# *Informe Técnico de Configuración de Servidor y Seguridad en Red*

## *Fase 1: Configuración de IP Estática y Verificación de Conectividad*

Objetivo:
Asignar una IP estática al servidor y verificar la conectividad hacia el exterior.

Pasos realizados:
- Se asignó manualmente una IP estática al servidor.
- Se ejecutaron pruebas de conectividad usando los comandos:
- ping hacia google.com.
- tracert para verificar la ruta de los paquetes (resultado: 8 saltos).
- Verificación satisfactoria de conexión a internet desde el servidor.

## *Fase 2: Creación de Usuarios, Grupos y Permisos*

Objetivo:
Establecer una jerarquía de permisos en función de distintos perfiles de usuario.

Pasos realizados:
- Creación de tres usuarios a través de:
Herramientas > Administración de equipos > Usuarios y grupos locales.
- Usuario1: Administrador (Control total).
- Usuario2: Usuario estándar (Leer y modificar).
- Usuario3: Invitado (Solo lectura).
- Se asignaron los usuarios a sus respectivos grupos de seguridad.
- Configuración de permisos en carpetas compartidas mediante:
Propiedades > Uso compartido avanzado.
- Asignación de permisos personalizados por usuario.

## *Fase 3: Instalación de Herramientas de Gestión y Acceso Remoto*

Objetivo:
Implementar herramientas de control sobre archivos y establecer el acceso remoto.

Pasos realizados:
- Instalación del Administrador de recursos del servidor de archivos desde:
Administrador del servidor > Agregar roles y características > Características.
- Configuración de:
- Cuotas de almacenamiento.
- Reglas de acceso a archivos.
- Filtros de archivos (bloqueo de archivos .exe en carpeta Prueba1).
- Configuración de acceso remoto:
- Activación del servicio de Escritorio Remoto.
- Inclusión de Usuario1 como autorizado.

- Verificación o creación de regla de entrada en el firewall para puerto TCP 3389.

# *Fase 4: Políticas de Seguridad y Configuración del Firewall*

Objetivo:
Reforzar la seguridad de los accesos remotos y prevenir accesos no autorizados.

Pasos realizados:
- Activación de autenticación a nivel de red en Escritorio Remoto:
- Solo equipos con Escritorio remoto autenticado pueden conectarse.
- Configuración del firewall con reglas personalizadas:
- Bloqueo de IP sospechosa mediante:
Herramientas > Firewall de Windows Defender con seguridad avanzada > Nueva regla.
- Aplicación de la regla para bloquear la conexión de dicha IP.

# *Fase 5: Resumen Final*

Resultados obtenidos:
- Implementación de segmentación de usuarios según privilegios.
- Accesos remotos restringidos y protegidos por políticas y firewall.
- Bloqueo de archivos ejecutables no deseados en carpetas compartidas.
- Control granular sobre lectura/modificación de archivos por tipo de usuario.