id.sims.co.uk/support/pages/version/82b3265c-0ff9-48a2-8fef-d29682079517

Figura 19

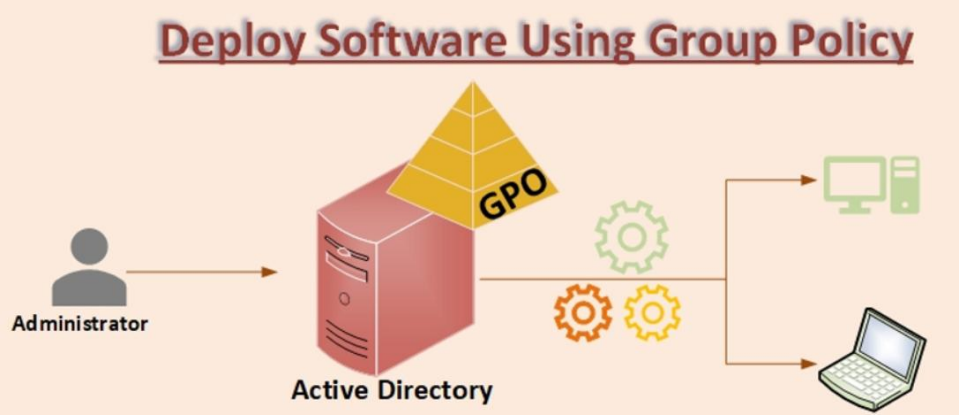
Acceso a recursos compartidos entre estaciones de trabajo



Nota. Esquema que representa el acceso a recursos compartidos en una red corporativa, donde las estaciones de trabajo autenticadas en el dominio acceden a servidores de archivos ubicados en distintas sedes. *Fuente*. https://www.grouppolicy.biz/2011/07/best-practice-configuring-a-software-library-for-group-policy-software-deployment/

Figura 20

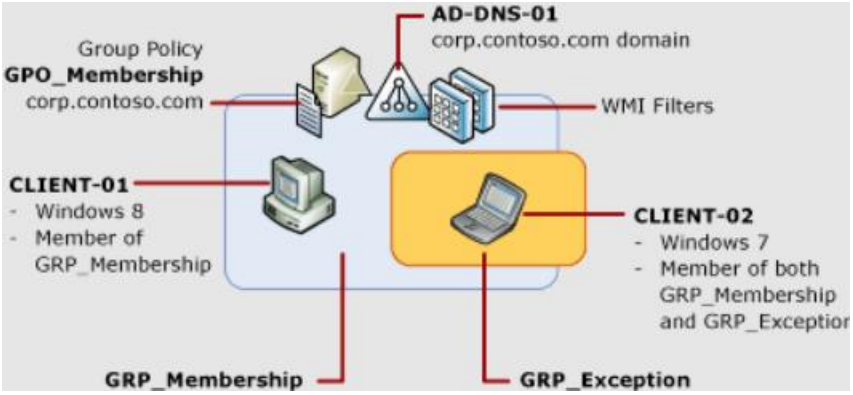
Despliegue de software mediante Políticas de Grupo (GPO)



Nota. Ilustración del uso de políticas de grupo para la distribución centralizada de software y configuraciones desde Active Directory hacia estaciones de trabajo del dominio. *Fuente*. https://bhanuwriter.com/deploy-software-using-group-policy/

Figura 21

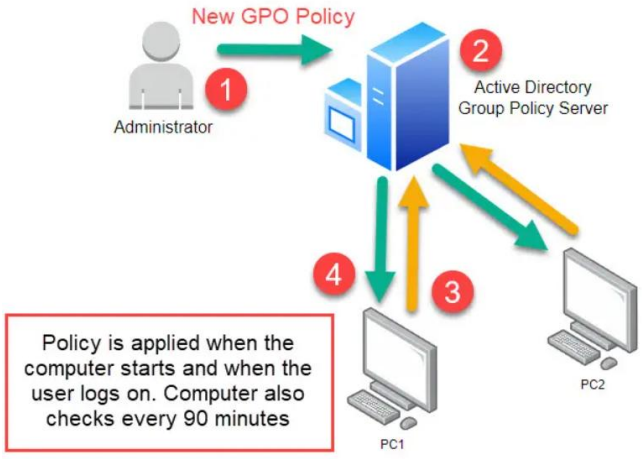
Aplicación de políticas de grupo según membresía y filtros



Nota. Diagrama que muestra cómo las políticas de grupo se aplican de forma selectiva según la pertenencia a grupos, excepciones y filtros WMI, permitiendo una administración granular. *Fuente*. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj899804%28v=ws.11%29

Figura 22

Ciclo de aplicación de políticas de grupo en Active Directory



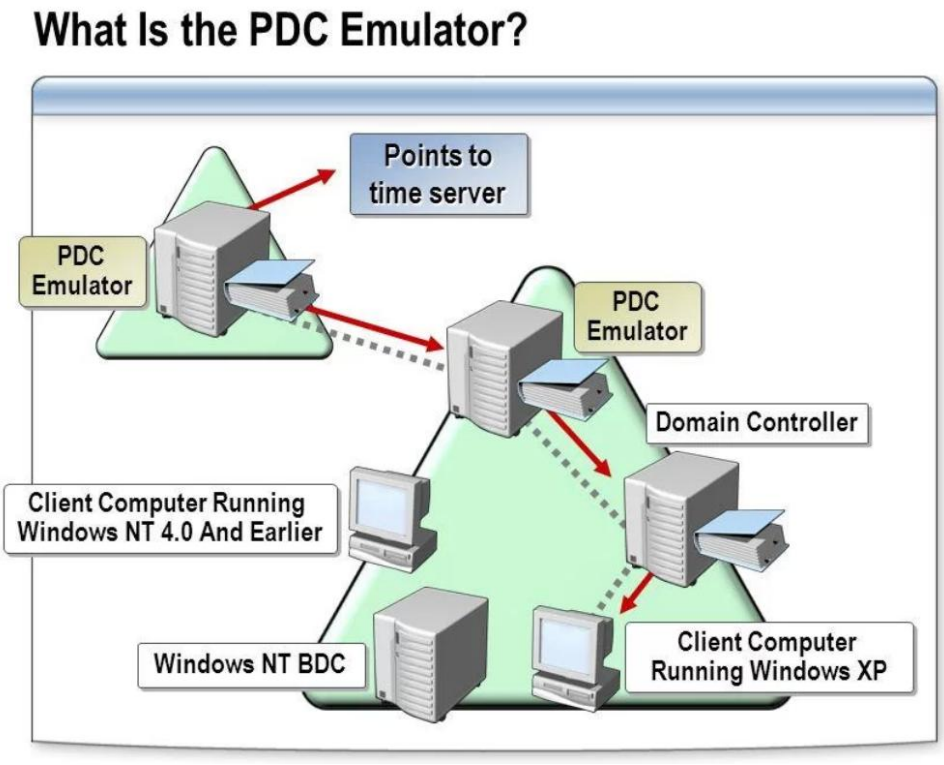
Nota. Flujo del proceso de aplicación de políticas de grupo, indicando los momentos en que las configuraciones se aplican a los equipos y usuarios durante el inicio de sesión y actualizaciones periódicas. *Fuente*. https://activedirectorypro.com/group-policy-guide/

Tipos de Controladores de Dominio

Los controladores de dominio normalmente se implementan como un clúster, para garantizar la alta disponibilidad y maximizar la confiabilidad. En un entorno Windows, un controlador de dominio actúa como controlador de dominio primario (Primary Domain Controller PDC) ver Figura 23; los demás servidores actúan como controladores de dominio de respaldo (Backup Domain Controller, BDC).

Figura 23

Rol del emulador PDC en entornos Windows



Nota. Diagrama que representa el rol del emulador PDC dentro de Active Directory, encargado de la sincronización horaria, compatibilidad con sistemas heredados y cambios críticos de autenticación. *Fuente.* https://windowstechno.com/primary-domain-controllerpdc-emulator/

En entornos basados en Unix, una máquina actúa como controlador de dominio maestro y otras actúan como controladores de dominio de réplica, replicando periódicamente la

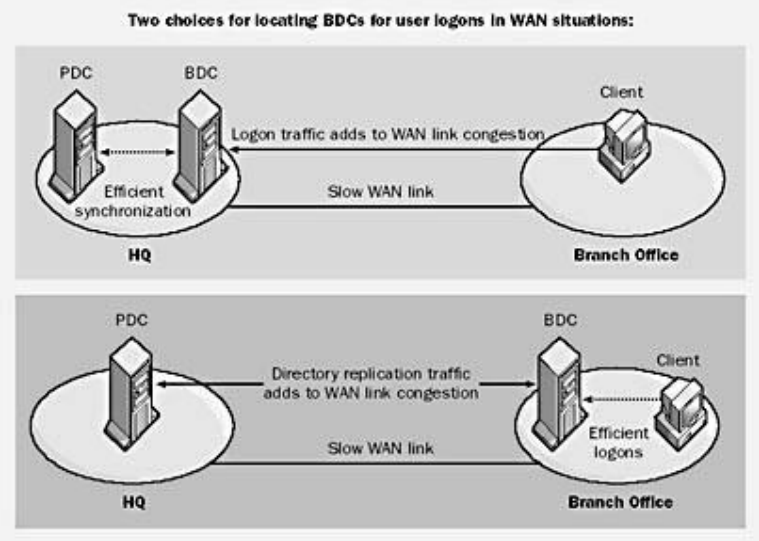
información de la base de datos del controlador de dominio principal y almacenándola en un formato únicamente de lectura. Para tenerlo más claro:

Controlador de dominio primario (PDC): En las primeras versiones de Windows Server, se designaba un controlador de dominio como PDC, que era responsable de mantener la copia maestra de la base de datos del usuario y administrar las solicitudes de inicio de sesión de los clientes. Si el PDC fallaba, se podía promover un controlador de dominio de respaldo (BDC) para que ocupara su lugar.

Controlador de dominio de respaldo (BDC): Los BDC se introdujeron para proporcionar redundancia a los PDC. Mantenían una copia de la base de datos de usuarios y podían autenticar a los clientes en caso de que el PDC no estuviera disponible.

Figura 24

Optimización de autenticación PDC/BDC en enlaces WAN

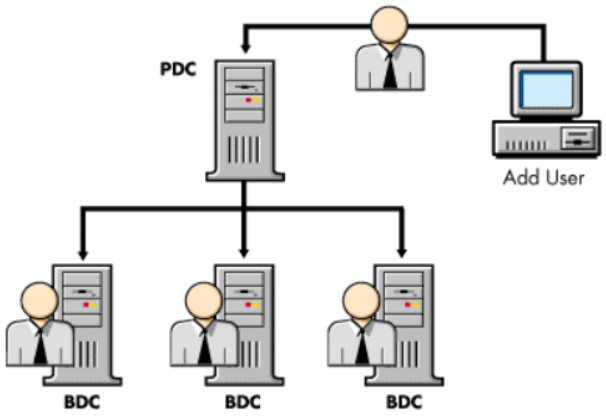


Nota. Comparación del tráfico de autenticación y replicación en enlaces WAN lentos, evidenciando la importancia de ubicar controladores de dominio cercanos a los usuarios para mejorar el rendimiento. *Fuente. https://networkencyclopedia.com/backup-domain-controller-bdc/*

Aun cuando hoy PDC y BDC ya no se usan en las redes modernas basadas en Windows, representan los dos tipos de controladores de dominio que se usaban en las primeras versiones de Windows Server. Desde Windows 2000, Active Directory (más adelante lo explicaremos) reemplazó las funciones de controlador de dominio principal y de controlador de dominio de respaldo.

Figura 25

Arquitectura clásica PDC y BDC



Nota. Representación del modelo clásico de controladores de dominio primario (PDC) y de respaldo (BDC), utilizado en versiones tempranas de Windows Server antes de la introducción de Active Directory.

Roles Especializados del Controlador de Dominio

Cuando se instala Windows Server en una computadora, se puede configurar una función de servidor específica para esa computadora. Cuando desee crear un dominio nuevo o un controlador de dominio adicional en un dominio existente, se configura el servidor con la función de controlador de dominio instalando Active Directory® Domain Services (AD DS).

Existen funciones de controlador de dominio especializadas que realizan funciones específicas en un entorno de AD DS.

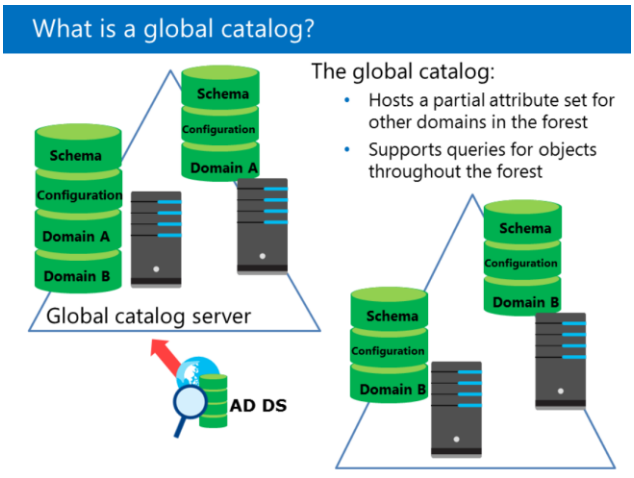
Servidores de catálogo global

Un servidor de catálogo global almacena su propia réplica de dominio completa y grabable (todos los objetos y todos los atributos) más una réplica parcial de solo lectura de todos los demás dominios. El sistema de replicación de AD DS crea y actualiza automáticamente el catálogo global. Los atributos de objeto que se replican en los servidores de catálogo global son los atributos que es más probable que se usen para buscar el objeto en AD DS. Los atributos que se replican en el catálogo global se identifican en el esquema como el conjunto de atributos parciales y Microsoft los define de forma predeterminada. Sin embargo, para optimizar la búsqueda, puede editar el esquema agregando o eliminando atributos almacenados en el catálogo global.

El catálogo global hace posible que los clientes busquen en AD DS sin tener que ser remitidos de un servidor a otro hasta que se encuentre un controlador de dominio que tenga la partición del directorio del dominio almacenando el objeto solicitado. De forma predeterminada, las búsquedas de AD DS se dirigen a servidores de catálogo global. El Catálogo Global permite realizar búsquedas y autenticaciones eficientes en entornos multidominio véase Figura 26.

Figura 26

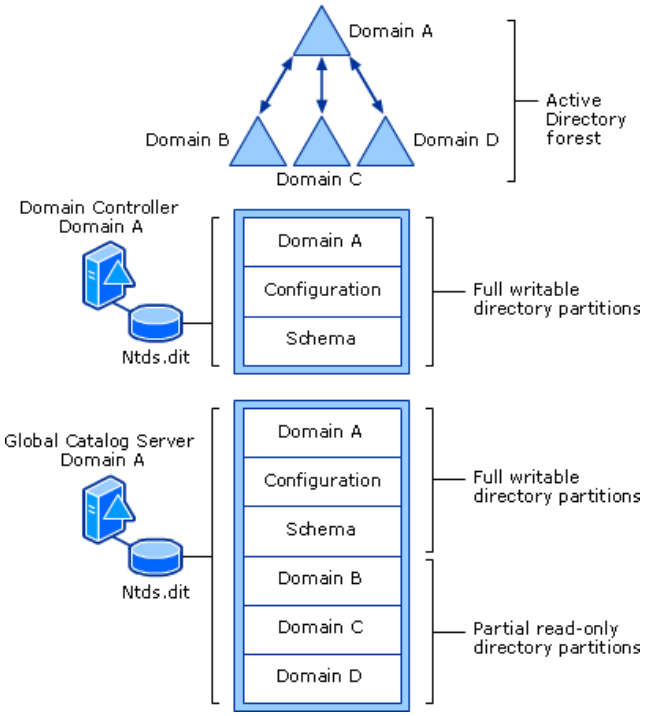
Función del Catálogo Global en Active Directory



Nota. Diagrama que ilustra el funcionamiento del Catálogo Global en Active Directory, mostrando cómo un servidor de catálogo global almacena una réplica completa de su dominio local y un conjunto parcial de atributos de otros dominios del bosque, permitiendo búsquedas y autenticación a nivel forestal. *Fuente*. https://www.youtube.com/watch?v=83Yk2YWe8YU

Figura 27

Diferencias entre un controlador de dominio estándar y un servidor de Catálogo Global



Nota. Comparación entre un controlador de dominio convencional y un servidor de Catálogo Global, evidenciando que este último almacenas particiones completas de su dominio y particiones parciales de solo lectura de los demás dominios del bosque, lo que optimiza las consultas distribuidas. *Fuente.* https://techiemaster.wordpress.com/2016/07/18/what-is-active-directory-global-catalog-server/

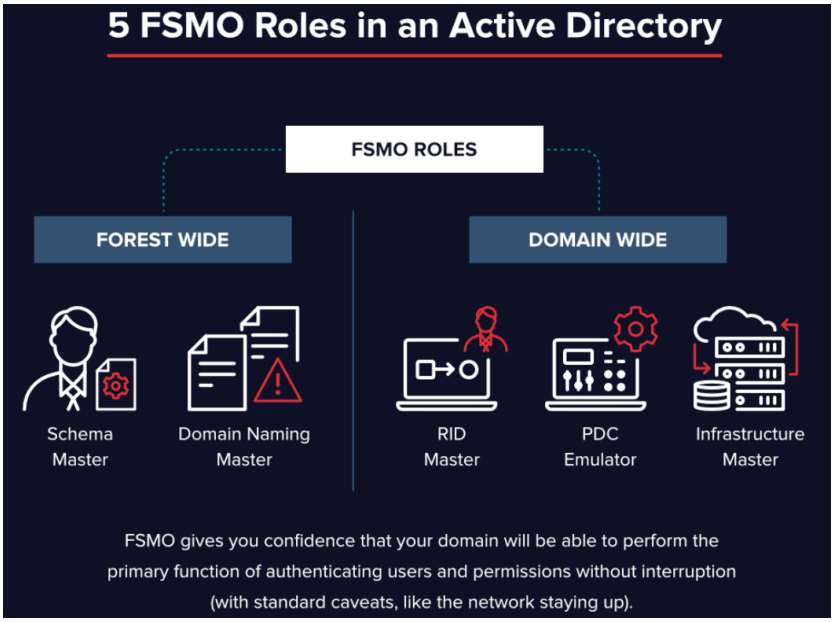
El primer controlador de dominio se crea automáticamente como servidor de catálogo global. A partir de entonces, pueden designar otros controladores de dominio para que sean

servidores de catálogo global si es necesario.

Los controladores de dominio que desempeñan funciones de maestro de operaciones están designados para realizar tareas específicas para garantizar la coherencia y eliminar la posibilidad de entradas conflictivas en la base de datos de Active Directory. AD DS define cinco funciones de maestro de operaciones: maestro de esquema, maestro de nombres de dominio, maestro de identificador relativo (relative identifier, RID), emulador de controlador de dominio principal (PDC) y maestro de infraestructura.

Figura 28

Roles FSMO en Active Directory a nivel de bosque y dominio



Nota. Representación de los cinco roles FSMO (Flexible Single Master Operations) en Active Directory, diferenciando los roles a nivel de bosque (Schema Master y Domain Naming Master) y los roles a nivel de dominio (RID Master, PDC Emulator e Infrastructure Master), esenciales para la coherencia y estabilidad del directorio. *Fuente*. https://www.zonasystem.com/2018/12/transferir-roles-fsmo-windows-server-y-purgado-de-servicios-del-dominio.html

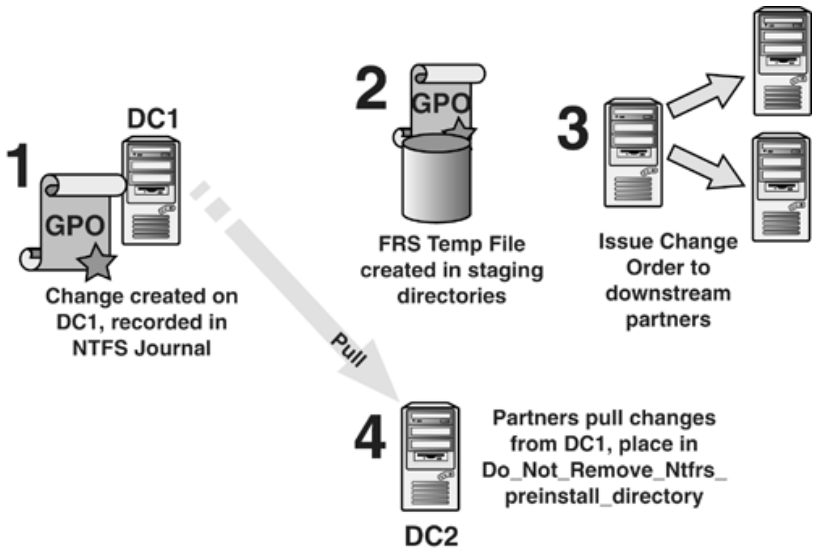
Políticas de Grupo (GPO)

La directiva de grupo puede representar la configuración de las directivas en el sistema de archivos localmente o en los servicios de dominio de Active Directory (AD DS). Cuando se usa con Active Directory (AD), la configuración de directiva de grupo se incluye en un objeto de directiva de grupo (GPO). Un GPO es una colección virtual de ajustes de directivas, permisos de seguridad y ámbito de administración (SOM) que puede aplicar a usuarios y equipos en Active Directory. Un GPO consta de dos componentes principales: el contenedor de directivas de grupo y la plantilla de directiva de grupo. El contenedor de directivas de grupo se almacena en la partición de dominio de Active Directory, mientras que la plantilla de directiva de grupo se encuentra en la carpeta SYSVOL de cada controlador de dominio (DC).

Estos componentes se replican entre DC a través de la replicación de AD y el servicio de replicación de archivos (FRS) o replicación del sistema de archivos distribuido (DFSR).

Figura 29

Replicación de Políticas de Grupo entre controladores de dominio



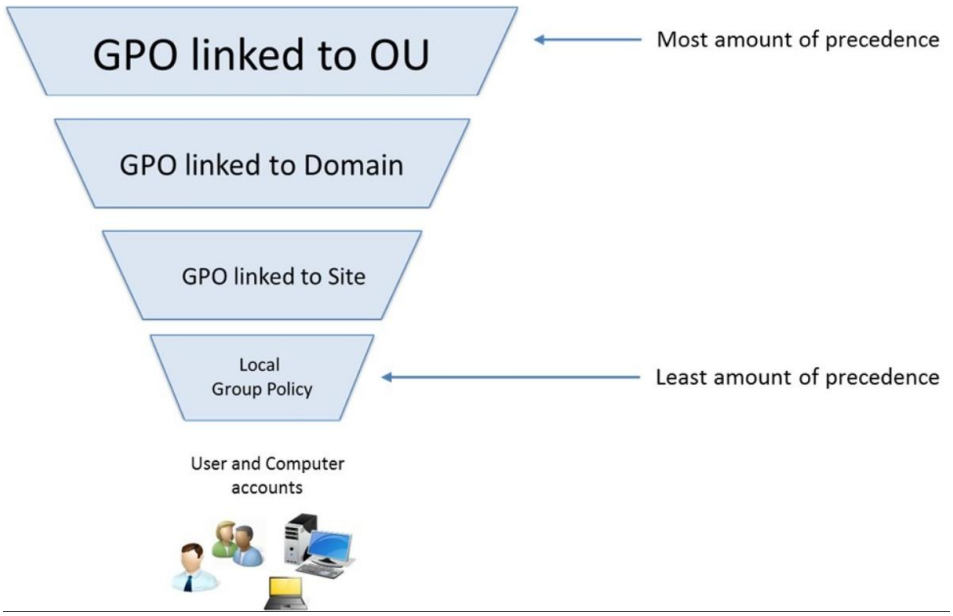
Nota. Diagrama que muestra el proceso de replicación de un objeto de directiva de grupo (GPO) entre controladores de dominio, utilizando los servicios de replicación FRS o DFSR para

garantizar la consistencia de las políticas en el dominio. *Fuente*. https://tutorial.wmlcloud.com/image/1304/File%20Replication%20Service%20Design%20and%20Implementation_1.jpg

Los GPO incluyen configuraciones tanto para el equipo como para el usuario. Las configuraciones de equipo se aplican a nivel del sistema y gestionan opciones como la gestión de energía y las normas de firewall. Las configuraciones de usuario solo afectan al usuario actual, con opciones como la configuración de Internet Explorer y el redireccionamiento de carpetas. Los GPO se pueden vincular a varios niveles dentro de la jerarquía de AD, como sitios, dominios y unidades organizativas (UO), que definen su ámbito de aplicación.

Figura 30

Precedencia de aplicación de Políticas de Grupo en Active Directory



Nota. Representación del orden de precedencia de las políticas de grupo, donde las GPO vinculadas a unidades organizativas tienen mayor prioridad que las aplicadas a nivel de dominio, sitio o política local. *Fuente*. https://emeneye.wordpress.com/2016/02/16/group-policy-order-of-precedence-faq/

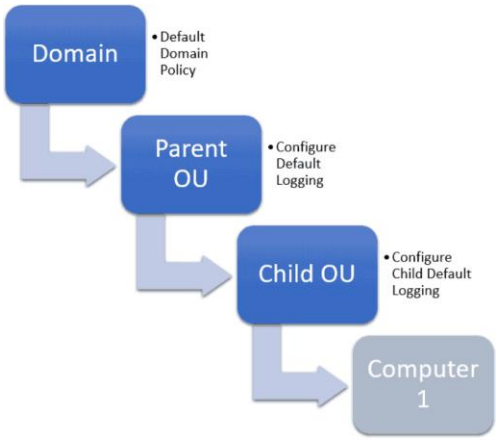
La configuración de directiva se aplica al inicio del equipo y al iniciar sesión del usuario. El servicio de directivas de grupo determina los GPO aplicables consultando el Active Directory según la pertenencia a sitios, dominios y unidades organizativas. Una extensión del lado cliente (CSE) aplica la configuración específica que dictan los GPO, administrando tareas como actualizaciones del registro y configuraciones de seguridad. Las configuraciones de directivas se aplican a los equipos cuando se inician y a los usuarios cuando inician sesión. Cuando se inicia un equipo, el servicio de directiva de grupo comprueba AD para determinar qué GPO están vinculados y aplicables al objeto de equipo, entre los que se incluyen:

- Sitio en el que reside el equipo.
- Dominio en el que el equipo es miembro.
- La unidad organizativa principal para la que el equipo es miembro directo y cualquier otra unidad organizativa por encima de la UO principal.

Las preferencias de directiva de grupo ofrecen funcionalidades de administración similares a las directivas de grupo estándar y se administran de la misma manera. Los administradores pueden crear y administrar GPO mediante el Editor de directivas de grupo local (gpedit.msc) para la configuración local o el Editor de objetos de directiva de grupo dentro de un complemento MMC relacionado con AD para la configuración de todo el dominio. Cada GPO tiene un identificador único global (GUID) y sigue la estructura jerárquica de AD para la evaluación de directivas. Una comprensión exhaustiva de cómo crear, modificar y vincular GPO dentro de AD es esencial para una administración de directivas eficaz. Los GPO se almacenan tanto en AD como en la carpeta SYSVOL de cada controlador de dominio, lo que facilita la administración centralizada y la aplicación de directivas.

Figura 31

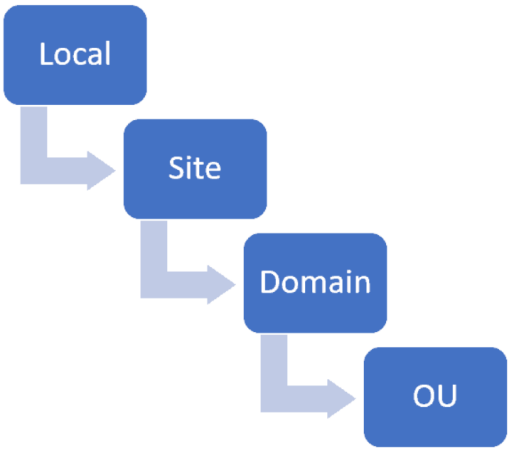
Aplicación jerárquica de GPO en dominios y unidades organizativas



Nota. Diagrama que muestra la herencia de políticas de grupo desde el dominio hacia unidades organizativas padre e hijas, evidenciando cómo las configuraciones se aplican progresivamente a los objetos finales. *Fuente*. https://4sysops.com/archives/understanding-group-policy-order/

Figura 32

Orden de evaluación de Políticas de Grupo (LSDOU)



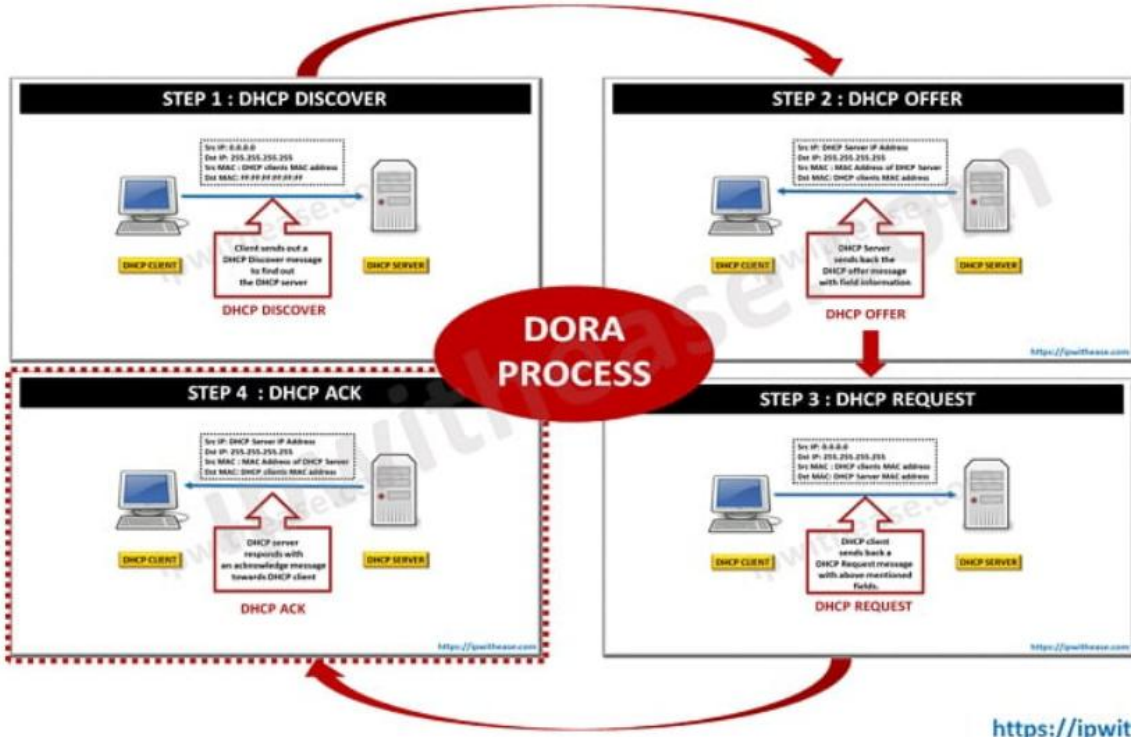
Nota. Esquema que representa el orden de evaluación de las políticas de grupo en Active Directory: Local, Site, Domain y Organizational Unit (LSDOU), determinando la prioridad de aplicación de las configuraciones. *Fuente*. https://4sysops.com/archives/understanding-group-policy-order/

DNS y DHCP

¿Qué son DHCP y DNS y cuáles son las diferencias entre ellos? Las creaciones del DHCP (Protocolo de configuración dinámica de host) y DNS (Sistema de nombres de dominio) nos facilitan el uso de red o el Internet. Sin embargo, los dos son diferentes en aplicaciones. El DHCP es un protocolo nos ayuda a asignar dirección IP y las informaciones relacionadas de IP a los computadores. Muchos switches de red también utilizan DHCP para proporcionar valiosos servicios de red TCP/IP, Tales como, nos ayuda a actualizar automáticamente el software en el sistema del cliente. Mientras que el DNS se utiliza para convertir el nombre de un sitio web como FS.com a su dirección IP y viceversa. Esto garantiza que nuestro computador encuentra el adecuado sitio, porque un computador sólo buscar un sitio no a través de su dirección IP, en lugar de su nombre de dominio.

Figura 33

Proceso DORA del protocolo DHCP



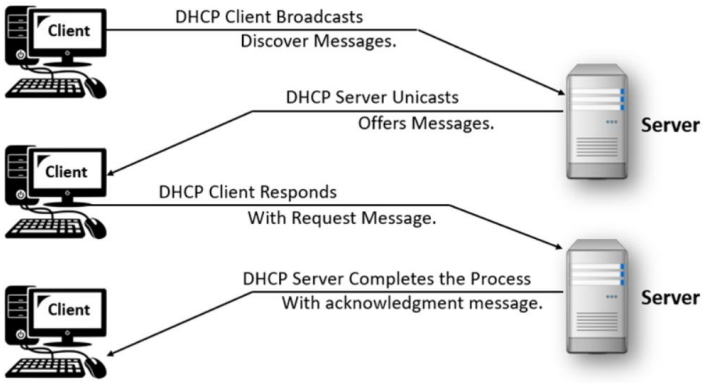
Nota. Diagrama que representa el proceso DORA (Discover, Offer, Request, Acknowledge) utilizado por el protocolo DHCP para el arrendamiento dinámico de direcciones IP entre un cliente y un servidor DHCP en una red TCP/IP. *Fuente*. https://ipwithease.com/understanding-dora-process-in-dhcp/

¿Cómo funciona el DHCP? El DHCP funciona mediante el arrendamiento direcciones IP y las informaciones IP al cliente de red en un período. Para realizarlo, los clientes DHCP necesitan interactuar servidores DHCP mediante una serie de los mensajes que incluyen principalmente DHCP DISCOVER, DHCP OFFER, DHCP REQUEST, y DHCP ACK, véase Figura 33, los procedimientos de cómo el servidor DHCP asigna una dirección IP dinámica son los siguientes.

¿Cómo funciona DNS? Como se muestra a continuación, al escribir un nombre de dominio en el navegador, por ejemplo, fs.com, el navegador a menudo no tiene idea de dónde está FS.com. Por lo tanto, enviará una consulta al LDNS (Servidor DNS local) haciendo preguntas como "cuál es la dirección IP de FS.com". Si el LDNS no tiene registros para FS.com, buscará en Internet para averiguar quién es el propietario de www.fs.com. Los procedimientos de trabajo detallados son los siguientes.

Figura 34

Comunicación cliente-servidor en el protocolo DHCP



Nota. Ilustración del intercambio de mensajes entre clientes y servidores DHCP, mostrando el uso de mensajes broadcast y unicast durante el proceso de asignación de direcciones IP. *Fuente*. https://www.pynetlabs.com/what-is-dhcp/

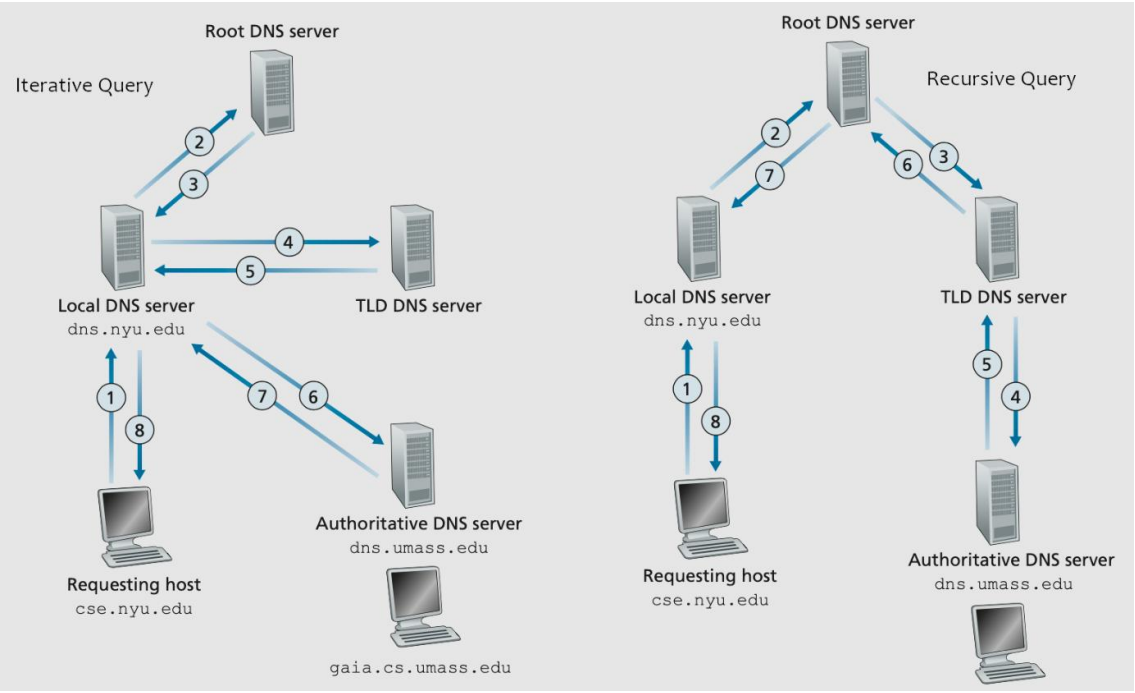
¿Cuáles son las diferencias entre DHCP y DNS?

De lo anterior, aunque tanto el DHCP como el DNS están relacionados con las direcciones IP, desempeñan funciones totalmente diferentes. Para ser claros, aquí se usa un gráfico para concluir las diferencias entre DHCP y DNS:

Para resumir, el servidor DHCP asigna las direcciones IP a las computadoras cliente, mientras que el servidor DNS las resuelve. Son dos tecnologías esenciales desarrolladas para que podamos utilizar la red o Internet de manera conveniente. Además, tanto DHCP como DNS son herramientas esenciales en el conjunto de herramientas del administrador de la red para administrar todos los dispositivos IP en una red corporativa.

Figura 35

Proceso de resolución de nombres DNS



Nota. Diagrama que muestra el proceso de resolución de nombres DNS mediante consultas recursivas e iterativas, involucrando servidores raíz, servidores de dominio de nivel superior (TLD) y servidores autoritativos. *Fuente*. https://toyos.dev/static/imgs/redes/dnsqueries.png

El proceso DHCP permite la asignación dinámica de direcciones IP mediante una secuencia de mensajes conocida como DORA (Discover, Offer, Request y Acknowledge), la cual establece la comunicación entre el cliente y el servidor.

Por su parte, el sistema DNS se encarga de la resolución de nombres de dominio a direcciones IP a través de consultas recursivas o iterativas entre servidores raíz, TLD y autoritativos.

VPN (Virtual Private Network)

Una VPN, o Red Privada Virtual, es una herramienta que crea una conexión segura y cifrada entre tu dispositivo e Internet, protegiendo tu privacidad y permitiendo el acceso a contenido restringido (Palo Alto Networks, Cloudflare.).

Definición y Funcionamiento

Una VPN (Virtual Private Network) es una tecnología que permite extender una red privada a través de una red pública, como Internet. Esto se logra mediante la creación de un "túnel" seguro que cifra los datos que se envían y reciben, lo que impide que terceros puedan interceptar o acceder a esta información.

Cuando te conectas a una VPN, tu dirección IP real se oculta y se reemplaza por la dirección IP del servidor VPN, lo que te permite navegar de forma anónima y acceder a contenido que puede estar bloqueado en tu región (Top10VPN, 2024; Palo Alto Networks).

Beneficios de Usar una VPN

Privacidad y Seguridad: Al cifrar tu conexión, una VPN protege tus datos personales y tu actividad en línea de posibles hackers y espías, especialmente en redes Wi-Fi públicas.

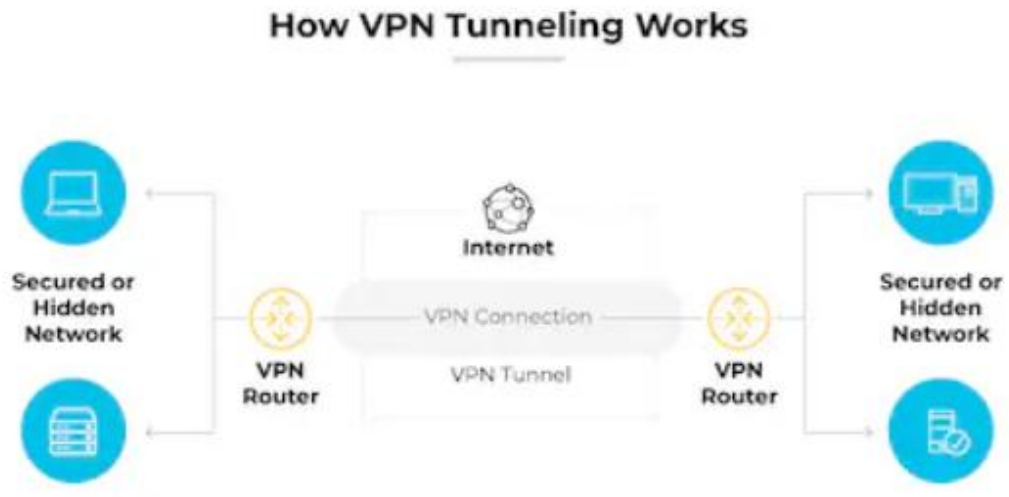
Acceso a Contenido Restringido: Las VPN permiten el acceso a sitios web y servicios que pueden estar bloqueados o restringidos en tu ubicación geográfica, como plataformas de streaming o redes sociales.

Conexiones Seguras para Empresas: Las empresas utilizan VPN para permitir que sus empleados accedan de forma segura a la red corporativa desde ubicaciones remotas, garantizando la integridad y confidencialidad de la información (Cisco Systems; Cloudflare).

Evitar la Censura: En algunos países, las VPN son utilizadas para eludir la censura gubernamental y acceder a información y servicios en línea sin restricciones.

Figura 36

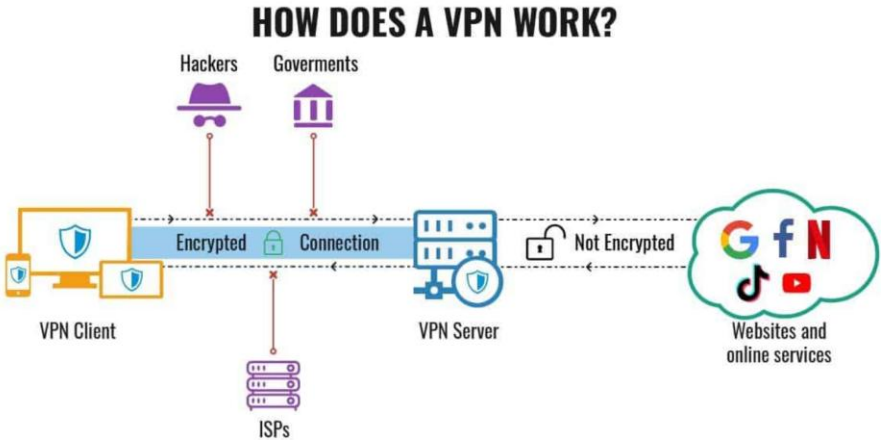
Funcionamiento del túnel VPN cifrado.



Nota.Ilustración del establecimiento de un túnel cifrado entre el cliente VPN y el servidor VPN a través de Internet. Adaptado de Top10VPN (2024).

Figura 37

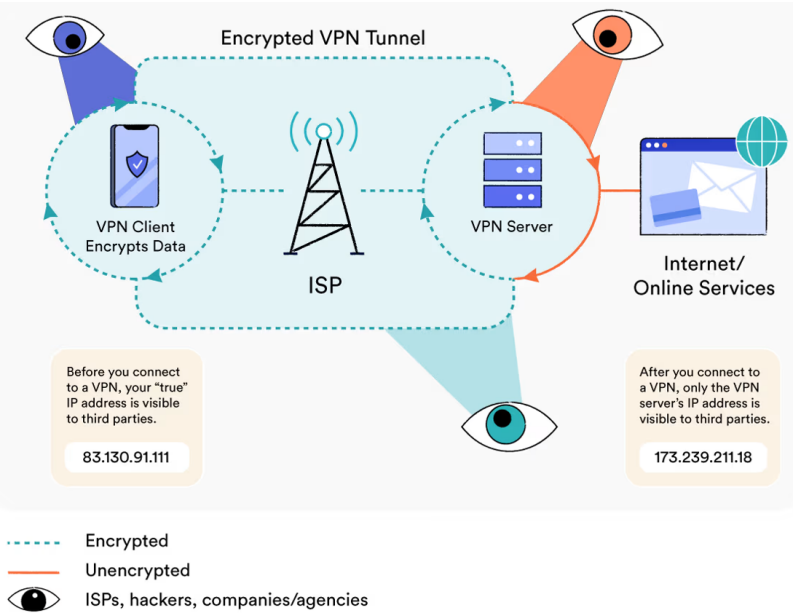
Proceso de ocultación de la dirección IP mediante una VPN.



Nota. Diagrama que muestra cómo la dirección IP real del usuario es reemplazada por la del servidor VPN, protegiendo la identidad del usuario en Internet. Adaptado de Cloudflare (s. f.).

Figura 38

Comunicación segura cliente–servidor mediante VPN.



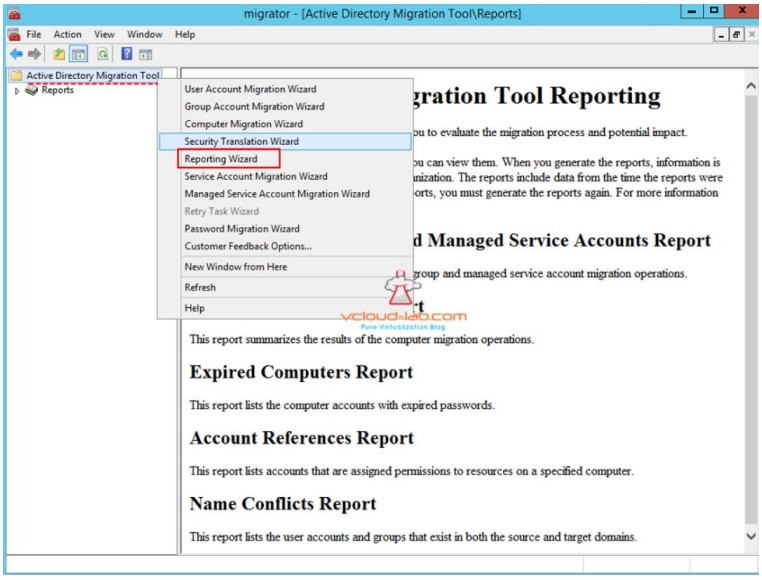
Nota. Representación del flujo de datos cifrados entre el cliente VPN, el proveedor de servicios de Internet (ISP) y el servidor VPN. Adaptado de Palo Alto Networks (s. f.).

Herramientas de Migración (ADMT, PowerShell)

La Herramienta de Migración de Active Directory (ADMT) es una aplicación de software desarrollada por Microsoft que permite administrar y ejecutar las operaciones necesarias para mover objetos dentro de Active Directory. Esta herramienta facilita la migración de cuentas de usuario, grupos, equipos y otros objetos, ya sea dentro del mismo bosque de dominios (migración intrabosque) o entre bosques distintos (migración interbosque), preservando atributos críticos como permisos y, opcionalmente, el historial de identificadores de seguridad (SIDHistory) (Microsoft Corporation, s. f.; Varonis, 2025).

Figura 39

Interfaz de reportes de la herramienta Active Directory Migration Tool (ADMT)



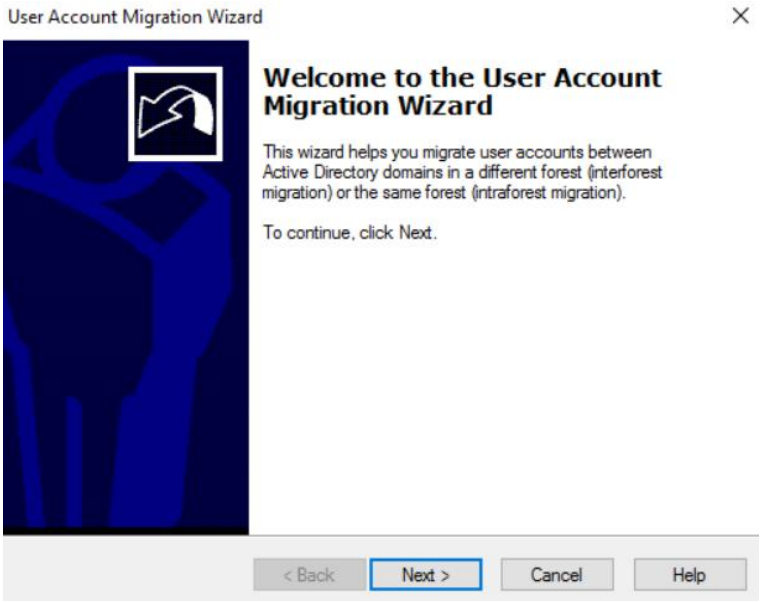
Nota. Interfaz de reportes de la Herramienta de Migración de Active Directory (ADMT), donde se visualizan opciones como *User Account Migration Wizard* y *Reporting Wizard*, utilizadas para evaluar y documentar el proceso de migración. *Fuente*. Varonis (2025).

Un escenario común de uso de ADMT corresponde a la migración intraforestal, donde se requiere trasladar objetos desde una unidad organizativa o dominio hacia otra ubicación dentro

del mismo bosque de Active Directory. Este tipo de migración suele presentarse durante procesos de reorganización administrativa, fusiones internas o estandarización de estructuras organizativas.

Figura 40

Asistente de migración de cuentas de usuario en ADMT



ADMT y PWDMIG – Migrar cuentas de usuarios de NT4 o W2K a W2K3 | Blog Bujarra.com

Nota. La imagen presenta la pantalla inicial del asistente de migración de cuentas de usuario, el cual permite mover usuarios entre dominios del mismo bosque (intrabosque) o entre bosques diferentes (interbosque), guiando paso a paso al administrador durante el proceso.

Consideraciones clave durante la migración intrabosque

Antes de ejecutar una migración mediante ADMT, es fundamental tener en cuenta varios aspectos críticos. En primer lugar, se deben verificar las relaciones de confianza entre los dominios, ya que una configuración incorrecta puede ocasionar pérdida de acceso a recursos después de la migración. Asimismo, es recomendable documentar detalladamente cada objeto

migrado, incluyendo su ubicación de origen y destino, para facilitar el seguimiento del proceso y la validación posterior.

Otro aspecto relevante es la necesidad de desarrollar un plan de pruebas, dado que ADMT no valida automáticamente la funcionalidad de los objetos migrados. Por esta razón, se deben comprobar manualmente accesos, permisos y servicios asociados. Finalmente, es importante considerar que ADMT no ofrece un mecanismo de reversión, por lo que cualquier cambio realizado es permanente; esto hace indispensable contar con respaldos completos antes de iniciar el proceso (Microsoft Corporation, s. f.).

Figura 41

Asistente de instalación de Active Directory Migration Tool (ADMT)

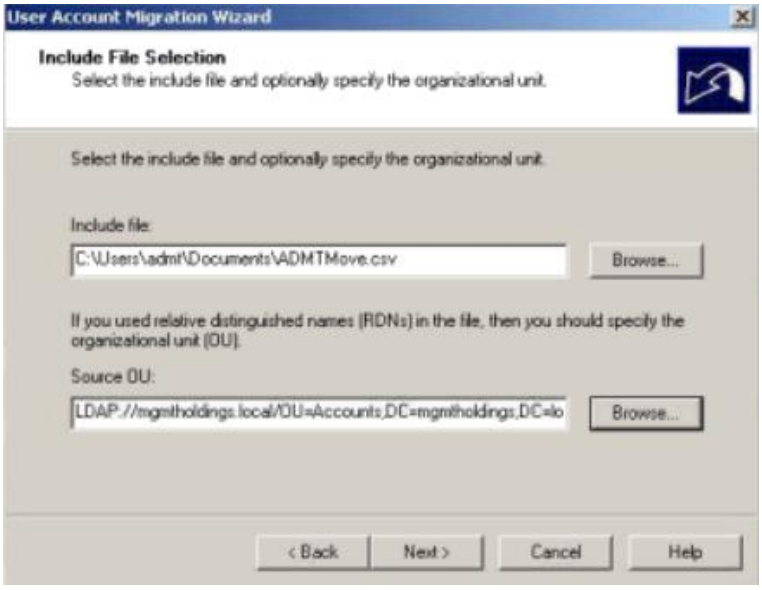
Nota. La imagen ilustra el proceso de instalación de ADMT, destacando los prerrequisitos necesarios como la configuración de una instancia de SQL Server, aspecto fundamental para el correcto funcionamiento de la herramienta de migración.

Uso de archivos de inclusión en ADMT

Para migraciones de gran escala, ADMT permite el uso de archivos de inclusión, los cuales facilitan la carga masiva de objetos a migrar. Mientras que las migraciones pequeñas pueden realizarse directamente desde la interfaz gráfica o mediante línea de comandos, los archivos de inclusión resultan esenciales cuando se manejan grandes volúmenes de cuentas.

Figura 42

Selección del archivo de inclusión durante la migración de usuarios con ADMT



Nota. La imagen muestra la etapa en la que se selecciona el archivo de inclusión (include file), utilizado para definir de forma masiva los objetos a migrar, así como la unidad organizativa de origen, facilitando la administración de migraciones a gran escala.

Un archivo de inclusión consiste en un listado estructurado donde cada línea representa un objeto a migrar y sus atributos de destino. Los campos más comunes incluyen:

- SourceName: nombre de la cuenta SAM de origen.
- TargetRDN: nuevo nombre distintivo relativo del objeto.
- TargetSAM: nuevo nombre SAM de destino.
- TargetUPN: nuevo nombre principal de usuario (aplica solo a usuarios).

Un ejemplo simple de archivo de inclusión sería:

Vader,CN=dvader,dvader@evilgalacticempire.org

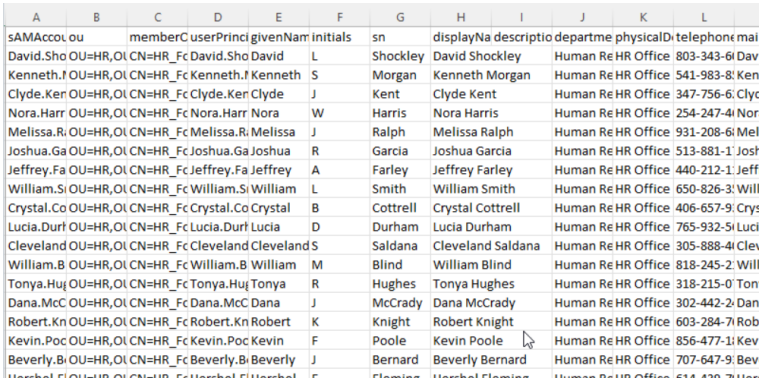
En este caso, únicamente es obligatorio el campo SourceName, mientras que los demás campos son opcionales y se utilizan cuando se requiere modificar atributos durante la migración.

Integración de ADMT con PowerShell

Además del uso de asistentes gráficos, ADMT puede complementarse con scripts en PowerShell, lo que permite automatizar tareas repetitivas, reducir errores humanos y ejecutar migraciones masivas de forma controlada. Esta integración resulta especialmente útil en entornos corporativos complejos donde se requiere coherencia, trazabilidad y escalabilidad durante el proceso de migración (Evotec, 2021).

Figura 43

Ejemplo de archivo de inclusión en formato CSV para ADMT

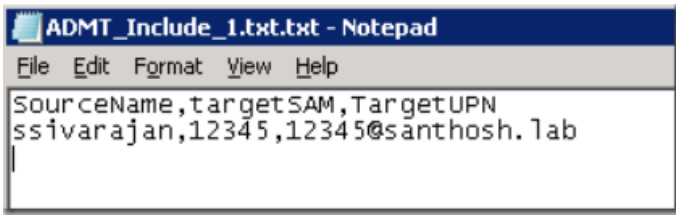


A	B	C	D	E	F	G	H	I	J	K	L	
sAMAccou	ou	memberC	userPrinci	givenNam	initials	sn	displayNa	descriptio	departme	physicalD	telephone	mai
David.Sho	OU=HR,OU	CN=HR_Fc	David.Sho	David	L	Shockley	David Shockley		Human Re	HR Office	803-343-6	Dav
Kenneth.M	OU=HR,OU	CN=HR_Fc	Kenneth.M	Kenneth	S	Morgan	Kenneth Morgan		Human Re	HR Office	541-983-8	Ken
Clyde.Ker	OU=HR,OU	CN=HR_Fc	Clyde.Ker	Clyde	J	Kent	Clyde Kent		Human Re	HR Office	347-756-6	Clyc
Nora.Harr	OU=HR,OU	CN=HR_Fc	Nora.Harr	Nora	W	Harris	Nora Harris		Human Re	HR Office	254-247-4	Nor
Melissa.R	OU=HR,OU	CN=HR_Fc	Melissa.R	Melissa	J	Ralph	Melissa Ralph		Human Re	HR Office	931-208-6	Mel
Joshua.Ga	OU=HR,OU	CN=HR_Fc	Joshua.Ga	Joshua	R	Garcia	Joshua Garcia		Human Re	HR Office	513-881-1	Josh
Jeffrey.Fa	OU=HR,OU	CN=HR_Fc	Jeffrey.Fa	Jeffrey	A	Farley	Jeffrey Farley		Human Re	HR Office	440-212-1	Jeff
William.Sı	OU=HR,OU	CN=HR_Fc	William.Sı	William	L	Smith	William Smith		Human Re	HR Office	650-826-3	Will
Crystal.Co	OU=HR,OU	CN=HR_Fc	Crystal.Co	Crystal	B	Cottrell	Crystal Cottrell		Human Re	HR Office	406-657-9	Crys
Lucia.Durl	OU=HR,OU	CN=HR_Fc	Lucia.Durl	Lucia	D	Durham	Lucia Durham		Human Re	HR Office	765-932-5	Luci
Cleveland	OU=HR,OU	CN=HR_Fc	Cleveland	Cleveland	S	Saldana	Cleveland Saldana		Human Re	HR Office	305-888-4	Clev
William.B	OU=HR,OU	CN=HR_Fc	William.B	William	M	Blind	William Blind		Human Re	HR Office	818-245-2	Will
Tonya.Hu	OU=HR,OU	CN=HR_Fc	Tonya.Hu	Tonya	R	Hughes	Tonya Hughes		Human Re	HR Office	318-215-0	Ton
Dana.McC	OU=HR,OU	CN=HR_Fc	Dana.McC	Dana	J	McCrady	Dana McCrady		Human Re	HR Office	302-442-2	Dan
Robert.Kn	OU=HR,OU	CN=HR_Fc	Robert.Kn	Robert	K	Knight	Robert Knight		Human Re	HR Office	603-284-7	Rob
Kevin.Poc	OU=HR,OU	CN=HR_Fc	Kevin.Poc	Kevin	F	Poole	Kevin Poole		Human Re	HR Office	856-477-1	Kev
Beverly.B	OU=HR,OU	CN=HR_Fc	Beverly.B	Beverly	J	Bernard	Beverly Bernard		Human Re	HR Office	707-647-9	Bev

Nota. La imagen presenta un ejemplo de archivo de inclusión estructurado en columnas como SourceName, TargetRDN y TargetUPN, el cual se emplea para migraciones masivas de cuentas de usuario dentro de un bosque de Active Directory.

Figura 44

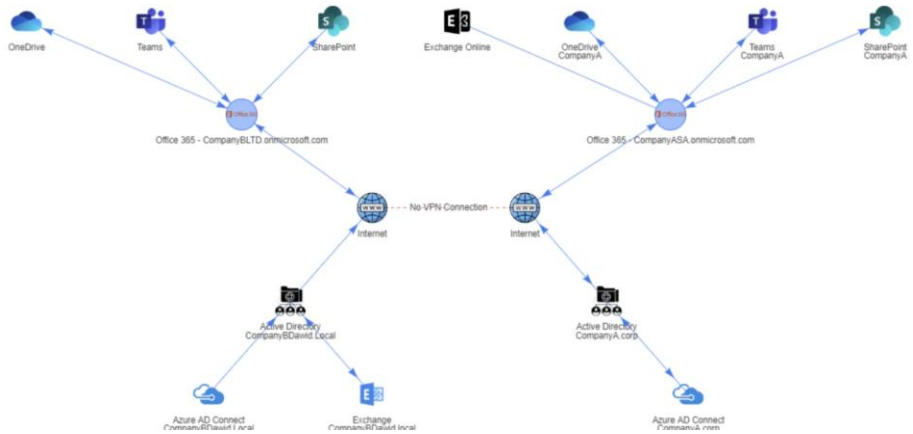
Archivo de inclusión en formato de texto plano para ADMT



Nota. La imagen muestra un archivo de inclusión simple en formato TXT, donde se especifican los atributos mínimos requeridos para la migración de usuarios, como SourceName, TargetSAM y TargetUPN, facilitando la automatización del proceso.

Figura 45

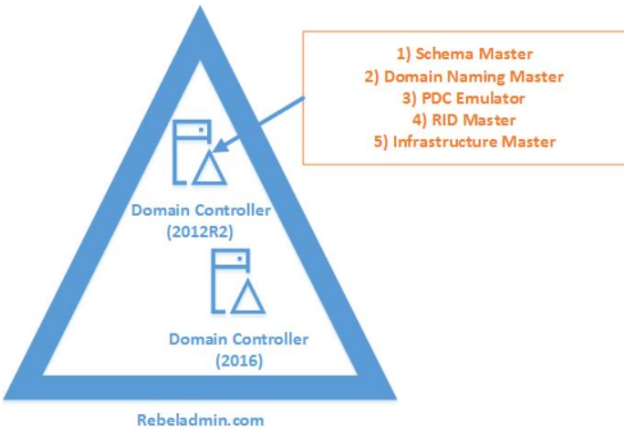
Diagrama conceptual de migración e integración de identidades con PowerShell



Nota. La imagen ilustra un escenario de migración e integración entre Active Directory local y servicios en la nube como Microsoft 365, mostrando cómo el uso de scripts y automatización puede apoyar procesos de migración complejos.

Figura 46

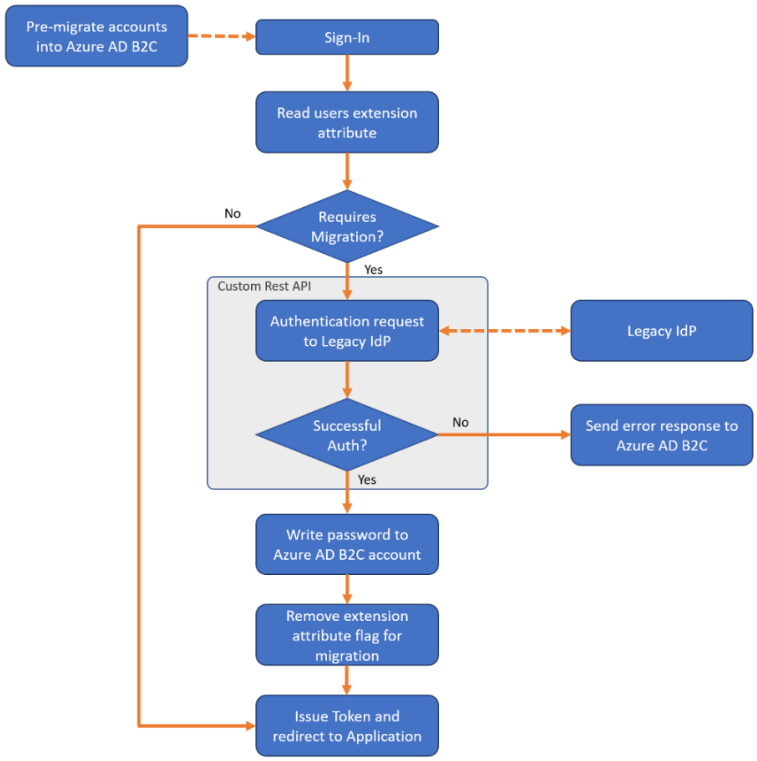
Representación de los roles FSMO en entornos de Active Directory



Nota. La imagen muestra los cinco roles FSMO (Schema Master, Domain Naming Master, RID Master, PDC Emulator e Infrastructure Master), los cuales deben considerarse cuidadosamente durante procesos de migración para evitar inconsistencias en el directorio.

Figura 47

Flujo de migración automatizada de identidades hacia Azure AD



Nota. La imagen presenta un flujo de migración de usuarios desde Active Directory local hacia Azure AD, mostrando procesos de autenticación, validación de credenciales y emisión de tokens, lo cual complementa el uso de ADMT con tecnologías modernas en la nube.

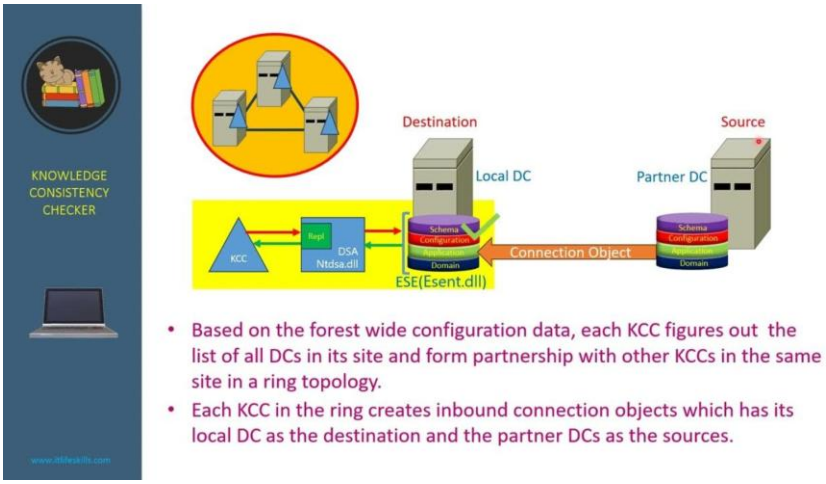
Replicación y Consistencia

Un objeto de conexión es un objeto de Active Directory que representa una conexión de replicación de un controlador de dominio de origen a un controlador de dominio de destino. Un controlador de dominio es miembro de un único sitio y se representa en el sitio mediante un objeto de servidor en Active Directory Domain Services (AD DS). Cada objeto de servidor tiene un objeto de configuración NTDS secundario que representa el controlador de dominio de replicación del sitio.

El objeto de conexión es un elemento secundario del objeto de configuración NTDS en el servidor de destino. Para que se produzca la replicación entre dos controladores de dominio, el objeto de servidor de uno de ellos debe tener un objeto de conexión que represente la replicación entrante del otro. Todas las conexiones de replicación de un controlador de dominio se almacenan como objetos de conexión en el objeto de configuración NTDS. El objeto de conexión identifica el servidor de origen de replicación, contiene una programación de replicación y especifica un transporte de replicación.

Figura 48

Generación automática de objetos de conexión por el KCC



Nota. El diagrama ilustra cómo el Knowledge Consistency Checker (KCC) utiliza la información de configuración del bosque para identificar los controladores de dominio dentro de un sitio y generar automáticamente objetos de conexión entrantes. Estos objetos definen las relaciones de replicación entre controladores de dominio origen y destino, garantizando la consistencia de los datos en Active Directory.

El Comprobador de coherencia de la información (KCC) crea los objetos de conexión automáticamente, pero también se pueden crear manualmente. Los objetos de conexión creados por KCC aparecen en el complemento Sitios y servicios de Active Directory como <generados automáticamente> y se consideran adecuados en condiciones de funcionamiento normales. Los objetos de conexión creados por un administrador son objetos de conexión creados manualmente. Un objeto de conexión creado manualmente se identifica por el nombre asignado por el administrador cuando se creó. Cuando se modifica un objeto de conexión <generado automáticamente>, se convierte en un objeto de conexión modificado administrativamente y el objeto aparece en forma de GUID. KCC no realiza cambios en los objetos de conexión manuales o modificados.

Un diagrama de topología de replicación de AD que muestra cómo los controladores de dominio (DCs) en diferentes sitios se conectan mediante objetos de conexión, ilustra claramente el concepto de “objeto de conexión” descrito.

Una captura del complemento Active Directory Sites and Services mostrando objetos de conexión generados automáticamente y modificados administrativamente (GUID), lo que apoya la explicación de la KCC y los objetos de conexión manuales.

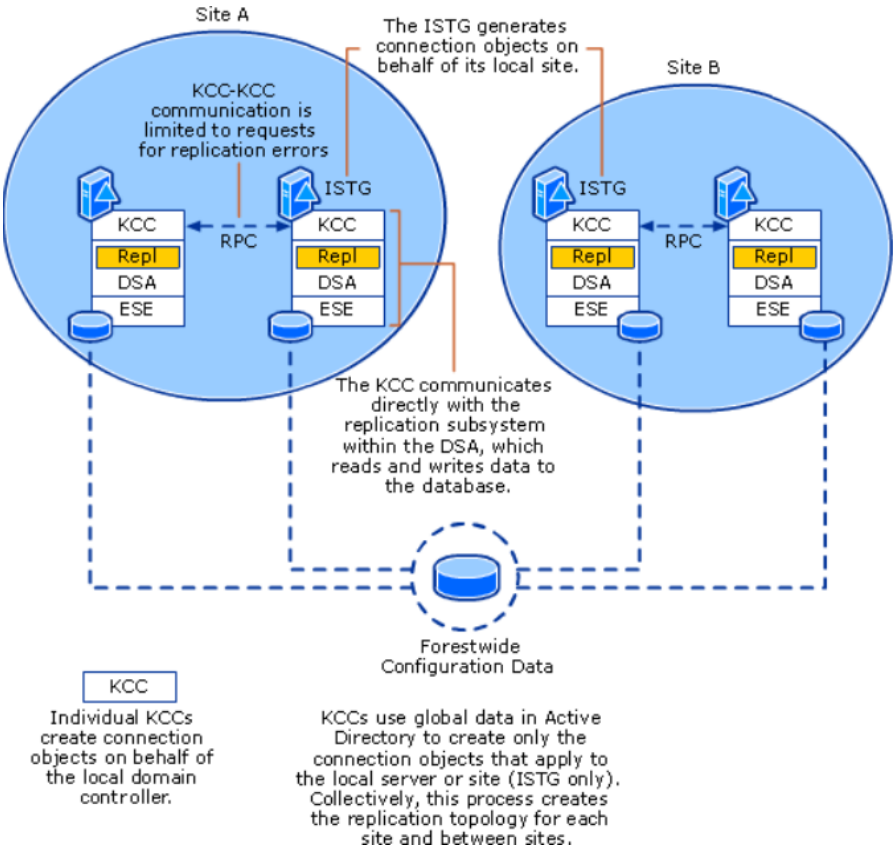
Un esquema que muestra el flujo de replicación y el transporte (RPC, SMTP) especificado en los objetos de conexión, enfatizando la consistencia de datos entre controladores de dominio.

KCC

KCC es un proceso integrado que se ejecuta en todos los controladores de dominio y genera la topología de replicación del bosque de Active Directory. KCC crea topologías de replicación independientes en función de si la replicación se produce dentro de un sitio (intrasitio) o entre sitios (intersitios). KCC también ajusta dinámicamente la topología para dar cabida a la adición de nuevos controladores de dominio, la eliminación de controladores de dominio existentes, el movimiento de controladores de dominio hacia y desde sitios, los cambios en costos y programaciones, y los controladores de dominio que no están disponibles temporalmente o en estado de error.

Figura 49

Comunicación del KCC e ISTG en la topología de replicación



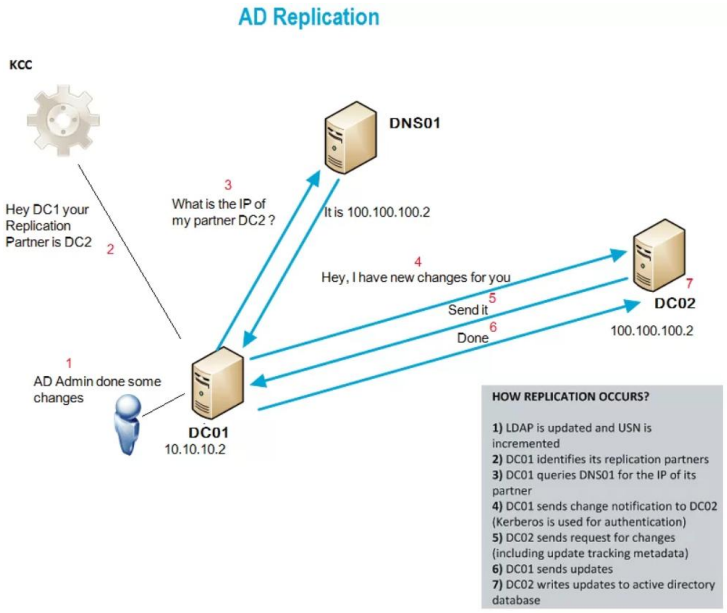
Nota. La imagen muestra el funcionamiento del KCC junto con el Inter-Site Topology Generator (ISTG), responsable de crear objetos de conexión entre sitios. Se observa cómo el KCC gestiona la replicación dentro de cada sitio, mientras que el ISTG coordina la replicación entre sitios, utilizando datos de configuración del bosque para construir una topología eficiente y tolerante a fallos.

Dentro de un sitio, las conexiones entre controladores de dominio disponibles para escritura siempre se organizan en un anillo bidireccional, con conexiones de acceso directo adicionales para reducir la latencia en sitios grandes. Por otro lado, la topología entre sitios es una capa de árboles de expansión, lo que significa que existe una conexión entre sitios entre dos sitios para cada partición del directorio y, por lo general, no contiene conexiones de acceso directo. Para obtener más información sobre los árboles de expansión y la topología de

replicación de Active Directory, consulte Referencia técnica de la topología de replicación de Active Directory (https://go.microsoft.com/fwlink/?LinkID=93578).

Figura 50

Flujo del proceso de replicación entre controladores de dominio



Nota. Este esquema representa el flujo del proceso de replicación entre controladores de dominio, desde la detección de cambios en LDAP, la identificación del socio de replicación mediante DNS, la autenticación con Kerberos y el intercambio de datos a través de RPC/IP. El proceso asegura que los cambios se propaguen correctamente y se mantenga la coherencia de la base de datos del directorio.

En cada controlador de dominio, KCC crea rutas de replicación mediante la creación de objetos de conexión de entrada unidireccionales que definen las conexiones desde otros controladores de dominio. En el caso de los controladores de dominio en el mismo sitio, KCC crea objetos de conexión automáticamente sin intervención administrativa. Cuando tenga más de un sitio, configure vínculos de sitio entre los sitios y un único KCC de cada sitio también crea automáticamente las conexiones entre los sitios.

Analizar la infraestructura actual de cada sede

El análisis de la infraestructura actual de cada sede tiene como finalidad identificar los elementos tecnológicos, arquitectónicos y operativos que intervienen en la gestión de los dominios corporativos, con el fin de establecer una base sólida para el diseño de una arquitectura unificada.

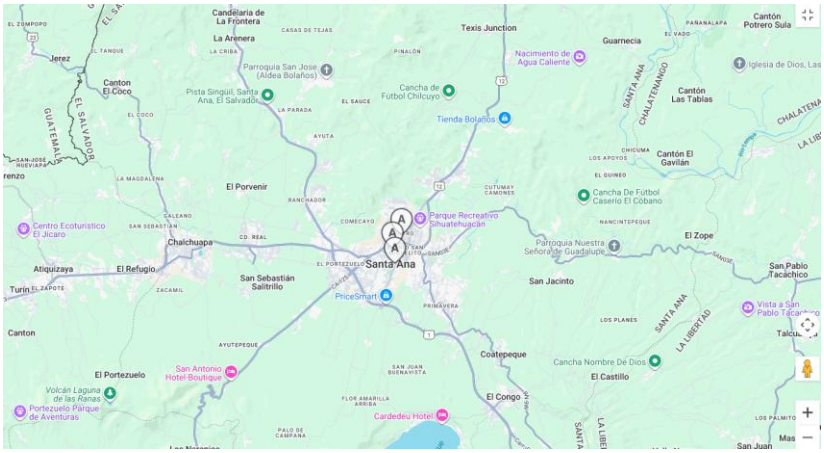
Las sedes del banco se distribuyen estratégicamente en tres países: El Salvador, Guatemala y Panamá. Cada sede cuenta con una infraestructura tecnológica que incluye redes privadas, servidores de autenticación, y sistemas de seguridad avanzados. Estas sedes están interconectadas mediante enlaces seguros que permiten la replicación de servicios y la administración centralizada de recursos. A continuación, se presenta un mapa ilustrativo de la distribución geográfica de las sedes.

Sede el Salvador

La sede en El Salvador cuenta con una infraestructura robusta que incluye múltiples servidores, equipos de red y enlaces redundantes. Se han identificado aproximadamente 12 switches, 4 routers, 2 firewalls y 3 controladores de dominio.

Figura 51

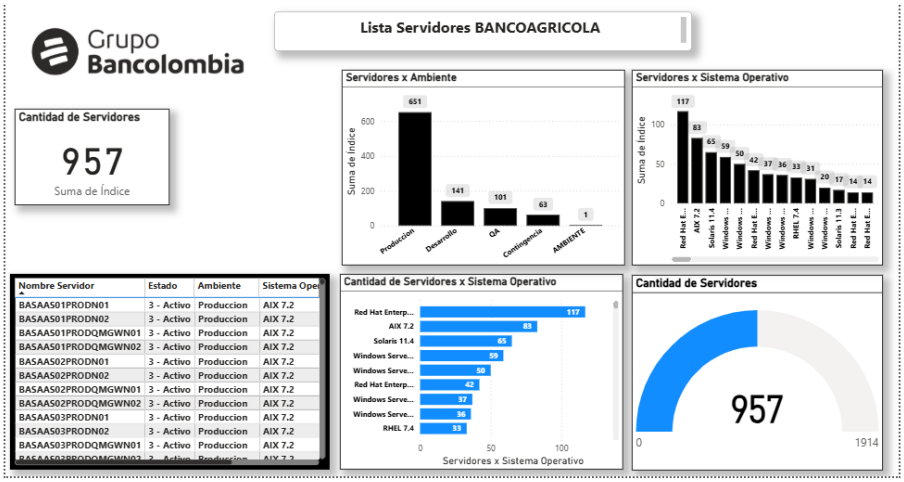
Ubicación Geográfica de la sede



Cantidad de Servidores Members en la sede de Salvador

Figura 52

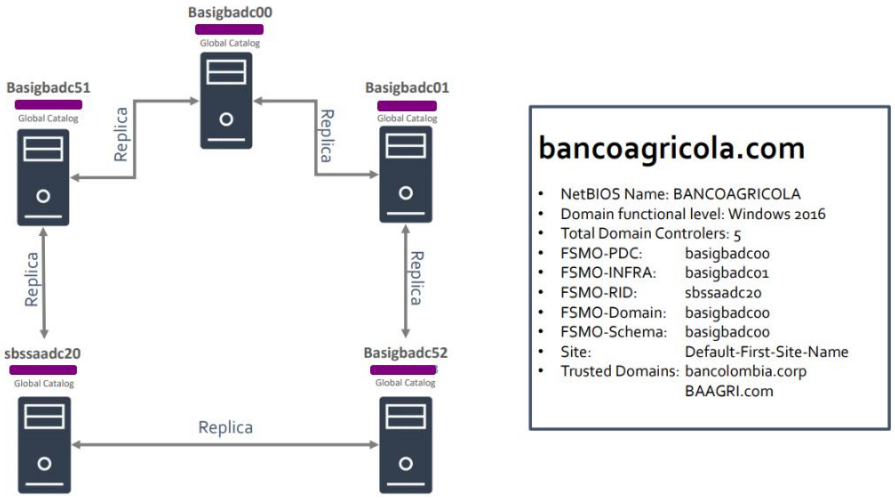
Lista de Servidores BANCOAGRICOLA en el Dashboard



Nota. Imágenes Salidas desde la Herramienta PowerBI, herramienta colaborativa de la Suite Off365 licenciada para BANCOLOMBIA.

Figura 53

Arquitectura Base sede Salvador



Nota. Imágenes Salidas de los repositorios oficiales de la compañía, donde se respaldan los actuales diseños e Infraestructuras de cada sede.

Evaluación Integral de Infraestructura, Seguridad y Conectividad

Antes de ejecutar una migración o actualización en entornos corporativos de Active Directory, es indispensable realizar una evaluación integral de la infraestructura tecnológica. Este análisis tiene como propósito identificar los componentes de red, los mecanismos de seguridad y las condiciones de conectividad que soportan los servicios críticos de la organización. La información recolectada en esta etapa servirá como base para garantizar una migración segura, ordenada y eficiente.

La evaluación de la infraestructura permite conocer el estado y capacidad de los recursos tecnológicos existentes, los cuales son fundamentales para la operación del directorio activo y otros servicios asociados. Este proceso asegura que la base tecnológica soporte de manera óptima las cargas derivadas de la replicación, autenticación y comunicación entre dominios.

Componentes Principales de la Infraestructura

Topología de red. Identificación del tipo de red utilizada en la sede (LAN, WAN o híbrida) y su esquema de interconexión.

VPNs, MPLS y SD-WAN. Verificación de las tecnologías de conexión seguras implementadas entre las sedes o sucursales, asegurando redundancia y disponibilidad.

Capacidad de ancho de banda. Determinación de la capacidad disponible para soportar la replicación de Active Directory, sincronización de políticas de grupo (GPOs) y transferencia de datos entre sitios.

Equipos de red. Inventario y revisión del estado de routers, switches, firewalls y balanceadores de carga para confirmar su compatibilidad con las políticas de seguridad y requerimientos de conectividad.

Servidores y roles de Active Directory. Validación de la correcta asignación de roles esenciales, tales como Controladores de Dominio (DC), DHCP y DNS.

Ciberseguridad

La ciberseguridad representa un pilar estratégico dentro del entorno de TI. En un dominio corporativo, mantener la integridad y confidencialidad de las credenciales y recursos es esencial para la continuidad operativa. Esta sección aborda las buenas prácticas y configuraciones mínimas recomendadas para proteger el entorno de Active Directory frente a amenazas internas y externas.

Medidas de Seguridad Recomendadas

Autenticación multifactor (MFA). Implementación de doble verificación para minimizar el riesgo de acceso no autorizado, combinando contraseñas con métodos biométricos o tokens.

Revisión de grupos de seguridad y delegación de permisos. Aplicación del principio de mínimo privilegio, garantizando que cada usuario y grupo cuenten únicamente con los permisos estrictamente necesarios.

Segmentación de red. Separación del tráfico administrativo y del tráfico de usuario para evitar la exposición de servicios críticos a redes menos seguras.

Protección contra amenazas avanzadas. Integración con soluciones EDR/XDR que permiten la detección y respuesta automatizada frente a comportamientos anómalos o intrusiones.

Cumplimiento normativo. Verificación del cumplimiento de las regulaciones locales, incluyendo la Ley de Protección de Datos Personales de El Salvador (2021) y estándares internacionales de privacidad y seguridad.

Telecomunicaciones y Conectividad

La disponibilidad de enlaces estables y configuraciones adecuadas de servicios de red es crucial para garantizar una replicación efectiva y comunicación fluida entre dominios. El correcto diseño de la interconexión entre sedes y el funcionamiento de los servicios DNS y NTP son elementos esenciales para evitar conflictos de autenticación o pérdida de sincronización.

Interconexión entre Sedes

Relaciones de confianza. Actualmente, los dominios corporativos mantienen una relación de confianza site-to-site bidireccional que garantiza una comunicación segura y continua.

Redundancia. Se dispone de conectividad redundante entre los sitios, lo cual asegura la continuidad operativa ante posibles fallos de comunicación o caída de enlaces.

Configuración de Servicios de Red

DNS y resolución de nombres. Los controladores de dominio ejecutan el rol de DNS, permitiendo la correcta resolución interna de nombres de equipos y servicios.

Zonas de búsqueda directa e inversa. Configuradas adecuadamente para la identificación precisa de IPs y nombres de host dentro de la red corporativa.

Replicación entre servidores DNS. Asegura la coherencia de datos de resolución de nombres entre todos los controladores de dominio.

Sincronización de tiempo (NTP). Elemento vital para el correcto funcionamiento del protocolo Kerberos y la autenticación entre dominios.

Conclusión del Módulo

El análisis integral de infraestructura, ciberseguridad y conectividad permite establecer un panorama completo del entorno actual.

A partir de estos resultados, se podrán definir estrategias de mejora, priorizar inversiones tecnológicas y diseñar un plan de migración que minimice riesgos operativos y garantice la estabilidad del entorno de Active Directory.

Metodología de Análisis

Describe cómo se está realizando el análisis:

La Recolección de la información fue obtenida mediante entrevistas, encuestas realizadas al personal de INFRA de cada region, revisión documental y herramientas de diagnóstico como ping castle

Herramientas utilizadas: Active Directory Health Checks, scripts de PowerShell, herramientas de monitoreo como PRTG, SolarWinds, etc.

Criterios de evaluación: compatibilidad, escalabilidad, seguridad, redundancia, etc.

Sede Guatemala

La sede en Guatemala presenta una arquitectura moderna con 10 switches, 3 routers, 2 firewalls y 2 controladores de dominio. La conectividad está garantizada mediante enlaces MPLS y VPNs seguras

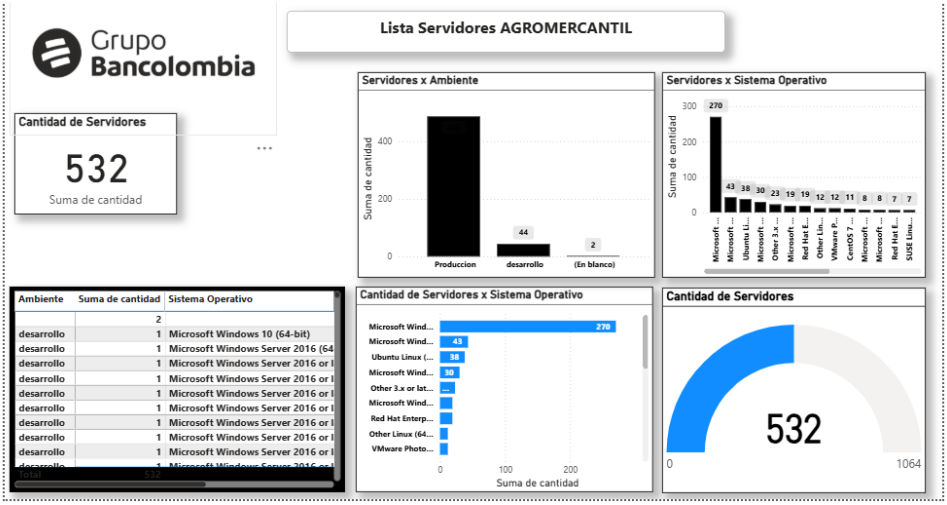
Figura 54

Ubicación geográfica de la sede Guatemala

Cantidad de Servidores Members en la Sede de Guatemala

Figura 55

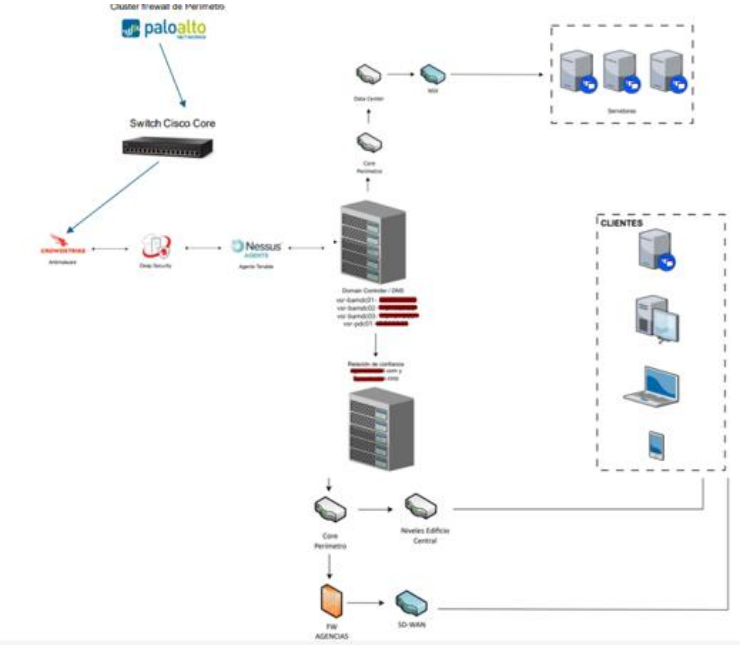
Lista de Serviedores AGROMERCANTIL Guatemala en el Dashboard



Nota. Imágenes Salidas desde la Herramienta PowerBI, herramienta colaborativa de la Suite Off365 licenciada para BANCOLOMBIA.

Figura 56

Arquitectura base Sede Guatemala



Nota. Imágenes Salidas de los repositorios oficiales de la compañía, donde se respaldan los actuales diseños e infraestructuras de cada sede.

Evaluación de Infraestructura Actual

Este apartado tiene como propósito analizar el estado actual de la infraestructura tecnológica de la organización, considerando los principales componentes que influyen en el desempeño, la disponibilidad y la confiabilidad del entorno de Active Directory y sus servicios asociados. El análisis permite identificar posibles limitaciones o áreas de mejora para garantizar una migración eficiente y segura.

Topología de red. Describe el tipo de red utilizada en la sede, incluyendo su diseño lógico y físico. Se evalúa la arquitectura actual (estrella, malla, jerárquica, etc.) para determinar su adecuación al tráfico de autenticación y replicación de servicios de directorio.

Conectividad y tecnologías implementadas. Se revisa la existencia de tecnologías de interconexión como VPN, MPLS o SD-WAN, fundamentales para el enlace entre sedes y la comunicación segura entre controladores de dominio distribuidos geográficamente.

Capacidad de ancho de banda. Se evalúa si la capacidad de enlace actual es suficiente para soportar la replicación de Active Directory (AD), sincronización de políticas de grupo (GPO) y transferencia de registros DNS, sin afectar el rendimiento general de la red.

Equipos de red. Incluye la identificación y evaluación de routers, switches, firewalls y balanceadores de carga. Se verifica su configuración y compatibilidad con los requerimientos de comunicación entre dominios, seguridad y redundancia.

Servidores y roles de Active Directory. Describe los servidores implementados y los roles de infraestructura que cumplen, como los Controladores de Dominio (DC), DHCP y DNS, esenciales para la autenticación, resolución de nombres y asignación de direcciones IP.

Ciberseguridad

Este componente analiza las políticas y mecanismos de seguridad aplicados dentro de la red corporativa, enfocándose en la protección de los datos, la identidad de los usuarios y la integridad de los servicios críticos.

Implementación de autenticación multifactor (MFA). Verifica la adopción de mecanismos MFA para reforzar la seguridad de inicio de sesión y mitigar accesos no autorizados a los recursos del dominio.

Revisión de grupos de seguridad y delegación de permisos. Analiza la correcta configuración de los grupos de seguridad, niveles de acceso y delegación de permisos en Active Directory para evitar privilegios excesivos o configuraciones inseguras.

Segmentación de red. Evalúa la separación del tráfico administrativo (administradores de sistemas y servicios críticos) respecto al tráfico de usuario común, aplicando principios de Zero Trust y defensa en profundidad.

Protección contra amenazas avanzadas. Se revisa la integración de soluciones EDR (Endpoint Detection and Response) o XDR (Extended Detection and Response), que permiten la detección, monitoreo y respuesta ante incidentes de seguridad.

Cumplimiento normativo. Analiza el cumplimiento de la Ley de Protección de Datos Personales de El Salvador y otras normativas locales aplicables, garantizando el manejo responsable y seguro de la información sensible.

Telecomunicaciones y Conectividad

El objetivo de esta sección es evaluar los mecanismos de interconexión entre sedes, la redundancia y la disponibilidad de los servicios de resolución de nombres y sincronización temporal, fundamentales para una migración estable del entorno Active Directory.

Interconexión entre sedes. Describe las relaciones de confianza entre dominios corporativos y la forma en que se establece la comunicación segura entre ellos.

Redundancia. Confirma la existencia de una configuración de redundancia site-to-site bidireccional, lo que asegura la continuidad operativa en caso de fallas en alguno de los enlaces.

DNS y resolución de nombres. Se valida que los Controladores de Dominio (DC) cumplen la función de servidores DNS, asegurando la correcta resolución de nombres internos.

Configuración de zonas. Verifica la configuración de las zonas de búsqueda directa e inversa en los servidores DNS, así como la replicación adecuada entre ellos.

Sincronización de tiempo (NTP).
Se analiza la configuración de sincronización de tiempo, aspecto crítico para la autenticación basada en Kerberos y la coherencia de los registros de seguridad.

Metodología de Análisis

Esta sección describe el enfoque utilizado para evaluar el entorno actual de Active Directory y sus dependencias. La metodología se fundamenta en la recopilación estructurada de información, la aplicación de herramientas especializadas y la definición de criterios técnicos.

Recolección de información. La información se obtuvo mediante entrevistas y encuestas dirigidas al personal del área de infraestructura (INFRA) de cada región, complementadas con revisión documental y herramientas de diagnóstico como PingCastle.

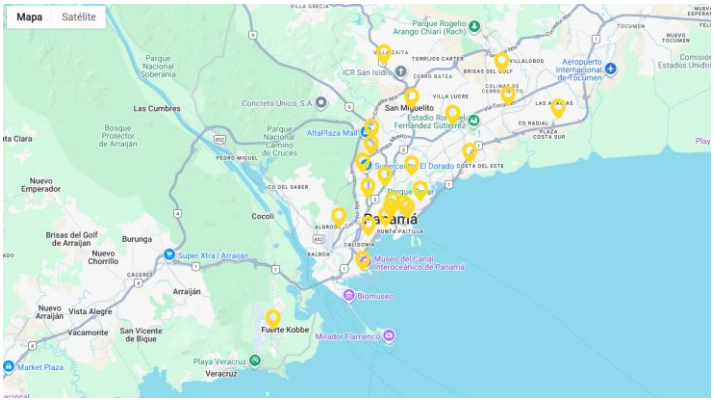
Herramientas utilizadas. Incluye el uso de Active Directory Health Checks, scripts de PowerShell y plataformas de monitoreo como PRTG y SolarWinds, que permiten identificar fallas, vulnerabilidades y métricas de desempeño.

Sede Panamá

La sede en Panamá dispone de una infraestructura consolidada con 8 switches, 2 routers, 2 firewalls y 2 controladores de dominio. La replicación de servicios se realiza de forma eficiente entre sedes.

Figura 57

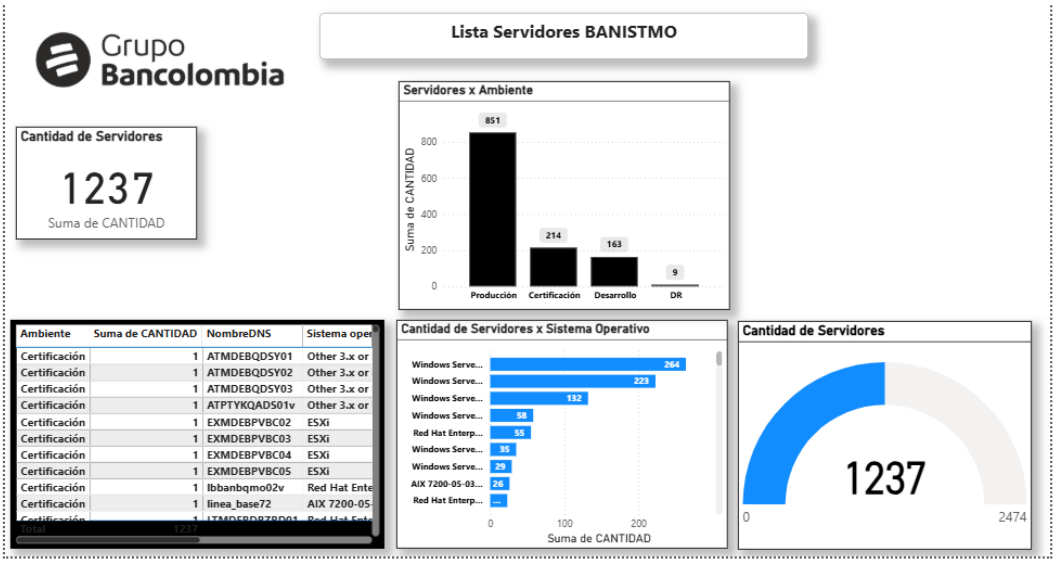
Ubicación geográfica de la sede Panama



Cantidad de Servidores Members en la sede de Panamá

Figura 58

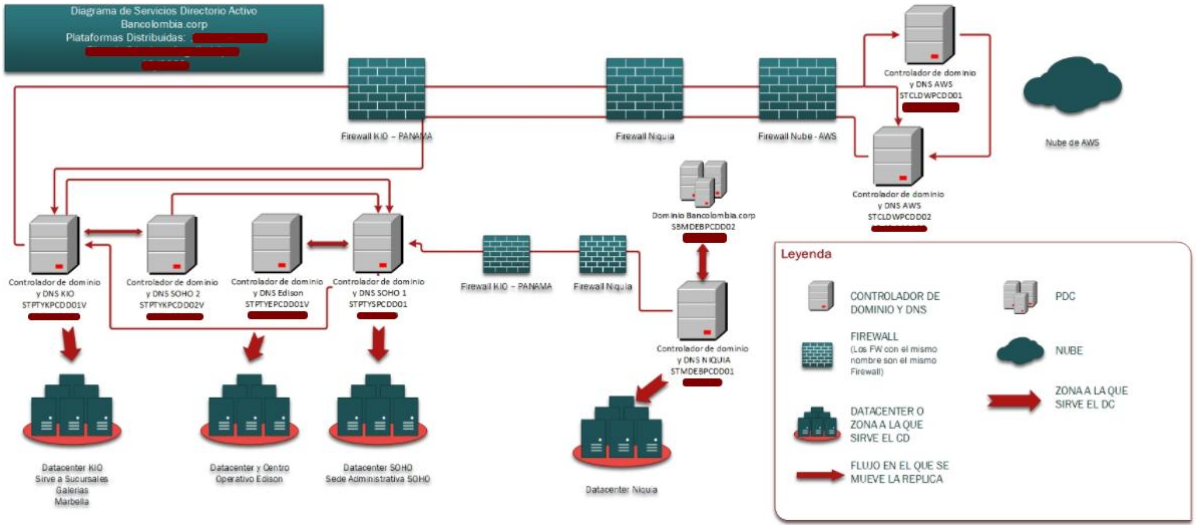
Lista de Servidores BANISTMO en el Dashboard



Nota. Imágenes Salidas desde la Herramienta PowerBI, herramienta colaborativa de la Suite Off365 licenciada para BANCOLOMBIA.

Figura 59

Arquitectura base Sede Panamá



Nota. Imágenes Salidas de los repositorios oficiales de la compañía, donde se respaldan los actuales diseños e Infraestructuras de cada sede.

Evaluación de Infraestructura Actual

En esta sección se presenta un análisis detallado de la infraestructura tecnológica actual que soporta los servicios de red y directorio activo de la organización. El objetivo es evaluar el entorno físico y lógico, la topología implementada, la disponibilidad de recursos de red, y la correcta distribución de roles de servidor que garantizan la continuidad operativa y la eficiencia de la administración del dominio corporativo.

Topología de Red. La topología de red utilizada en la sede define la estructura lógica y física sobre la cual se establecen las conexiones entre los diferentes dispositivos de red y los servidores del dominio.

Conectividad y Protocolos. En esta infraestructura se han implementado diferentes tecnologías de interconexión como:

VPNs: Redes privadas virtuales para conexiones seguras entre sedes o usuarios remotos.

MPLS: Tecnología orientada a la priorización del tráfico de red, optimizando la velocidad y calidad de los servicios.

SD-WAN: Implementación moderna que permite una gestión más eficiente y centralizada del tráfico entre diferentes puntos geográficos.

Capacidad de Ancho de Banda. Se cuenta con una capacidad de ancho de banda suficiente para soportar las operaciones de replicación del Active Directory, la sincronización de políticas de grupo (GPO) y otros procesos críticos que dependen de la disponibilidad y estabilidad del enlace de red.

*Equipos de Red***.** La infraestructura está compuesta por una variedad de dispositivos esenciales que aseguran el flujo de información y la seguridad de los datos:

Routers: Permiten la conexión entre diferentes segmentos de red.

Switches: Facilitan la comunicación interna de los equipos.

Firewalls: Proveen una capa de seguridad perimetral ante amenazas externas.

Balanceadores de carga: Distribuyen el tráfico para mejorar la disponibilidad y rendimiento de los servicios.

Servidores y Roles de Active Directory. Dentro de la infraestructura se encuentran implementados diversos roles esenciales:

Controladores de Dominio (DC): Encargados de la autenticación y administración de usuarios.

Servidores DHCP: Asignan dinámicamente direcciones IP dentro del dominio.

Servidores DNS: Gestionan la resolución de nombres, garantizando la comunicación entre equipos de la red.

Ciberseguridad

La ciberseguridad representa uno de los pilares fundamentales en la protección del entorno de TI. Este apartado describe las medidas adoptadas para mitigar vulnerabilidades, controlar accesos y garantizar el cumplimiento de políticas y regulaciones de seguridad.

Autenticación y Control de Acceso

Autenticación Multifactor (MFA): Se implementa MFA para reforzar la seguridad de inicio de sesión, reduciendo el riesgo de accesos no autorizados.

Grupos de Seguridad y Permisos: Se revisan periódicamente los grupos de seguridad y las delegaciones de permisos administrativos, asegurando que se mantenga el principio de mínimo privilegio.

Segmentación y Protección

Segmentación de Red: Se separa el tráfico administrativo del tráfico de usuario, mitigando el impacto de posibles amenazas.

Protección ante Amenazas Avanzadas: Integración con plataformas EDR/XDR para la detección y respuesta frente a ataques sofisticados.

Cumplimiento Normativo

Se verifica la conformidad con las regulaciones locales, particularmente con la Ley de Protección de Datos Personales de El Salvador, garantizando el tratamiento seguro de la información corporativa.

Telecomunicaciones y Conectividad

El componente de telecomunicaciones es esencial para la interoperabilidad entre las sedes y la adecuada sincronización de servicios. Esta sección detalla los mecanismos de interconexión y redundancia configurados para garantizar una migración fluida y segura.

Interconexión y Redundancia

Relación entre Sedes: Se mantiene una relación de confianza entre dominios corporativos.

Redundancia: Se dispone de conexiones site-to-site bidireccionales para asegurar la continuidad ante fallos.

DNS y Resolución de Nombres

Roles de DNS en DC: Los controladores de dominio (DC) tienen asignado el rol de servidores DNS.

Configuración de Zonas: Se gestionan correctamente las zonas de búsqueda directa e inversa.

Replicación DNS: Garantiza la consistencia de los registros a través de los diferentes servidores.

Sincronización de Tiempo (NTP). El servicio NTP es vital para el correcto funcionamiento de Kerberos y la autenticación entre dominios, asegurando la integridad temporal y la validez de las credenciales.

Metodología de Análisis

El análisis de la infraestructura y los servicios de red se basa en una metodología técnica y estructurada que permite obtener información confiable y verificable sobre el estado actual de la organización.

Recolección de Información

La información fue obtenida mediante entrevistas, encuestas realizadas al personal de infraestructura de cada región, revisión documental y uso de herramientas de diagnóstico como PingCastle.

Herramientas Utilizadas. Se emplearon utilidades de monitoreo y diagnóstico como: Active Directory Health Checks, Scripts de PowerShell, Plataformas de monitoreo (PRTG, SolarWinds, entre otros).

Componentes de Infraestructura Evaluados. Este apartado detalla los principales componentes analizados dentro del entorno tecnológico actual, con el propósito de determinar el estado de la infraestructura base que soporta los servicios de Active Directory y los procesos críticos de la organización.

La evaluación se realizó teniendo en cuenta los criterios de desempeño, disponibilidad, seguridad y escalabilidad, permitiendo identificar oportunidades de mejora en cada uno de los subsistemas.

Infraestructura de Red. La infraestructura de red constituye el pilar fundamental de la comunicación entre los diferentes recursos tecnológicos de la organización. En esta sección se analizan los elementos clave que aseguran la conectividad, el rendimiento y la seguridad de las interconexiones entre sedes.

Topología de red (LAN/WAN): Se evaluó la estructura de interconexión interna y externa de las sedes, verificando la segmentación lógica y física de los dispositivos de red.

Equipos de red (switches, routers, firewalls): Se revisó la configuración, marca, modelo y capacidad de los equipos, así como su compatibilidad con los estándares actuales de red.

Segmentación y VLANs: Se comprobó la existencia de redes separadas para usuarios, servidores, administración y seguridad, asegurando la correcta aplicación de políticas de tráfico.

Conectividad entre sedes (VPN, MPLS, SD-WAN): Se analizó la arquitectura de conexión entre las sedes de El Salvador, Guatemala y Panamá, determinando los niveles de redundancia, cifrado y rendimiento.

Infraestructura de Servidores. El análisis de servidores permitió identificar la diversidad de entornos presentes y su relación con los servicios de autenticación, administración de recursos y soporte de aplicaciones críticas.

Tipos de servidores (físicos, virtuales, cloud): Se determinó el modelo operativo híbrido, con servidores físicos en sedes principales y máquinas virtuales para servicios específicos.

Sistemas operativos utilizados: Se validaron versiones y niveles de actualización, identificando sistemas Windows Server 2016, 2019 y 2022.

Roles de servidor (AD DS, DNS, DHCP, File Server, etc.): Se registraron los roles y funciones principales asignados a cada servidor.

Ubicación y redundancia: Se comprobó la distribución geográfica de los servidores y la existencia de planes de respaldo ante fallos o desastres.

Servicios de Directorio. En esta sección se evaluaron los servicios de directorio que sustentan la autenticación y autorización dentro del dominio corporativo.

Estructura de Active Directory (dominios, árboles, bosques): Se analizó la organización jerárquica y la relación de confianza entre dominios.

Controladores de dominio: Se identificaron los controladores activos, sus roles FSMO y los tiempos de replicación.

Políticas de grupo (GPOs): Se revisó la estructura y coherencia de las políticas aplicadas a usuarios y equipos.

Trusts entre dominios: Se verificaron las relaciones de confianza configuradas entre sedes y su correcta sincronización.

Seguridad. El componente de seguridad fue evaluado como eje transversal del entorno tecnológico, garantizando la protección de identidades, recursos y comunicaciones.

Políticas de autenticación y autorización: Se analizó la aplicación de mecanismos de control de acceso y autenticación multifactor (MFA).

Sistemas de detección y prevención (antivirus, EDR, SIEM): Se verificó la integración de herramientas de monitoreo y respuesta ante amenazas.

Gestión de identidades (IAM): Se evaluó la implementación de procesos centralizados para la administración de credenciales y roles.

Auditorías y cumplimiento: Se revisó la trazabilidad de eventos de seguridad y su alineación con la Ley de Protección de Datos.

Diseñar la arquitectura del dominio unificado

Este apartado detalla la necesidad de consolidar los dominios corporativos en una única arquitectura centralizada que permita mejorar la administración, incrementar la seguridad, escalar los servicios y garantizar la continuidad operativa entre las sedes de El Salvador, Guatemala y Panamá.

La unificación de dominios constituye la base para optimizar la gestión de identidades, políticas de seguridad y sincronización entre entornos, eliminando redundancias y fortaleciendo la infraestructura corporativa.

Consideraciones Previas

Antes de proceder con la implementación del nuevo modelo, es indispensable revisar los aspectos fundamentales identificados durante el análisis técnico.

Estas consideraciones permiten establecer un punto de partida realista que contemple las limitaciones actuales, los requerimientos de negocio y las exigencias normativas aplicables al entorno.

Resultados del análisis de infraestructura actual.

Limitaciones técnicas y operativas detectadas.

Requisitos de negocio y de TI.

Normativas de seguridad y cumplimiento aplicables.

Principios de Diseño

El nuevo diseño de arquitectura se rige por principios rectores que garantizan su sostenibilidad y alineación con las mejores prácticas de administración de entornos corporativos basados en Active Directory. Estos principios buscan un equilibrio entre simplicidad operativa, seguridad, rendimiento y escalabilidad futura.

Simplicidad: Minimizar la complejidad administrativa.

Escalabilidad: Capacidad de crecimiento futuro.

Seguridad: Protección de identidades y recursos.

Alta disponibilidad: Redundancia y tolerancia a fallos.

Interoperabilidad: Compatibilidad entre sistemas existentes.

Modelo de Arquitectura Propuesta

Este modelo describe la estructura técnica que permitirá unificar los dominios bajo un esquema corporativo centralizado, integrando los servicios críticos y manteniendo la resiliencia operativa entre sedes.

Incluye la definición de la estructura de Active Directory, controladores de dominio, servicios asociados y estrategias de conectividad.

Estructura de Active Directory

Un único bosque con un dominio raíz corporativo.

Posibles dominios hijos o sitios para cada sede si se requiere segmentación lógica.

Uso de Organizational Units (OUs) para delegación administrativa.

Controladores de Dominio

Distribución geográfica de DCs por sede.

Roles FSMO centralizados o distribuidos según necesidad.

Replicación entre DCs con políticas de optimización de ancho de banda.

Servicios Integrados

DNS y DHCP integrados con AD.

Sincronización con Azure AD si se contempla una estrategia híbrida.

Integración con servicios como Microsoft 365, Intune, Defender for Identity.

Políticas de Grupo (GPOs)

Diseño jerárquico de GPOs por OU.

Políticas de seguridad, auditoría, acceso remoto, etc.

Identidad y Acceso

Estrategia de autenticación: Kerberos, NTLM, MFA.

Gestión centralizada de usuarios y grupos.

Delegación de permisos por sede y función.

Red y Conectividad

Diseño de sitios y subredes en AD.

Configuración de replicación entre sitios.

VPNs o enlaces dedicados para conectividad segura.

Diagramas de Arquitectura

Para una comprensión integral del diseño, se incluyen los diagramas lógicos y físicos que representan la estructura del bosque, los dominios y la replicación entre controladores. Estos diagramas permiten visualizar las relaciones entre sedes, los flujos de autenticación y las dependencias críticas de comunicación.

Diagrama lógico del bosque y dominios.

Diagrama físico de controladores de dominio y replicación.

Flujo de autenticación y acceso entre sedes.

Ventajas del Diseño Propuesto

Este modelo proporciona beneficios tangibles en términos de eficiencia, seguridad y gobernanza. Permite una administración centralizada, reduce los costos operativos y mejora la

capacidad de respuesta ante incidentes o cambios organizacionales.

Reducción de costos operativos.

Mejora en la administración de usuarios y recursos.

Mayor seguridad y control.

Facilidad para implementar políticas globales.

Riesgos y Mitigaciones

Se identifican los riesgos potenciales asociados a la implementación de la arquitectura unificada, junto con las estrategias de mitigación que garantizan la estabilidad y confiabilidad del entorno.

Riesgos de replicación lenta o fallida.

Posibles conflictos de nombres o SID.

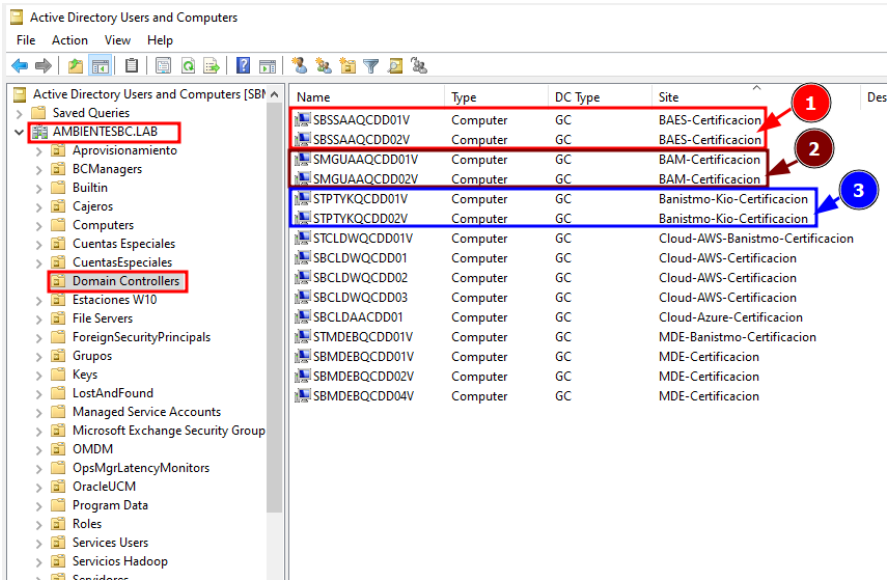
Estrategias de respaldo y recuperación ante desastres.

Imágenes y Diagramas

Ambientes NO Productivos:

Figura 60

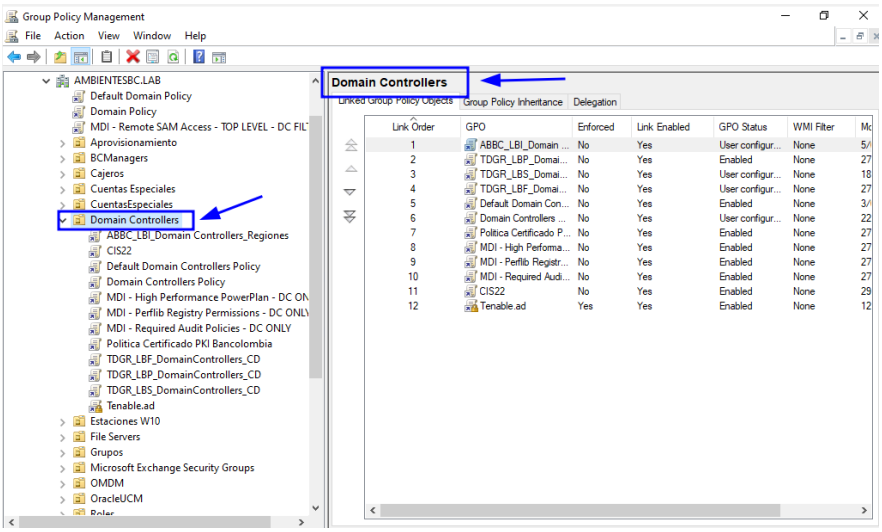
Imagen Actual del Directorio Activo en Ambientes NO Productivos



A nivel de GPO´s se muestran a continuación: Las políticas son administradas por los Administradores del dominio con cuentas elevadas Global Admin

Figura 61

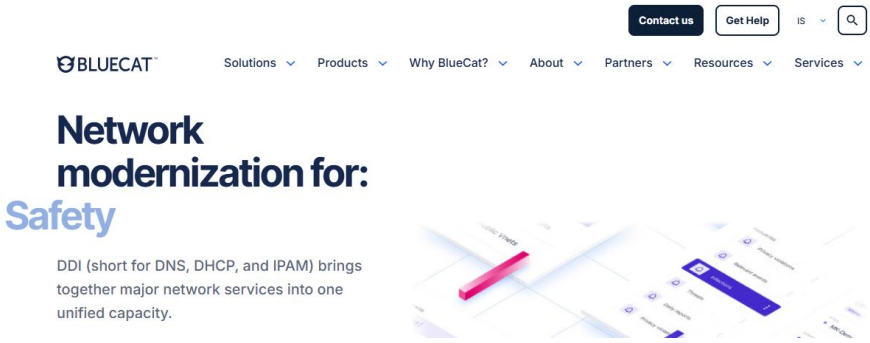
Imagen Actual de la configuración de las GPO´´s en Ambientes Productivos



Los roles que actualmente tiene los controladores de dominio de cada región son el de Directorio Activo debido a que el servicio de DNS y DHCP fue entregado al área de TELCO de la compañía, ellos actualmente tienen todo el gobierno de este servicio a través de una herramienta llamada Bluecat.

Figura 62

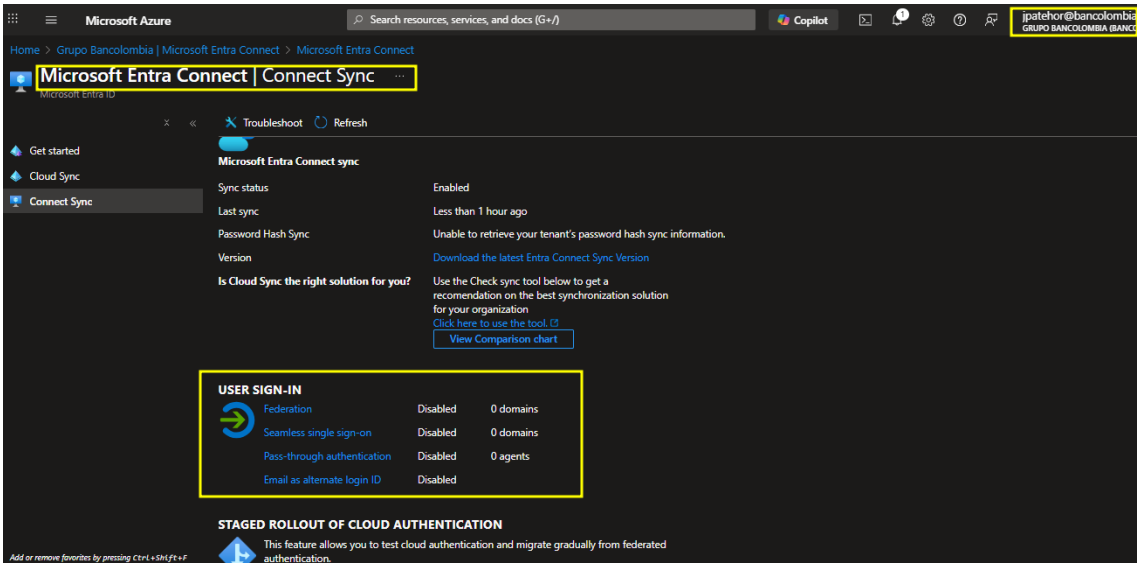
Imagen de la Aplicación llamada BLUECAT la cual es Administrada por el Área de TELECOMUNICACIONES



La sincronización de todos los objetos creados en los Controladores de dominio OnPremise se realizan a través de un servicio en un Servidor Llamado ADConnect el cual esta encargado de sincronizar automáticamente todos los objetos hacia el servicio en nube llamado ENTRA ID.

Figura 63

Imagen Actual salida del TENAT de BANCO la cual muestra la configuración actual del ADCONNECT para la Sincronización de Usuarios

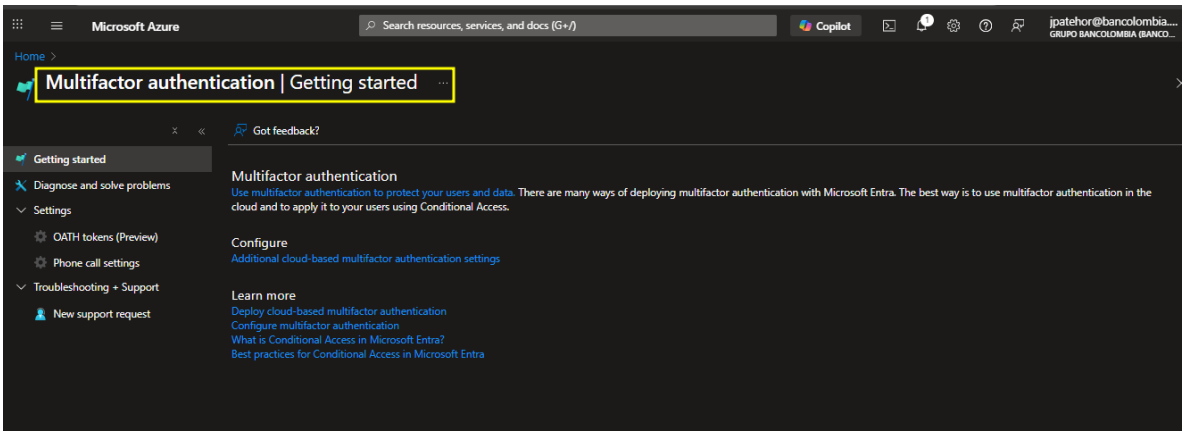


Allí finalmente se tiene todo el Gobierno a nivel de los usuarios al momento de realizar la Autenticación donde se está brindando a todas las regiones la seguridad por medio del Servicio de Doble Factor de Autenticación MFA.

A continuación, se presenta información detallada que permite visualizar el procedimiento.

Figura 64

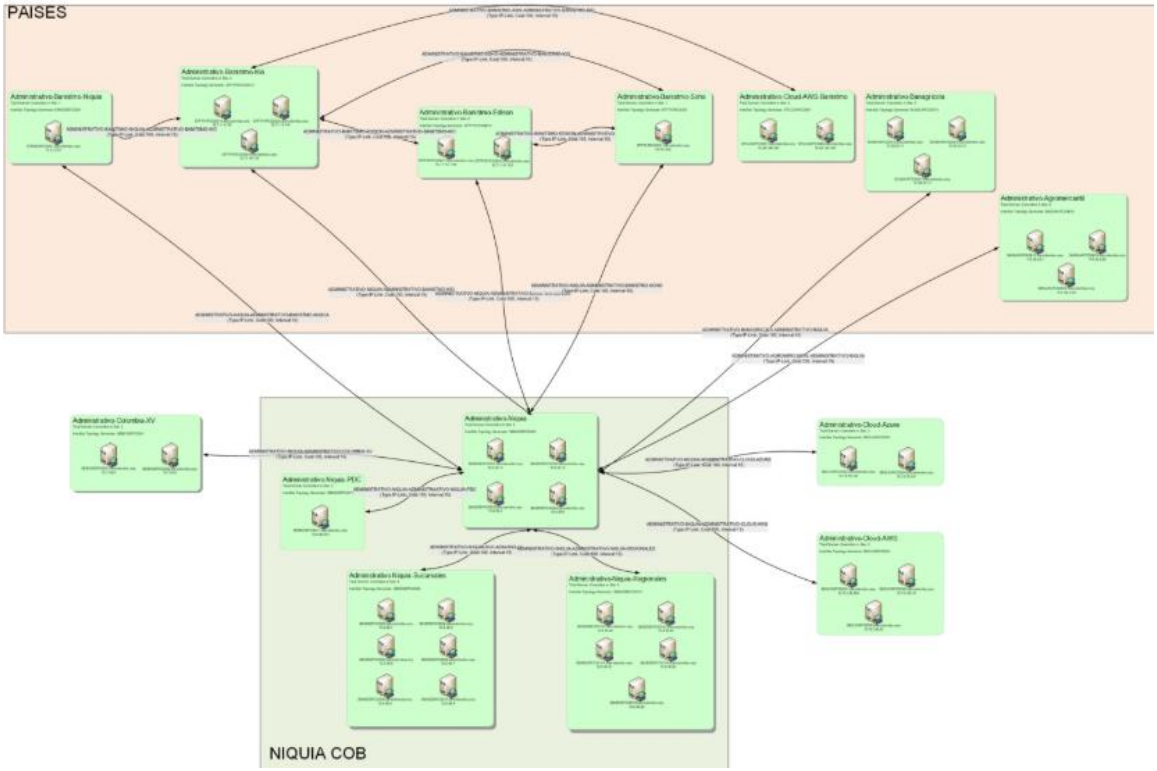
Imagen salida del TENANT de BANCO donde se evidencia la configuración del servicio MFA: Multi Factor Autenticator.



Anexo la arquitectura de como esta hoy día funcional el servicio corporativo para Colombia y todas las regiones:

Figura 65

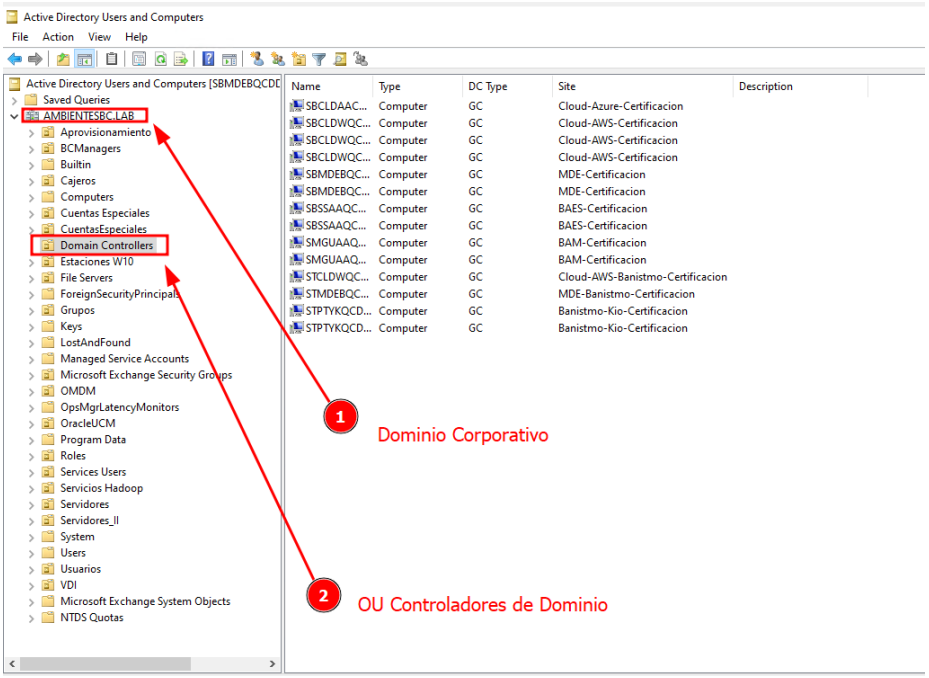
Arquitectura Actual de todo el Ecosistema de BANCO



Active Directory: Anexo el esquema actual del Directorio active en Ambientes NO productivos

Figura 66

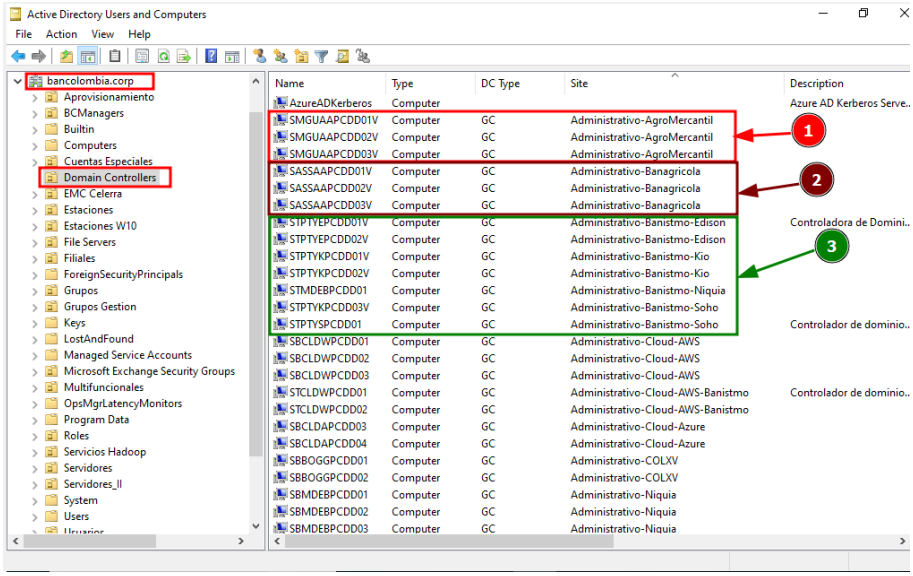
Imagen que contiene la configuración de la OU (Unidad Organizacional) donde están Almacenados todos los Controladores de Dominio de las Diferentes Sedes.



Ambientes Productivos

Figura 67

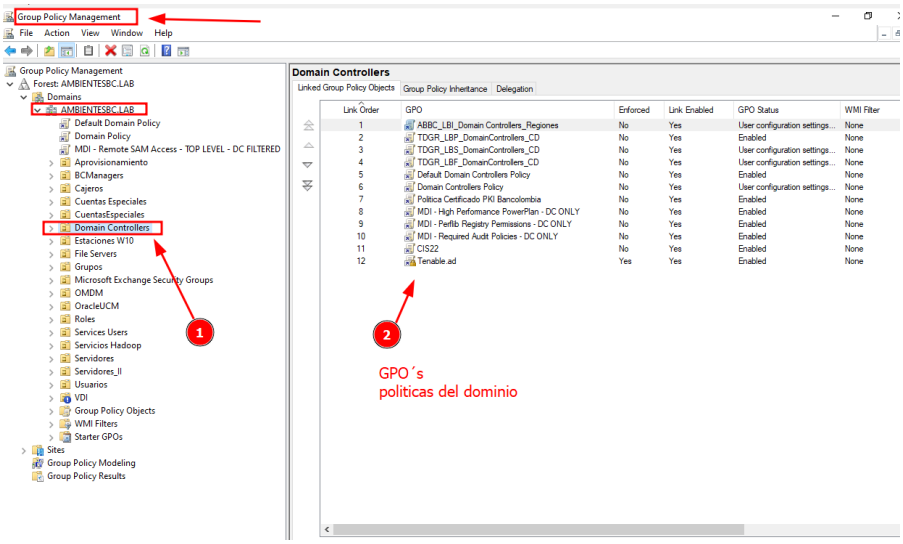
Imagen Actual del Directorio Activo en Ambientes Productivos



GPO´S: Politicas del Dominio

Figura 68

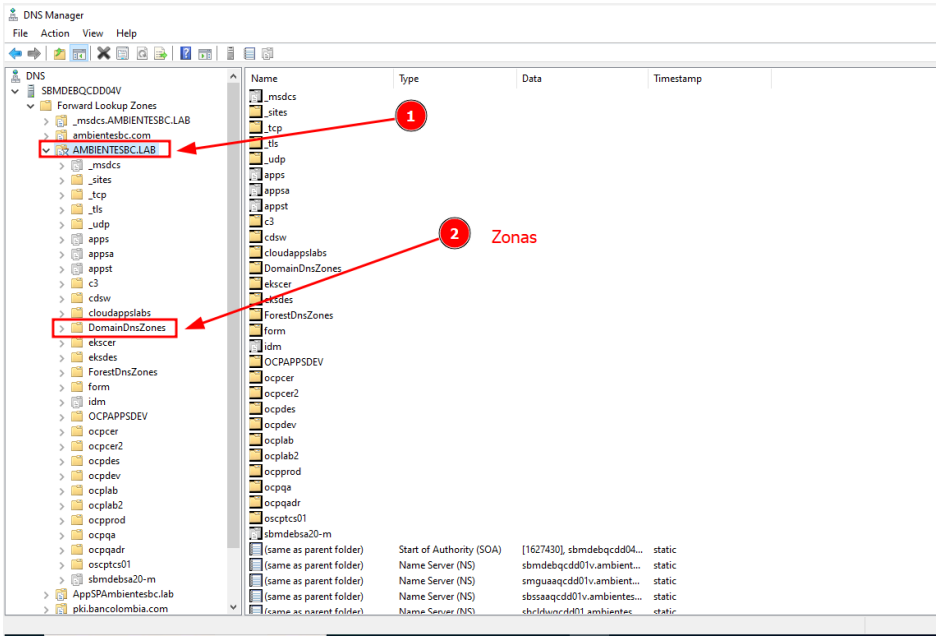
Imagen Actual con las Directivas de Grupo}



DNS y DHCP: el servicio de DHCP es administrado directamente por el área de TELECOMUNICACIONES.

Figura 69

Configuración del Servicio DNS el cual esta Administrado por TELECOMUNICACIONES.



Establecer políticas de seguridad y replicación

Este objetivo define el conjunto de políticas técnicas y operativas destinadas a proteger las identidades y recursos en el dominio corporativo unificado y a garantizar la replicación

coherente y resiliente del Active Directory entre sedes (El Salvador, Guatemala y Panamá). Las políticas están alineadas con buenas prácticas Microsoft, NIST e ISO/IEC 27001 y contemplan controles de acceso, replicación, backups, monitoreo y recuperación ante incidentes.

Las políticas de seguridad definen controles de identidad, autenticación, autorización, gobernanza de privilegios y monitoreo. Están diseñadas para minimizar el riesgo de compromisos de cuentas, proteger GPOs y evitar movimientos laterales dentro de la red.

Control de acceso y autenticación. Implementar MFA para cuentas administrativas y accesos remotos (Azure AD/AD FS/third-party). Kerberos como protocolo primario; eliminación de NTLMv1 y restricción de NTLMv2.

Políticas de bloqueo de cuentas y control de sesión administrativa (Just-In-Time / Just-Enough-Administration si aplica).

Figura 70

Flujo de autenticación Kerberos aplicado en el dominio corporativo

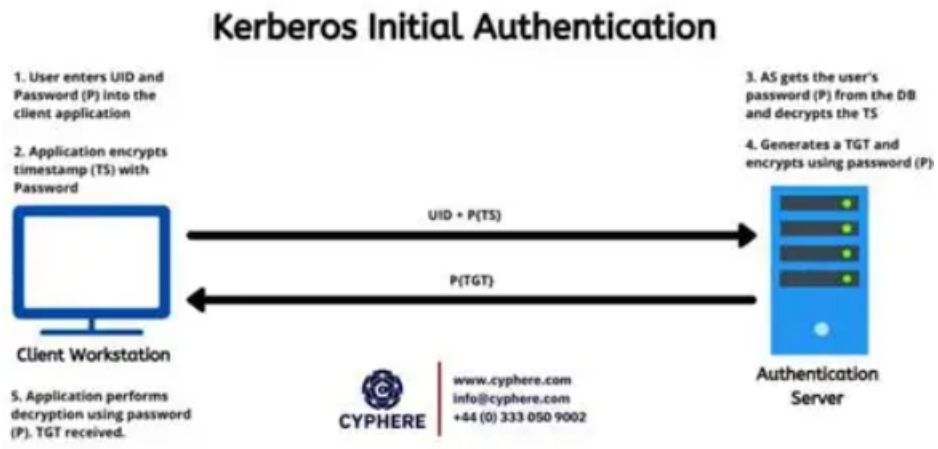
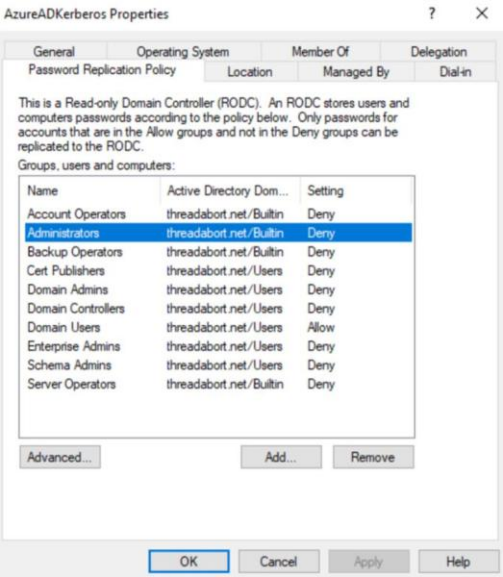


Figura 71

Configuración de políticas de seguridad en Controlador de Dominio de Solo Lectura



Cómo comprobar la política de contraseñas de Active Directory

Políticas de contraseñas y bloqueo

Contraseña mínima: 12 caracteres; complejidad (mayúsc/minúsc/números/caracteres).

Caducidad: cada 90 días; historial: retener 5 contraseñas previas. Bloqueo automático tras 5 intentos fallidos; desbloqueo manual documentado. Implementación a través de GPO (Password Policy + Fine-Grained Password Policies si se requiere granularidad).

Figura 72

Buenas prácticas implementadas para la gestión de contraseñas

Fuente. https://www3.gobiernodecanarias.org/educacion/cau_ce/servicios/web/noticias/noticia-politica_contrasenas

Figura 73

Ejemplos de contraseñas inseguras consideradas en la definición de políticas

Fuente. https://www3.gobiernodecanarias.org/educacion/cau_ce/servicios/web/noticias/noticia-politica_contrasenas

Segmentación, RBAC y delegación (SoD)

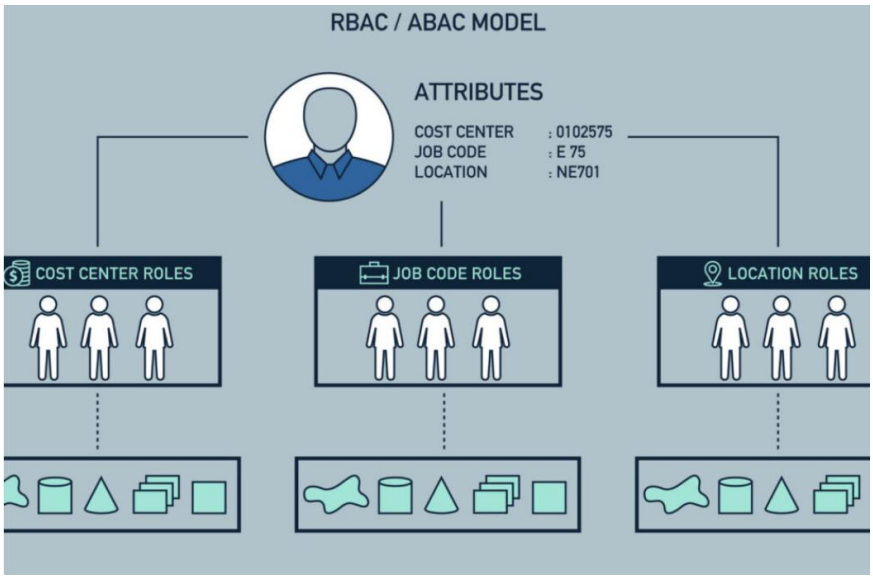
Modelo RBAC: definir roles (Domain Admins, Server Operators, Helpdesk) y OUs con delegación.

Separación de funciones (SoD) para evitar concentrar privilegios; aplicar PIM/JIT donde sea posible.

Revisiones trimestrales de membresías y uso de logs para detectar privilegios sobredimensionados.

Figura 74

Modelo de control de acceso RBAC/ABAC aplicado a la infraestructura



Fuente. https://cyberhoot.com/es/cybrario/control-de-acceso-basado-en-roles-rbac/

Monitoreo y auditoría

Centralizar logs: Windows Event Forwarding → SIEM (Microsoft Sentinel / Splunk).

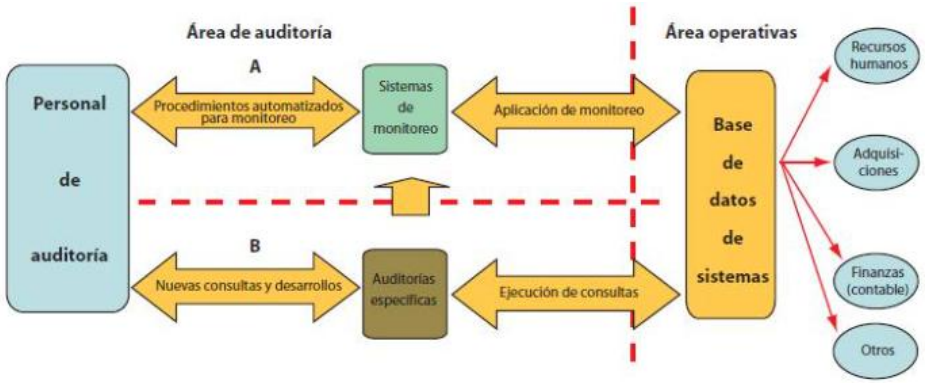
Auditar: cambios en objetos críticos, inicios de sesión privilegiados, fallos de replicación.

Retención mínima de logs: 180 días (ajustable por normativa).

Alertas automatizadas (SOAR playbooks) para detección de actividad anómala.

Figura 75

Flujo operativo de auditoría y monitoreo de sistemas



Fuente. https://www.auditool.org/blog/auditoria-interna/auditoria-de-monitoreo-continuo-de-las-operaciones?highlight=WyJjb250cm9sIiwiYWwiXQ==

Figura 76

Panel de monitoreo para supervisión de la infraestructura tecnológica

Políticas de replicación

Las políticas de replicación garantizan que los datos del AD se propaguen de forma consistente, eficiente y segura entre DCs; además definen topología, horarios, límites de ancho de banda, validaciones y alertas.

Diseño de topología y Site Links

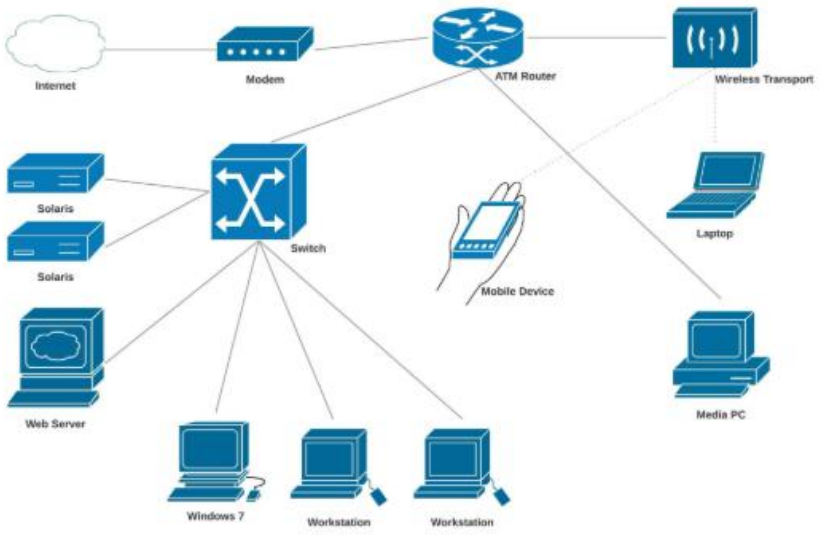
Definir Sites y Subnets en AD con Site Links entre ubicaciones (costos basados en ancho de banda).

Intrasite: replicación casi instantánea (RPC). Intersite: programada (RPC/SMTP según escenario).

Optimizar costos y schedule para replicación intersite en ventanas de baja carga

Figura 77

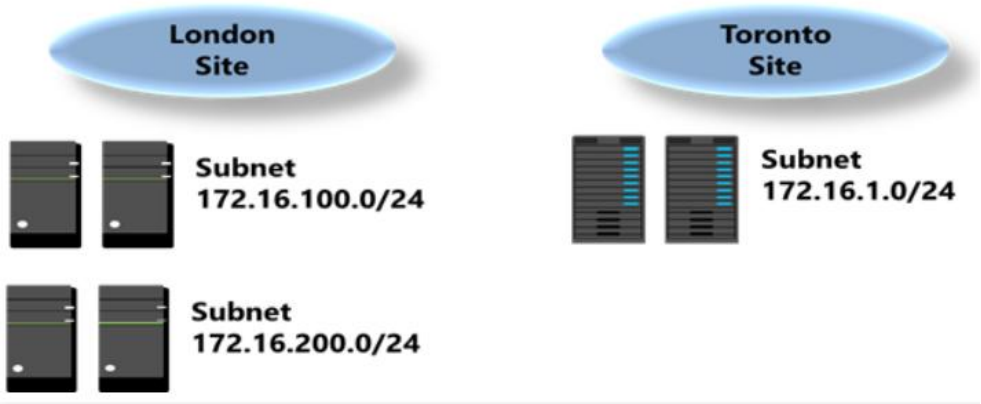
Topología de red utilizada como base para definir políticas de seguridad



Nota. Diagrama de la topología de red corporativa que integra servidores, estaciones de trabajo y dispositivos móviles, sirviendo como referencia para la aplicación de políticas de seguridad y segmentación de red.

Figura 78

Segmentación de sedes y subredes para optimizar replicación



Nota. Representación de la segmentación por sitios y subredes IP utilizada para optimizar los procesos de autenticación y replicación de Active Directory entre las diferentes sedes de la organización. *Fuente.* https://thisismyclassnotes.blogspot.com/2017/06/windows-server-sites-subnet-and-site.html

KCC y objetos de conexión (conexiones generadas vs manuales)

KCC genera automáticamente objetos de conexión para intrasite/intersite replicación.

Política: usar conexiones automáticas por defecto; crear manuales sólo para optimización o contingencia.

Documentar cualquier conexión manual y evitar que KCC la modifique (marcar como administratively modified).

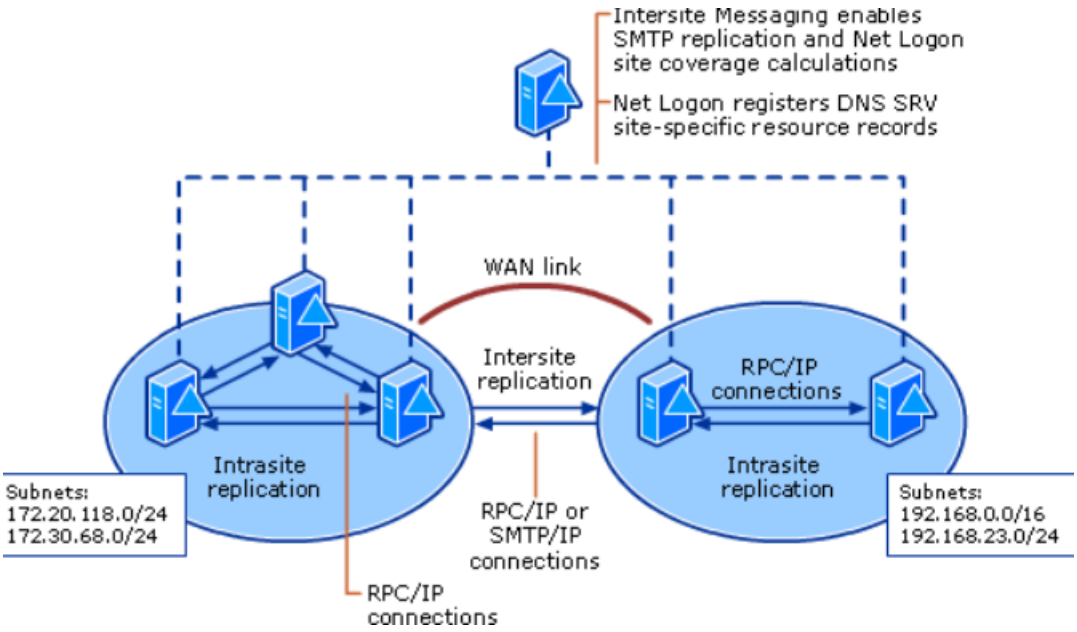
Frecuencia, throttling y QoS

Intrasite: inmediato; Intersite: default 180 min (ajustable).

Establecer throttling de replicación (AD replication schedule) para enlaces WAN con bajo ancho de banda. Implementar QoS en la red para priorizar tráfico de replicación y RPC entre DCs.

Figura 79

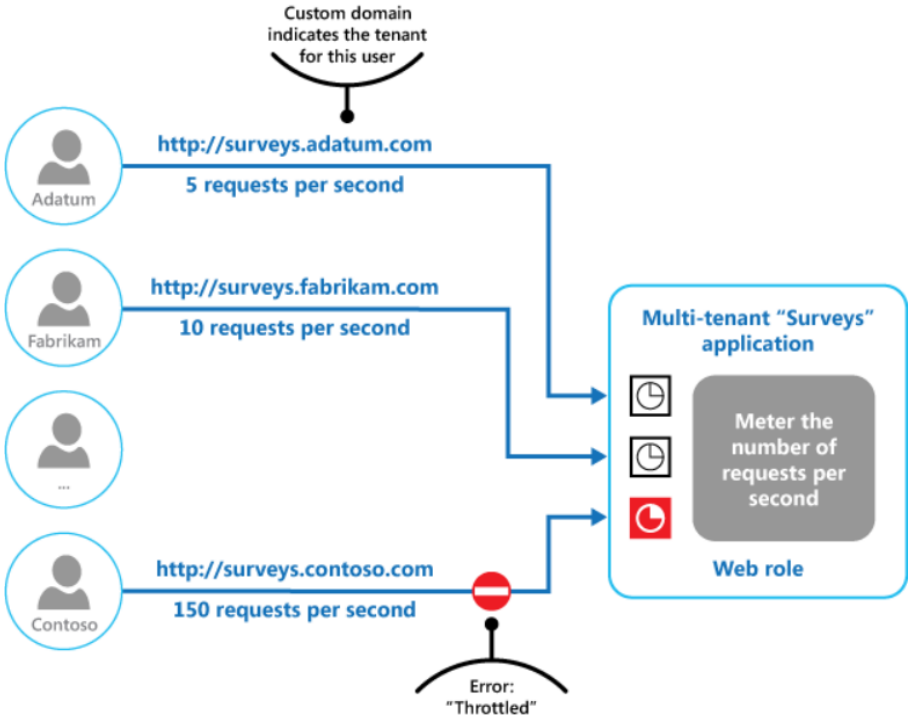
Replicación intra-sitio e inter-sitio configurada en Active Directory



Fuente. https://learn.microsoft.com/es-es/previous-versions/windows/it-pro/windows-server-2003/images/cc811568.3e66bd18-c51f-410a-9e2b-1af8ded96938(ws.10).gif

Figura 80

Control de consumo y limitación de solicitudes (Throttling) en aplicaciones multi-tenant



Fuente. https://learn.microsoft.com/es-es/azure/architecture/patterns/_images/throttling-multi-tenant.png

Monitoreo de replicación (herramientas y alertas)

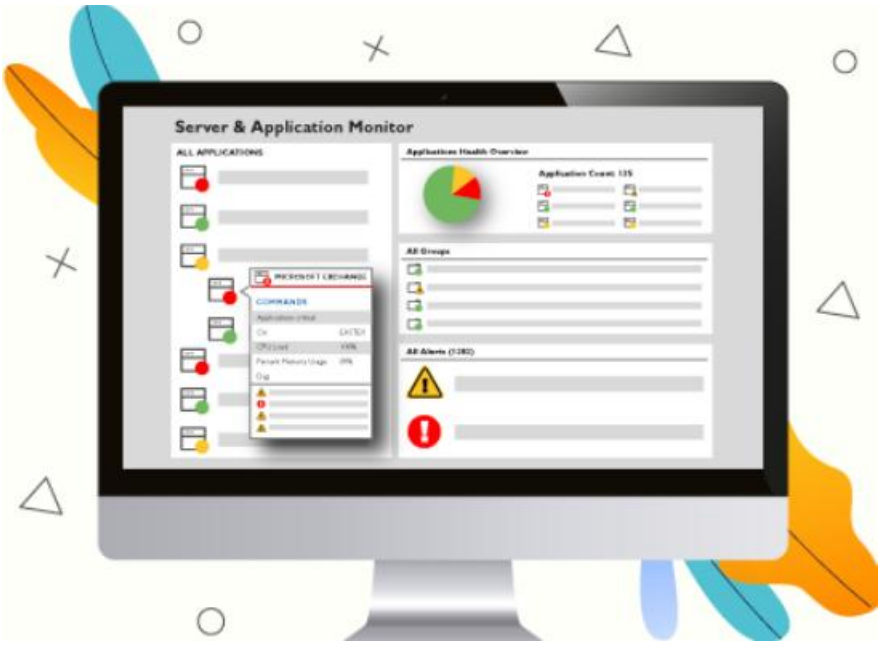
Supervisar una topología de replicación es un aspecto importante en la implementación de la replicación. Debido a que la actividad de replicación se distribuye, es fundamental realizar un seguimiento de la actividad y el estado de todos los equipos que participan en la replicación

Herramientas: repadmin, dcdiag, ADREPLSTATUS, PowerShell (Get-ADReplicationPartnerMetadata), y monitorización SNMP/PRTG para latencia/paquetes perdidos.

Políticas de alerta: fallos de replicación, errores de USN rollback, latencia > umbral, event IDs críticos (1026, 1311, etc.). Reportes diarios y panel operativo (dashboard SIEM/Monitor).

Figura 81

Panel de monitoreo de servidores y aplicaciones



Top 10 Server & Application Monitoring Tools

Estrategias de resiliencia y recuperación

Para garantizar la continuidad del negocio y la resiliencia cibernética, es fundamental imp lementar estrategias de resiliencia y recuperación para el Directorio Activo; Define políticas de backup, restauración, alta disponibilidad y tests de DR para garantizar la recuperación del AD tras fallos o incidentes.

Figura 82

Relación entre resiliencia del negocio, gestión de crisis y recuperación ante desastres

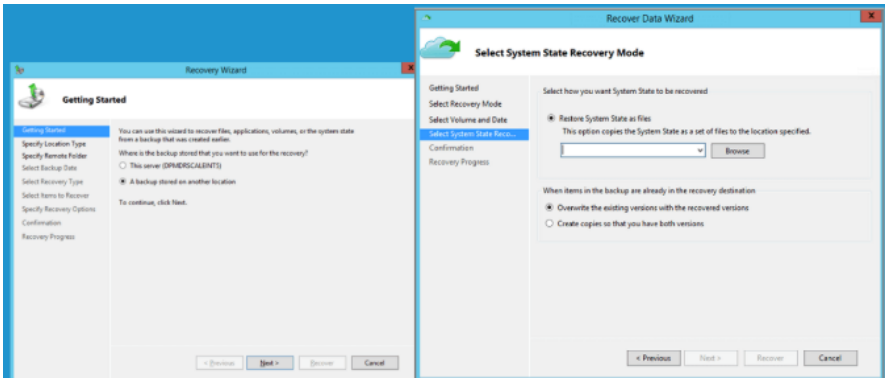
Backups y Authoritative/Non-Authoritative Restore

Backups System State semanales (cifrado y almacenamiento fuera de sitio).

Procedimientos documentados para Authoritative (cuando se desea restaurar objetos perdidos) y Non-Authoritative Restore. Pruebas de restore anual en entorno aislado.

Figura 83

Proceso de respaldo y restauración de Active Directory



Fuente. https://www.easeus.com/todo-backup-guide/backup-and-restore-active-directory.html

Redundancia geográfica y Global Catalog. Mantener mínimo 2 DCs por sitio, con al menos un Global Catalog replicado. Balancear roles FSMO si la latencia lo exige (p. ej., mantener algunos FSMO locales para rendimiento). Asegurar reubicación planeada de FSMO si se cambia topología

Figura 84

Esquema de redundancia para protección de la información

Nota. Almacenamiento de los mismos datos varias veces en diferentes lugares. *Fuente*. https://www.emaze.com/@AORFRIIFO/Bases-de-datos

Políticas de auditoría y cumplimiento

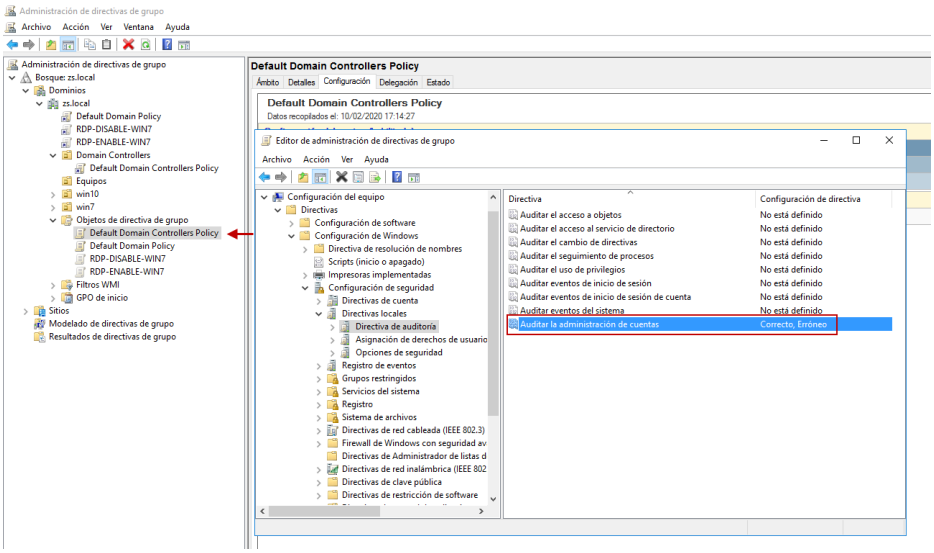
Define qué eventos auditar, dónde centralizar logs, procedimientos de retención y su alineamiento con normativas (Ley de Protección de Datos, ISO/IEC 27001). Las políticas de auditoría y cumplimiento son fundamentales para garantizar la calidad, consistencia y objetividad en las auditorías. Estas políticas deben ser claras, concisas y comprensibles para todos los involucrados en el proceso, desde los auditores hasta los responsables de las áreas auditadas.

Eventos auditados y retención. Los logs de eventos de Active Directory se pueden ver con el Visor de eventos, que es una herramienta nativa proporcionada por Microsoft. Pero primero se debe activar la directiva de auditoría de su dominio. Auditar cambios en OU, cuentas con privilegios, modificaciones de GPO, eventos de replicación fallida y accesos administrativos.

Retención: mínimo 180 días en SIEM; conservar extractos críticos por 3–7 años según regulaciones.

Figura 85

Configuración de directivas de seguridad mediante Group Policy Objects (GPO)



Administración de directivas de grupo (GPO) sobre MS Windows Server 2012 R2 – RAGASYS SISTEMAS

Integración con soluciones corporativas y beneficios

Integración: Defender for Identity, Azure AD Connect (para híbrido), SIEM/SOAR.

Beneficios: consistencia, menor TTR (time to recover), menor superficie de ataque, cumplimiento. Al limpiar y organizar el AD, las empresas podrán integrarlo de manera efectiva con otras soluciones de IAM y evitarán problemas como la falta de acceso a recursos de datos no estructurados y la retención de acceso a datos por parte de empleados que ya no deberían tenerlo.

Figura 86

Servicios y áreas soportadas por la infraestructura tecnológica

Fuente. https://blog.hubspot.es/sales/integracion-empresarial

Ejecutar pruebas piloto de migración

El proceso de ejecución de pruebas piloto de migración representa una etapa crítica en la transición hacia una infraestructura de Active Directory (AD) unificada y modernizada. Estas pruebas permiten validar la planificación, las herramientas, los procedimientos y las configuraciones antes de implementar el cambio definitivo en el entorno productivo. Su correcta ejecución garantiza la integridad de los datos, la consistencia de la replicación, la preservación de permisos y la continuidad operativa del servicio de directorio.

Figura 87

Sincronización automática de usuarios y estados durante pruebas piloto de migración

Nota. proceso de sincronización automática entre el Directorio Activo y los sistemas de gestión de usuarios y seguridad, donde se integran equipos, usuarios y grupos. *Fuente.* https://learn.microsoft.com/en-us/training/modules/active-directory-domain-services-migration/

Planeación de la Prueba Piloto

La planeación de la prueba piloto debe definir los objetivos específicos, el alcance, los criterios de éxito y los riesgos asociados. Este proceso asegura que las actividades ejecutadas en entornos controlados sean representativas del entorno de producción.

Definición del Alcance

El alcance debe determinar los objetos que serán migrados (usuarios, grupos, computadoras o unidades organizativas) y las dependencias asociadas a los mismos, garantizando que la muestra seleccionada represente adecuadamente la complejidad del entorno productivo.

Criterios de Éxito

Los criterios de éxito deben estar orientados a verificar:

La correcta migración de los objetos seleccionados.

La preservación de permisos y pertenencias a grupos.

La replicación oportuna entre controladores de dominio.

El mantenimiento de la autenticación de los usuarios sin interrupciones.

Componentes clave de una prueba piloto exitosa:

Realizar una prueba y verificar los resultados: comparar los grupos, agentes, organizaciones, clientes y tickets de origen y destino por IDs. Puede volver a ejecutar su Demo tantas veces como sea necesario para obtener el resultado deseado. También puede revertir la Demo y eliminar los datos migrados.

Preparación del Entorno de Pruebas

Configuración del Entorno Controlado

Se recomienda implementar un entorno aislado, replicando las configuraciones críticas del entorno productivo. Este debe incluir:

Controladores de dominio con roles equivalentes.

Configuración DNS y DHCP coherente.

Políticas de grupo (GPOs) aplicables.

Relaciones de confianza simuladas.

Herramientas de Soporte. Las principales herramientas utilizadas incluyen:

ADMT (Active Directory Migration Tool): para el movimiento controlado de objetos.

PowerShell AD Cmdlets: para automatización y validación.

Event Viewer y Repadmin: para diagnóstico de replicación.

PingCastle y AD Health Check: para evaluación de estado postmigración.

Entorno de laboratorio simulado para prueba piloto de migración

Pruebe siempre el plan de migración en una configuración de laboratorio controlada antes de implementarlo en toda la organización. En el entorno de prueba, se necesita al menos un equipo para cada tipo de sistema operativo desde el que se migran los datos.

Una vez que todo el proceso de migración se prueba en un único equipo que ejecuta cada uno de los sistemas operativos de origen de la organización, realice una migración piloto con un pequeño grupo de usuarios. Después de migrar algunos estados de usuario típicos al almacén intermedio, tenga en cuenta el espacio necesario y ajuste los cálculos iniciales en consecuencia. Para obtener más información sobre cómo calcular el espacio necesario para la migración, consulte Estimación del tamaño del almacén de migración. Es posible que sea necesario ajustar la información de configuración del Registro y ubicación del archivo en los archivos de regla de migración. Si se realizan cambios, vuelva a probar la migración y compruebe que todos los datos y la configuración se migraron según lo esperado. Una migración piloto también ofrece la oportunidad de probar las estimaciones de espacio para el almacén intermedio.

Ejecución de la Prueba Piloto

Migración de Usuarios y Grupos. Durante esta fase se emplean scripts de PowerShell y ADMT para migrar los usuarios, grupos y sus relaciones jerárquicas. Se recomienda validar los

atributos críticos (SIDHistory, UPN y pertenencias a grupos) mediante auditorías posteriores a la migración.

Validación de Permisos y Políticas

Una vez completada la migración inicial, se debe verificar que:

Las políticas de grupo se apliquen correctamente.

Los usuarios puedan autenticarse sin errores.

Las rutas de acceso a recursos compartidos permanezcan operativas.

Replicación y Sincronización

Se monitorea la replicación entre controladores de dominio mediante el uso de comandos como repadmin /replsummary y la validación del estado de sincronización en AD Sites and Services. Esto garantiza que no existan demoras ni errores en la propagación de los cambios.

Flujo de replicación durante la migración piloto

Análisis de Resultados y Documentación

Reporte de Resultados

Se elabora un informe consolidado que describa:

Objetos migrados correctamente.

Errores encontrados y su causa raíz.

Tiempo total de ejecución y desempeño del sistema.

Validación de replicación y autenticación.

Retroalimentación y Ajustes

Con base en los resultados, se implementan ajustes en las configuraciones, scripts y políticas antes de proceder a la migración definitiva. Este proceso iterativo fortalece la robustez del diseño y mitiga riesgos operativos.

Indicadores de Éxito del Proyecto

Tabla 1

Indicadores de existo del proyecto

	Formula	Meta
Porcentaje de usuarios migrados exitosamente al nuevo dominio corporativo	(Usuarios migrados sin errores / Total de usuarios) × 100	≥ 95%
Disponibilidad del servicio de autenticación post-migración	(Horas de disponibilidad / Horas totales del periodo evaluado) × 100	≥ 99.5%
Tiempo promedio de replicación entre controladores de dominio	Tiempo medio de replicación medido con herramientas como repadmin	≤ 15 minutos
Número de incidencias técnicas reportadas durante la migración	Conteo de tickets o reportes generados por usuarios o técnicos	≤ 5 incidencias críticas
Cumplimiento del cronograma del proyecto	(Tareas completadas en tiempo / Total de tareas) × 100	≥ 90%
Aplicación efectiva de políticas de grupo (GPO)	(GPO aplicadas correctamente / GPO planificadas) × 100	100%

Desarrollo de la Implementación

La presente fase tiene como finalidad describir de manera detallada el proceso metodológico adoptado para la ejecución del proyecto. La metodología seleccionada corresponde a un enfoque cuantitativo-descriptivo, con componentes experimentales y aplicados, cuyo propósito es resolver un problema técnico real dentro de una infraestructura de red distribuida. Este desarrollo se compone de cinco fases principales, en las cuales se abordan tareas específicas, herramientas utilizadas y criterios de validación que garantizan la efectividad del proceso de migración hacia un dominio unificado.

Diagnóstico y Análisis de la Infraestructura Actual

Objetivo

Comprender y evaluar el estado actual de los dominios distribuidos en las sedes de Colombia, Guatemala, El Salvador y Panamá, con el fin de identificar las condiciones técnicas iniciales, los elementos dependientes y los riesgos potenciales del entorno.

Tareas Específicas

Inventariar controladores de dominio, usuarios, grupos, directivas (GPOs) y servicios activos.

Evaluar la topología de red, niveles de conectividad, y mecanismos de seguridad implementados.

Identificar dependencias locales, servicios críticos y vínculos interdominio.

Herramientas Utilizadas

Active Directory Users and Computers, repadmin, dcdiag, netdiag, y PowerShell fueron las herramientas principales utilizadas para obtener métricas y evidencias técnicas sobre la infraestructura actual.

Diseño de la Arquitectura del Dominio Unificado

Objetivo

Diseñar una estructura lógica y física que permita consolidar todos los dominios bajo una única entidad corporativa, garantizando seguridad, rendimiento y escalabilidad.

Tareas Específicas

Definir la jerarquía de Unidades Organizativas (OU).

Asignar los roles FSMO y planificar la estrategia de replicación entre sedes.

Diseñar políticas de grupo (GPO) centralizadas y coherentes con los niveles jerárquicos administrativos.

Planificar la infraestructura de VPN segura que soporte la replicación entre sitios remotos.

Herramientas Utilizadas

Se emplearon Active Directory Sites and Services, Group Policy Management Console y Microsoft Visio para el modelado de la estructura jerárquica y el diseño lógico de la red.

Preparación del Entorno y Pruebas Piloto

Objetivo

Validar la viabilidad técnica del diseño propuesto mediante la ejecución de un entorno controlado (sandbox) que permita identificar posibles errores antes de la migración completa.

Tareas Específicas

Implementar un entorno de pruebas con infraestructura virtual.

Simular la migración de objetos utilizando ADMT.

Ejecutar pruebas de replicación, autenticación y aplicación de GPOs entre sedes.

Herramientas Utilizadas

ADMT, PowerShell, Wireshark y Event Viewer fueron utilizadas para capturar métricas, analizar tráfico de red y verificar la correcta replicación de objetos.

Ejecución de la Migración

Objetivo

Consolidar los dominios de las sedes remotas en el dominio corporativo centralizado, garantizando continuidad operativa y mínima interrupción para los usuarios finales.

Tareas Específicas

Migrar usuarios, grupos y equipos a la nueva estructura de dominio.

Reconfigurar perfiles de usuario y políticas de acceso.

Redirigir servicios, recursos compartidos y rutas DNS hacia el dominio unificado.

Herramientas Utilizadas

ADMT, PowerShell, robocopy y DNS Manager se emplearon para la ejecución controlada de las tareas de migración.

Documentación y Entrega de Resultados

Objetivo

Registrar y consolidar todos los procedimientos técnicos, resultados y evidencias del proceso de migración.

Tareas Específicas

Elaborar manuales de administración del nuevo dominio.

Documentar incidencias, soluciones y lecciones aprendidas.

Preparar un informe técnico final para presentación ante el comité académico y la empresa.

Herramientas Utilizadas

Microsoft Word, Visio, Excel, y capturas de consola para la generación de documentación y reportes visuales.

Consideraciones

Documentar diferencias funcionales y estructurales entre dominios.

Identificar posibles incompatibilidades o riesgos de pérdida de datos durante la migración.

Garantizar la escalabilidad futura del entorno.

Asegurar la delegación de administración por cada sede sin comprometer la integridad del dominio principal.

Medir los tiempos de replicación entre controladores.

Validar la integridad y consistencia de los objetos migrados.

Minimizar el impacto en los usuarios finales mediante ventanas de mantenimiento planificadas.

Ejecutar copias de seguridad previas y validaciones posteriores a la migración.

Garantizar la trazabilidad de todas las fases ejecutadas.

Incluir indicadores de éxito y métricas de rendimiento (tiempo, usuarios migrados, replicación exitosa).

Beneficiarios

El presente proyecto de migración y unificación de dominios corporativos beneficiará a múltiples actores dentro de la organización, tanto a nivel técnico como operativo. A continuación, se detallan los principales beneficiarios:

Área de Tecnología (TI):

Mejora en la administración centralizada de usuarios, equipos y políticas.

Reducción de la complejidad operativa y de los tiempos de respuesta ante incidentes.

Mayor control sobre la seguridad y cumplimiento normativo.

Usuarios Finales de las Sedes (Colombia, Guatemala, El Salvador y Panamá):

Acceso más rápido y seguro a los recursos corporativos.

Experiencia de usuario unificada y consistente en todas las sedes.

Reducción de interrupciones por problemas de autenticación o configuración.

Gerencia y Alta Dirección:

Visibilidad centralizada del estado de la infraestructura tecnológica.

Optimización de costos operativos y de licenciamiento.

Mejora en la toma de decisiones basada en una infraestructura más robusta y confiable.

Equipo de Seguridad Informática:

Aplicación uniforme de políticas de seguridad y auditoría.

Mayor capacidad de respuesta ante amenazas o vulnerabilidades.

Consolidación de registros y eventos para análisis forense y cumplimiento.

Estudiante Investigador (Juan Pablo Atehortua Arenas):

Aplicación práctica de conocimientos adquiridos en la carrera de Ingeniería en Telecomunicaciones.

Desarrollo de competencias en diseño de infraestructura, migración de servicios y gestión de proyectos.

Generación de un aporte académico y técnico con impacto real en una organización.

Conclusiones

El proyecto demostró que la unificación de dominios de Active Directory en múltiples sedes internacionales es técnica y operativamente viable cuando se apoya en un diagnóstico riguroso, un diseño arquitectónico bien estructurado y la aplicación de buenas prácticas de seguridad y replicación.

La arquitectura de dominio unificado permitió mejorar significativamente la administración centralizada, la coherencia de las políticas de seguridad y la eficiencia operativa, reduciendo la complejidad administrativa y fortaleciendo la gobernanza de identidades a nivel corporativo.

La implementación de políticas de seguridad, mecanismos de replicación bidireccional y pruebas piloto controladas garantizó la integridad de los datos, la continuidad del servicio y la mitigación de riesgos durante el proceso de migración, evitando impactos negativos en la operación de las sedes.

El proyecto dejó una infraestructura de Active Directory escalable, resiliente y preparada para el crecimiento futuro de la organización, sirviendo como base para nuevas integraciones, auditorías de seguridad y procesos de mejora continua en la gestión de la infraestructura tecnológica.

Bibliografia

ActiveDirectoryPro. (s. f.). Group Policy diagram: User and computer settings flow. https://activedirectorypro.com/group-policy-guide/

Cloudflare, Inc. (s. f.). What is a VPN? https://www.cloudflare.com/learning/access-management/what-is-a-vpn/

Evotec. (2021, enero 3). Creating Office 365 migration diagram with PowerShell. https://evotec.xyz

FAQforge. (s. f.). How to migrate AD users in a forest using ADMT v3.2. https://faqforge.com

IONOS. (2023, marzo 23). What is Active Directory and how does it work? https://www.ionos.ca/digitalguide/server/know-how/what-is-active-directory/

ISO/IEC. (2022). ISO/IEC 27001:2022 — Information security management systems. https://pentestingteam.com/servicios/auditoria-directorio-activo/

Microsoft. (2021). Troubleshoot Active Directory replication with ADREPLSTATUS. Microsoft Docs. https://learn.microsoft.com/es-es/sql/relational-databases/replication/monitor/monitor-performance-with-replication-monitor?view=sql-server-ver16

Microsoft. (2022). Back up and restore Active Directory in Windows Server. Microsoft Docs. https://www.semperis.com/es/resources/recovering-active-directory-the-missing-piece-in-your-operational-resilience-plan/

Microsoft. (2022). Collect security events from Active Directory and Windows servers. Microsoft Learn. https://learn.microsoft.com/en-us/azure

Microsoft. (2022). Configure replication schedules and site link costs. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/networking/technologies/qos/qos-policy-top

Microsoft. (2022). Protect identities with Microsoft Defender for Identity. Microsoft Docs. https://learn.microsoft.com/en-us/defender-for-identity/

Microsoft. (2023). Active Directory security and replication best practices. Microsoft Learn. https://learn.microsoft.com/es-es/microsoft-365/backup/backup-view-edit-policies?view=o365-worldwide&tabs=sharepoint

Microsoft. (2023). Active Directory replication overview. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/replication/active-directory-replication-concepts

Microsoft. (2023). Knowledge Consistency Checker (KCC) in Active Directory. Microsoft Learn. https://learn.microsoft.com/es-es/previous-versions/windows/it-pro/windows-server-2003/cc755326(v=ws.10)

Microsoft. (2023). Password policies and account lockout policies. Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy

Microsoft Corporation. (2023). Kerberos authentication flow [Imagen]. https://learn.microsoft.com/en-us/windows-server/identity/images/kerberos-flow.png

Microsoft Corporation. (2025). Active Directory Domain Services overview. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Microsoft Corporation. (2025). Understanding the Active Directory logical model. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model

Microsoft Learn. (2024). Set up a test lab for Active Directory migration. https://learn.microsoft.com/es-es/windows/deployment/usmt/usmt-test-your-migration

Microsoft Docs. (2023). Post-migration validation in ADMT. https://learn.microsoft.com/en-us/training/modules/active-directory-domain-services-migration/

NIST. (2019). Role-based access control (RBAC) overview. https://csrc.nist.gov/glossary/term/role_based_access_control

Palo Alto Networks. (s. f.). What is a VPN tunnel? https://www.paloaltonetworks.com/cyberpedia/what-is-a-vpn-tunnel

Top10VPN. (2024). How VPN works: Encrypted tunnel diagram [Imagen]. https://www.top10vpn.com/guides/how-vpns-work/

Varonis. (2022, marzo 3). Active Directory Domain Services (AD DS): Overview and functions. https://www.varonis.com/blog/active-directory-domain-services

Varonis. (2025). Active Directory Migration Tool (ADMT): An essential guide. https://www.varonis.com

Wikipedia. (2025). Active Directory. https://en.wikipedia.org/wiki/Active_Directory