INFORME CONTRATO No. 522-2025

El presente informe detalla la ejecución técnica del contrato 522-2025, donde la DTB continua con la modernización de su infraestructura tecnológica. Los informes se centran en la implementación de un sistema integral de respaldos en la nube mediante Microsoft Azure, garantizando la seguridad y recuperación de datos críticos ante posibles fallos. Además, se documenta la configuración de un Directorio Activo para gestionar usuarios y permisos de manera organizada en diversas áreas administrativas. Las evidencias visuales confirman la correcta creación de copias de seguridad, la validación de procesos de restauración y el cumplimiento de normativas de seguridad de la información. En conjunto, las fuentes demuestran el avance en la continuidad operativa y la protección de los activos digitales de la entidad.

Dentro del contrato se desarrollaron los siguientes componentes:

- Infraestructura Azure: Configuración de máquinas virtuales bajo Windows Server 2019, garantizando el uso de IPs privadas estáticas y almacenamiento SSD para optimizar la latencia transaccional.
- Seguridad Informática: Implementación y endurecimiento del Directorio Activo (AD), configuración de Unidades Organizativas y despliegue de seguridad perimetral avanzada mediante Firewall F5 WAF y Palo Alto virtual.
- Bases de Datos: Optimización y monitoreo de motores PostgreSQL (en arquitectura maestro-réplica) y SQL Server, esenciales para los servicios de la entidad.
- Estrategia de Backups: Aseguramiento de la continuidad de negocio mediante *Azure Recovery Services Vault*.
- Aplicaciones Misionales: Soporte técnico y transferencia de conocimiento en plataformas y Moviliza.

Para mitigar riesgos operativos y garantizar la calidad del servicio, se implementaron los siguientes mecanismos de control:

- Mesas de Trabajo Técnicas y Actas de entrega: Se realizaron sesiones presenciales y virtuales, donde se validaron configuraciones de red, seguridad perimetral y analítica.
- Auditoría de Logs y Eventos: Se constató la veracidad técnica mediante la revisión de reportes de Azure Monitor, verificando el estado de replicación de servidores.
- Compulsa de Evidencias en Sitio: Validación directa de la transferencia de conocimiento y acceso a los repositorios SFTP, asegurando que la DTB posee el control sobre su información.

KM 4 VIA GIRON -TELEFONO: 3174347156
Código Postal: 680005
www.transitobucaramanga.gov.co
Bucaramanga, Departamento de Santander, Colombia

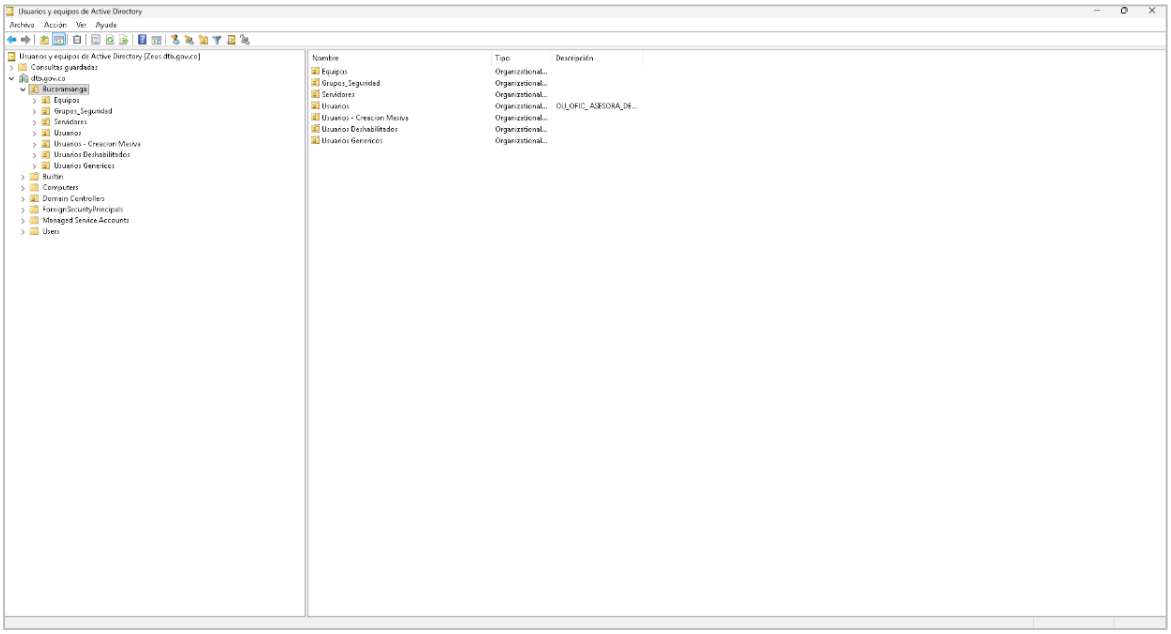
DIRECTORIO ACTIVO:

La configuración de seguridad y roles en el Directorio Activo (AD) de la Dirección de Tránsito de Bucaramanga se basa en una infraestructura centralizada en la nube que busca garantizar la autenticación, administración y control de identidades de forma segura y eficiente. Además, con el directorio activo, se busca centralizar la administración de identidades, fortalecer la seguridad institucional y garantizar la trazabilidad de las operaciones.

A continuación, se detallan los componentes principales de esta configuración:

1. Infraestructura, Roles y Configuración del Directorio Activo:

- Arquitectura en la Nube (Microsoft Azure): Se implementó el servicio de Directorio Activo sobre una infraestructura robusta en Microsoft Azure, garantizando alta disponibilidad, seguridad y escalabilidad para la gestión centralizada de identidades.
- Servidor Dedicado: Se desplegó una máquina virtual denominada “Zeus”, configurada con Windows Server 2019 Datacenter, seleccionada por su estabilidad, rendimiento y soporte extendido para servicios críticos de identidad.
- Red Segura (VNet): El servidor fue integrado en una red virtual (VNet) dentro de una subred exclusiva para AD DS, con dirección IP privada estática y sin exposición a Internet (sin IP pública), asegurando que el acceso se realice únicamente a través de redes internas o autorizadas, fortaleciendo así los controles de seguridad.
- Active Directory Domain Services (AD DS): Se instaló y configuró este rol como componente principal, permitiendo la gestión centralizada de usuarios, equipos, políticas de seguridad y procesos de autenticación dentro del dominio.
- Controlador de Dominio (Domain Controller - DC): La máquina virtual fue promovida como Controlador de Dominio, consolidando la administración de identidades y la aplicación de políticas organizacionales de manera centralizada y segura.
- Servidor DNS Integrado: Se habilitó el servicio de DNS integrado con AD DS, garantizando una correcta resolución de nombres interna, requisito fundamental para el funcionamiento del dominio y los procesos de autenticación.
- Integración y Buenas Prácticas: La implementación conjunta de estos componentes configura una plataforma de identidad segura, controlada y alineada con estándares técnicos, optimizando la operación de los servicios institucionales y reduciendo riesgos de acceso no autorizado.



Estructura del DA (conexión realizada Herramientas de Administración Remota del Servidor RSAT)

2. Estructura Lógica y Roles Administrativos:

La administración se organiza a través de una estructura lógica que permite delegar permisos ajustados a las responsabilidades de cada área:

- Unidades Organizativas (OU): Se crearon OUs para organizar y/o clasificar usuarios, equipos, grupos y servicios de manera estructurada (ej. OU_FINANCIERA, OU_TALENTO_HUMANO, OU_SISTEMAS, etc.). Esto permite aplicar políticas de seguridad de forma segmentada.
- Grupos de Seguridad: Se utilizan para asignar permisos de acceso y roles operativos de manera centralizada.
- Modelo de Mínimo Privilegio: Se definieron grupos de seguridad y cuentas de usuario con permisos ajustados estrictamente a sus responsabilidades funcionales.
- Integración con Aplicativos: El Directorio Activo sirve como el corazón de la autenticación para otras plataformas, utilizando protocolos como LDAP/LDAPS para la validación de credenciales.

En el directorio activo se ha implementado una estructura jerárquica de Unidades Organizativas (OU) diseñada para organizar usuarios, equipos, grupos y servicios de la Dirección de Tránsito de Bucaramanga de manera segmentada.

Las unidades organizativas creadas son:

A. Estructura Principal de la Entidad

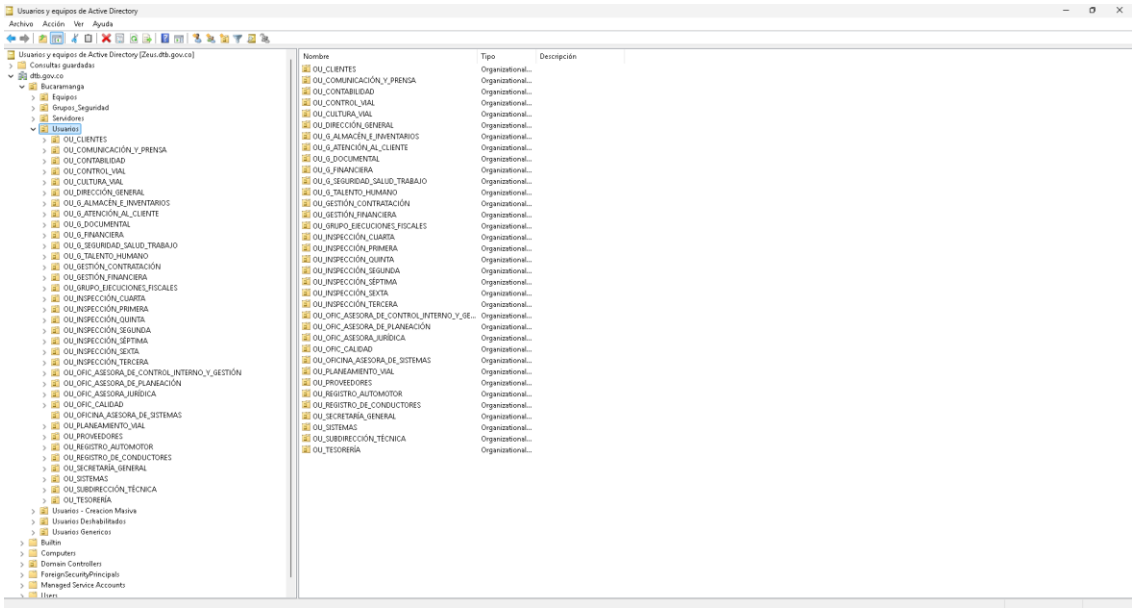
Bajo el nodo principal de la entidad se encuentran las carpetas base de administración:

- Equipos: Para la gestión de estaciones de trabajo y dispositivos.
- Grupos_Seguridad: Donde se centralizan los grupos para asignación de permisos.
- Servidores: Para la organización de la infraestructura de servidores en el dominio.
- Usuarios: Contenedor principal que alberga las sub-unidades por dependencias.

B. Unidades Organizativas por Dependencia (Dentro de "Usuarios")

Se han creado Ous específicas para cada área funcional de la entidad, permitiendo aplicar políticas de grupo (GPO) diferenciadas y delegación administrativa:

- Administrativas y de Gestión:
  - OU_G_ADMINISTRATIVA
  - OU_G_ALENTO_HUMANO
  - OU_G_ALMACÉN_E_INVENTARIOS
  - OU_G_DOCUMENTAL
  - OU_G_FINANCIERA / OU_GESTIÓN_FINANCIERA
  - OU_G_TALENTO_HUMANO
  - OU_GESTIÓN_CONTRATACIÓN
  - OU_SECRETARÍA_GENERAL
  - OU_TESORERÍA
- Oficinas Asesoras y Control:
  - OU_OFIC_ASESORA_DE_CONTROL_INTERNO_Y_GESTIÓN
  - OU_OFIC_ASESORA_DE_PLANEACIÓN
  - OU_OFIC_ASESORA_JURÍDICA
  - OU_OFIC_CALIDAD
  - OU_OFICINA_ASESORA_DE_SISTEMAS
- Operativas y Misionales:
  - OU_CONTROL_VIAL / OU_PLANEAMIENTO_VIAL
  - OU_CULTURA_VIAL
  - OU_DIRECCIÓN_GENERAL
  - OU_REGISTRO_AUTOMOTOR
  - OU_REGISTRO_DE_CONDUCTORES
  - OU_SUBDIRECCIÓN_TÉCNICA
- Inspecciones de Tránsito:
  - Ous individuales para cada inspección: PRIMERA, SEGUNDA, TERCERA, CUARTA, QUINTA, SEXTA y SÉPTIMA.
- Otras Unidades de Servicio:
  - OU_CLIENTES / OU_G_ATENCIÓN_AL_CLIENTE
  - OU_COMUNICACIÓN_Y_PRENSA
  - OU_CONTABILIDAD
  - OU_G_SEGURIDAD_SALUD_TRABAJO
  - OU_GRUPO_EJECUCIONES_FISCALES
  - OU_PROVEEDORES
  - OU_SISTEMAS



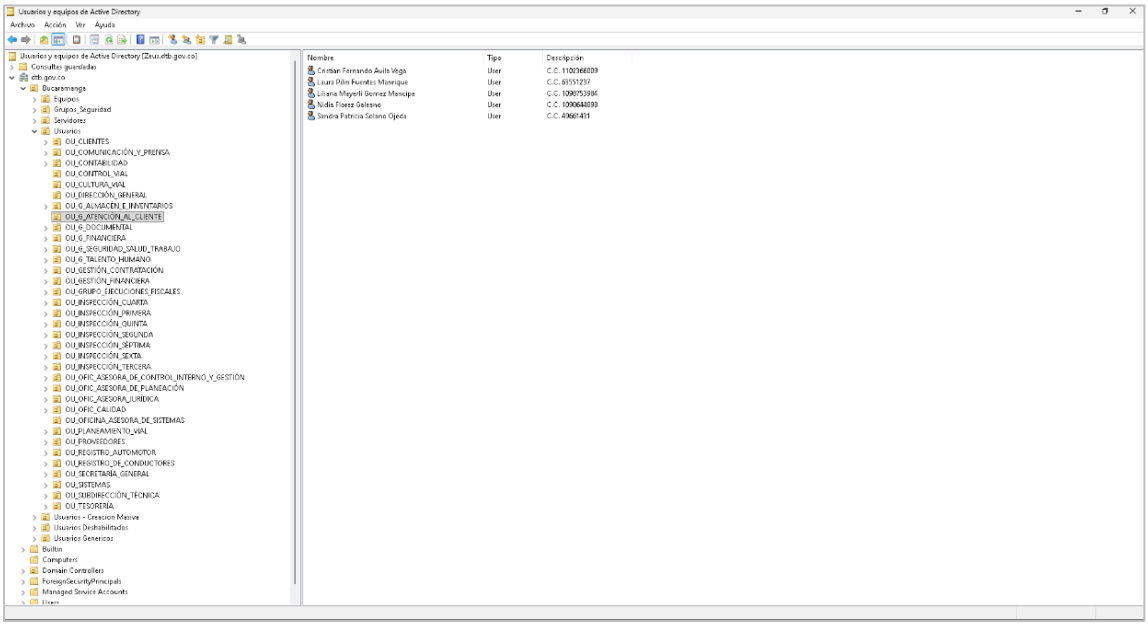
Unidades organizativas

C. Carpetas de Gestión de Cuentas

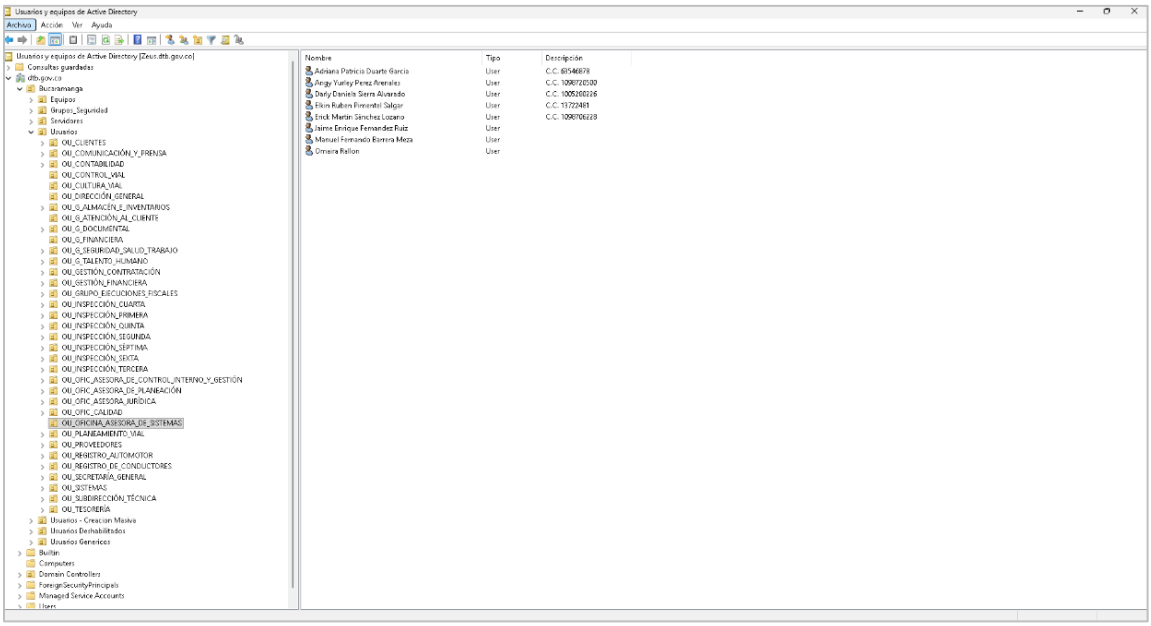
Adicionalmente, se configuraron contenedores para el manejo del ciclo de vida de las identidades:

- Usuarios – Creacion Masiva: Para procesos de carga masiva de personal.
- Usuarios Deshabilitados: Donde se reubican las cuentas inactivas para mantener el orden y la seguridad.
- Usuarios Genericos: Para cuentas de servicios o funciones compartidas específicas.

Esta organización permite que las áreas técnicas y operativas cuenten con permisos ajustados estrictamente a sus responsabilidades, siguiendo el modelo de mínimo privilegio.



Usuarios en OU_ATENCION_CLIENTE



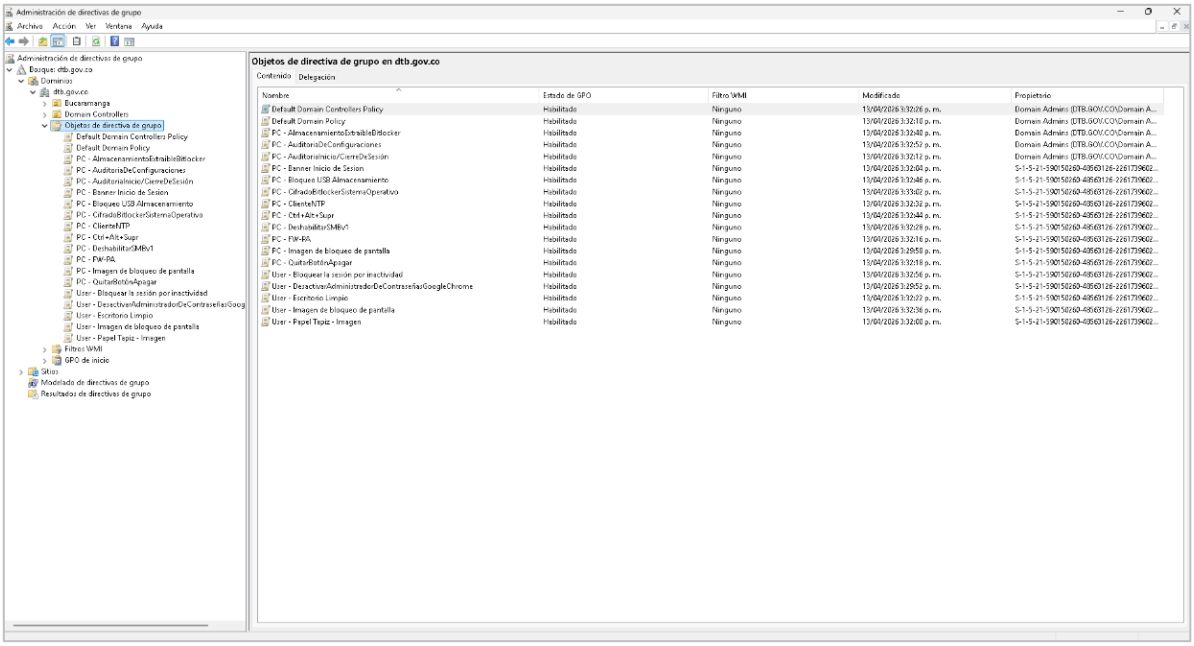
Usuarios en OU_SISTEMAS

3. Políticas de Grupo (GPO) para Seguridad

Las GPO son el mecanismo central para aplicar controles de seguridad y restricciones administrativas en todo el dominio. Las principales políticas configuradas incluyen:

- Políticas de Contraseñas y Bloqueo: Se exigen contraseñas robustas (mínimo 10-14 caracteres, con complejidad y registro de historial) y se establece el bloqueo de cuentas tras 5 intentos fallidos por un periodo de 30 minutos.
- Auditoría Avanzada: Se registran eventos de inicio y cierre de sesión, cambios en el AD y accesos a archivos (tanto éxitos como fallos) para garantizar la trazabilidad de las acciones de los usuarios.
- Protección de Datos y Dispositivos: Se implementa el cifrado de discos del sistema operativo y de dispositivos extraíbles mediante BitLocker.
- Restricciones de Hardware y Software: Se configuraron políticas para bloquear el uso de dispositivos USB extraíbles y deshabilitar protocolos inseguros.
- Seguridad del Sistema: Incluye la deshabilitación de protocolos antiguos e inseguros y la configuración de banners de advertencia legal al iniciar sesión.

Las políticas de contraseñas y bloqueo de cuentas están configuradas principalmente a través de Objetos de Directiva de Grupo (GPO) en Active Directory, con especificaciones distintas según el alcance de la directiva.



Evidencias de políticas creadas

A continuación, se detallan las configuraciones establecidas:

3.1. Política para Controladores de Dominio (Default Domain Controllers Policy)
Esta política define los parámetros de seguridad más estrictos aplicados específicamente a los Controladores de Dominio:

- Configuración de Contraseñas:
  - Longitud mínima: 14 caracteres.
  - Complejidad: Debe cumplir con los requerimientos de complejidad (letras, números y símbolos).
  - Historial: Se recuerdan las últimas 24 contraseñas para evitar su reutilización inmediata.
  - Vigencia máxima: La contraseña caduca cada 30 días.
  - Vigencia mínima: 1 día.
- Bloqueo de Cuentas:
  - Umbral de bloqueo: La cuenta se bloquea tras 5 intentos fallidos de inicio de sesión.
  - Duración del bloqueo: 30 minutos.
  - Reinicio del contador: El contador de intentos fallidos se resetea después de 30 minutos.

Si un usuario olvida su contraseña o su cuenta queda bloqueada, el procedimiento a seguir es el siguiente:

- En caso de que la contraseña esté bloqueada o el usuario no pueda ingresar, se debe crear un caso solicitando el desbloqueo de la cuenta. La interfaz de inicio de sesión también muestra una opción de “¿Olvidó su contraseña?” para iniciar procesos de recuperación.
- Bloqueo automático por intentos fallidos: Si el usuario intenta ingresar una contraseña incorrecta repetidamente (olvido), las políticas de Active Directory establecen que la cuenta se bloqueará automáticamente tras 5 intentos fallidos.
- Duración del bloqueo: Una vez bloqueada por intentos fallidos, la cuenta permanecerá en ese estado durante 30 minutos antes de permitir un nuevo intento, a menos que un administrador realice el desbloqueo manual.
- Soporte Técnico: Las solicitudes de acceso o cambios menores son categorizadas con una prioridad baja (P4) dentro de la matriz de la Mesa de Servicio. El Nivel 1 (Mesa de Servicio) es el encargado de registrar y categorizar estos incidentes para su pronta solución.
- Primer inicio de sesión: Es importante recordar que, cuando se crea un usuario nuevo o se restablece una contraseña administrativamente, el sistema está configurado para obligar al usuario a cambiar la contraseña en el siguiente inicio de sesión por motivos de seguridad.

3.2. Política de Dominio General (Default Domain Policy)

Aplica restricciones generales a todos los equipos y usuarios integrados al dominio:

- Configuración de Contraseñas: Exige un mínimo de 10 caracteres, mantiene la complejidad activa, el historial de 24 contraseñas y la caducidad cada 30 días.
- Bloqueo de Cuentas: Mantiene el bloqueo tras 5 intentos fallidos durante un periodo de 30 minutos.

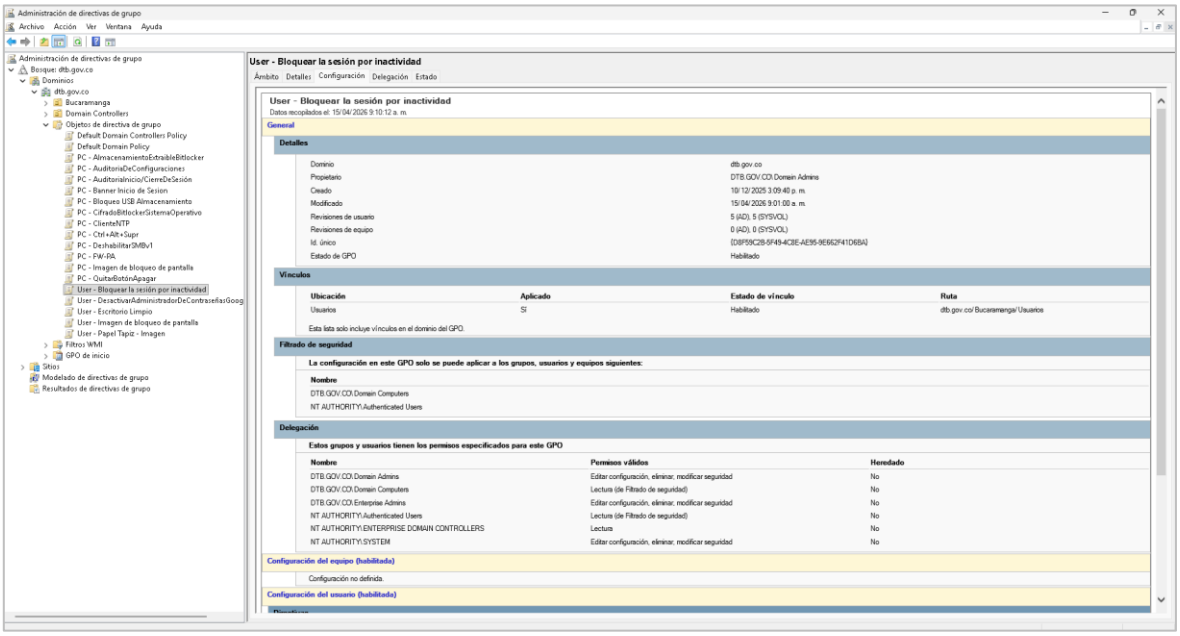
El bloqueo por inactividad de cinco minutos funciona a través de una Política de Grupo (GPO) específica denominada “User – Bloquear la sesión por inactividad”, configurada en el Directorio Activo.

- Mecanismo de activación: La política activa el protector de pantalla del sistema operativo.
- Tiempo de espera: Está configurada con un tiempo de espera de 300 segundos, lo que equivale exactamente a 5 minutos de inactividad total por parte del usuario.
- Requisito de desbloqueo: Una vez transcurrido este tiempo, el protector de pantalla se inicia y queda protegido por contraseña. Esto significa que, para retomar el trabajo en el equipo, el usuario debe ingresar nuevamente sus credenciales.
- Objetivo de seguridad: Esta configuración busca aumentar la seguridad física de las estaciones de trabajo, asegurando que si un equipo se deja desatendido, se bloquee automáticamente para evitar el acceso de personas no autorizadas.

Esta directiva se complementa con otras políticas de usuario, como la que prohíbe a los usuarios cambiar el protector de pantalla o el fondo de escritorio, garantizando que el bloqueo sea consistente en toda la organización.

3.3. Otras Políticas de Seguridad Relacionadas

- Gestión de Credenciales: Se desactiva explícitamente el administrador de contraseñas en Google Chrome mediante GPO para evitar que el navegador guarde credenciales corporativas automáticamente.



Detalle de la política: Bloquear sesión por inactividad

4. Seguridad de Red y Acceso Externo

El acceso al Directorio Activo está protegido por múltiples capas de red:

- VPN y Firewall: Las comunicaciones se realizan exclusivamente a través de túneles VPN cifrados gestionados por un firewall Palo Alto, evitando la exposición pública del servidor.
- Protocolos Seguros: Se utiliza LDAPS (LDAP sobre SSL/TLS) para cifrar las comunicaciones de autenticación entre el AD y otros componentes de la infraestructura, protegiendo credenciales y datos sensibles.
- IP Estática: El controlador de dominio posee una dirección IP privada estática dentro de su subred dedicada en Azure para asegurar una identidad de red consistente y estabilidad en los servicios.

5. Mecanismos de Respaldo y Recuperación

Para asegurar la continuidad operativa frente a incidentes, se configuran respaldos periódicos mediante Azure Backup:

- Backup del Estado del Sistema: Es fundamental para los controladores de dominio, ya que resguarda los metadatos de Active Directory, el registro de Windows y los objetos de seguridad esenciales para la restauración del servicio.
- Respaldo de la VM: Se realizan copias periódicas de toda la máquina virtual para asegurar una recuperación rápida ante fallas operativas o desastres.

HERRAMIENTAS DEL DIRECTORIO ACTIVO:

El personal técnico y de infraestructura utiliza un conjunto de herramientas especializadas, tanto locales como en la nube, para la gestión integral del Directorio Activo de la entidad.

Las principales herramientas son las siguientes:

1.Herramientas de Gestión Remota y Servidor

- RSAT (Herramientas de Administración Remota del Servidor): Es la herramienta principal utilizada para realizar la conexión y administración remota de la estructura del Directorio Activo desde estaciones de trabajo autorizadas.
- Server Manager (Administrador del Servidor): Se utiliza directamente en el servidor “Zeus” para gestionar los roles de AD DS y DNS, monitorear el estado operativo de los servicios y acceder a las consolas de configuración.
- PowerShell: Se emplea como alternativa técnica para la ejecución de comandos, automatización de tareas y la instalación de roles y características del sistema.

2. Consolas de Administración Específicas

Dentro del entorno de Windows Server, se utilizan consolas dedicadas para tareas puntuales:

- Usuarios y Equipos de Active Directory (Active Directory Users and Computers): Es la consola central para la creación, modificación y organización de Unidades Organizativas (OU), cuentas de usuario, grupos de seguridad y equipos.
- Administración de Directivas de Grupo (Group Policy Management): Herramientas utilizada para crear, editar y vincular los objetos de política (GPO) que aplican las restricciones de seguridad y configuraciones en todo el dominio.

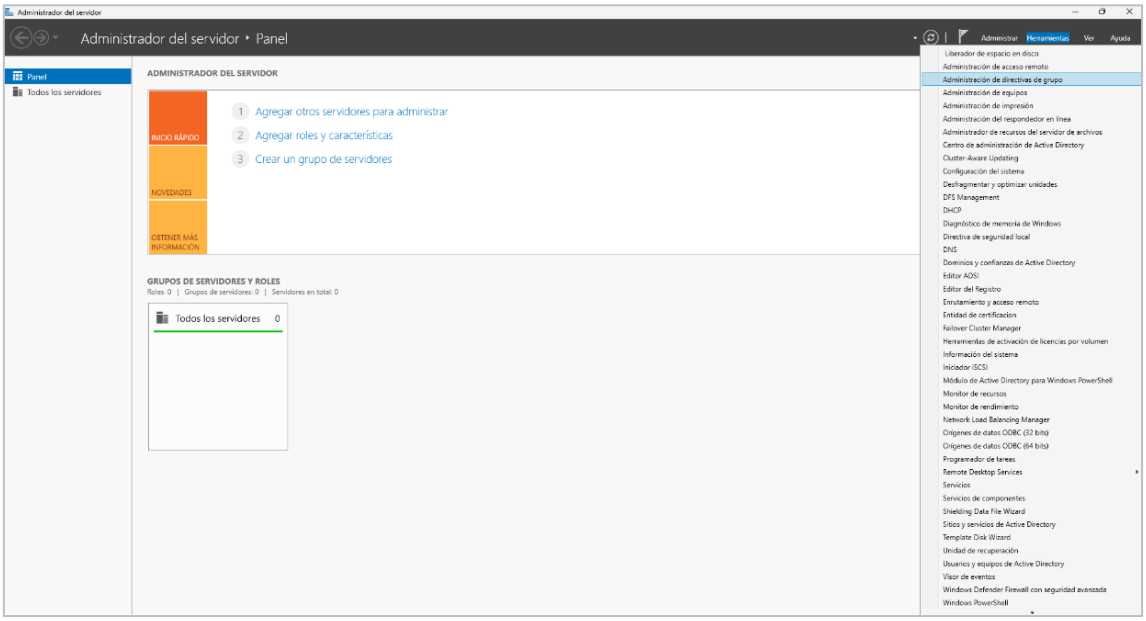
3. Herramientas de Infraestructura y Seguridad en la Nube

- Portal de Microsoft Azure: Se utiliza para la administración de la infraestructura subyacente, incluyendo la gestión de la Vnet (Red Virtual), subredes, direcciones IP estáticas y la propia máquina virtual Zeus.
- Azure Active Directory (RBAC): Se emplea para el control de acceso basado en roles, permitiendo gestionar quién puede realizar acciones críticas como restauraciones en el *Recovery Services Vault* o administrar recursos en el entorno de nube.
- Azure Backup / Recovery Services Vault: Herramientas para la configuración, monitoreo y validación de los respaldos del estado del sistema y de la máquina virtual del controlador de dominio.

KM 4 VIA GIRON -TELEFONO: 3174347156
Código Postal: 680005
www.transitobucaramanga.gov.co
Bucaramanga, Departamento de Santander, Colombia

4. Herramientas de Integración y Soporte

- Consola de Administración de Firewall Palo Alto: Utilizada para la integración de AD con la red mediante perfiles de servidor LDAP/LDAPS, permitiendo que las identidades del directorio se usen para políticas de seguridad de red y autenticación VPN.



Ingreso al servidor del Directorio Activo para configuración

PROTOCOLOS DE SEGURIDAD DESHABILITADOS:

Como parte del fortalecimiento de la infraestructura tecnológica, se han deshabilitado protocolos de red antiguos o inseguros para reducir la superficie de ataque y prevenir vulnerabilidades conocidas.

Los protocolos específicamente deshabilitados o restringidos son:

- SMBv1 (Server Message Block versión 1): Se ha implementado una política de grupo (GPO) denominada "PC - DeshabilitarSMBv1" que desactiva este protocolo en el servidor. El objetivo es mitigar riesgos asociados a este protocolo antiguo de compartición de archivos, el cual es propenso a diversas vulnerabilidades de seguridad.
- Acceso Público a Bases de Datos: En la configuración de Azure SQL Database, se ha deshabilitado explícitamente el acceso desde la red pública. Esto impide conexiones directas desde Internet, obligando a que el tráfico se mantenga dentro de redes internas controladas o vía VPN.
- HTTP no cifrado: En las aplicaciones web, se ha configurado el servidor para forzar el uso exclusivo de HTTPS como único canal de comunicación, lo que en la práctica deshabilita o restringe el uso del protocolo HTTP convencional para garantizar la confidencialidad de la información.
- LDAP (No seguro): Aunque no se prohíbe explícitamente el protocolo base, la arquitectura prioriza y recomienda el uso de LDAPS (LDAP sobre SSL/TLS) para las comunicaciones de autenticación entre el Directorio Activo y otros componentes como el firewall Palo Alto, asegurando que las credenciales viajen de forma cifrada.

Estas medidas se complementan con reglas de firewall estrictas que aplican un cierre global de todo el tráfico no permitido (Block-All) por defecto.

CUENTAS DE USUARIOS DESHABILITADOS:

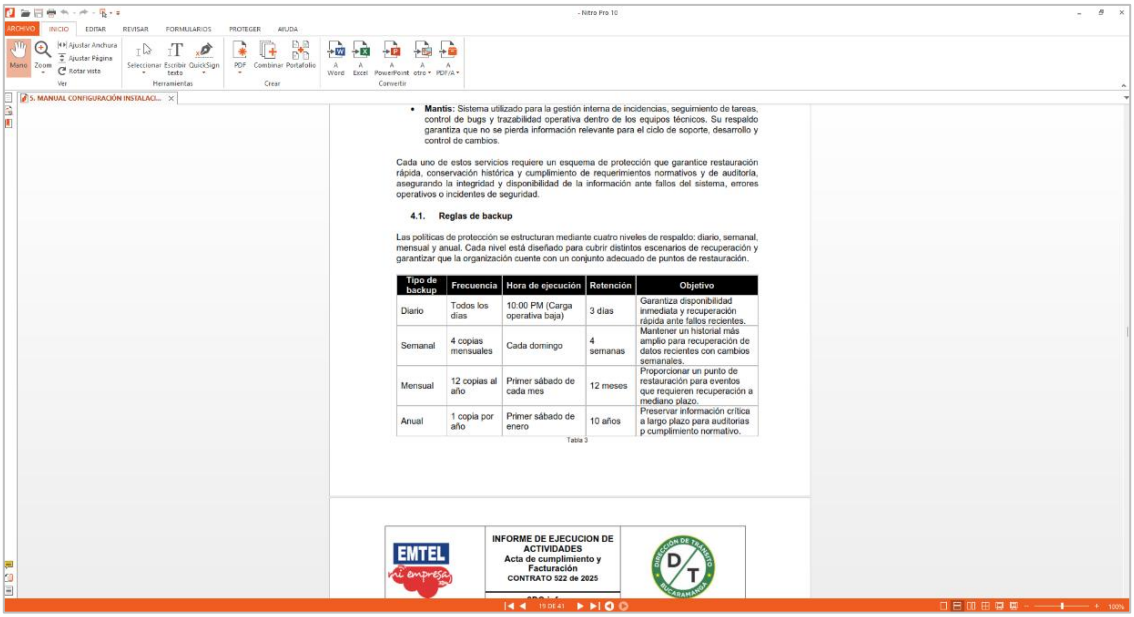
La gestión de las cuentas de usuarios deshabilitados en el Directorio Activo de la entidad se realiza de manera organizada y centralizada mediante el uso de contenedores específicos dentro de la estructura lógica del dominio, el proceso se basa en los siguientes puntos:

- Unidad Organizativa Dedicada: Se ha creado una Unidad Organizativa (OU) específica denominada "Usuarios Deshabilitados". Esta carpeta se encuentra al mismo nivel jerárquico que el contenedor principal de "Usuarios" y otras dependencias, lo que facilita su identificación inmediata por parte de los administradores.
- Control y Orden del Dominio: La reubicación de cuentas inactivas en este contenedor permite mantener un control ordenado del dominio. Al segregar estas cuentas de las OUs operativas (como las de proveedores, sistemas o dependencias

administrativas), se reduce el ruido administrativo y se mejora la visibilidad sobre el personal que actualmente tiene acceso activo.

- Seguridad y Aplicación de Políticas: Esta organización segmentada permite asegurar que las cuentas que ya no deben tener acceso a los recursos institucionales no se vean afectadas accidentalmente por Políticas de Grupo (GPO) destinadas a usuarios activos, reforzando así la seguridad perimetral y el modelo de mínimo privilegio.
- Trazabilidad: Al mantener las cuentas en este repositorio en lugar de eliminarlas inmediatamente, se preserva la trazabilidad histórica de las acciones realizadas por ese usuario en el pasado, lo cual es fundamental para procesos de auditoría y cumplimiento normativo.

En resumen, la gestión consiste en el traslado administrativo y técnico de las cuentas que pierden su vigencia hacia este repositorio seguro y controlado, garantizando que el entorno de identidades permanezca limpio y protegido contra accesos no autorizados de cuentas huérfanas.



- **Mantis**: Sistema utilizado para la gestión interna de incidencias, seguimiento de tareas, control de bugs y trazabilidad operativa dentro de los equipos técnicos. Su respaldo garantiza que no se pierda información relevante para el ciclo de soporte, desarrollo y control de cambios.

Cada uno de estos servicios requiere un esquema de protección que garantice restauración rápida, conservación histórica y cumplimiento de requerimientos normativos y de auditoría, asegurando la integridad y disponibilidad de la información ante fallos del sistema, errores operativos o incidentes de seguridad.

4.1. Reglas de backup

Las políticas de protección se estructuran mediante cuatro niveles de respaldo: diario, semanal, mensual y anual. Cada nivel está diseñado para cubrir distintos escenarios de recuperación y garantizar que la organización cuente con un conjunto adecuado de puntos de restauración.

Tipo de backup	Frecuencia	Hora de ejecución	Retención	Objetivo
Diario	Todos los días	10:00 PM (Carga operativa baja)	3 días	Garantiza disponibilidad inmediata y recuperación rápida ante fallos recientes.
Semanal	4 copias mensuales	Cada domingo	4 semanas	Mantener un historial más amplio para recuperación de datos recientes con cambios semanales.
Mensual	12 copias al año	Primer sábado de cada mes	12 meses	Proporcionar un punto de restauración para eventos que requieren recuperación a mediano plazo.
Anual	1 copia por año	Primer sábado de enero	10 años	Preservar información crítica a largo plazo para auditorias p cumplimiento normativo.

Tabla 3

EMTEL mi empresa

INFORME DE EJECUCION DE ACTIVIDADES
Acta de cumplimiento y Facturación
CONTRATO 322 de 2025

Políticas de respaldos del proveedor

KM 4 VIA GIRON -TELEFONO: 3174347156
Código Postal: 680005
www.transitobucaramanga.gov.co
Bucaramanga, Departamento de Santander, Colombia

COPIAS DE SEGURIDAD:

El respaldo del estado del sistema en Azure es un componente fundamental de la estrategia de continuidad para servidores críticos, específicamente para aquellos que funcionan como Controladores de Dominio (Active Directory).

1. Elementos que componen el respaldo

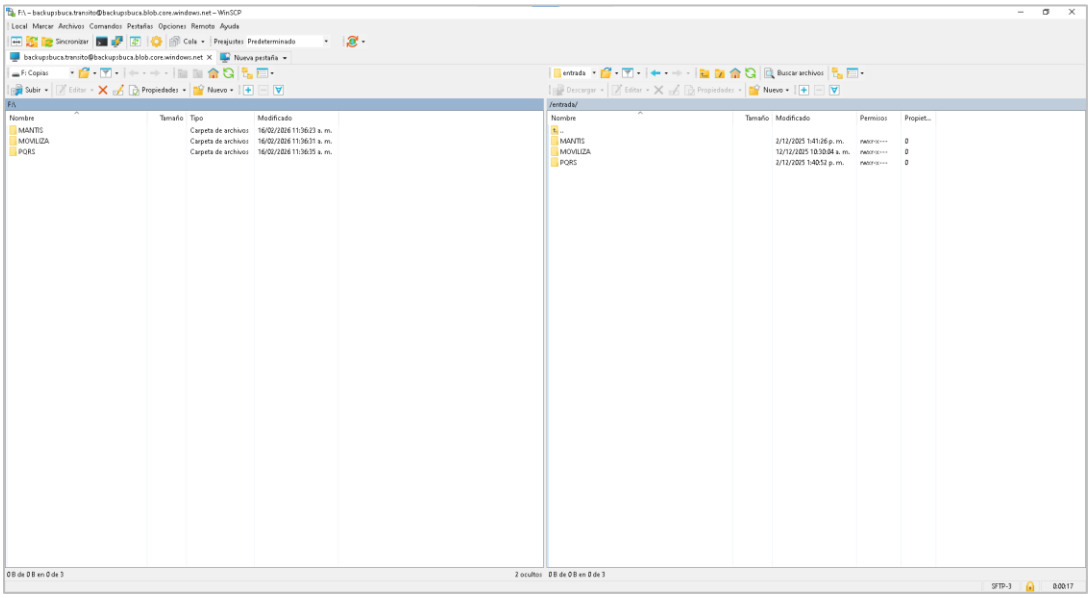
A diferencia de un respaldo de archivos común, el respaldo del estado del sistema resguarda los metadatos y configuraciones vitales para que el Directorio Activo pueda ser restaurado íntegramente. Esto incluye:

- Base de datos de Active Directory: El núcleo de las identidades y permisos.
- Registro de Windows: Configuraciones del sistema operativo.
- Archivos de arranque: Necesarios para la inicialización del servidor.
- Componentes esenciales de seguridad: Objetos y metadatos necesarios para la restauración del dominio.

2. Infraestructura y Tecnología utilizada

- Azure Backup y Recovery Services Vault: El respaldo se gestiona de forma centralizada a través de una bóveda o almacén de servicios de recuperación (Vault), que actúa como el repositorio seguro para los puntos de restauración.
- Consistencia vía VSS: Para servidores Windows, Azure Backup utiliza el servicio de instantáneas de volumen (VSS - Volume Shadow Copy Service). Esto permite capturar una copia consistente a nivel de sistema operativo y aplicación sin interrumpir el funcionamiento del servidor.
- Almacenamiento Incremental: El proceso captura instantáneas que solo guardan los cambios realizados desde el último respaldo, lo que optimiza el espacio y acelera la transferencia de datos a la nube.

KM 4 VIA GIRON -TELEFONO: 3174347156
Código Postal: 680005
www.transitobucaramanga.gov.co
Bucaramanga, Departamento de Santander, Colombia



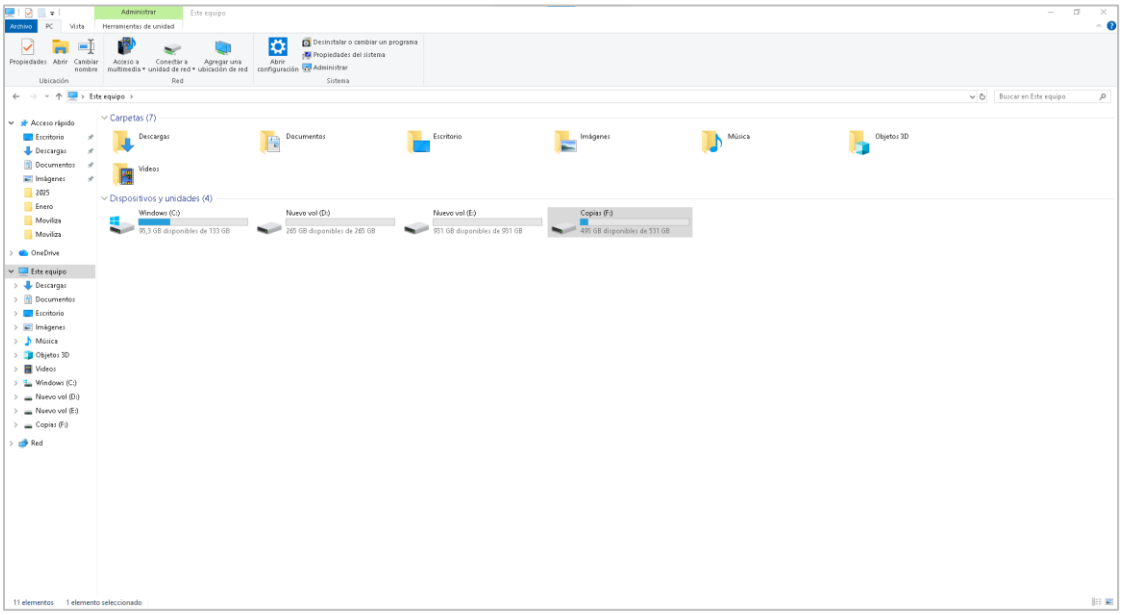
Sistema de archivos del ordenador local (izquierda) y el servidor remoto (derecha).

3. Operación y Gestión

- Automatización: Se configuran políticas periódicas (diarias, semanales, mensuales y anuales) para que el respaldo se ejecute automáticamente sin intervención manual.
- Redundancia Geográfica (GRS): Los datos del estado del sistema se replican automáticamente en un segundo centro de datos en una región distinta para garantizar la recuperación incluso ante un desastre regional total.
- Verificación: El estado de estos respaldos se supervisa desde el portal de Azure, donde se puede acceder a la sección "Elementos de respaldo" (Backup Items) para validar que los puntos de recuperación se estén generando correctamente.

4. Objetivo del respaldo

Este mecanismo permite que, ante fallas lógicas, incidentes de seguridad o corrupción de datos, el entorno de autenticación de la entidad pueda recuperarse rápidamente, minimizando las interrupciones en el acceso corporativo y preservando la integridad del dominio.



Discos duros del servidor de copia local

5. Frecuencia y Esquema de Retención

El sistema opera bajo un modelo de niveles escalonados que permite recuperaciones tanto inmediatas como históricas:

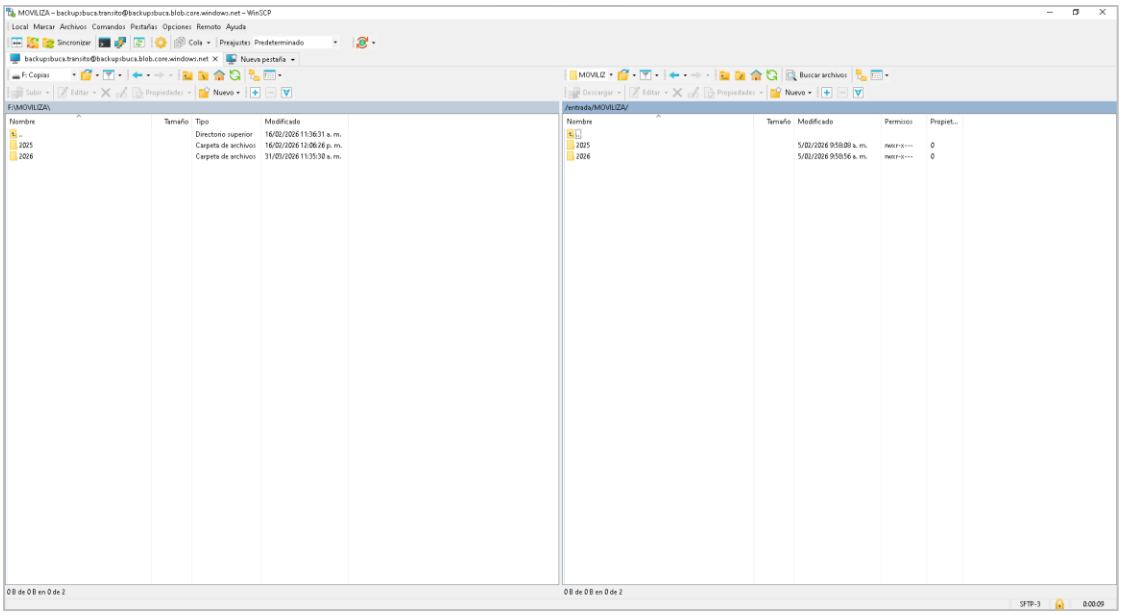
- Copias Diarias: Se ejecutan todos los días a las 8:00 PM o 10:00 PM (en horarios de baja carga). Tienen un objetivo de disponibilidad inmediata y una retención que varía según el recurso (de 3 a 30 días).
- Copias Semanales: Se realizan cada domingo a las 10:00 PM y se conservan durante 4 semanas.
- Copias Mensuales: Se ejecutan el primer sábado de cada mes a las 10:00 PM y se retienen por 12 meses.
- Copias Anuales: Se realizan el primer sábado de enero y se conservan por 10 años para cumplimiento normativo y auditorías.

Para el caso específico de las bases de datos PostgreSQL, existe una programación adicional que ejecuta un script de respaldo de estructura y datos a las 02:30 AM.

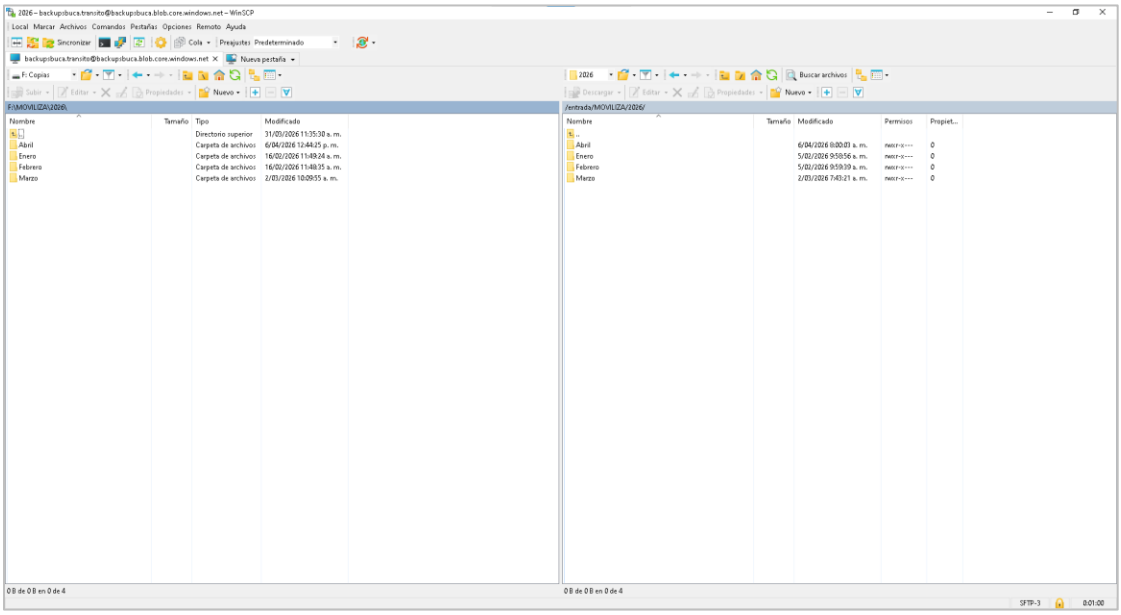
Las políticas de protección se estructuran en cuatro niveles escalonados:

Tipo de Backup	Frecuencia	Hora de Ejecución	Retención	Objetivo
Diario	Todos los días	10:00 PM	3 días*	Recuperación rápida ante fallos recientes.
Semanal	Cada domingo	10:00 PM	4 semanas	Historial para situaciones no detectadas de inmediato.
Mensual	1er sábado/mes	10:00 PM	12 meses	Auditoría técnica/financiera y análisis histórico.
Anual	1er sábado/enero	10:00 PM	10 años	Cumplimiento normativo y legal a largo plazo.

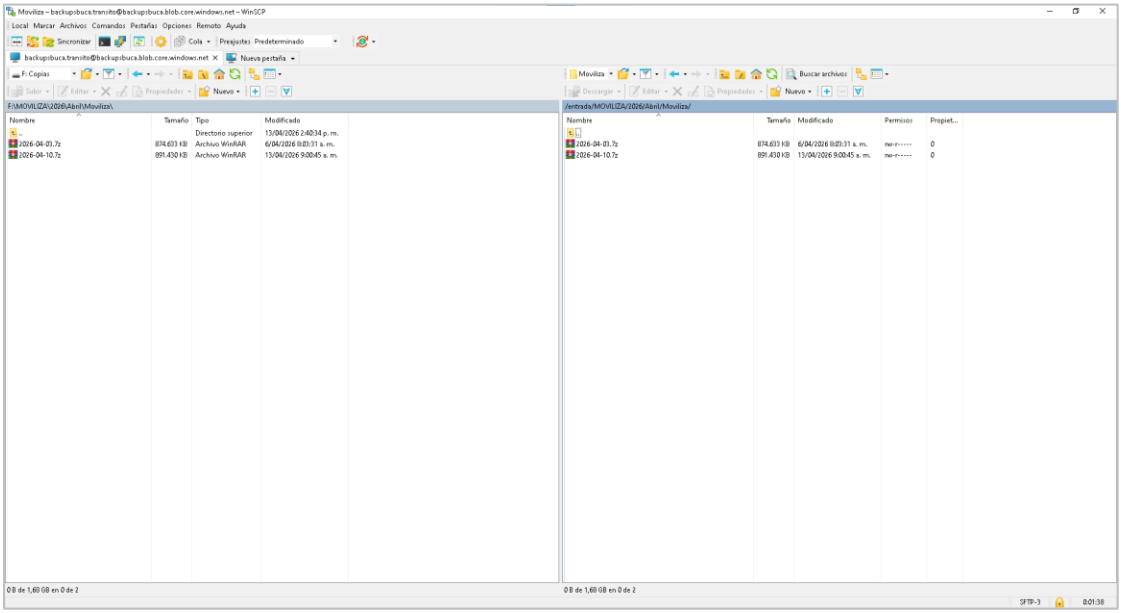
**Nota: La retención operativa diaria puede ser de hasta 30 días para ciertos recursos.*



Carpetas anuales de las copias



Carpetas mensuales de las copias

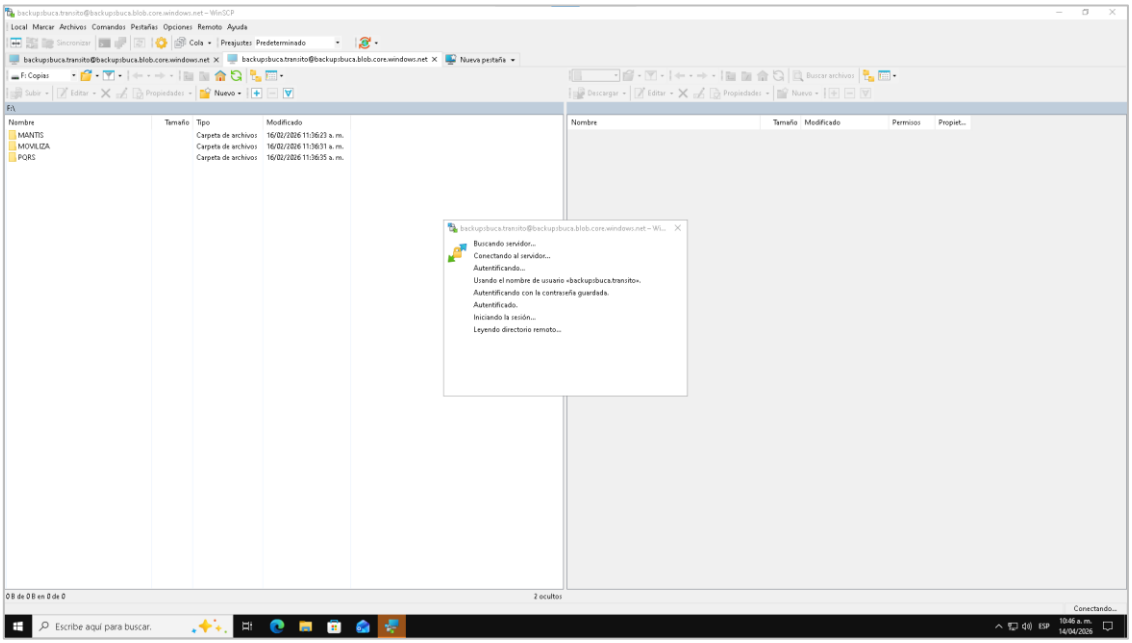


Archivos de las copias

6. Cómo se accede a las copias

El acceso está restringido y se realiza a través de dos mecanismos principales:

- Portal de Azure (Administración): El personal técnico accede al recurso Recovery Services Vault. Dentro de la sección "Elementos de respaldo" (Backup Items), se pueden visualizar los puntos de restauración por máquina virtual o base de datos.
- Acceso vía SFTP (Repositorio Complementario): Se ha configurado un contenedor en Azure Storage con soporte SFTP. Los administradores utilizan la herramienta WinSCP con credenciales generadas (URL, usuario y contraseña SSH) para descargar o auditar los archivos de respaldo directamente.



Conexión con WinSCP al repositorio de copias del proveedor

7. Tamaño y Almacenamiento

- Capacidad de Base de Datos: La base de datos SQL (PQRS) tiene un tamaño máximo configurado de 250 GB.
- Discos de Servidores: El servidor de Directorio Activo (Zeus) cuenta con un disco de sistema de 128 GB (SSD Premium).
- Optimización: El sistema utiliza respaldos incrementales, lo que significa que solo se guardan los cambios realizados desde la última copia, reduciendo el tráfico de red y el espacio ocupado.

8. Recursos Protegidos

Las copias de seguridad cubren los componentes más críticos de la entidad:

- Active Directory (Zeus): Incluye el respaldo del "Estado del Sistema" (base de datos de AD, registro y archivos de arranque).
- Bases de Datos: SQL Server (PQRS/Analítica) y PostgreSQL (Mantis/Orfeo).
- Aplicativos: Servidores web y de aplicaciones.
- Configuraciones de Red: Respaldos de reglas y políticas del Firewall Palo Alto y Balanceador F5.

9. Seguridad y Confiabilidad

- Cifrado: La información se cifra tanto en tránsito (TLS) como en reposo utilizando claves administradas por la plataforma.
- Pruebas de Restauración: Se realizan validaciones periódicas (semestrales o mensuales para DBs) donde se montan los discos de respaldo para verificar la integridad de los datos y asegurar que el tiempo de recuperación cumpla con los objetivos institucionales.
- Alertas: El sistema está integrado con Azure Monitor, enviando notificaciones automáticas por correo electrónico ante cualquier falla o advertencia en los trabajos de respaldo.

KM 4 VIA GIRON -TELEFONO: 3174347156
Código Postal: 680005
www.transitobucaramanga.gov.co
Bucaramanga, Departamento de Santander, Colombia

CONCLUSIONES

- Modernización Tecnológica: Se continua con la modernización de la infraestructura tecnológica de la Dirección de Tránsito de Bucaramanga (DTB) mediante la implementación de soluciones avanzadas en la nube.

- Garantía de Continuidad del Negocio: Se estableció un sistema integral de respaldos en Microsoft Azure que asegura la recuperación de datos críticos ante fallos, incluyendo una estrategia de retención escalonada que cumple con la normativa legal a largo plazo (hasta 10 años).

- Fortalecimiento Robusto de la Seguridad: La implementación del Directorio Activo (AD) centralizado en la nube ha permitido un control estricto de identidades, reduciendo significativamente los riesgos de acceso no autorizado.

- Mitigación de Vulnerabilidades y Riesgos: Se logró una reducción efectiva de la superficie de ataque mediante la deshabilitación de protocolos obsoletos e inseguros y el bloqueo del acceso público a bases de datos, priorizando canales cifrados como VPN, LDAPS y HTTPS.

- Optimización de Activos Digitales: La configuración de servidores bajo Windows Server 2019 con almacenamiento SSD y redes privadas garantiza una baja latencia transaccional y una alta disponibilidad de los servicios institucionales.

- Trazabilidad y Control Operativo: Mediante herramientas como Azure Monitor y la auditoría avanzada de logs, la entidad cuenta ahora con una capacidad de supervisión permanente y total sobre los cambios e intentos de acceso en su infraestructura crítica.

- Resiliencia Institucional: La ejecución técnica del contrato actúa como una respuesta directa y efectiva para fortalecer la seguridad de la información, mitigando vulnerabilidades y asegurando la protección de los activos digitales de la entidad frente a futuros incidentes.

- Transferencia de Conocimiento y Control: Se validó la transferencia técnica de conocimiento y el acceso a repositorios seguros, garantizando que la DTB posee el control sobre su información y plataformas misionales.

KM 4 VIA GIRON -TELEFONO: 3174347156
Código Postal: 680005
www.transitobucaramanga.gov.co
Bucaramanga, Departamento de Santander, Colombia

ANEXOS

1. Informes y manuales técnicos.
2. Actas de reuniones y entregas.
3. Capturas de pantalla.

Cordialmente,



MIGUEL ALEXANDER PORTILLA VILLAMIZAR
Asesor Oficina de Sistemas