Actividad 1: Configuración de Seguridad en Sistemas Windows Server y Windows 11 según CCN-STIC

Julio Ortiz Bort
Universidad Internacional de La Rioja
Fecha: 29 de noviembre de 2025

Introducción

El objetivo de esta práctica es implementar y verificar las políticas de seguridad del Centro Criptológico Nacional (CCN) mediante las guías CCN-STIC 570A/23 y CCN-STIC 599A/23, aplicadas a un entorno Windows Server 2022 y un cliente Windows 11 unidos en un dominio Active Directory.

Descripción del laboratorio

El laboratorio se compone de dos máquinas virtuales desplegadas en VirtualBox: un servidor Windows Server 2022 con servicios AD DS, DNS y DHCP; y un cliente Windows 11 configurado como miembro del dominio.

Windows Server 2022

- Nombre del servidor: `WS23861607`
- Dominio: `d23861607.es`
- Usuario del dominio: `u23861607`
- IP interna: 192.168.5.2

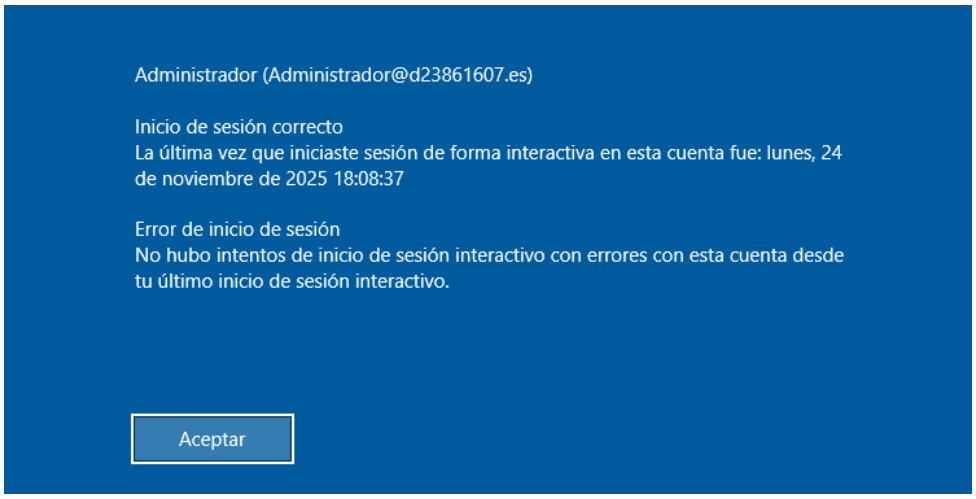

Figura 1: Inicio de sesión como admin en el servidor.

Figura 2: Administración del servidor – Servidor local.

Windows 11 Cliente

- Nombre del equipo: `W23861607`
- Dominio aplicado: `d23861607.es`

Figura 3: Inicio de sesión en el dominio `d23861607.es`.

Configuración de Seguridad para Windows Server (CCN-STIC 570A/23)

Estructura del dominio y OU Clientes Windows

Se creó la unidad organizativa **Clientes Windows**, y se movió el equipo `W23861607` desde *Computers* a la nueva OU, siguiendo buenas prácticas ENS.

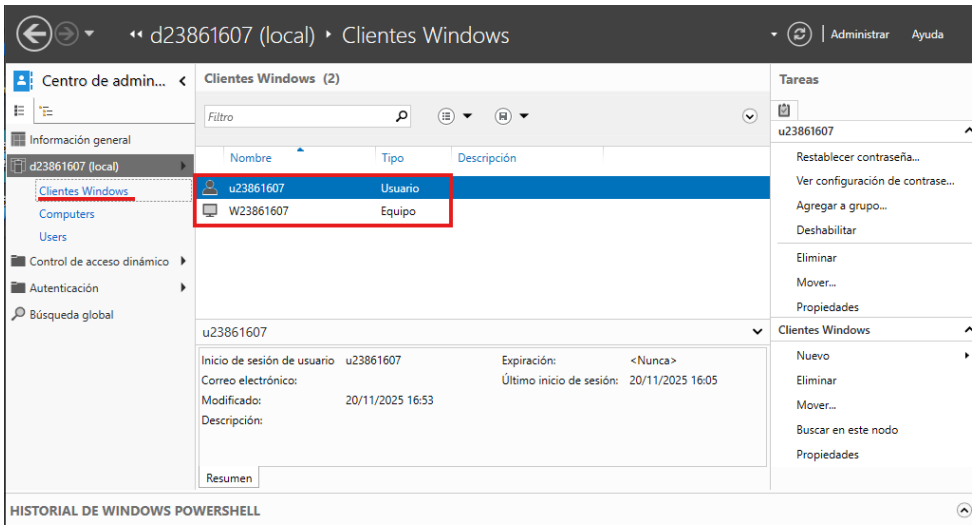

Figura 4: OU Clientes Windows y equipo movido.

Políticas Implementadas

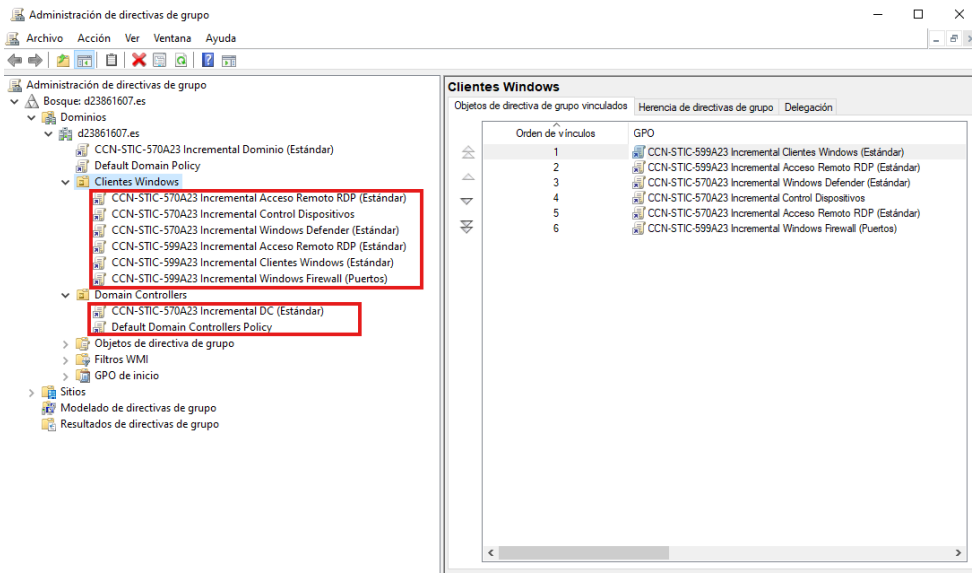

Figura 5: Políticas Implementadas.

Políticas ENS aplicada al Dominio

Política de contraseñas

- Longitud mínima: 10 caracteres
- Complejidad habilitada
- Historial: 5 contraseñas
- Validez máxima: 90 días

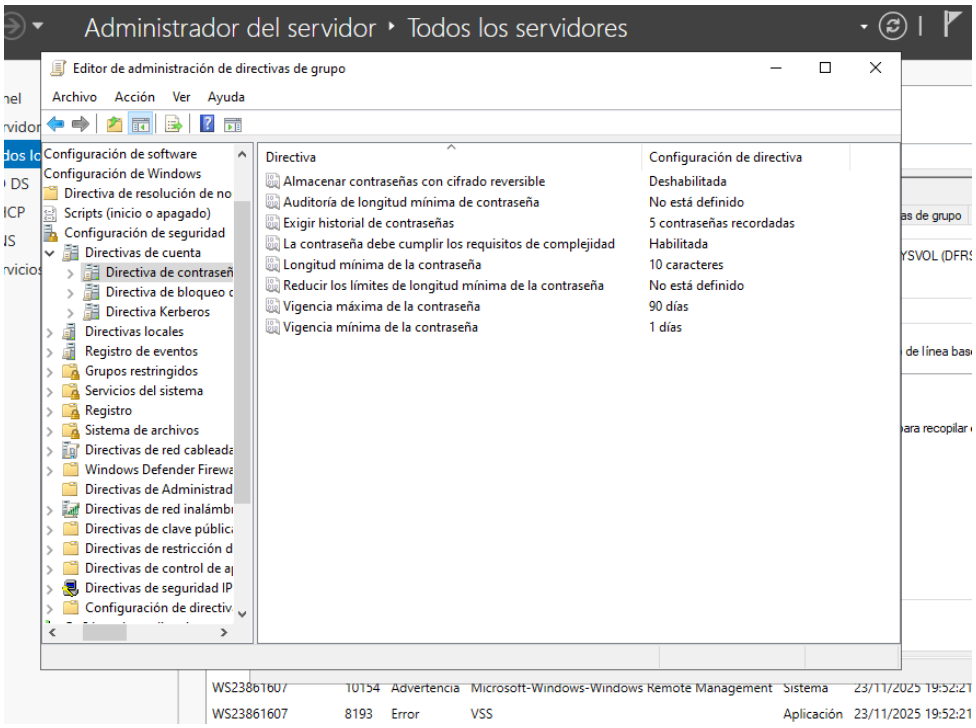

Figura 6: Configuración de directiva de contraseñas.

Bloqueo de cuentas

- 5 intentos fallidos
- Detección y bloqueo a 15 minutos

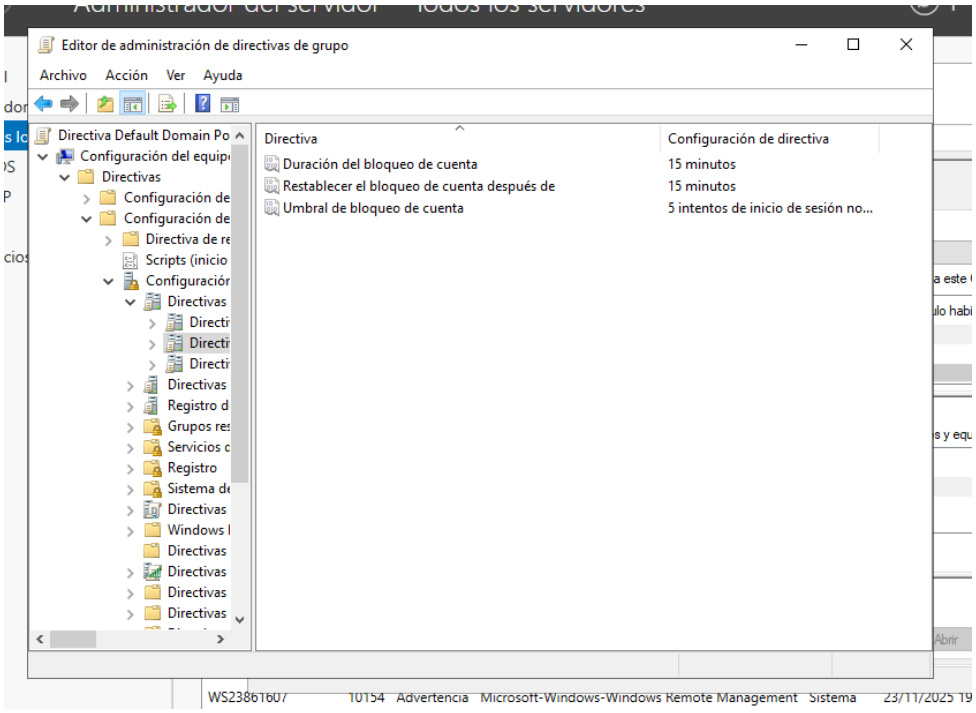

Figura 7: Directiva de bloqueo de cuentas.

Cifrado Kerberos

Se habilitaron únicamente algoritmos robustos:

- AES128-HMAC-SHA1
- AES256-HMAC-SHA1

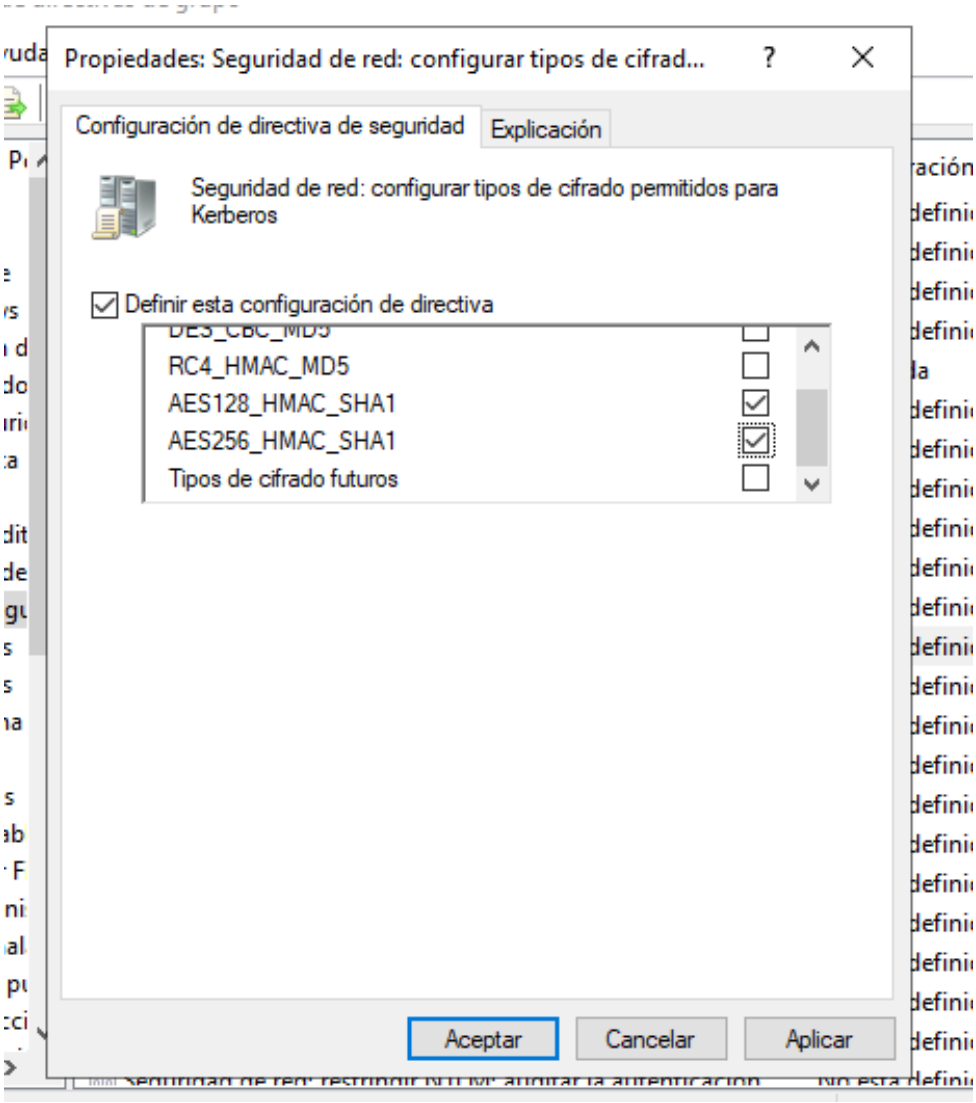

Figura 8: Cifrado Kerberos AES habilitado.

Análisis código dañino

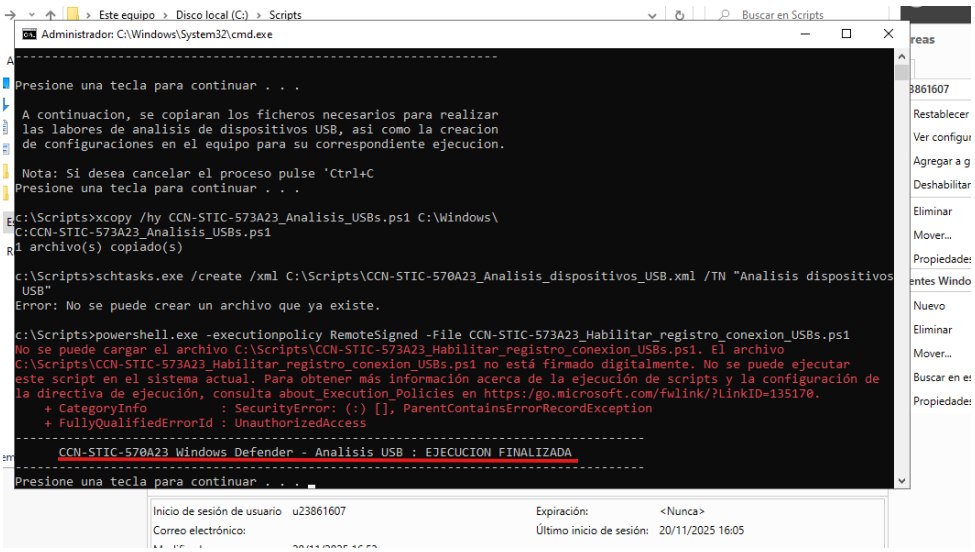

Figura 9: Script para activar el análisis de USB.

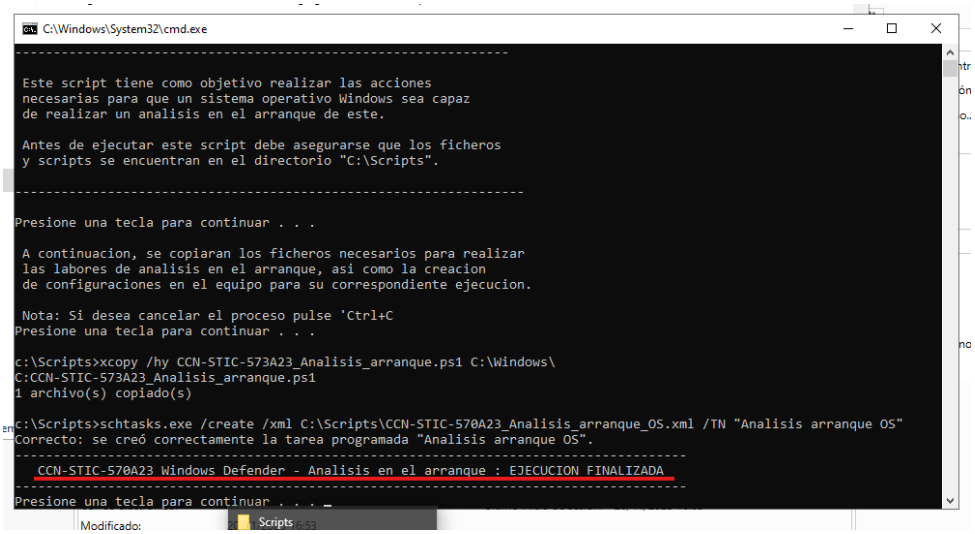

Figura 10: Script para activar el análisis de arranque.

Evidencias de prueba y error (Windows Server)

Prueba 1: Contraseña débil rechazada

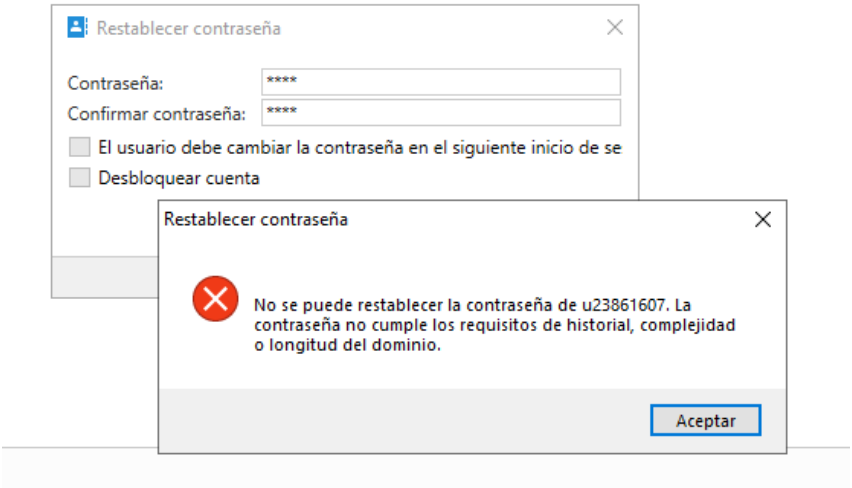

Figura 11: Rechazo de contraseña débil.

Prueba 2: Bloqueo de cuenta por intentos fallidos

Figura 12: Bloqueo de cuenta.

Configuración de Seguridad para Clientes Windows (CCN-STIC 599A/23)

Mostrar inicio de sesión anteriores

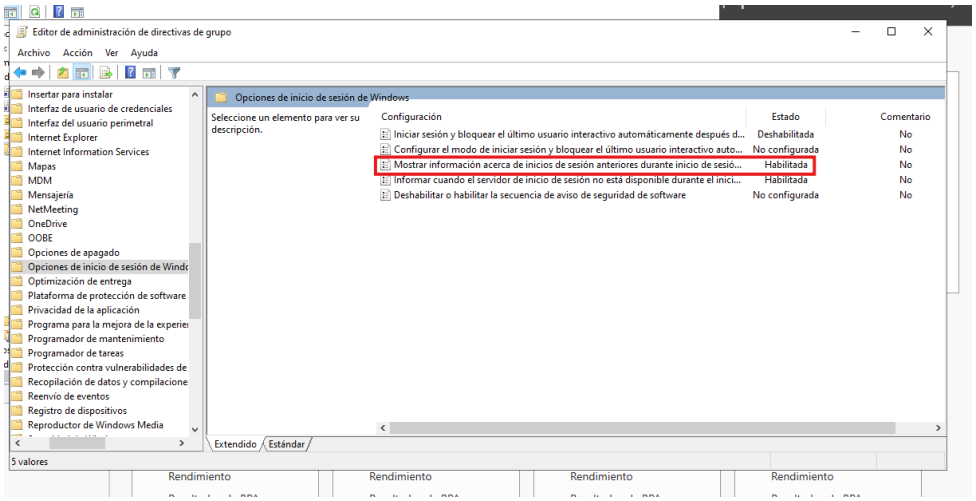

Figura 13: Activar mostrar incios de sesion anteriores.

Configuración de copia de seguridad

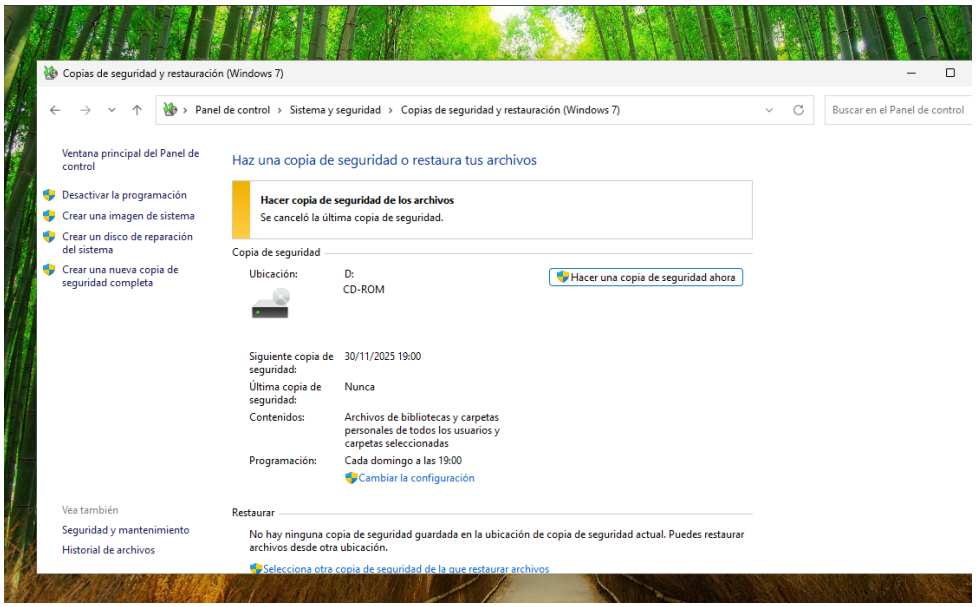

Figura 14: Copia de seguridad configurada.

Asignación de derechos de usuario

- Denegar RDP a usuarios estándar
- Apagar el sistema → solo administradores
- Acceso desde red → usuarios autenticados + administradores

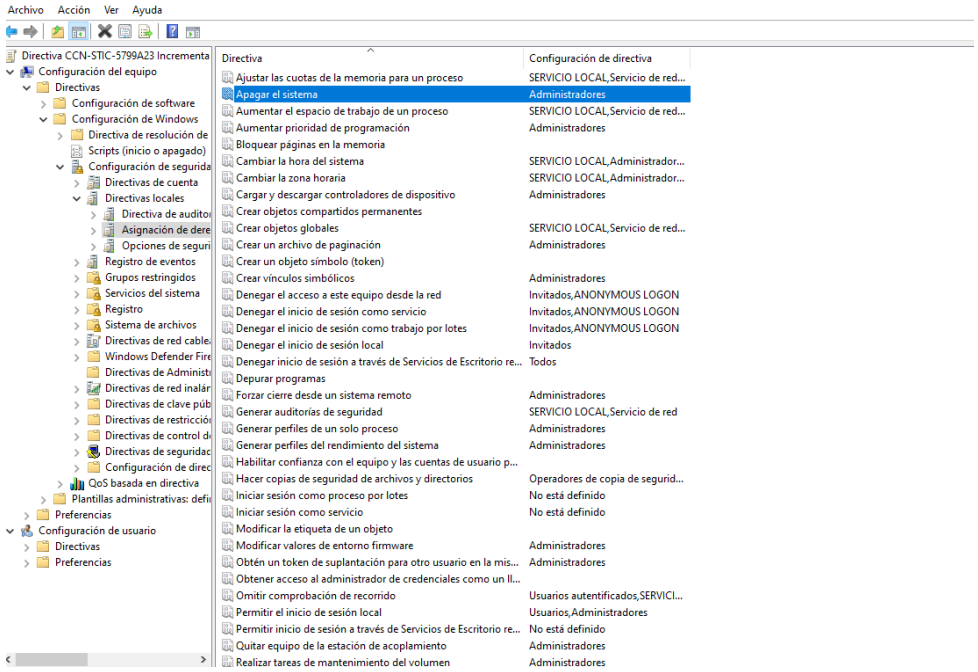

Figura 15: Asignación de derechos de usuario.

Protección de la Integridad y la Autenticidad

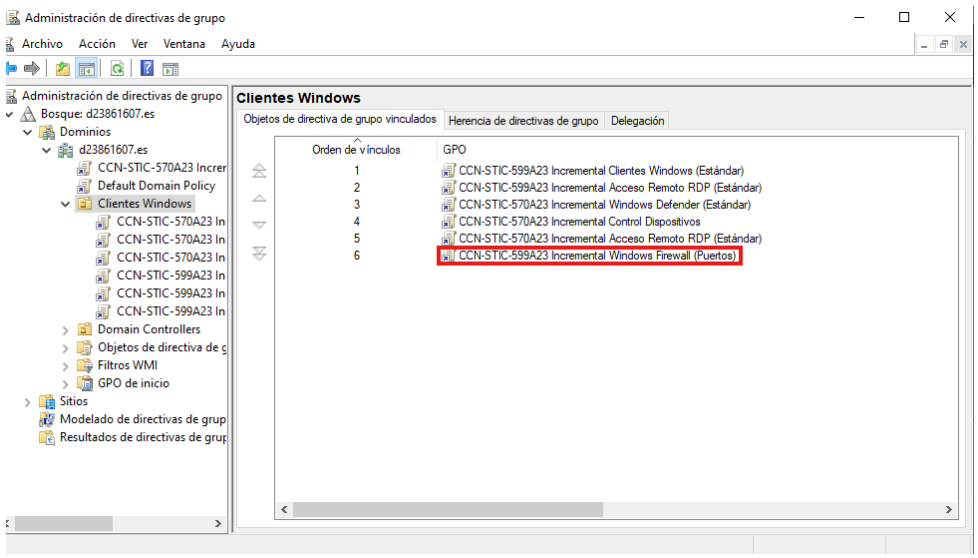

Figura 16: Política aplicada.

Acceso Remoto

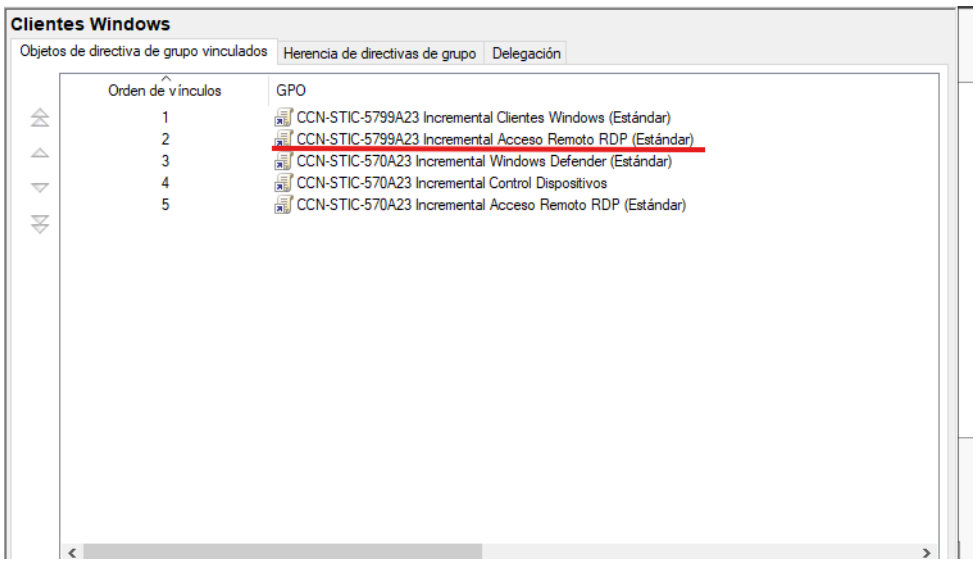

Figura 17: Política de acceso remoto aplicada.

Prueba de funcionamiento 1: Denegación de acceso RDP a usuario estándar

Para verificar la correcta aplicación de las políticas ENS relacionadas con la asignación de derechos de usuario, se intentó establecer una conexión RDP hacia el cliente Windows utilizando un usuario estándar del dominio. Dado que en la GPO se configuró la directiva *"Denegar inicio de sesión a través de Servicios de Escritorio Remoto"* para el grupo `Usuarios`, el intento de acceso debe ser bloqueado.

El resultado confirmó el comportamiento esperado: el sistema impidió el acceso remoto mostrando un mensaje indicando que el usuario no dispone de los permisos necesarios.

Figura 18: Intento de conexión RDP denegado a usuario estándar.

Prueba de funcionamiento 2: Verificación de auditoría mediante eventos de inicio de sesión

Para comprobar que la auditoría avanzada configurada en la GPO de clientes Windows se aplica correctamente, se realizó un inicio de sesión interactivo en el equipo cliente. Posteriormente, se accedió al Visor de eventos del sistema para verificar la generación de registros asociados.

Tal como establece el ENS en materia de trazabilidad, el equipo registró un evento **4624** (inicio de sesión satisfactorio), evidenciando el correcto funcionamiento de la directiva *"Auditar inicio de sesión"* en modo Éxito + Error.

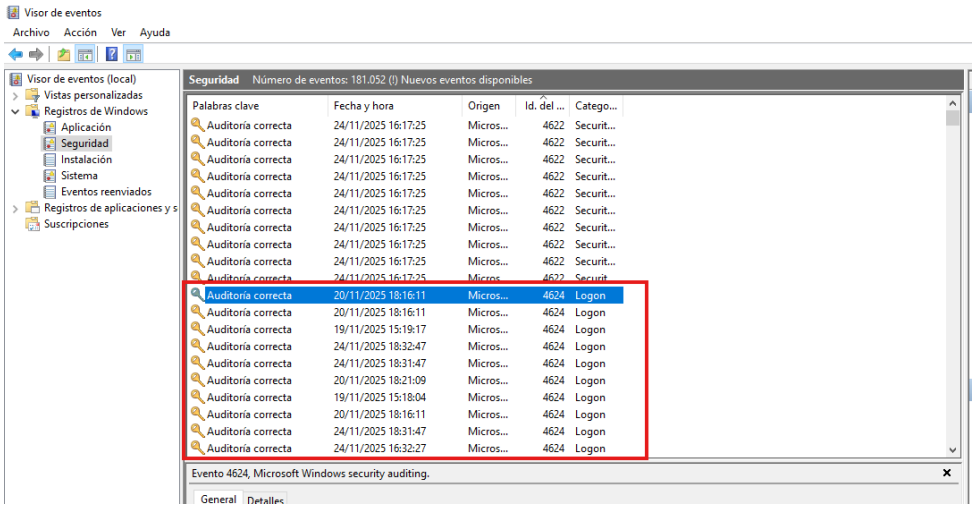

Figura 19: Eventos 4624 generados tras un inicio de sesión en el cliente Windows.

Conclusiones

La implementación de las guías CCN-STIC 570A/23 y 599A/23 en el dominio `d23861607.es` permite cumplir los requisitos del ENS categoría Básica. Las medidas aplicadas mejoran la trazabilidad, reducen la superficie de ataque y fortalecen la autenticación y control de acceso.