UNIVERSIDAD TECNOLOGICA NACIONAL

Trabajo Práctico Integrador

Arquitectura y Sistemas Operativos

Seguridad en Sistemas Operativos

Alumnos

Maximiliano Rao – rao.maximiliano.l@gmail.com

Mauricio Lopez – rinaldi.el@hotmail.com

Profesor: Martín Aristiaran

Tecnicatura Universitaria en Programación - Universidad Tecnológica Nacional.

05 de junio de 2025

Índice

1- Introducción

La seguridad en los sistemas operativos cumple un rol fundamental en la protección, tanto de la integridad del propio sistema como de la información personal y empresarial que gestiona el mismo. Para lograrlo, los sistemas operativos disponen de diversas herramientas diseñadas para prevenir, detectar y mitigar ataques cibernéticos. En el presente trabajo nos enfocaremos en una de estas herramientas de mitigación: las Group Policy Objects (GPO), conocidas en español como Políticas de Grupo. Analizaremos cómo se crean, configuran e implementan adecuadamente para fortalecer la seguridad del entorno operativo.

2- Marco Teórico

Las Group Policy Objects (GPO), o Políticas de Grupo, fueron introducidas en Windows 2000 junto con Active Directory, con el objetivo de facilitar la administración centralizada de configuraciones y políticas de seguridad en entornos corporativos. Antes de su implementación, los administradores debían configurar cada equipo de forma manual, lo cual resultaba ineficiente y propenso a errores.

Una GPO está compuesta por dos tipos principales de configuraciones:

- **Configuraciones de usuario:** Permiten aplicar restricciones y establecer parámetros específicos para los usuarios, independientemente del equipo que utilicen.
- **Configuraciones de equipo:** Modifican el comportamiento del sistema operativo y de las aplicaciones instaladas, afectando al equipo sin importar qué usuario inicie sesión.

Creación y Configuración

Para crear y configurar una GPO de manera adecuada, se deben seguir estos pasos:

1- Acceder al Editor de Políticas de Grupo (gpmc.msc) en un sistema con privilegios administrativos.

2- Crear una nueva GPO y vincularla a un dominio, sitio o unidad organizativa (OU) dentro de Active Directory. Definir las configuraciones según las necesidades de seguridad y administración.

3- Definir las configuraciones necesarias según los requerimientos de seguridad y administración del entorno.

4- Aplicar filtros y establecer permisos que controlen qué usuarios o equipos estarán sujetos a la política.

Las GPO se procesan en el siguiente orden:

1. Política de grupo local (configurada directamente en el equipo).
2. GPO vinculadas al sitio (aplican a todos los equipos dentro de una ubicación geográfica).
3. GPO vinculadas al dominio (afectan a todos los usuarios y equipos del dominio).
4. GPO vinculadas a unidades organizativas (OU) específicas (permiten mayor granularidad en la aplicación de políticas).

En caso de conflicto entre políticas, se aplica la última en orden de precedencia, sobrescribiendo las configuraciones anteriores.

Mantenimiento y Mejores Prácticas

- Para garantizar una gestión eficaz de las GPO, se recomienda seguir las siguientes buenas prácticas:
- Realizar auditorías y monitoreo constante para detectar problemas, verificar el cumplimiento de las políticas y evaluar su impacto.
- Resolver conflictos mediante una correcta jerarquización de las políticas aplicadas.
- Evitar bloqueos de herencia innecesarios, ya que estos pueden impedir la correcta aplicación de políticas superiores y generar inconsistencias.

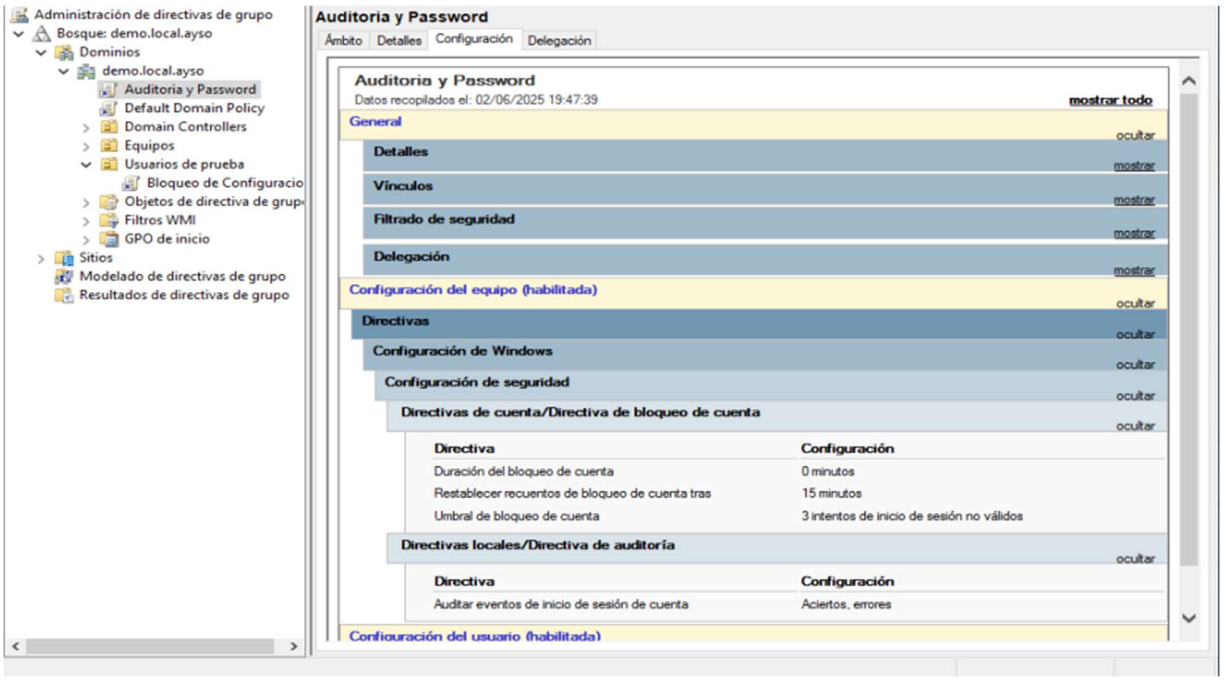
3- Caso Práctico

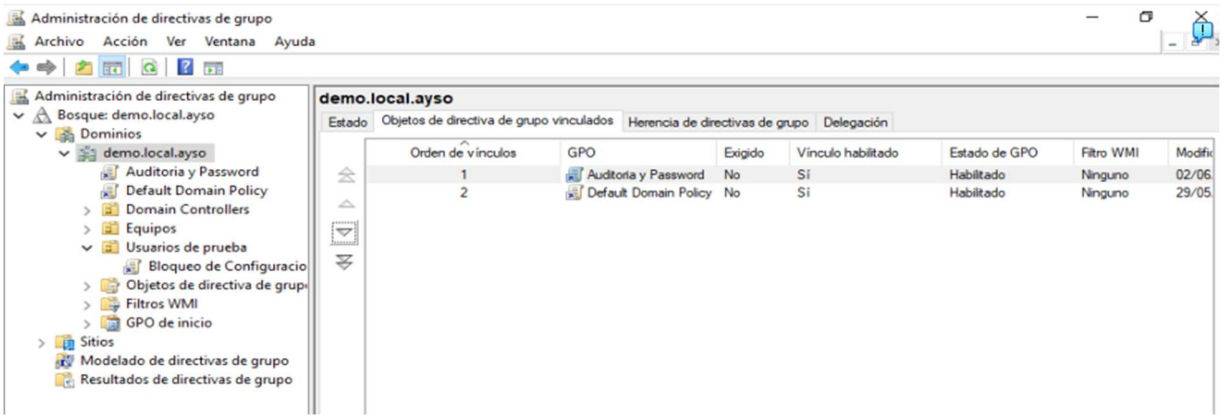
Una empresa del sector tecnológico ha decidido reforzar la seguridad de sus estaciones de trabajo mediante la aplicación de restricciones a los usuarios estándar. El objetivo es impedir el acceso a configuraciones críticas del sistema, como los ajustes de red, opciones de seguridad, configuraciones del sistema (Panel de Control). Además, se busca implementar monitoreos que permitan registrar y auditar los inicios de sesión de los empleados.
Para simular esta situación en un entorno controlado, se implementó un laboratorio compuesto por dos máquinas virtuales:

- Una con Windows Server 2022 configurada como **Controlador de Dominio (Active Directory).**
- Otra con Windows 10 unida al dominio, funcionando como estación cliente.

El equipo de Tecnología de la Información (TI) llevó a cabo las siguientes acciones:

1- **Configuración del entorno de dominio:**
   - Instalación y configuración de Active Directory en la VM servidor.
   - Unión de la VM cliente al dominio.
2- **Creación de usuario de dominio** (test) para acceso desde la máquina cliente.
3- **Creación de una nueva GPO** desde la consola de administración de políticas de grupo (Group Policy Management Console).
   a. Se creó la política “Auditoria y Password” vinculada al dominio para registrar los intentos de inicio de sesión tantos exitosos como erróneos y que bloquee la cuenta tras 3 intentos fallidos y permanezca en ese estado hasta que un Administrador de dominio la desbloquee. Esta política se prioriza por encima de la “Default Domain Policy”

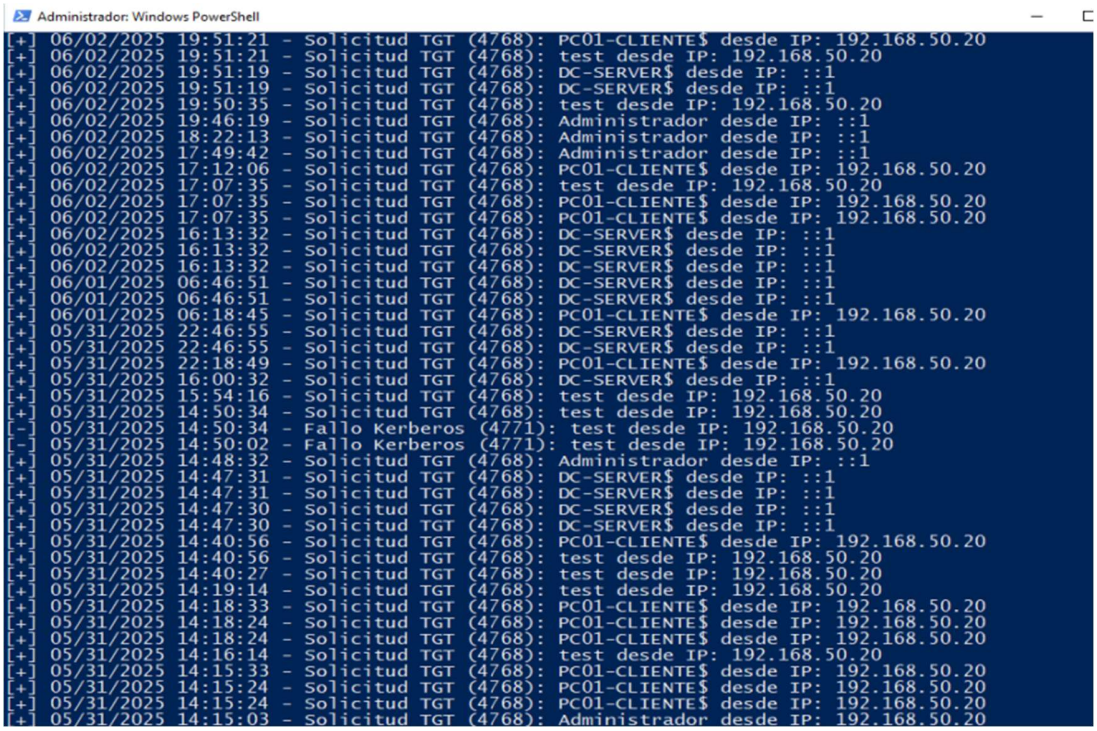




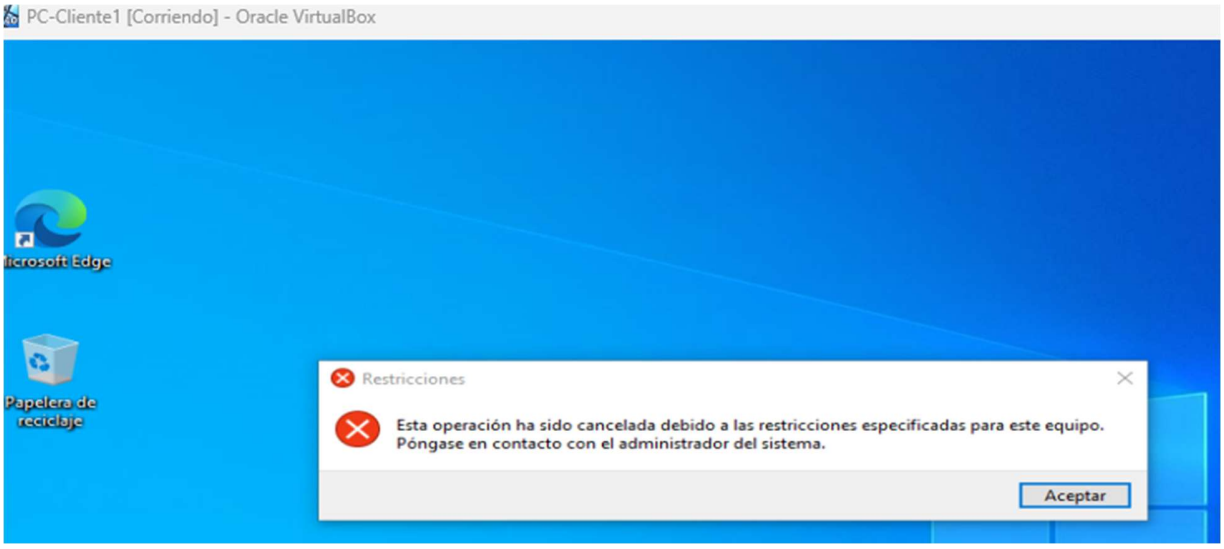
b. Se crea la política “Bloqueo de Configuración” vinculada a la OU “Usuarios de prueba” donde se encuentra creado el usuario de prueba y se le configura el bloqueo del acceso al panel de control.

4- **Pruebas y verificación** del correcto funcionamiento de las restricciones y del registro de eventos en el Visor de Sucesos (Event Viewer). Se creó un script en el controlador de dominio para extraer los inicios de sesión de los usuarios y exportarlos a un archivo .csv.

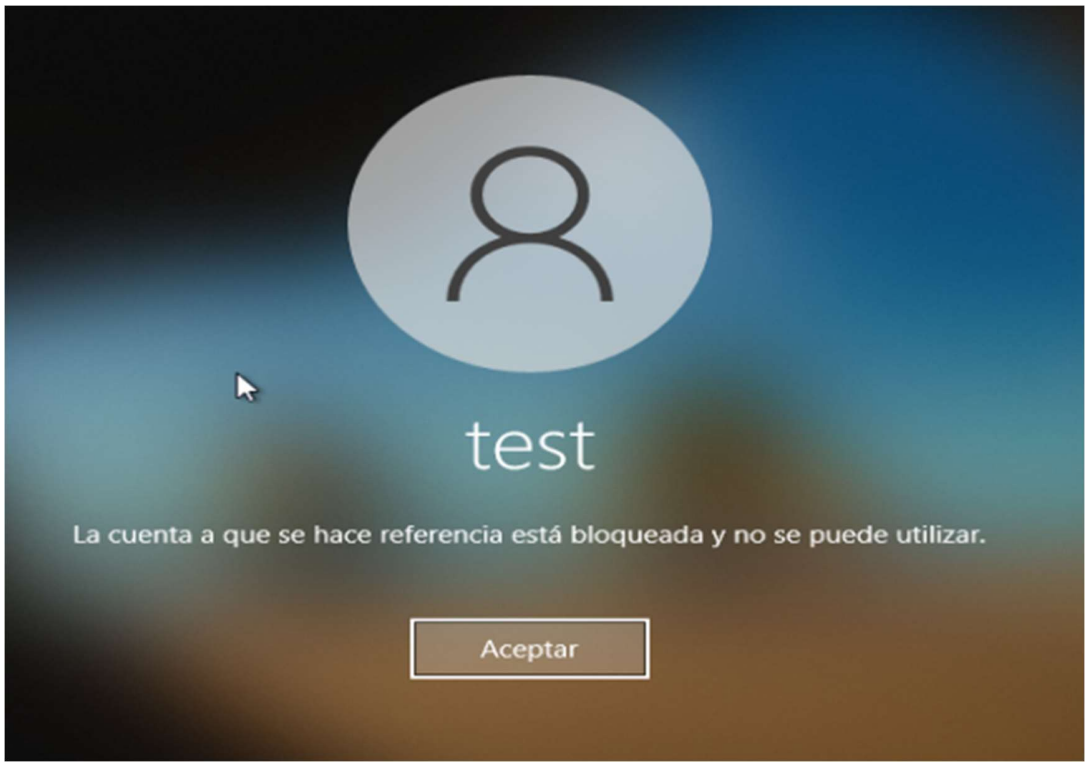
Salida de scripts:

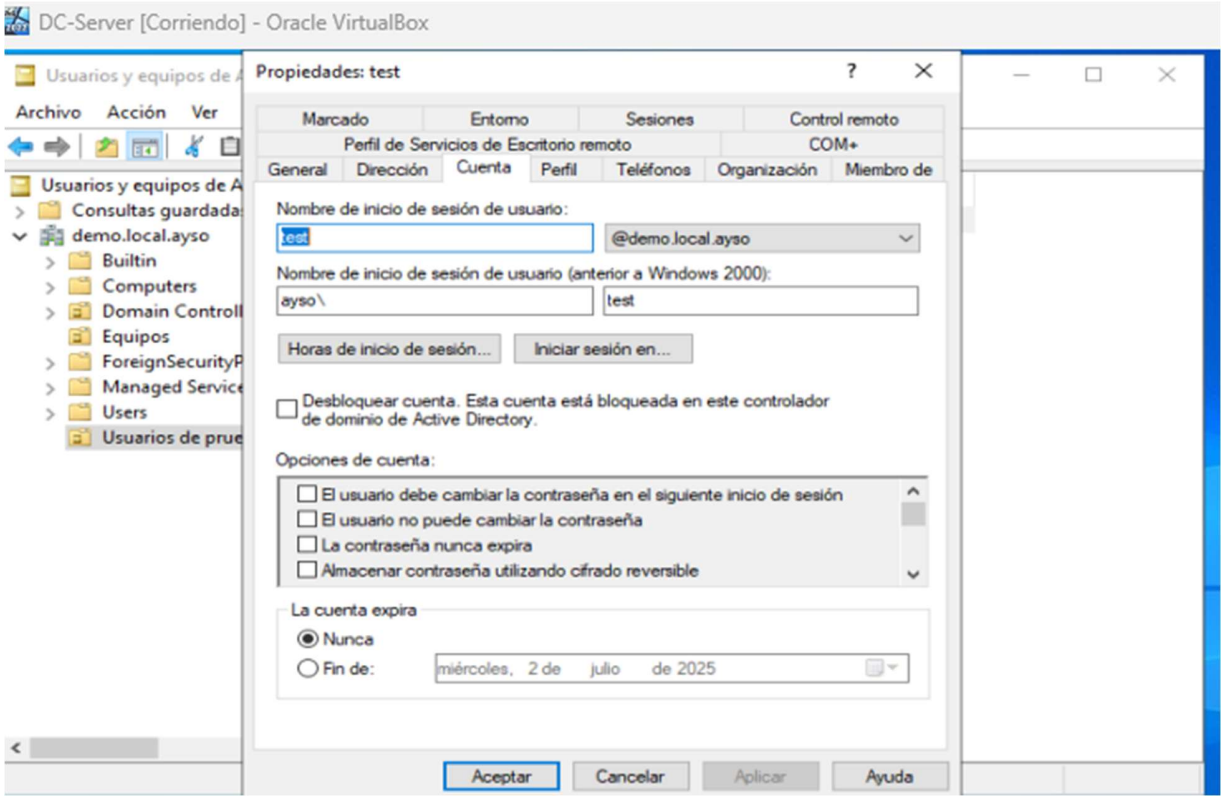


Al intentar abrir el panel de control:



Luego de 3 intentos fallidos:





Con esta implementación, la empresa logra aumentar la seguridad de los sistemas, evitando modificaciones no autorizadas y obteniendo visibilidad sobre los accesos al sistema por parte de los empleados.

4- Metodología Utilizada

Para el desarrollo del trabajo práctico se adoptó una metodología experimental en un entorno de laboratorio controlado, con el objetivo de simular la implementación real de políticas de seguridad mediante GPO en un dominio de Active Directory. Los pasos seguidos fueron los siguientes:

1. **Diseño del entorno de laboratorio**
   Se crearon dos máquinas virtuales utilizando VirtualBox. Una de ellas fue configurada con Windows Server 2022 para cumplir el rol de **Controlador de Dominio (DC)**, y la otra con Windows 10, configurada como **cliente del dominio**.
2. **Configuración de Active Directory y servicios asociados**:
   En la máquina servidor se instalaron los roles de **Active Directory Domain Services (AD DS)** y **DNS**, y se promovió el servidor a controlador de dominio.
3. **Unión del cliente al dominio**:
   La máquina cliente fue unida al dominio previamente configurado, permitiendo la aplicación centralizada de políticas de grupo.
4. **Creación y aplicación de una GPO**:
   Desde la consola de administración de directivas de grupo (*Group Policy Management Console*), se creó una nueva GPO con configuraciones específicas de seguridad, como:
   - Restricción de acceso al Panel de Control y CMD.
   - Auditoría de inicios de sesión.
5. **Creación del usuario de dominio:** Se creó el usuario test en la unidad organizativa “Usuarios de prueba” para el acceso en la máquina cliente.
6. **Pruebas funcionales y verificación**:
   Se iniciaron sesiones en la máquina cliente con usuarios del dominio para comprobar que las políticas se aplicaban correctamente. También se verificó la auditoría de inicios de sesión a través del Visor de Eventos del AD.

Esta metodología, junto con el uso de la función de pantalla compartida de AnyDesk, permitió que ambos integrantes del equipo pudieran colaborar activamente en tiempo real, manipulando las máquinas virtuales de forma conjunta. De este modo, se logró validar el

funcionamiento de las políticas de grupo en un entorno controlado, simulando una situación real de implementación en una empresa.

5- Resultados Obtenidos

A partir de la implementación del entorno simulado y la aplicación de las políticas de grupo, se obtuvieron resultados positivos en la mayoría de los casos planificados.

Aspectos que funcionaron correctamente:

- Las restricciones aplicadas mediante GPO fueron efectivas: se logró bloquear el acceso al Panel de control.
- La auditoría de inicios de sesión quedó correctamente configurada, y se pudieron visualizar los eventos correspondientes en el Visor de Eventos.
- La GPO aplicada a la Unidad Organizativa (OU) fue heredada correctamente por los usuarios pertenecientes a esa unidad.
- El entorno de dominio funcionó de forma estable durante las pruebas, permitiendo aplicar y actualizar las políticas sin inconvenientes.

Casos de prueba realizados:

- Iniciar sesión con una cuenta de dominio restringida (usuario: test) para verificar el bloqueo de herramientas del sistema.
- Intentar acceder al Panel de Control para comprobar el error.
- Ingresar contraseñas erróneas en el usuario 3 veces para verificar su bloqueo.
- Revisar el registro de eventos relacionados con inicio y cierre de sesión del usuario.

Dificultades encontradas y errores corregidos:

- Inicialmente en la configuración de red de las VM que debimos ponerlas en la misma Red Interna dentro de VirtualBox para poder configurar sus IPs, por defecto ambas VMs poseían la misma IP.
- La GPO no tenía efecto sobre el usuario de prueba, lo que se solucionó al verificar que no estaba correctamente ubicado dentro de la OU vinculada a la política.

- En una de las pruebas, los cambios en la política no se aplicaban inmediatamente. Esto se resolvió forzando la actualización de políticas en la máquina cliente con el comando gpupdate /force.
- Se detectó que algunos cambios requerían reiniciar la sesión del usuario o incluso el sistema para surtir efecto completo.
- Una política por defecto “Default Domain Policy” desestimaba nuestros cambios por la prioridad, lo cual se soluciono colocando la creada con una prioridad superior.

6- Conclusiones

La realización de este trabajo práctico nos permitió afianzar conocimientos teóricos y prácticos sobre la implementación de medidas de seguridad a través de las Políticas de Grupo (GPO) en sistemas operativos Windows. Trabajar en un entorno virtualizado nos brindó la posibilidad de experimentar libremente, aplicar restricciones y monitorear su impacto sin comprometer sistemas reales.

Uno de los principales aprendizajes fue entender cómo se pueden establecer controles de seguridad centralizados mediante Active Directory, como el bloqueo de acceso a funciones críticas (Panel de Control) o la configuración de auditorías para supervisar la actividad de los usuarios. Esto nos permitió ver cómo una correcta administración de GPO contribuye directamente a reducir la superficie de ataque, prevenir accesos no autorizados y garantizar un entorno de trabajo más seguro para los usuarios.

También aprendimos a utilizar herramientas como el Editor de Políticas de Grupo, el Visor de Sucesos y comandos como gpupdate, gpresult para gestionar la aplicación de políticas y monitorear su funcionamiento.

Como posible mejora para futuras prácticas, sería interesante ampliar la implementación de GPO con políticas más avanzadas, como redirección de carpetas, ejecución de scripts de inicio/cierre de sesión, o configuraciones específicas por grupos de seguridad.

En cuanto al trabajo en equipo, el uso de la pantalla compartida a través de AnyDesk permitió una colaboración efectiva, resolviendo problemas en tiempo real y dividiendo tareas técnicas de manera equitativa.

7- Bibliografía

- Microsoft. (s.f.). *Introducción a Windows Server*. https://learn.microsoft.com/es-mx/windows-server/get-started/get-started-with-windows-server
- Microsoft. (s.f.). *Descripción general de las directivas de grupo (Group Policy)*. https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview
- Microsoft. (s.f.). *Descarga de Windows Server 2022*. https://www.microsoft.com/es-es/evalcenter/download-windows-server-2022
- Aula Virtual. (2025). *Material proporcionado por el docente – Arquitectura y Sistemas - Operativos*. Instituto Universidad Tecnológica Nacional.

8- Anexo

- Scripts para extracción de logs de inicio de sesión
- Archivos HTML con la configuración realizada en cada política.
- Link de video: https://youtu.be/MatiWHX3a5s