P05 WIN- SEGURIDAD EN ACTIVE DIRECTORY

ANA OROZCO ASENSIO

2ºASIR
I.E.S. ANTONIO MACHADO
ASO

Contenido

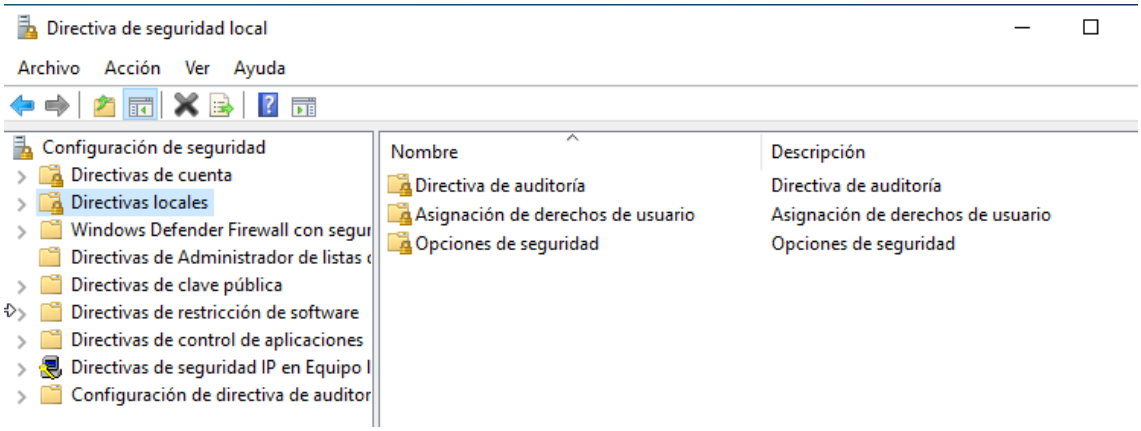
1.Directivas de Seguridad.

Visualizar las directivas de seguridad local de un cliente 10 y las del Controlador del dominio. ¿Qué diferencias muestran?

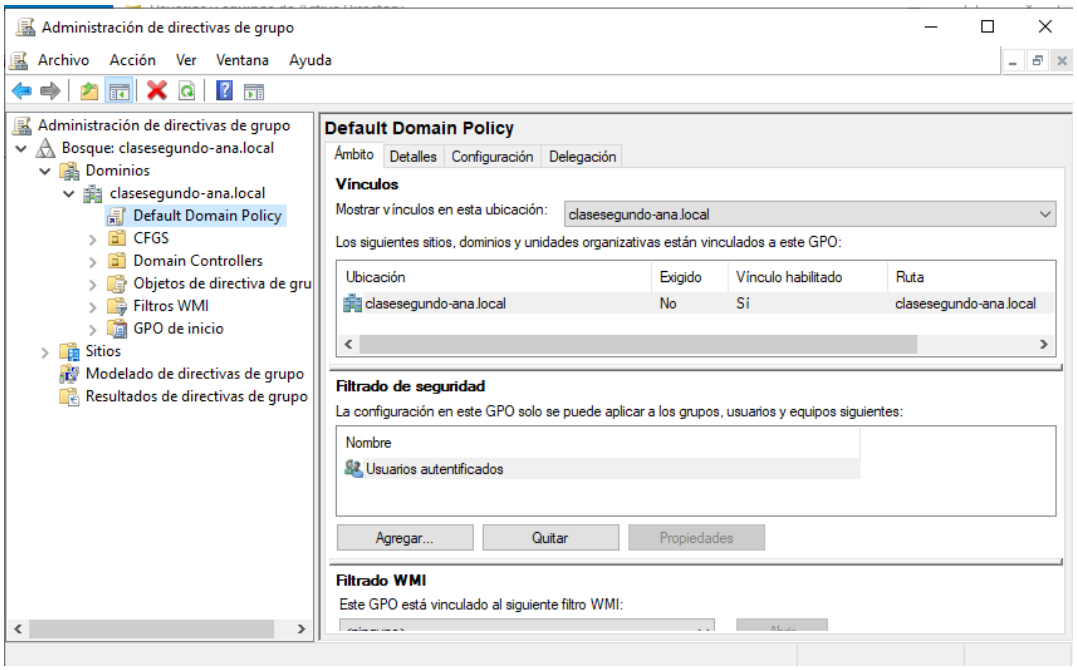
Las políticas de seguridad locales afectan únicamente a la máquina en la que se configuran, mientras que las establecidas en el controlador de dominio se extienden y aplican a todos los dispositivos que forman parte del dominio.

En las configuraciones locales no se incluyen opciones avanzadas como la administración de derechos de usuario o las políticas de grupo de seguridad. En cambio, el Controlador de Dominio permite acceder a configuraciones avanzadas, como la gestión de derechos de usuario, restricciones de software y ajustes para grupos de seguridad.

Windows 10:

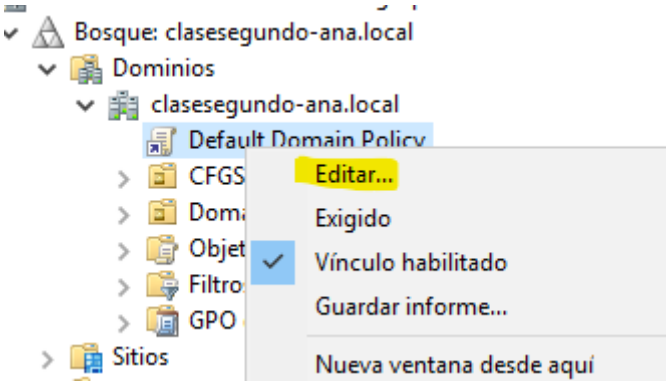


Dominio:

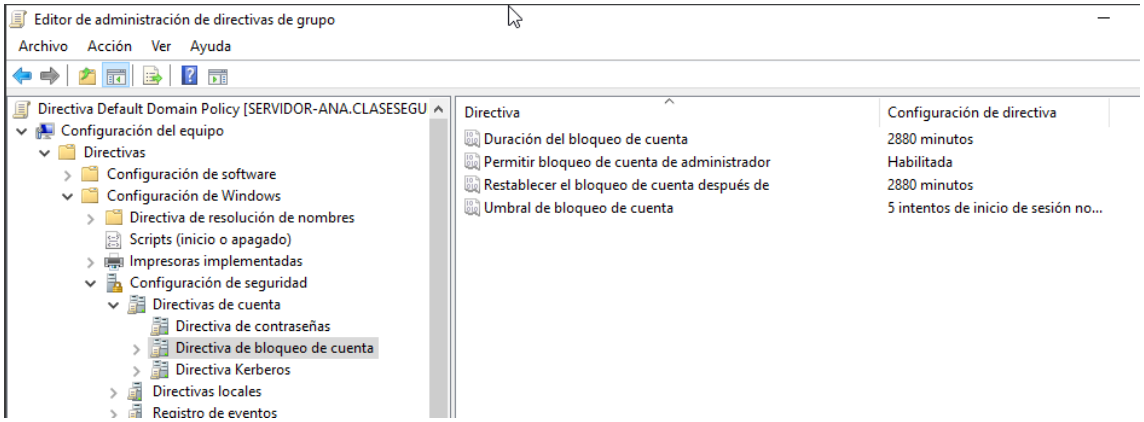


Modificar las directivas de bloqueo de cuentas para todos los equipos del dominio, de forma que se contabilicen cinco intentos y la duración del bloqueo sea de 48 horas.

Para realizar este ajuste, accedemos al editor de administración de directivas de grupo y navegamos a Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta, donde se pueden modificar las políticas relacionadas con el bloqueo de cuentas.

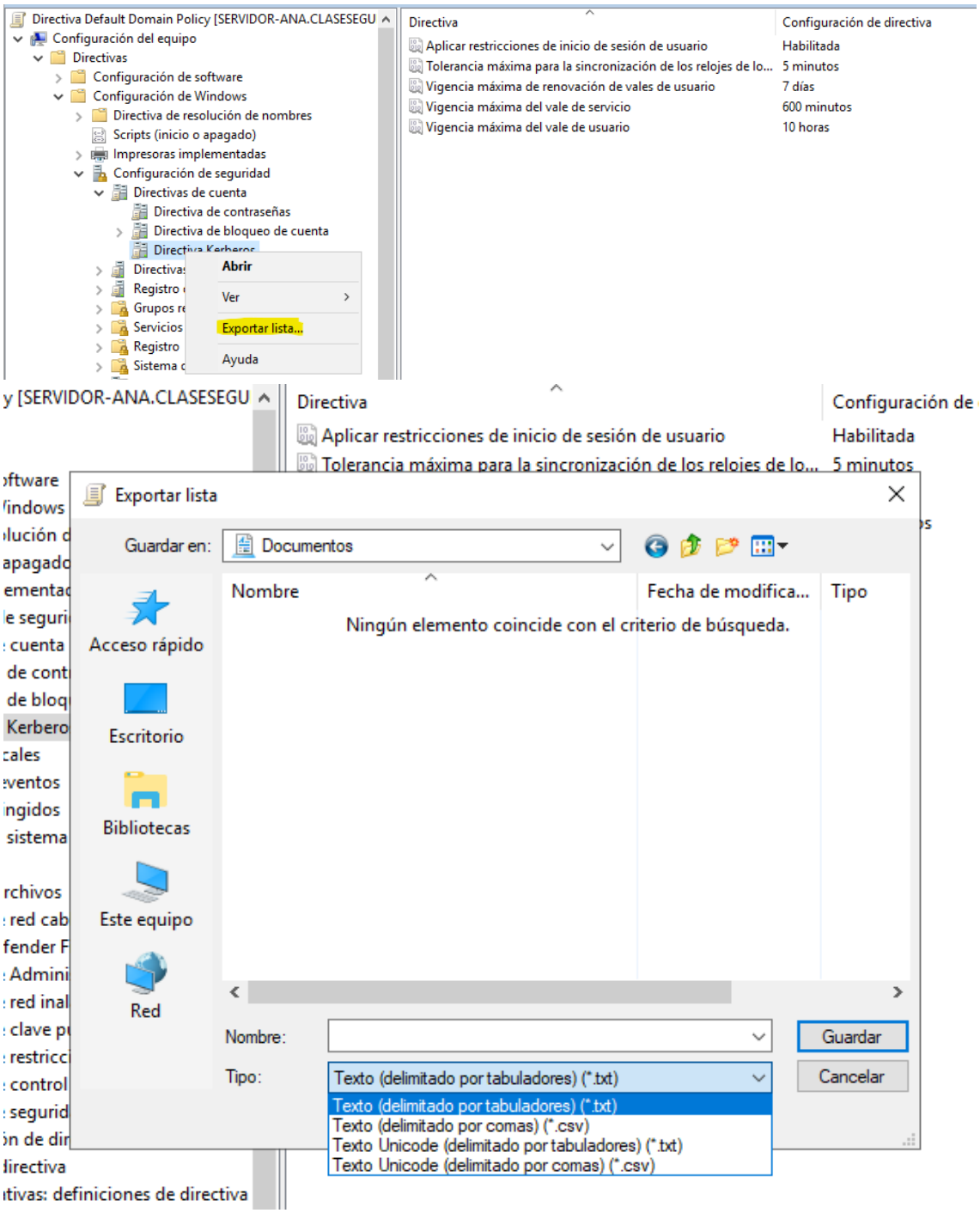


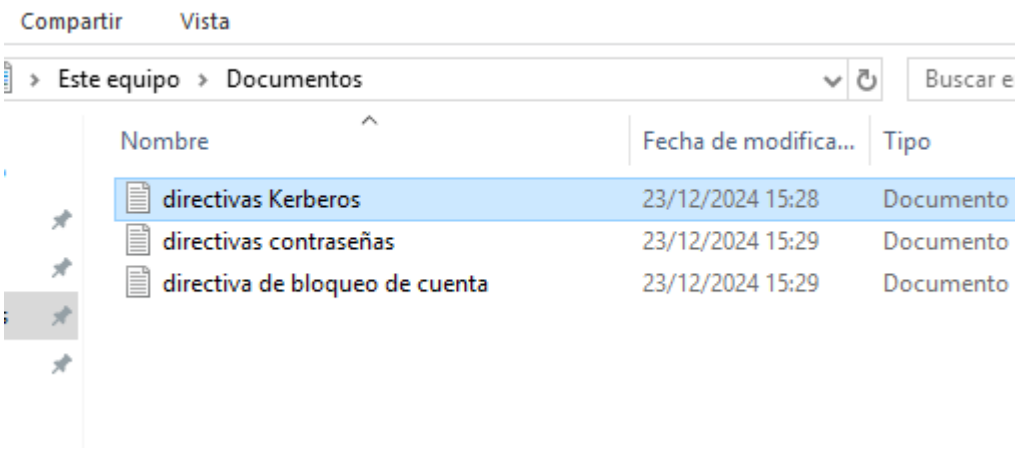
Pondremos 2880 minutos(que son 48 horas) ya que no permite el formato de horas, y ponemos el umbral de bloqueo en 5 intentos.



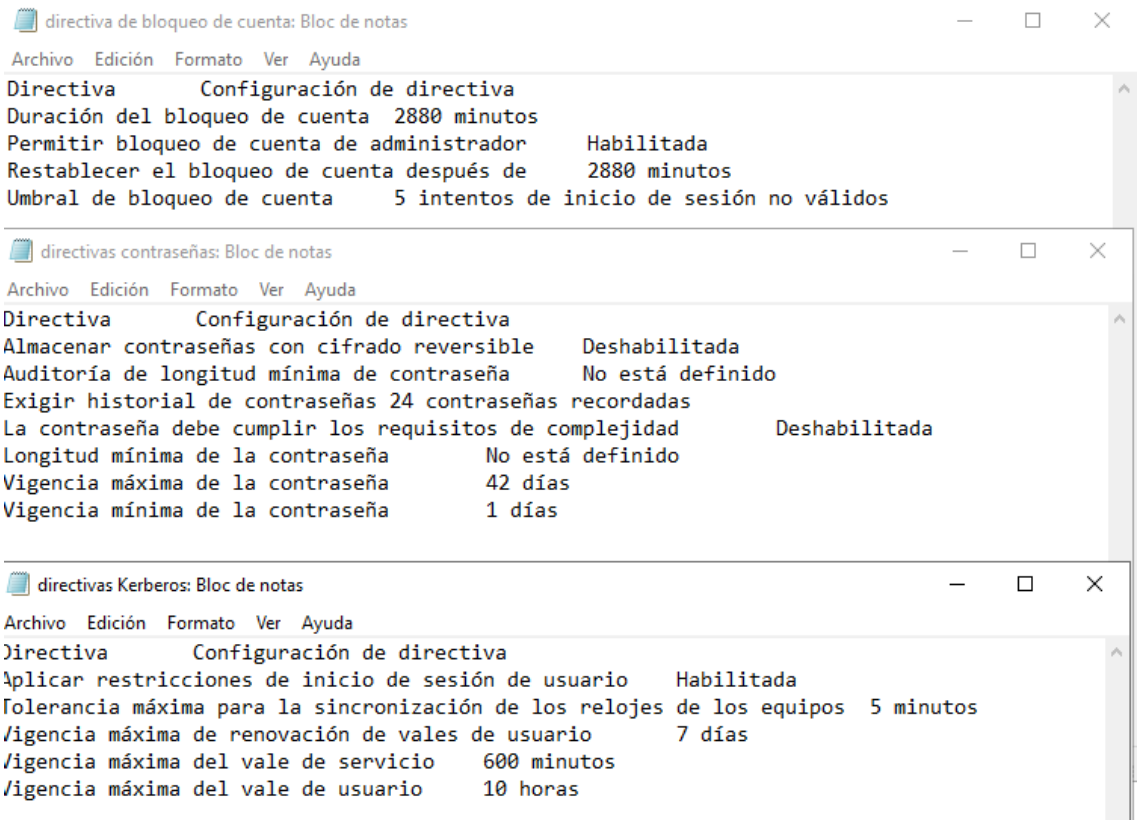
Exportar a tres archivos de texto que guardaremos en Documentos las directivas de contraseña, las directivas de bloqueo de cuenta y las directivas Kerberos, y visualizar sus contenidos. ¿Qué otras posibilidades de exportación tenemos?

Para ello haremos clic derecho en la directiva Kerberos y le daremos a exportar lista.





Existen dos formatos principales para guardar archivos: .txt y .csv. Ambos pueden estar en formato Unicode o no. La diferencia principal entre ellos radica en cómo separan los parámetros: el formato .csv utiliza comas como separadores, mientras que en el .txt se emplea el tabulador (representado por un espacio generado al presionar la tecla de tabulación).



¿Para qué sirve la exportación en formato .inf?¿En qué apartado (a qué nivel) se utiliza?

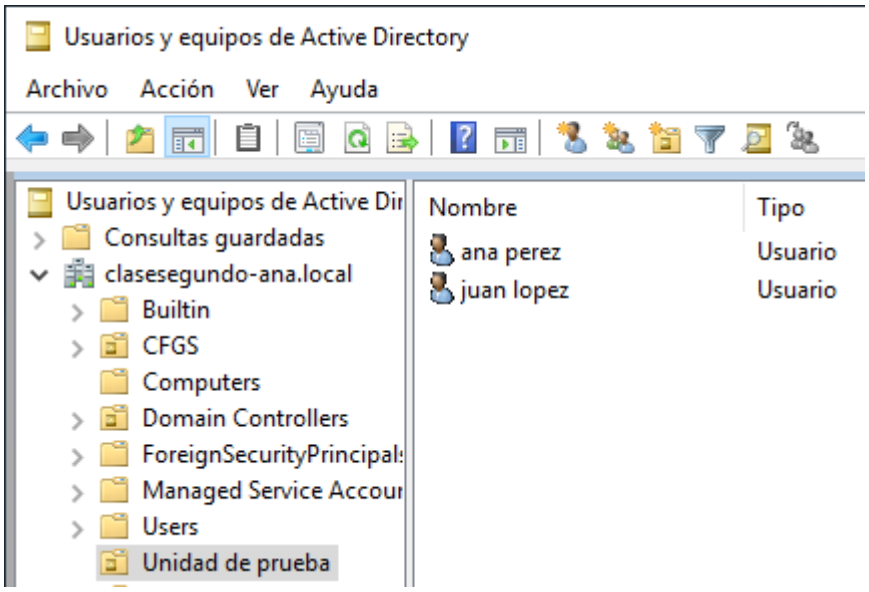
La exportación en formato .inf se utiliza para guardar plantillas de seguridad, que contienen un conjunto de configuraciones relacionadas con la seguridad del sistema. A nivel del sistema operativo, Windows emplea estos archivos para administrar configuraciones específicas, como la instalación de controladores

durante el arranque y las actualizaciones. Sin embargo, en las versiones actuales de Windows Server, esta opción ya no está disponible para exportar.

2.Directivas de Grupo

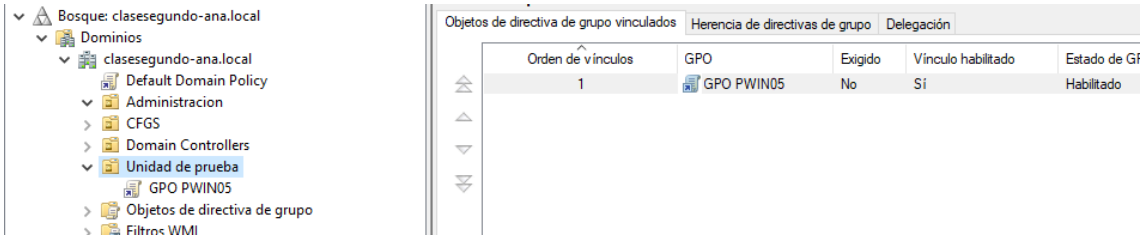
Añadir una nueva unidad organizativa al dominio llamada Unidad de prueba. Crear los usuarios, Ana Pérez (contraseña: aperez99) y Juan López (contraseña jlopez99) en Unidad de prueba.

Crearemos los usuarios tal y como aprendimos en prácticas anteriores.



Crear una nueva directiva de grupo para la Unidad organizativa que acabamos de crear, llamándola GPO práctica WIN05.

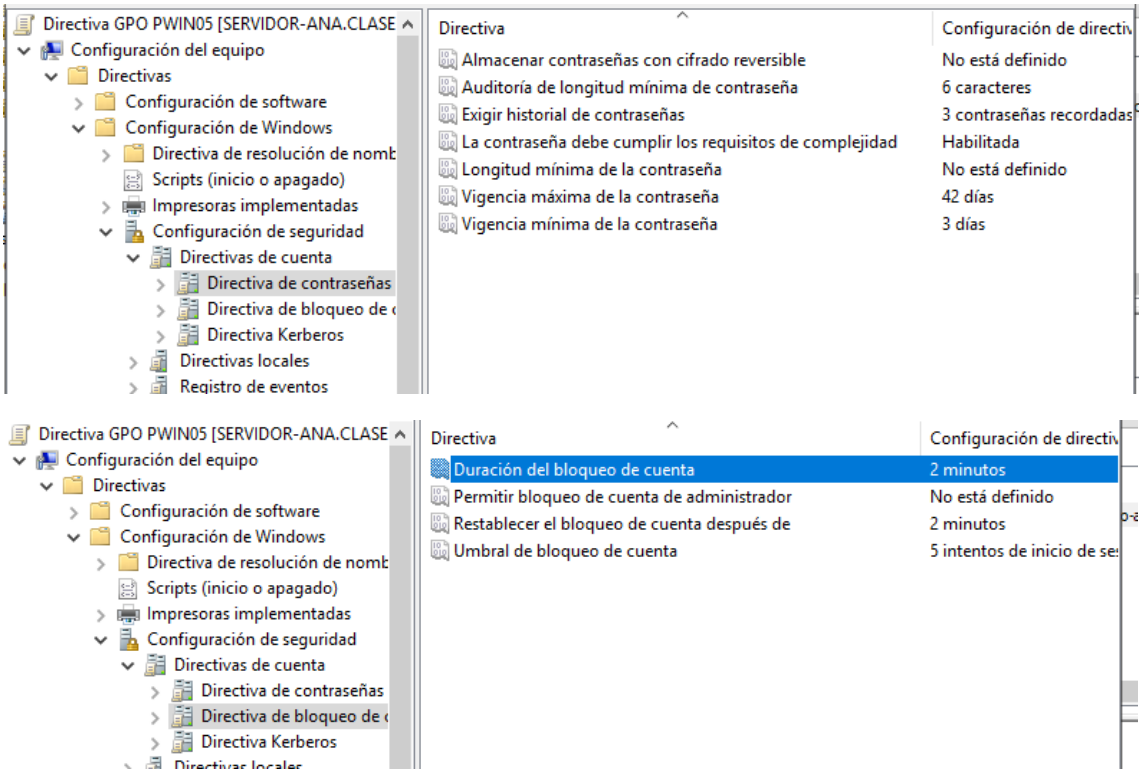
Creamos una GPO para nuestra unidad de prueba.



Modificar la directiva anterior con las siguientes características:

· Modifica las directivas de contraseñas y de bloqueo de cuentas para el equipo (con valores distintos a los especificados para el dominio).

Cambiaré algunos parámetros:

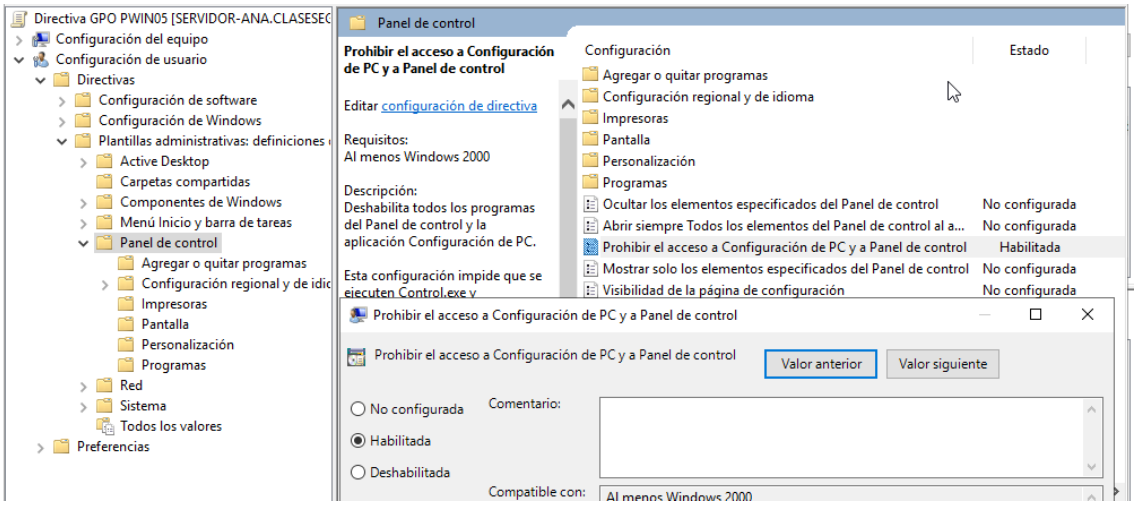


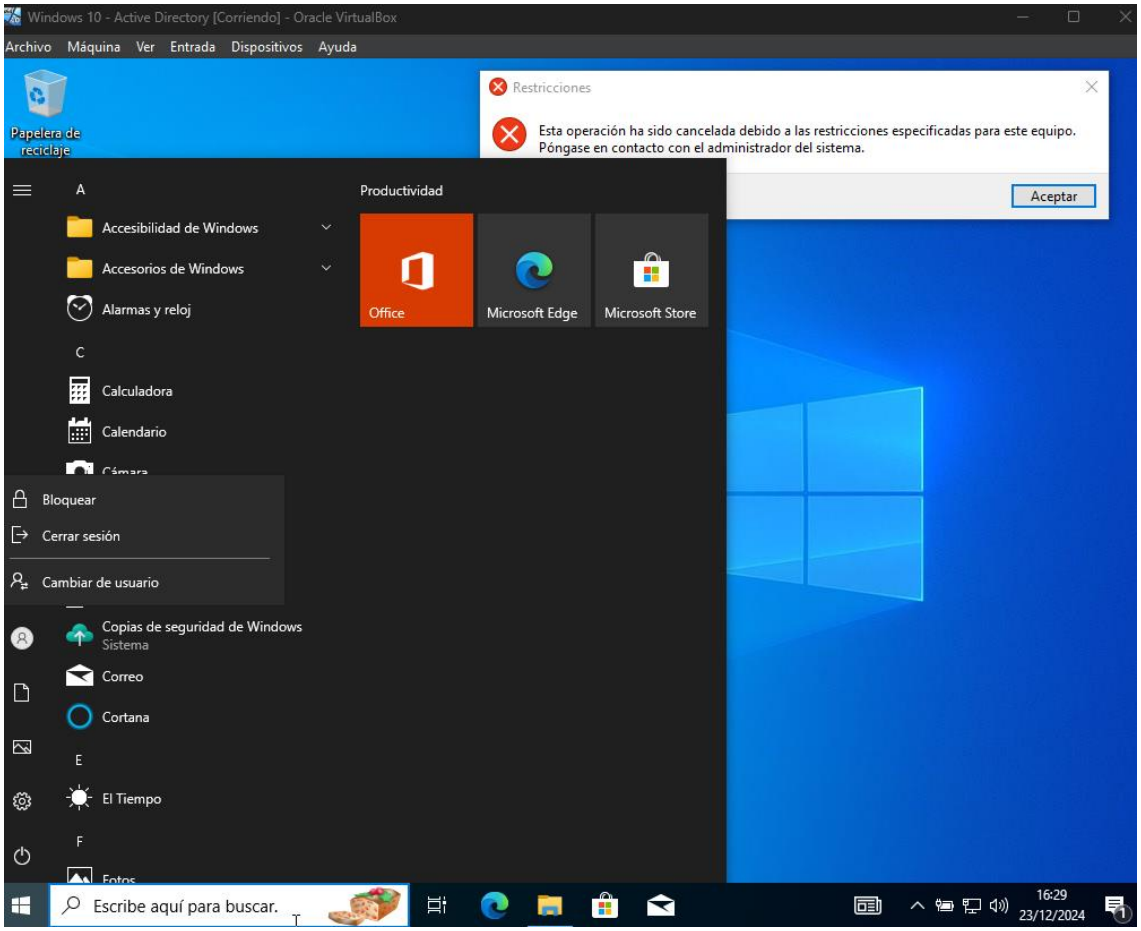
· Accede desde un cliente con algunos de los usuarios del dominio. ¿Qué prevalecerá: las directivas del dominio o las de la unidad organizativa?

Cuando accedemos desde un cliente utilizando un usuario del dominio que pertenece a una unidad organizativa, las directivas de esta unidad organizativa tendrán prioridad sobre las directivas generales del dominio. Si las directivas de la OU no definen una configuración específica, se aplicará la configuración establecida a nivel del dominio.

· Modifica el valor que prefieras del Panel de Control para el usuario.

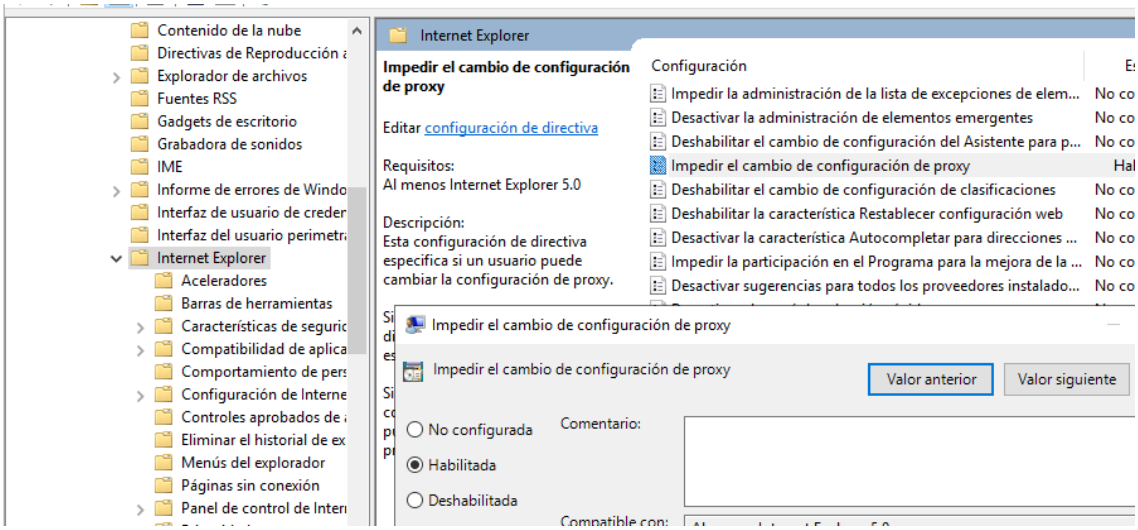
Cuando entro con un usuario de la unidad organizativa funcionará restringiendo el uso del panel de control.





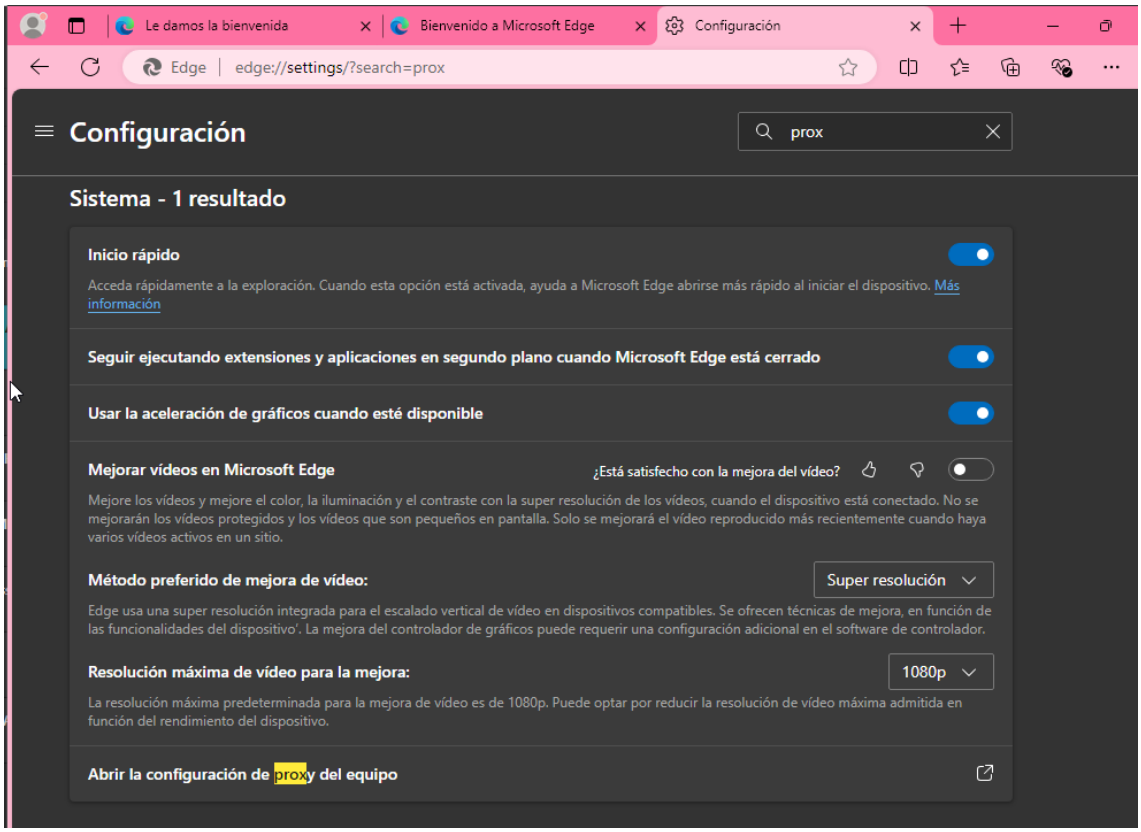
· Modifica las características de Internet Explorer de forma que el usuario no pueda tocar la configuración del Proxy.

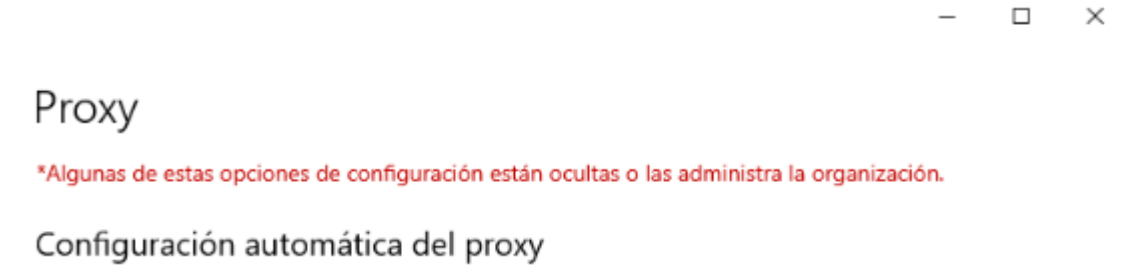
Habilitamos la opción.



· Accede desde cualquier cliente para comprobar los cambios.

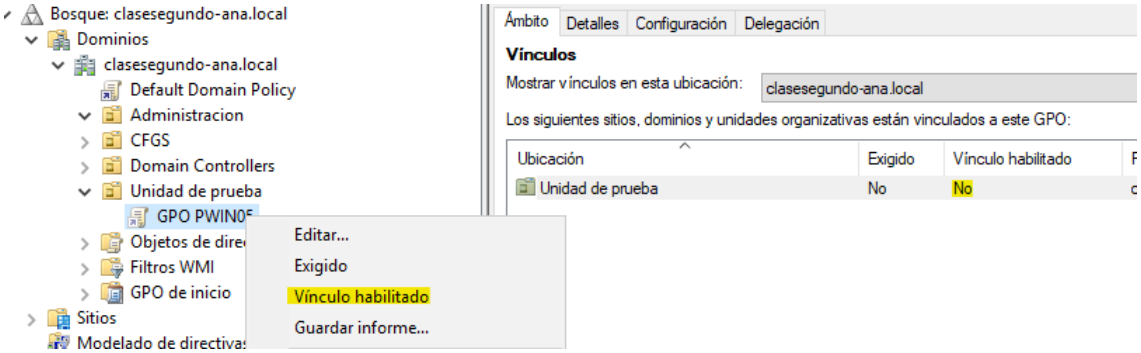
Lo probaré desde el navegador:



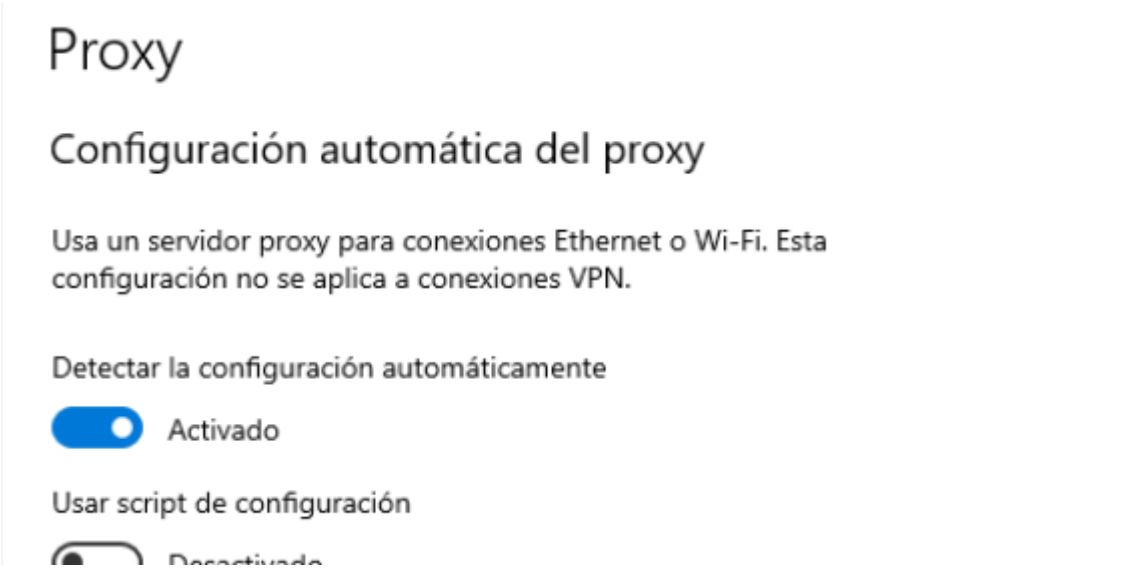


Quita el vínculo de la directiva de grupo que acabas de crear con el contenedor.

Hacemos clic derecho sobre la directiva de grupo y seleccionamos “Vínculo habilitado”.

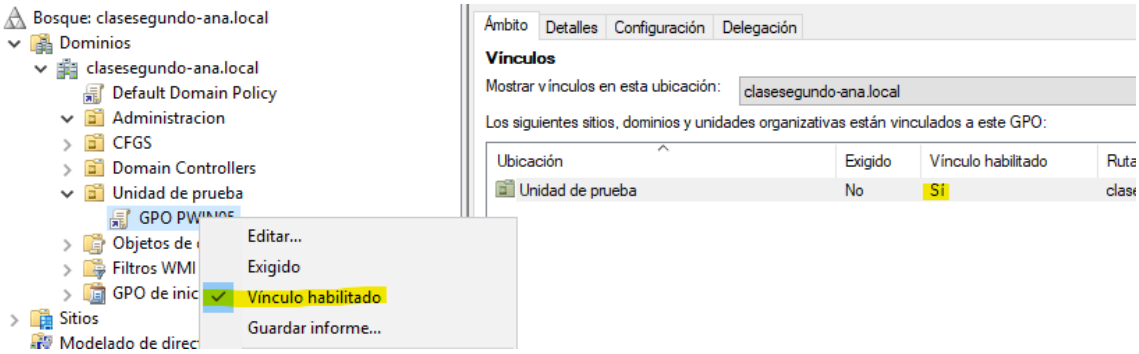


Ahora si intentamos acceder y editar el Proxy nos dejará:

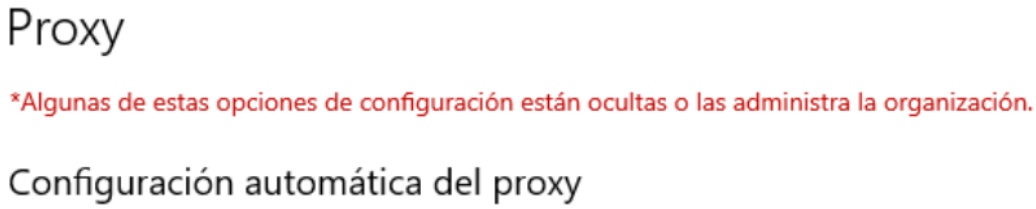


Vuelve a establecer el vínculo con el contenedor.

Para esto haremos clic de nuevo en vinculo habilitado:

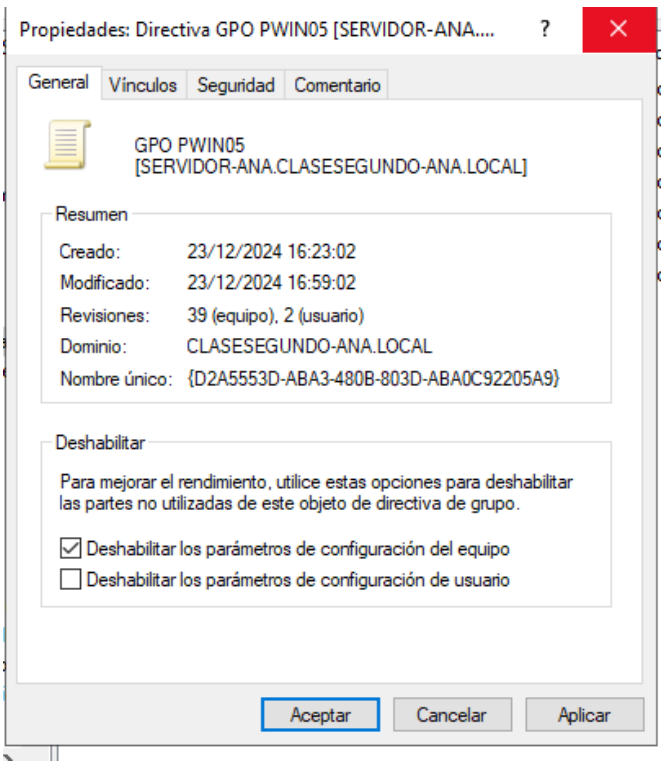


Y si probamos, nos dará el mismo error del Proxy.



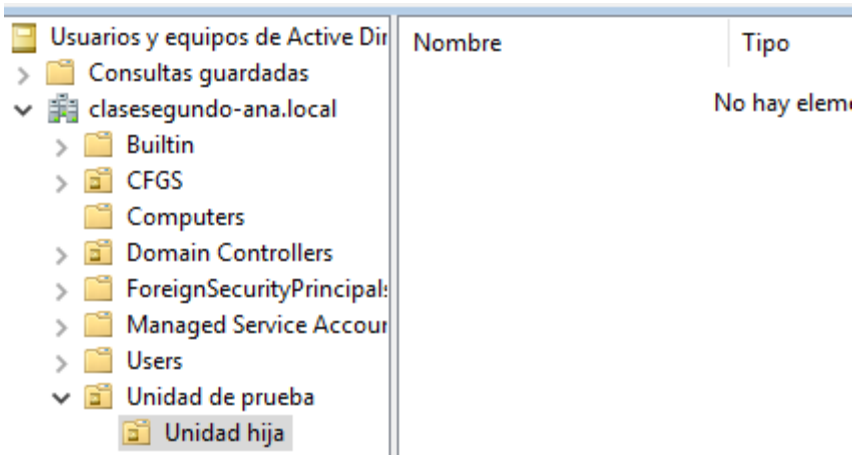
Deshabilita únicamente la configuración del equipo de la directiva de grupo.

Vamos a darle a propiedades y en general y le daremos a deshabilitar los parámetros del equipo.



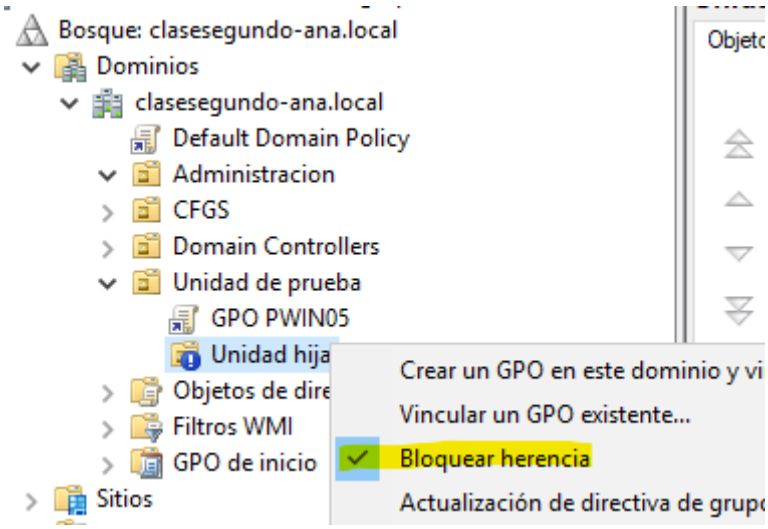
Crea una nueva Unidad Organizativa dentro de Unidad de prueba, llamándola Unidad hija.

Creamos dentro de unidad de prueba la unidad: “unidad hija”.



Bloquear la herencia de la Unidad hija. ¿Qué acabamos de hacer?

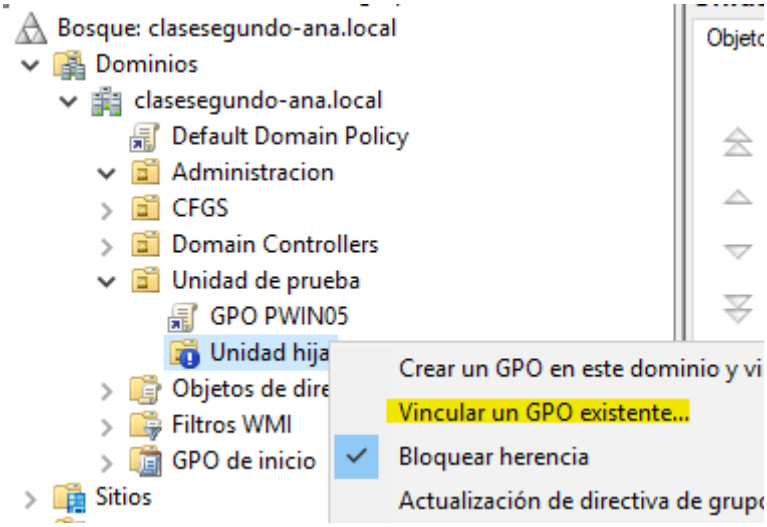
Esto garantiza que solo se apliquen las GPO creadas específicamente dentro de dicha unidad organizativa, evitando que se vean afectadas por otras directivas externas.



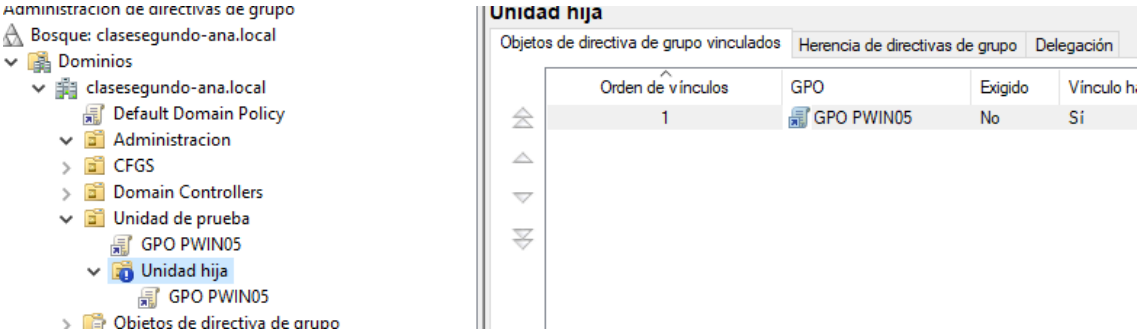
Vincular cualquiera de las directivas disponibles creadas anteriormente a la Unidad hija.

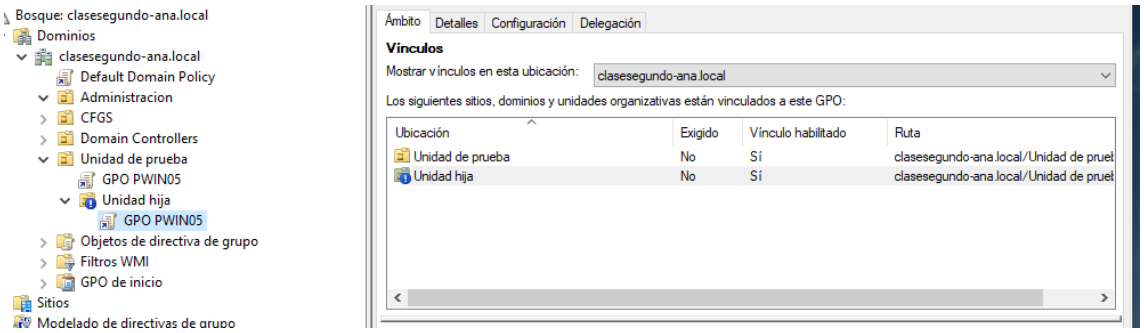
Asignaremos una de las directivas creadas previamente.

Para hacerlo, basta con hacer clic derecho sobre la unidad organizativa correspondiente y vincular la GPO seleccionada.



Mirar ahora a qué Unidades Organizativas se está aplicando esta última directiva.

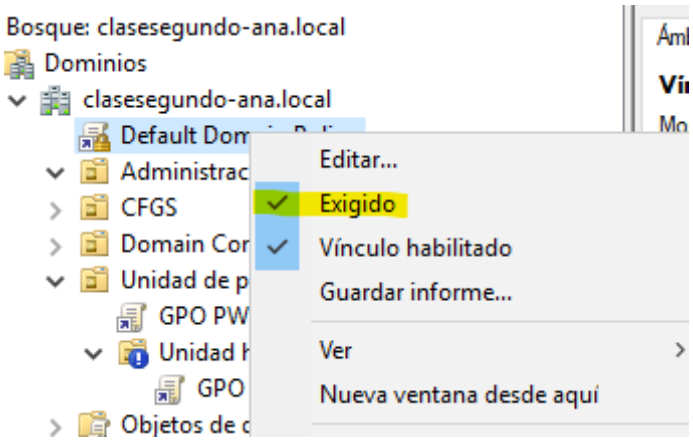




Como se aprecia en la imagen, aparecen ambas unidades.

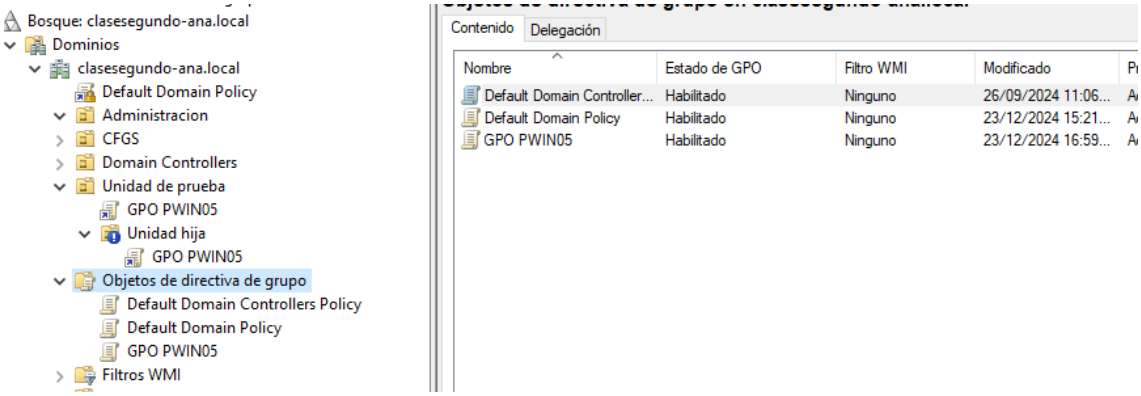
Hacer que la directiva Default Domain Policy sea siempre heredable para todas las Unidades Organizativas del dominio.

Cuando una directiva de grupo se configura como “Forzar”, tendrá prioridad sobre cualquier otra directiva que intente bloquear su herencia en una unidad organizativa (OU). Para establecer esta opción, simplemente hacemos clic derecho sobre la GPO y seleccionamos “Exigido”.

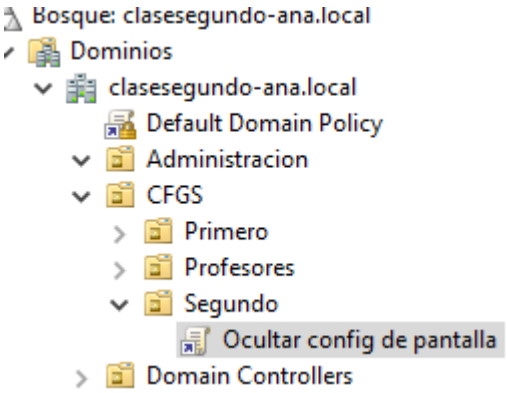


Obtener el listado de todas las directivas definidas.

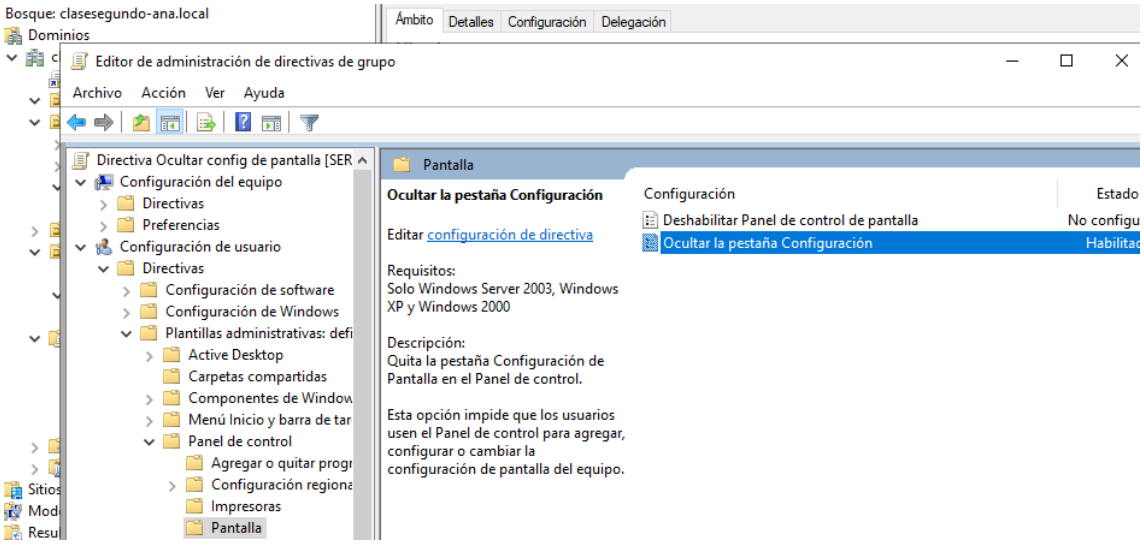
Podemos observar diferentes objetos de directiva de grupo, como los predefinidos, como Default Domain Policy, así como los personalizados, como Práctica WIN05.



Asignar la directiva de grupo Ocultar configuración de pantalla a los alumnos de segundo.

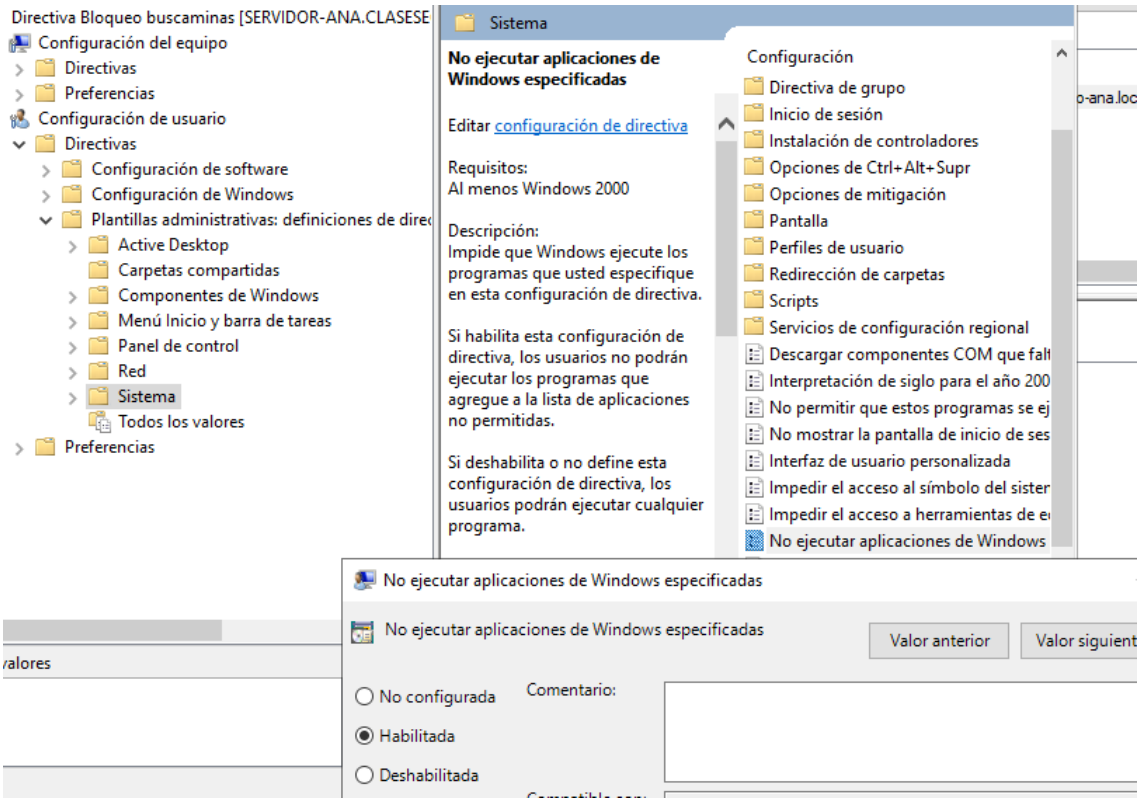


Vamos a editar la GPO y accedemos a “Conguración de usuario” → “Directivas” → “Plantillas administrativas” → “Panel de control” → “Ocultar la pestaña configuración” y lo activamos.

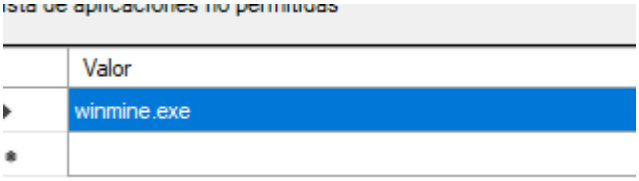


Crear, en la Unidad Organizativa CFGS, una directiva de grupo que impida el uso del Buscaminas a los alumnos. Los profesores sí podrán utilizarlo. Se deberá optimizar y explicar la solución propuesta.

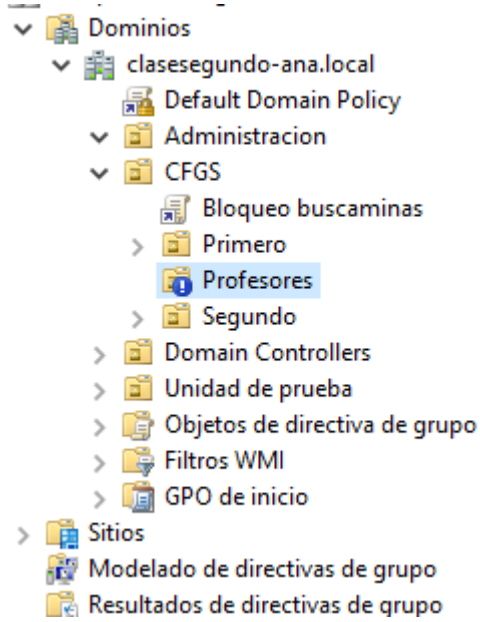
Para hacer eso iremos a Configuración de usuario → Directivas → Plantillas administrativas definiciones de directivas → Sistema y aquí habilitamos la opción de “no ejecutar aplicaciones de Windows especificadas”



Pondremos winmine.exe para bloquear el ejecutable del juego buscaminas, le daremos a aplicar.



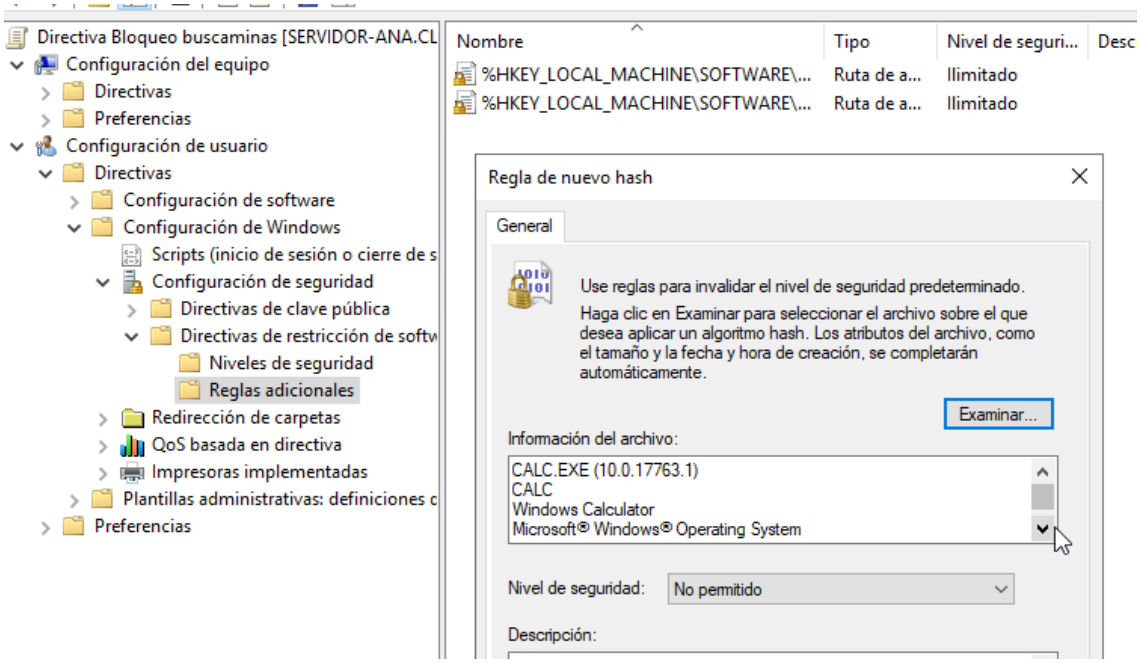
Para que esta política no funcione con los profesores debemos bloquear la herencia a profesores y así la regla solo se heredará a las unidades primero y segundo.



Crear una regla Hash para impedir el uso de la calculadora.

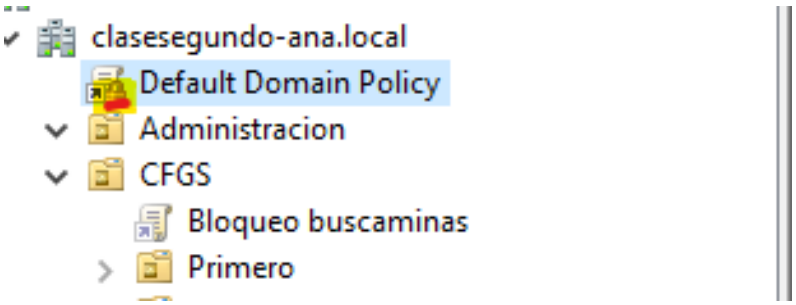
Para esto iremos a “Configuración de usuario” → “Directivas” → “Configuración de Windows” → “Configuración de seguridad” → “Directivas de restricción de software” → “Reglas adicionales” → “Crear nueva regla hash”.

Aquí le daremos a examinar y buscaremos calc:



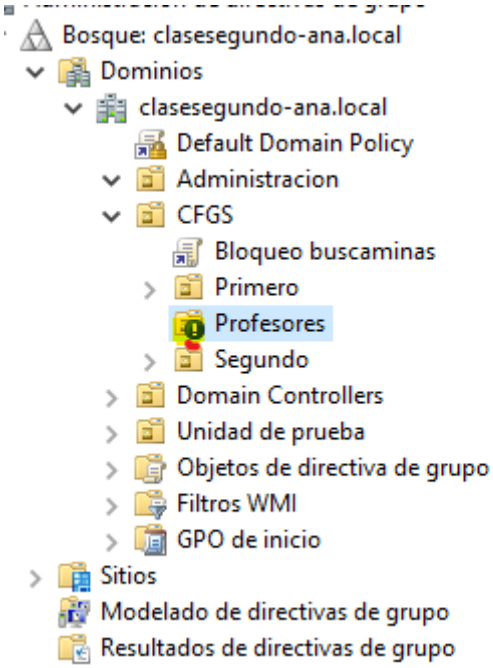
¿Cómo podemos saber que una Directiva de grupo está forzada?

Cuando una directiva está forzada tendrá un candado en su icono.



¿Cómo podemos saber que se ha bloqueado la herencia de una Unidad Organizativa?

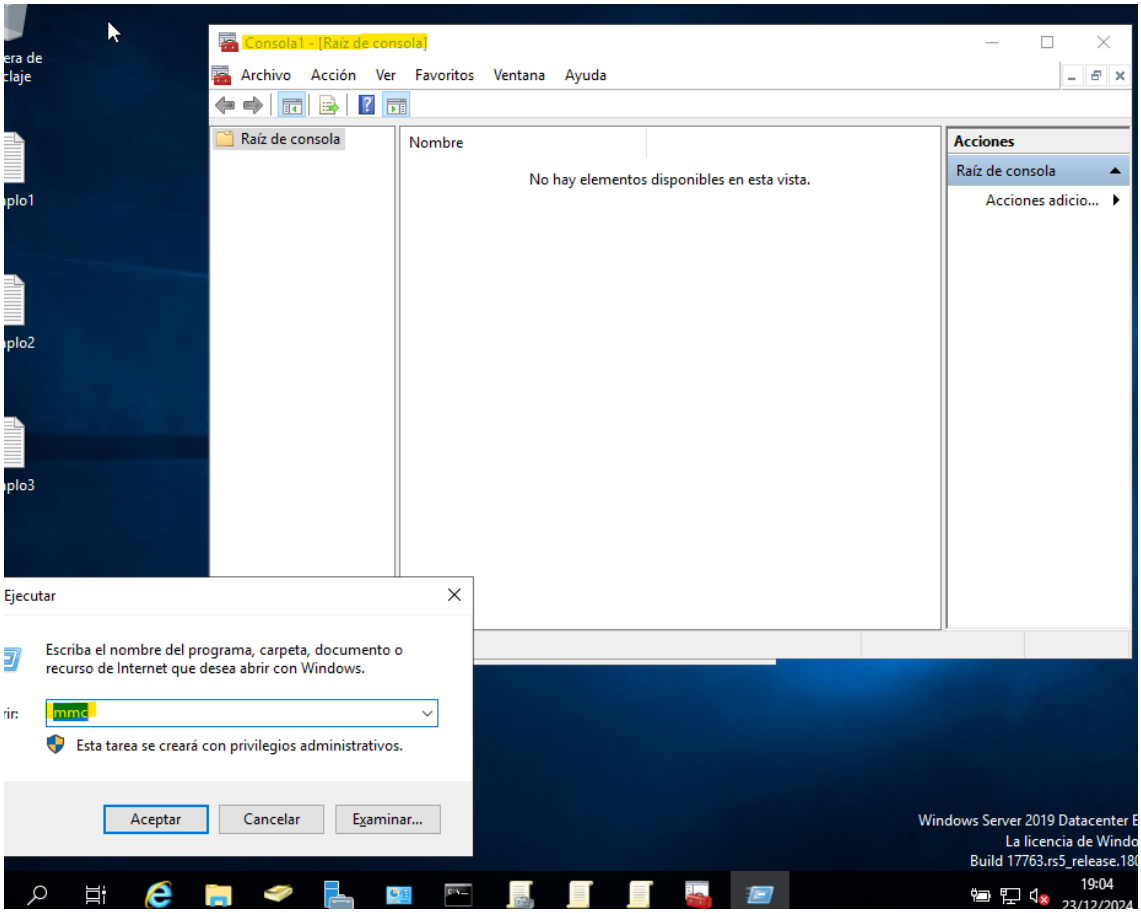
Porque aparecerá un círculo azul con una exclamación en su icono.



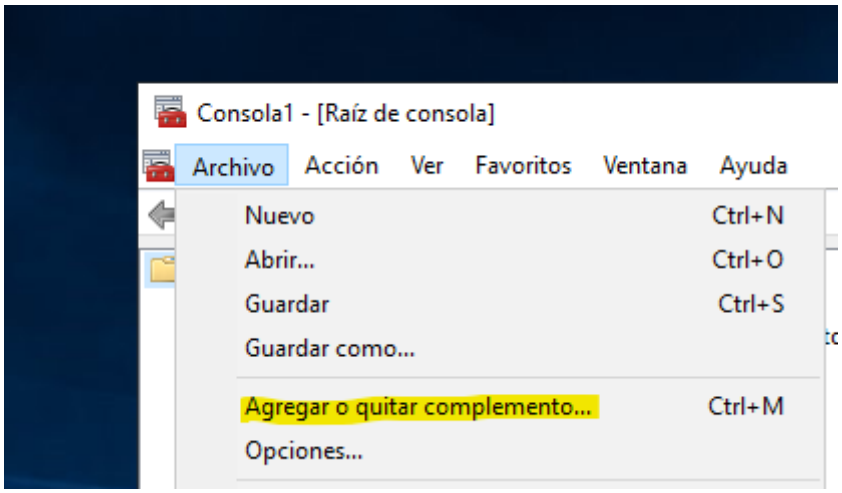
3. Plantillas de seguridad.

Crear una consola, en el equipo servidor, llamada Consola de Seguridad e incorporarle los complementos Plantillas de Seguridad y Configuración y análisis de seguridad.

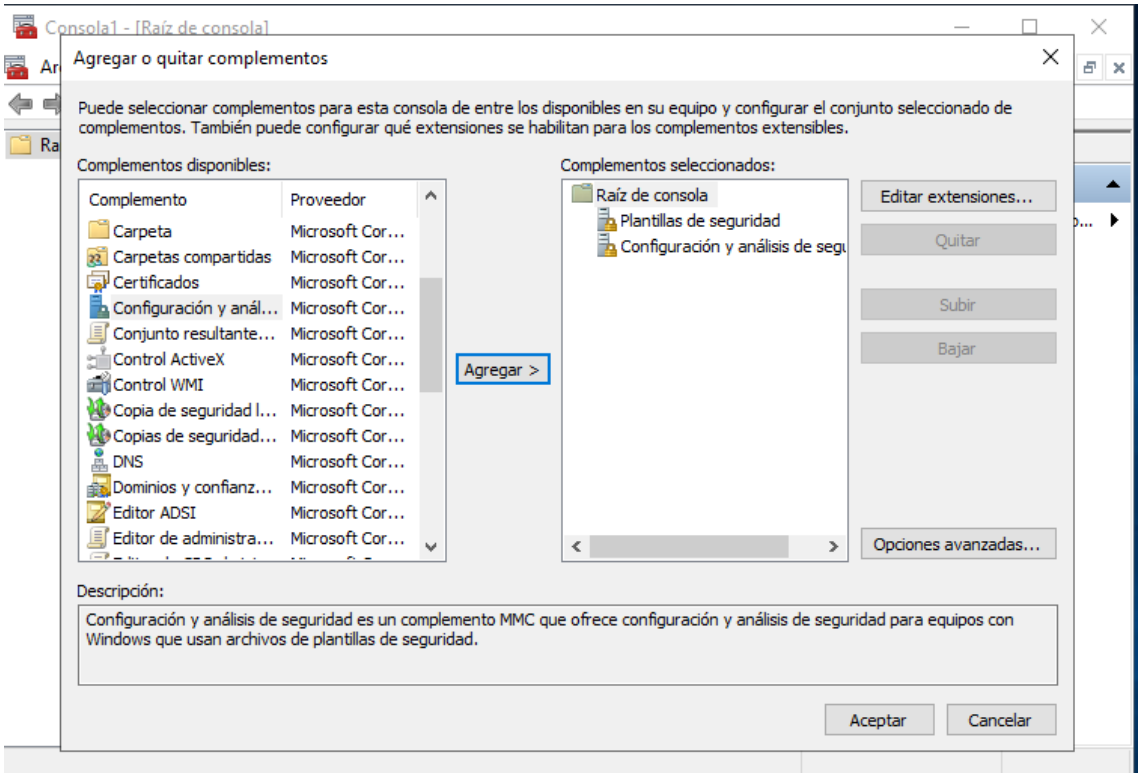
Para comenzar, presionaré Win + R para abrir el cuadro de ejecución y escribiré mmc.



Una vez dentro, seleccionaré Archivo > Agregar o quitar completo...

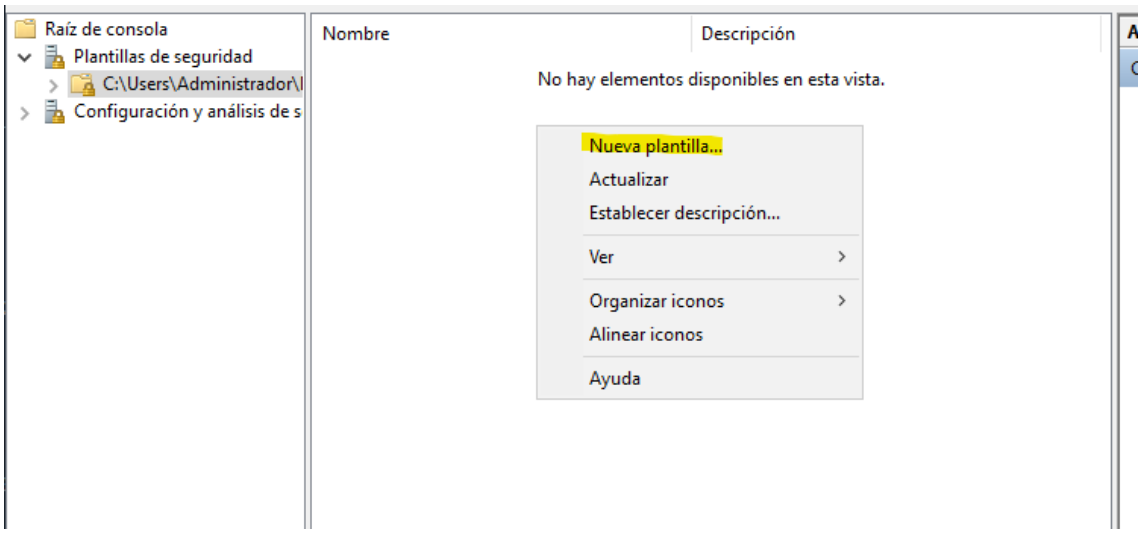


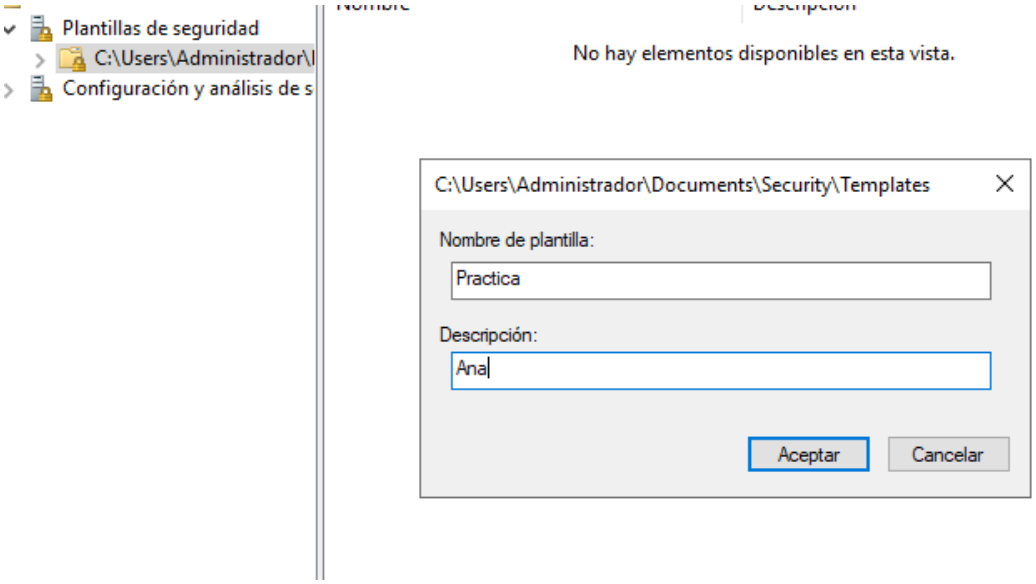
Ahora agregaremos “Plantillas de seguridad” y “Configuración y análisis de seguridad” y le daré a aceptar.



Crear con el complemento Plantillas de Seguridad una nueva plantilla llamada Práctica.

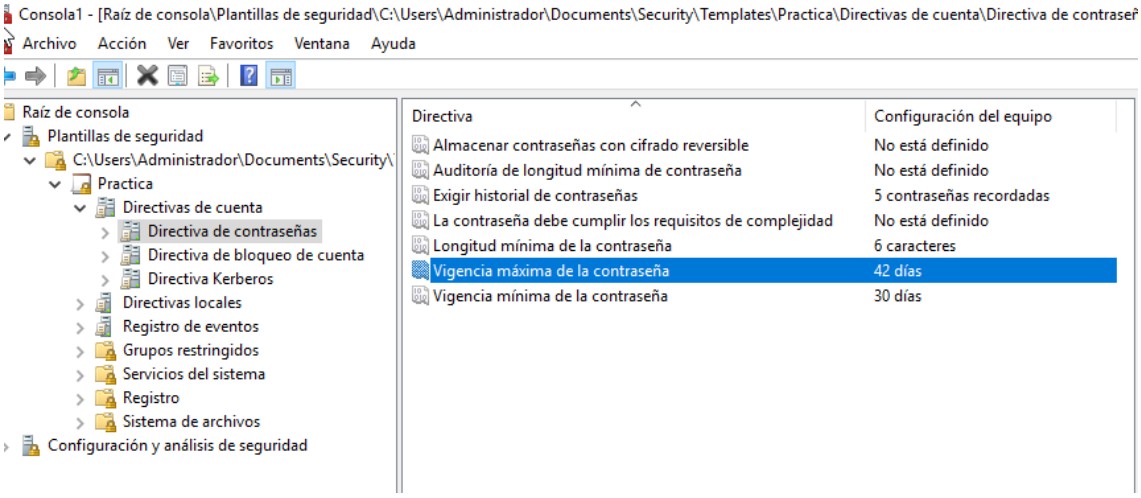
Para ello haremos clic derecho dentro de la carpeta Plantillas de seguridad y seleccionaremos Crear nueva plantilla. Le daremos el nombre Práctica a la nueva plantilla.

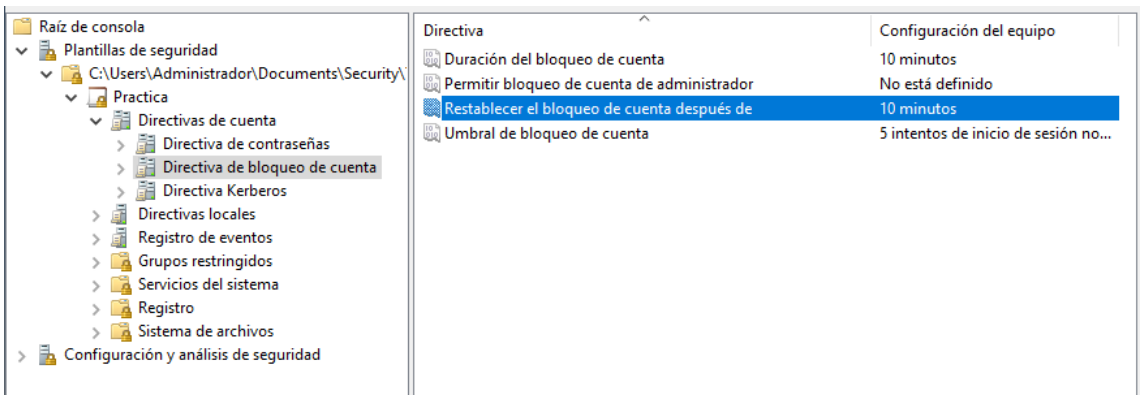




Configurar la plantilla creada modificando las directivas de contraseña y de bloqueo de cuenta de acuerdo con los criterios del alumno (hay que indicarlos).

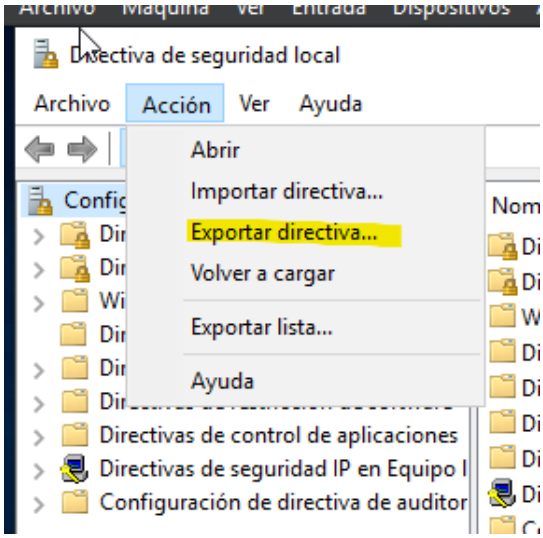
Al abrir la plantilla Práctica, veremos las directivas disponibles. Editaremos algunas de ellas según nuestras preferencias y, al finalizar, guardaremos los cambios.

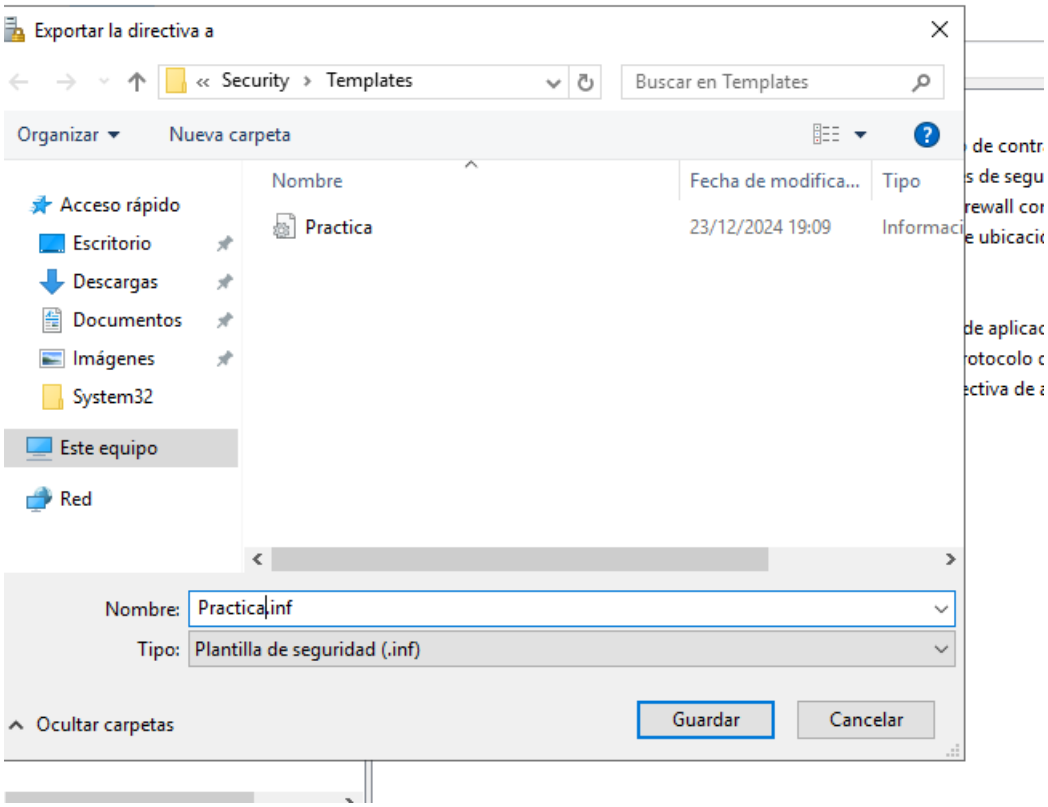




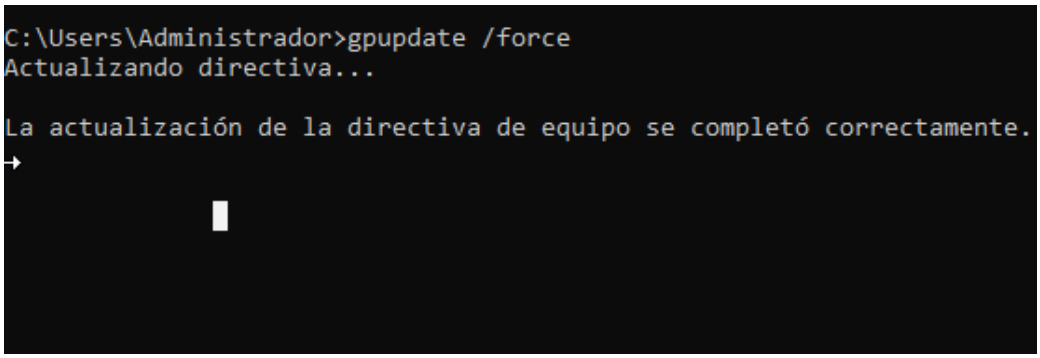
Exportar las características definidas en la plantilla a las Directivas de Seguridad del dominio. Hay que hacer una comparación mediante capturas de pantallas de la configuración de seguridad del dominio antes y después de la exportación. ¿Qué quiere decir lo que hemos hecho?

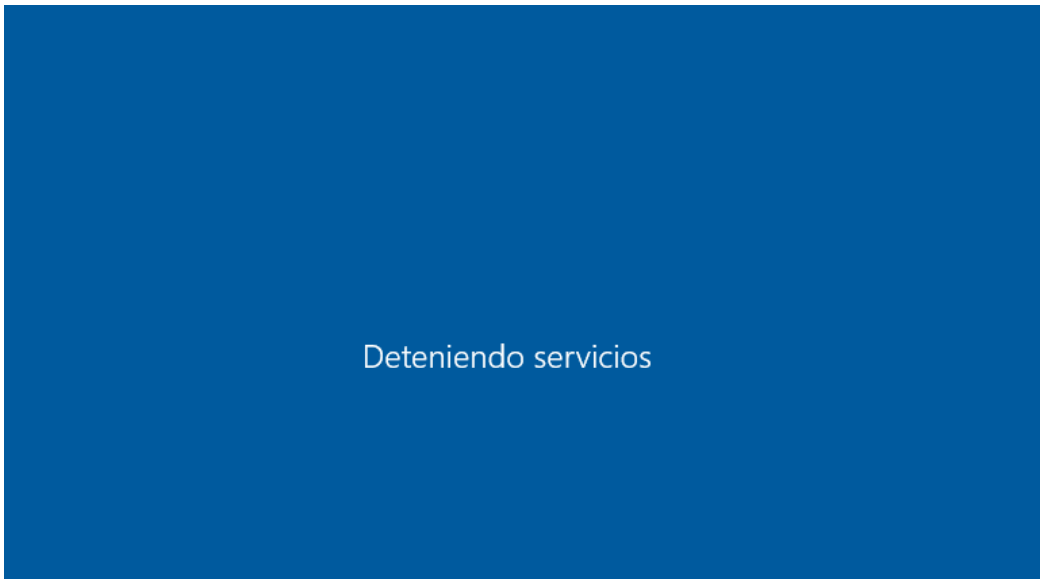
Entraremos en Directivas de seguridad y seleccionaremos la opción Importar (asegurándonos de haber guardado previamente la consola). Luego, cargaremos la consola llamada Práctica.





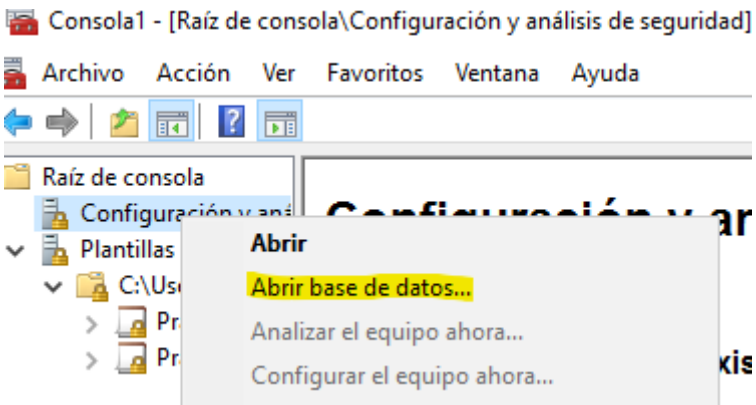
Haremos gpupdate /force para aplicar los cambios y reiniciará el servidor.

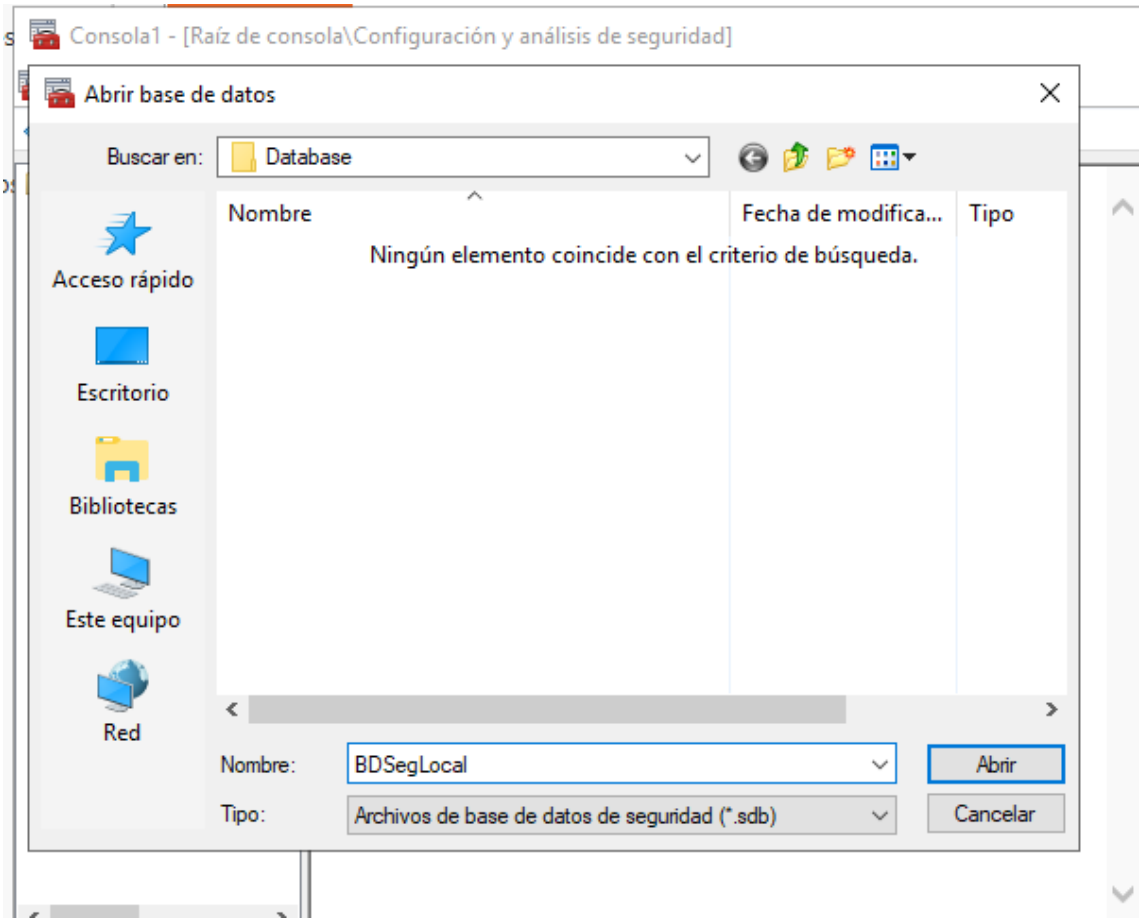


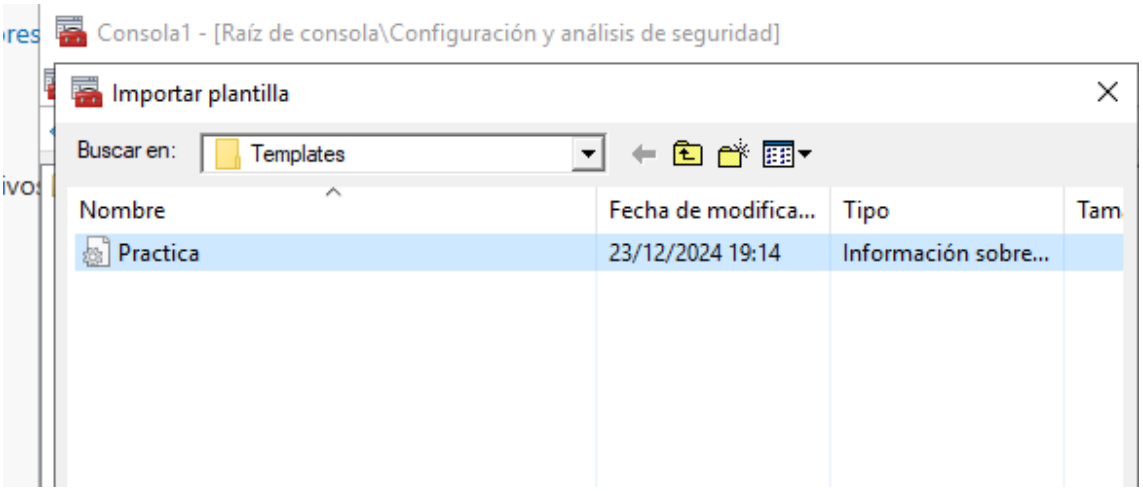


Crear con el complemento Configuración y análisis de Seguridad, una base de datos llamada BDSegLocal, e importar la plantilla Práctica.

Haremos clic derecho sobre el complemento Configuración y análisis de seguridad de nuestra consola y seleccionaremos Abrir base de datos. Aquí añadiremos el nombre que deseemos.

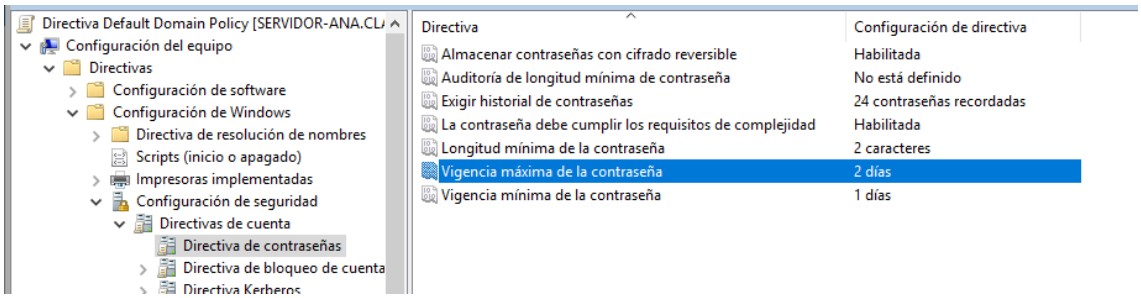



Consola1 - [Raíz de consola\Configuración y análisis de seguridad]
Abrir base de datos
Buscar en:
Database
Nombre
Fecha de modifica...
Tipo
Ningún elemento coincide con el criterio de búsqueda.
Acceso rápido
Escritorio
Bibliotecas
Este equipo
Red
Nombre:
BDSegLocal
Abrir
Tipo:
Archivos de base de datos de seguridad (*.sdb)
Cancelar


Consola1 - [Raíz de consola\Configuración y análisis de seguridad]
Importar plantilla
Buscar en:
Templates
Nombre
Fecha de modifica...
Tipo
Tam
Practica
23/12/2024 19:14
Información sobre...

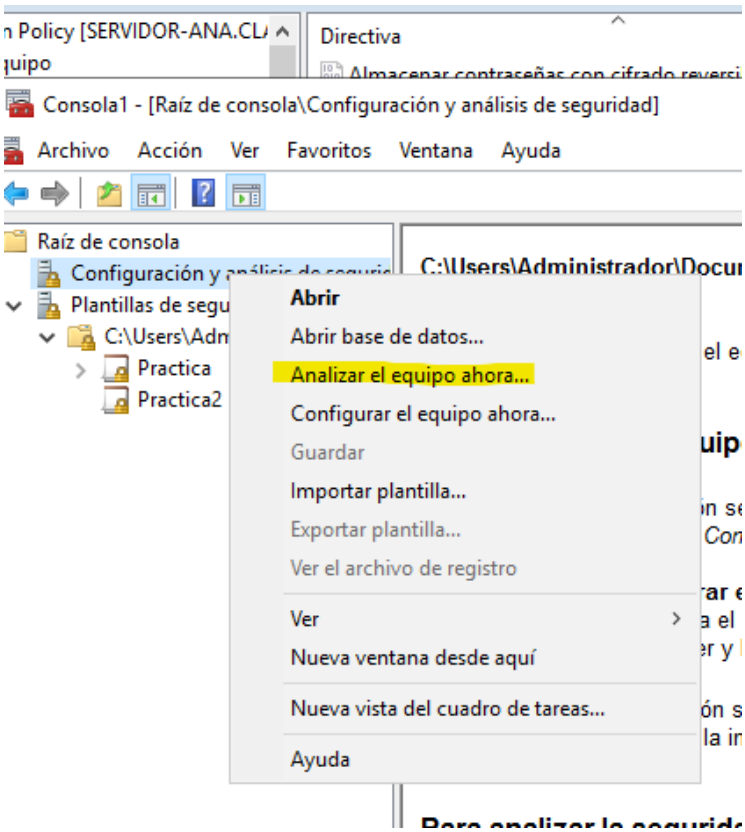
Realiza la configuración local del equipo, modificando características de las contraseñas para que se provoquen errores.

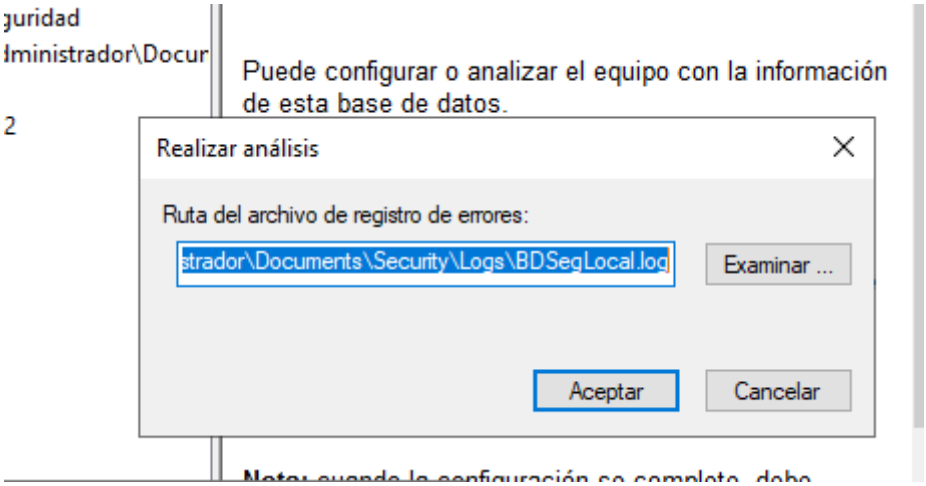
Lo modifico para que provoque algún error.

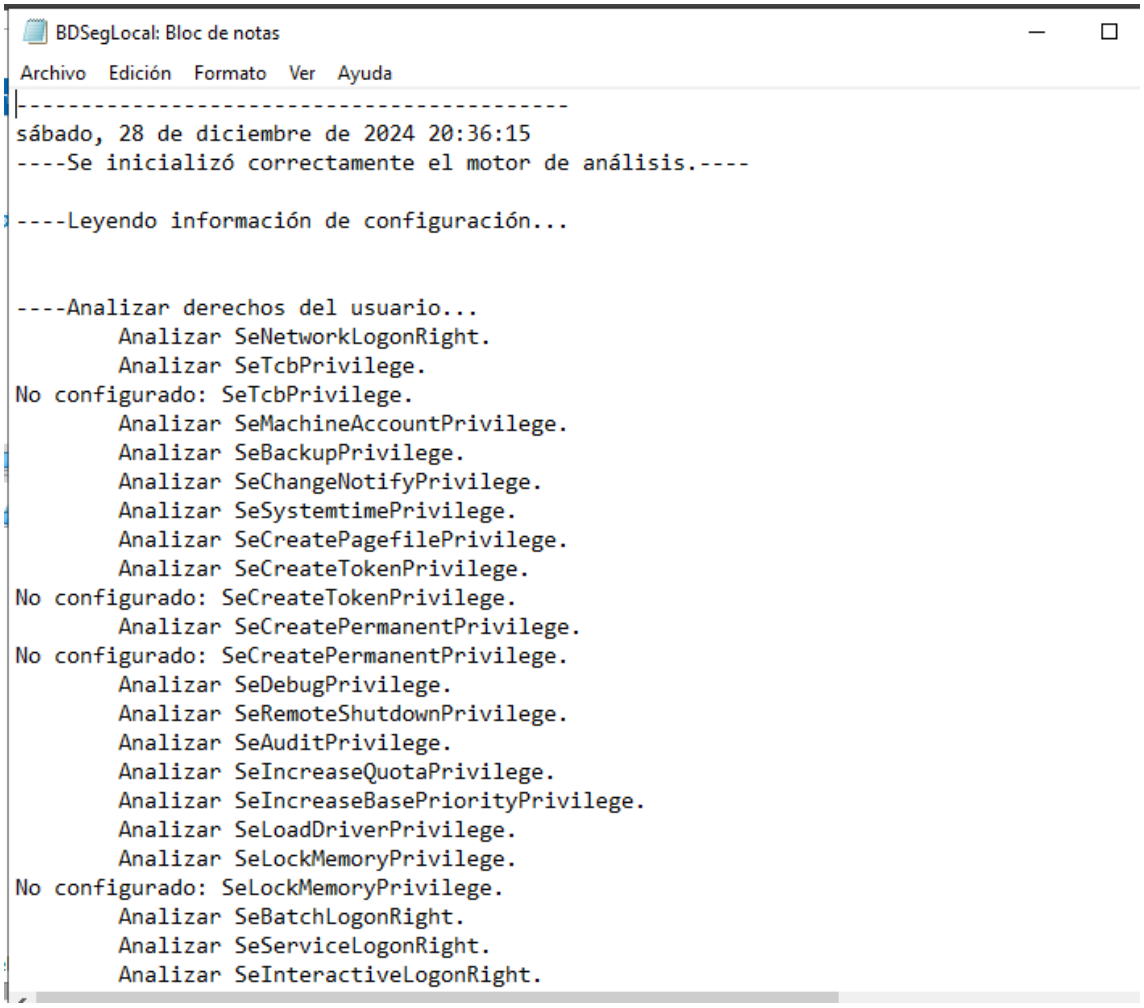


Realiza el análisis del equipo en base a la configuración establecida y genera el archivo errores de seguridad local.log. Analiza los errores producidos y toma las medidas necesarias para que no se vuelvan a producir.

Para realizar el análisis, haremos clic derecho en Configuración y análisis del equipo y seleccionaremos Realizar análisis. El sistema nos pedirá que indiquemos la ubicación donde se guardará el análisis.



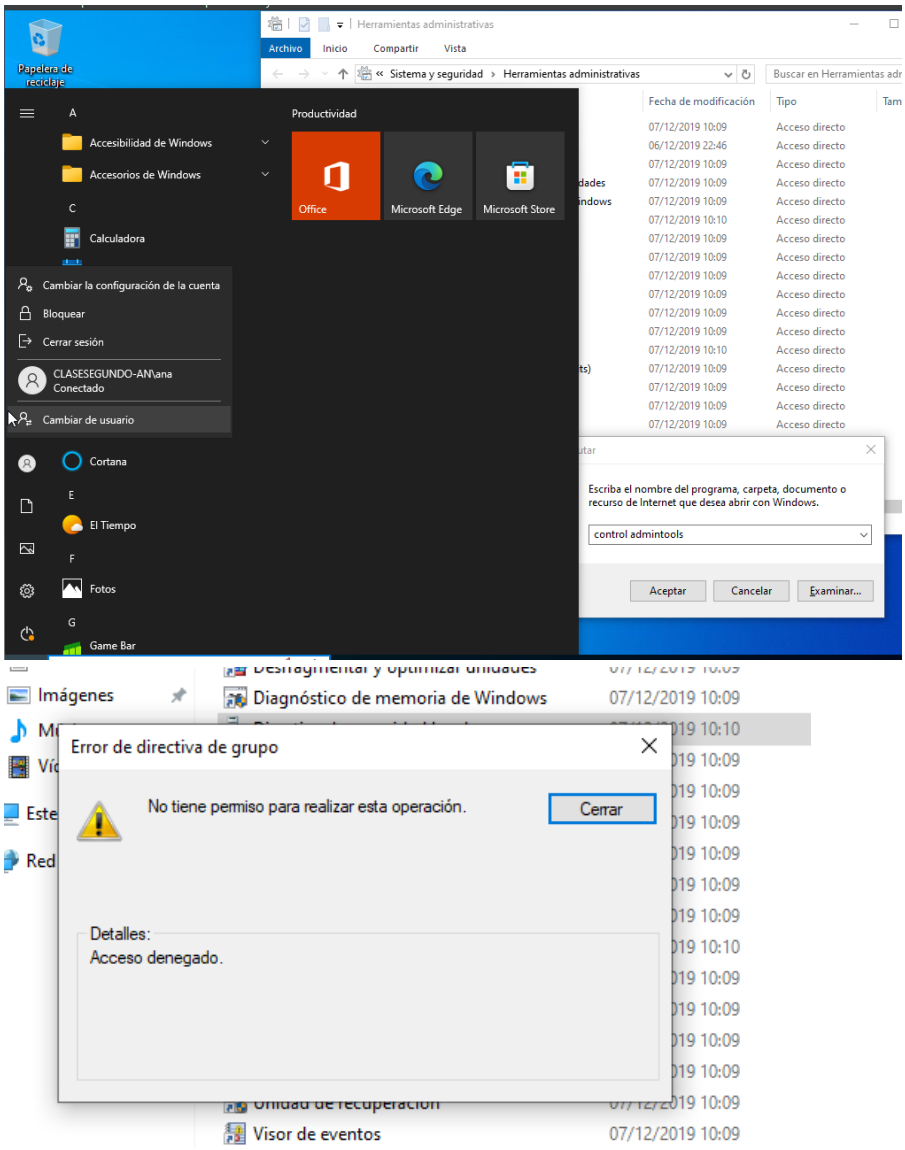

guridad
dministrador\Docur
2
Puede configurar o analizar el equipo con la información de esta base de datos.
Realizar análisis
Ruta del archivo de registro de errores:
strador\Documents\Security\Logs\BDSegLocal.log
Examinar ...
Aceptar
Cancelar


BDSegLocal: Bloc de notas
Archivo Edición Formato Ver Ayuda
----
sábado, 28 de diciembre de 2024 20:36:15
----Se inicializó correctamente el motor de análisis.----
----Leyendo información de configuración...
----Analizar derechos del usuario...
Analizar SeNetworkLogonRight.
Analizar SeTcbPrivilege.
No configurado: SeTcbPrivilege.
Analizar SeMachineAccountPrivilege.
Analizar SeBackupPrivilege.
Analizar SeChangeNotifyPrivilege.
Analizar SeSystemtimePrivilege.
Analizar SeCreatePagefilePrivilege.
Analizar SeCreateTokenPrivilege.
No configurado: SeCreateTokenPrivilege.
Analizar SeCreatePermanentPrivilege.
No configurado: SeCreatePermanentPrivilege.
Analizar SeDebugPrivilege.
Analizar SeRemoteShutdownPrivilege.
Analizar SeAuditPrivilege.
Analizar SeIncreaseQuotaPrivilege.
Analizar SeIncreaseBasePriorityPrivilege.
Analizar SeLoadDriverPrivilege.
Analizar SeLockMemoryPrivilege.
No configurado: SeLockMemoryPrivilege.
Analizar SeBatchLogonRight.
Analizar SeServiceLogonRight.
Analizar SeInteractiveLogonRight.

4.Ejecutar como.

En un cliente, inicia sesión como un usuario sin privilegios de administrador y utiliza Ejecutar como para acceder a las utilidades de Herramientas administrativas. (Hay que detallar las tareas realizadas).

Vamos a un cliente sin privilegios, abriremos Ejecutar y buscaremos control admintools.

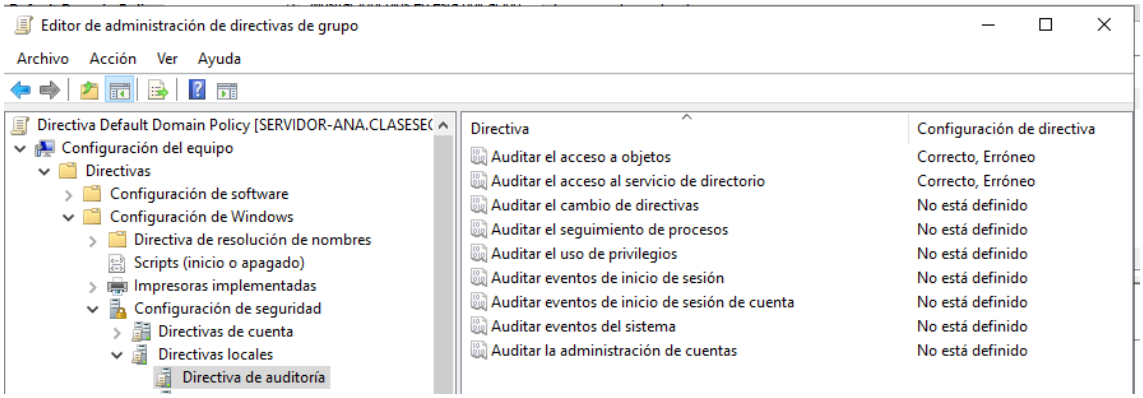


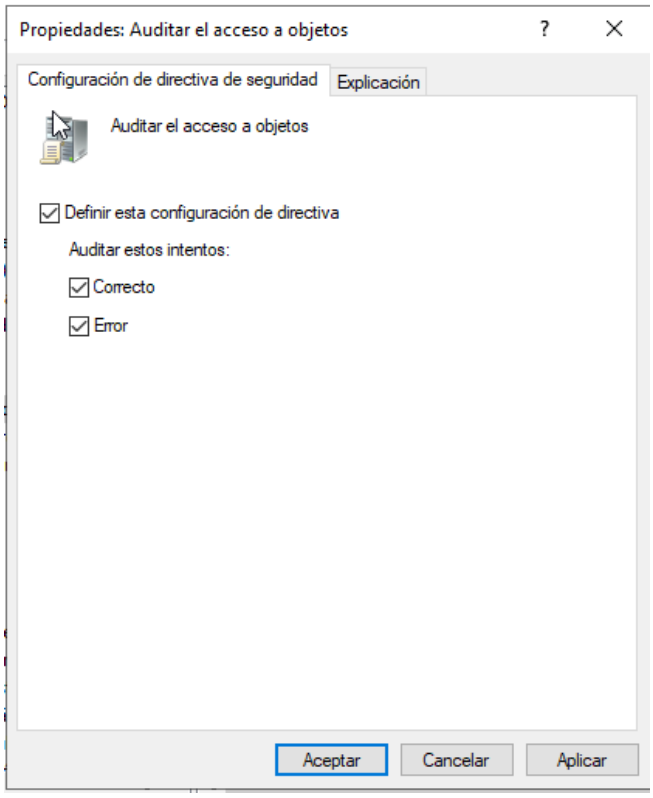
Al intentar acceder a algunas herramientas, aparecerá un error de permisos o se nos solicitará ingresar un usuario y contraseña con privilegios de administrador.

5.Auditorías.

Habilita las directivas Auditar el acceso a objetos y Auditar el acceso del servicio de directorio para todos los equipos del dominio.

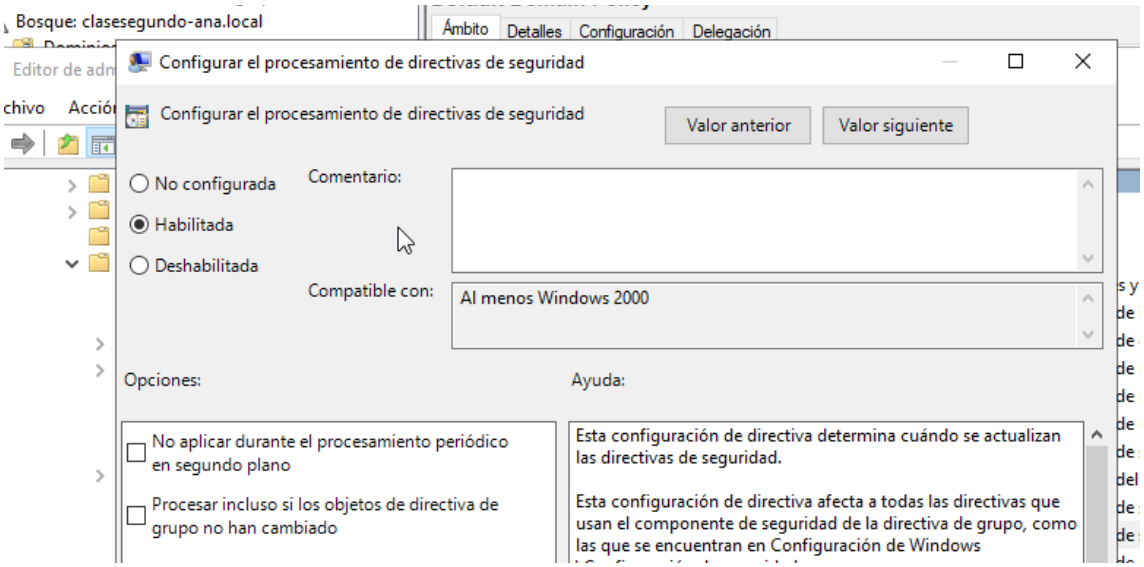
Para ello, modificamos la "Política de dominio predeterminada" y accedemos a la "Configuración del equipo", luego a "Configuración de Windows", después a "Configuración de seguridad", luego a "Directivas locales" y finalmente a "Directiva de auditorías". En este punto, habilitamos las opciones "Correcto" y "Erróneo" para las directivas "Auditar el acceso a objetos" y "Auditar el acceso al servicio del directorio".





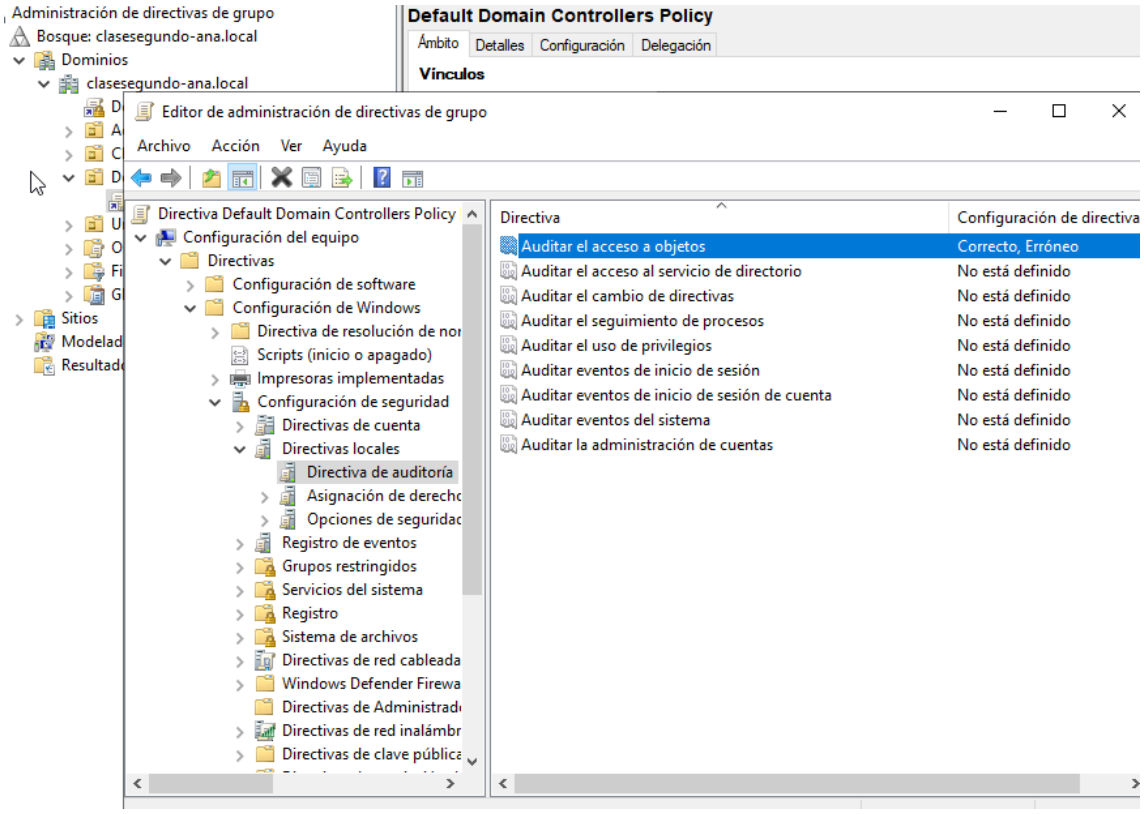
Configurar el procesamiento de las directivas de seguridad con sus valores predeterminados por defecto para la sincronización de las directivas de grupo.

A continuación, habilitamos la opción "Configurar el procesamiento de directivas" en "Configuración de equipo", luego accedemos a "Directivas", después a "Plantillas administrativas definiciones", luego a "Sistema" y finalmente a "Directivas de grupo".



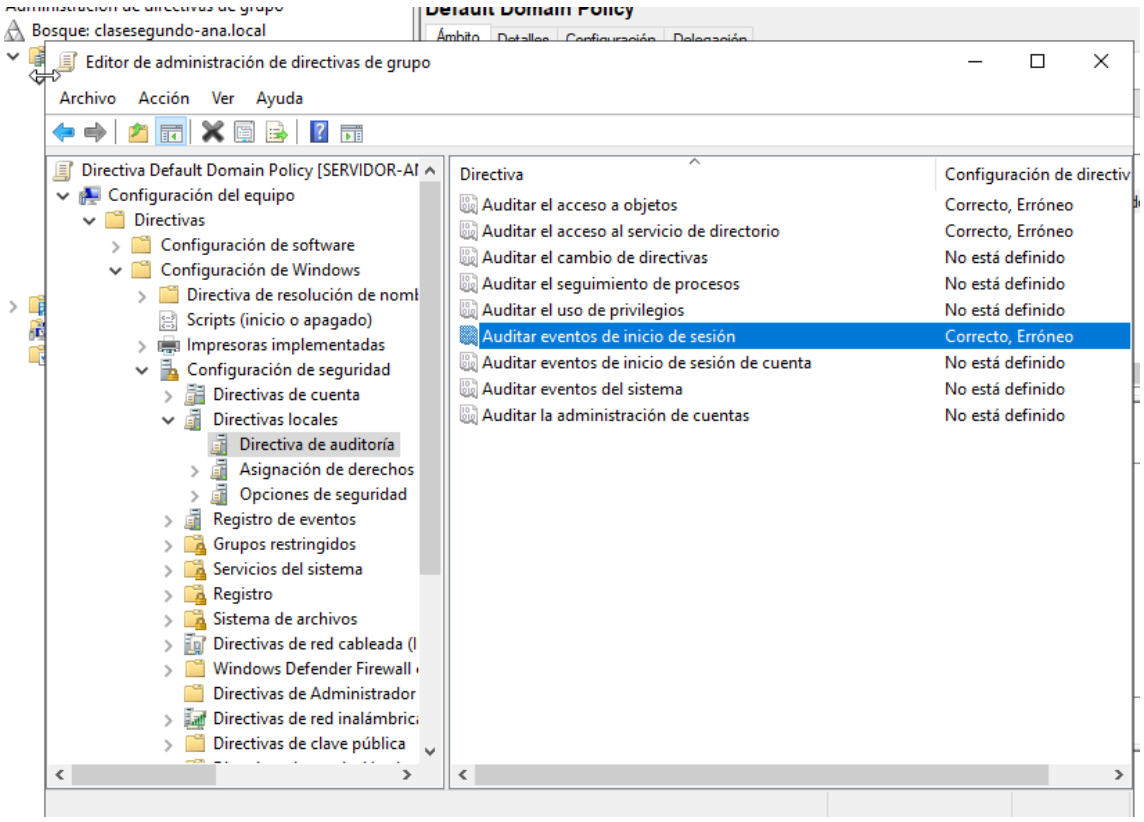
Auditar el acceso a objetos (correcto y errores) para el controlador de dominio. ¿Qué conseguimos con ello?

A continuación, volveremos a habilitar las opciones "Correcto" y "Erróneo" para la directiva "Auditar el acceso a objetos", pero esta vez desde la "Política de controladores de dominio predeterminada", con el fin de que aparezca el registro de auditoría de acceso a objetos de los controladores de dominio.

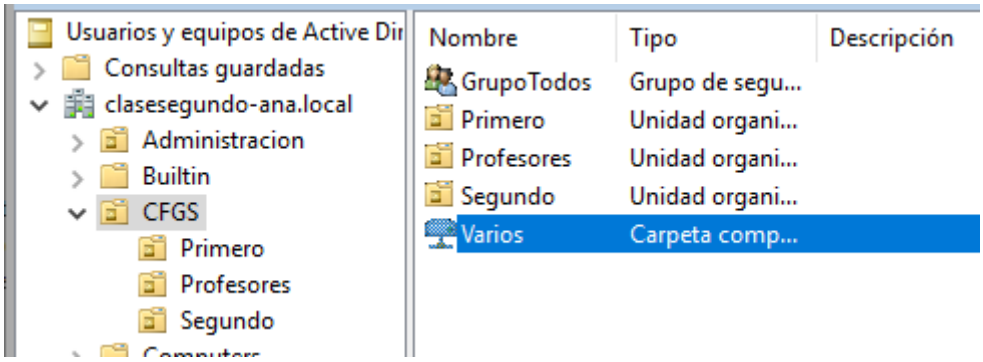


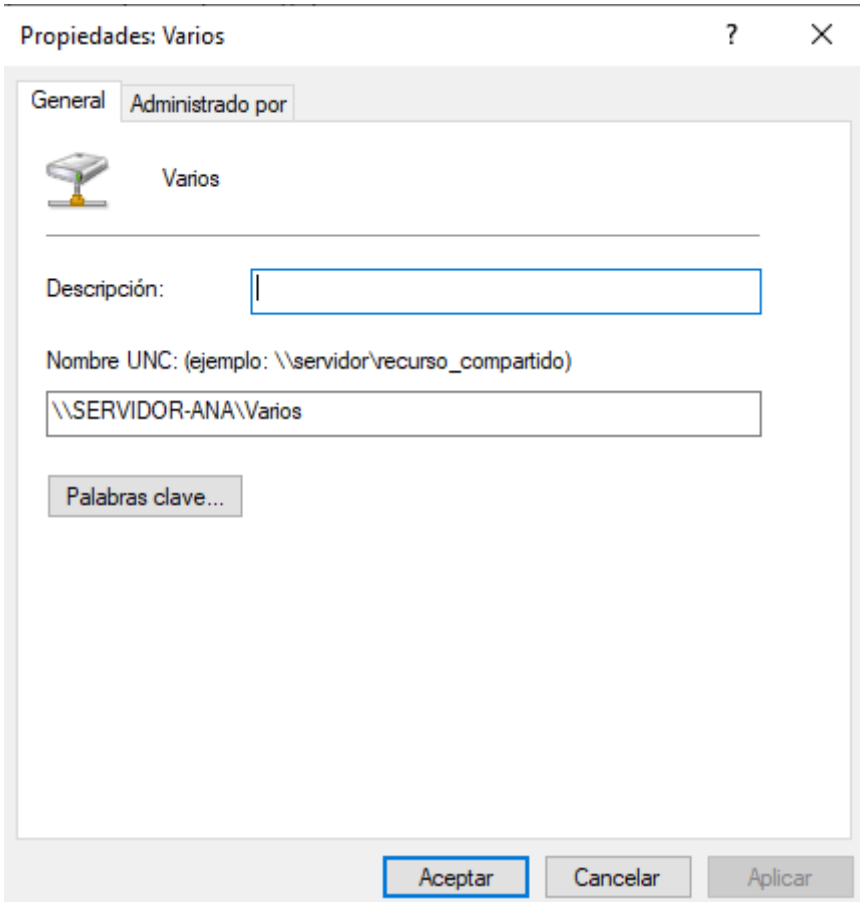
Auditar los errores de inicio de sesión en el servidor.

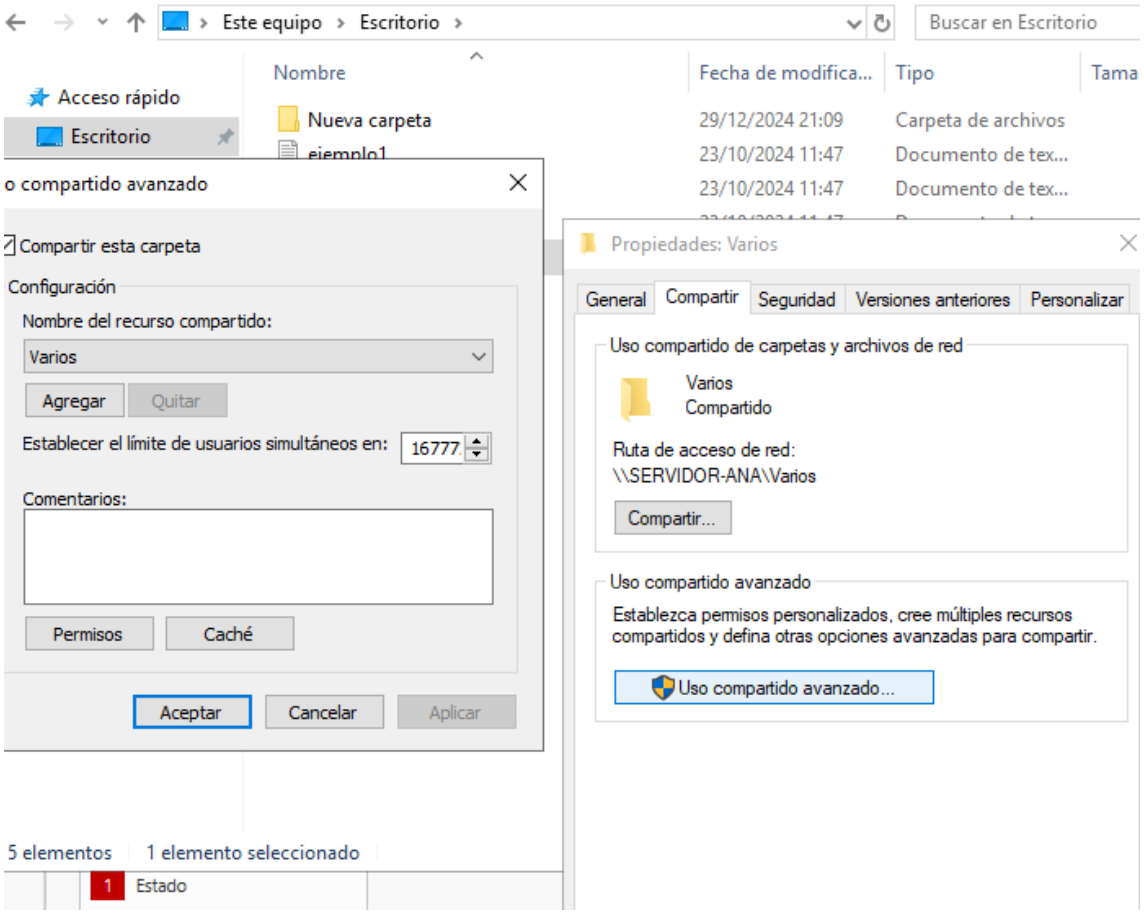
Para ello, accedemos a "Directivas", luego a "Configuración de Windows", después a "Configuración de seguridad" y modificamos la "Directiva de auditoría", seleccionando la opción que muestre los errores y éxitos durante el inicio de sesión.



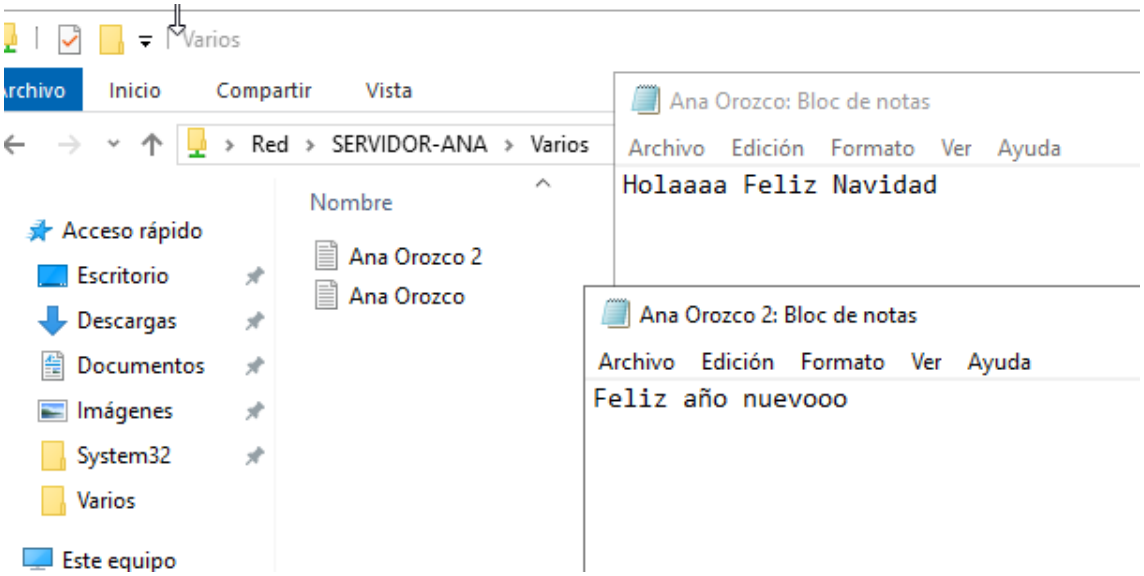
Crear una carpeta Varios en el directorio CFGS del servidor. Con ella:



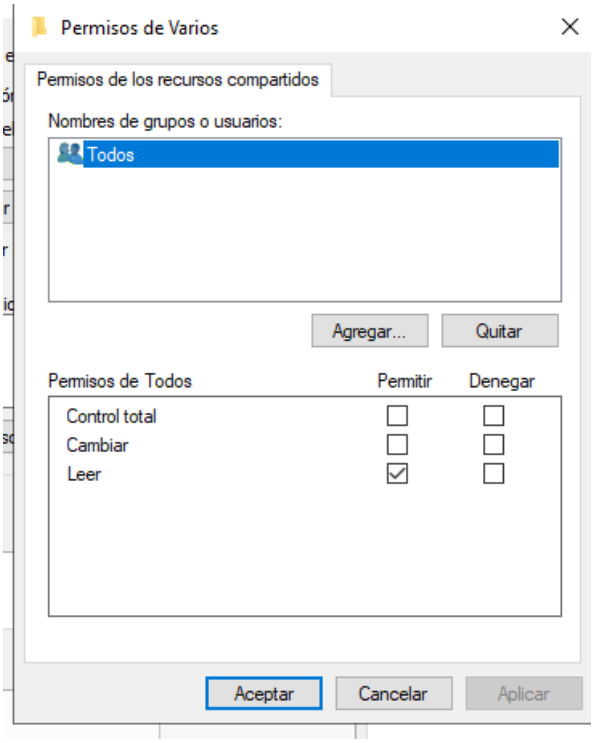




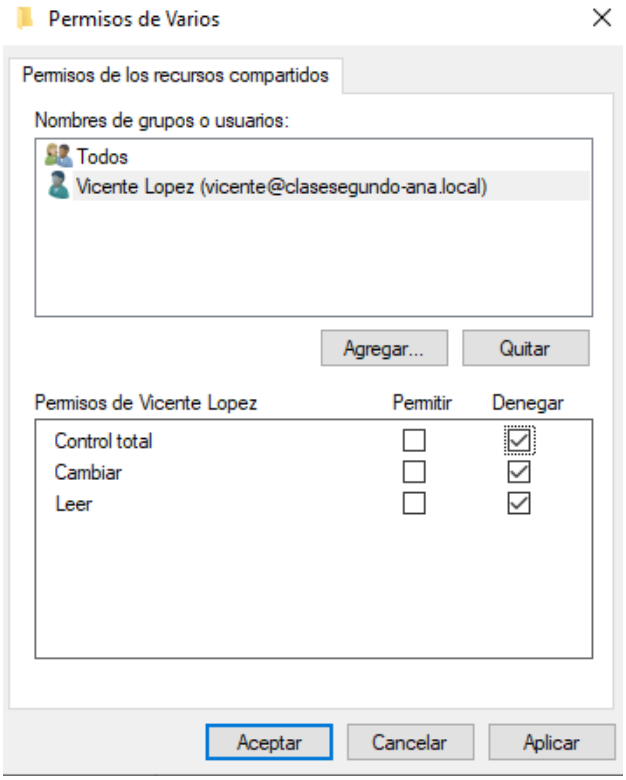
- Crear algunos archivos de texto en su interior que contengan, al menos, una línea.



- Compartirla para todos los usuarios con permisos únicamente de lectura

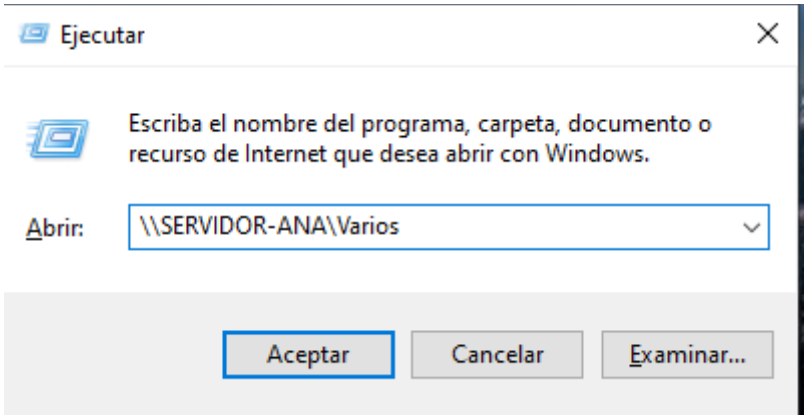


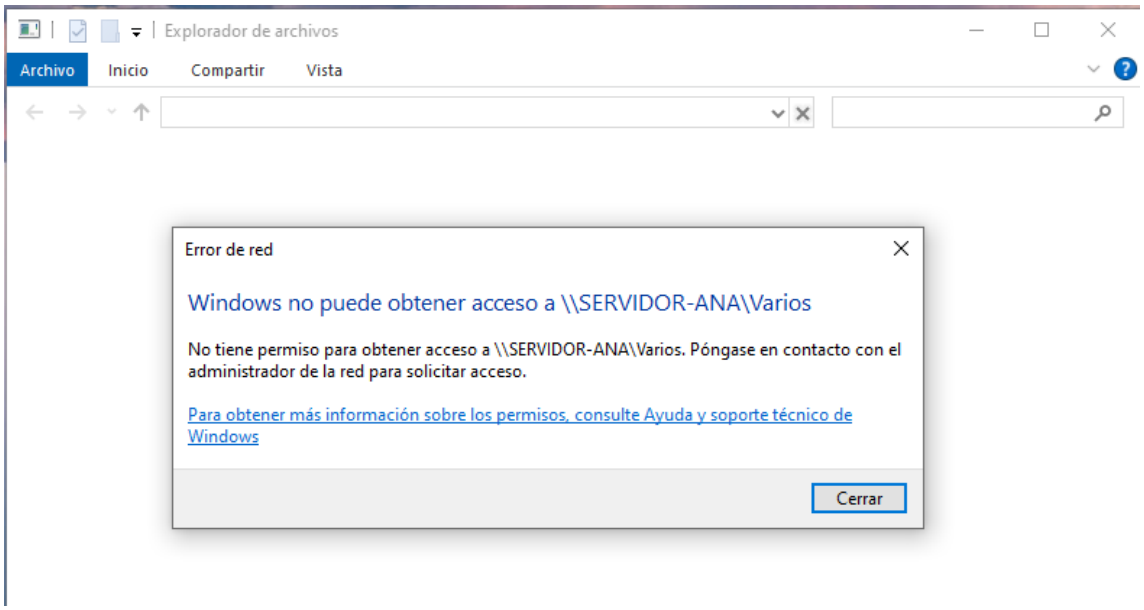
- Quitar todos los permisos al usuario Vicente



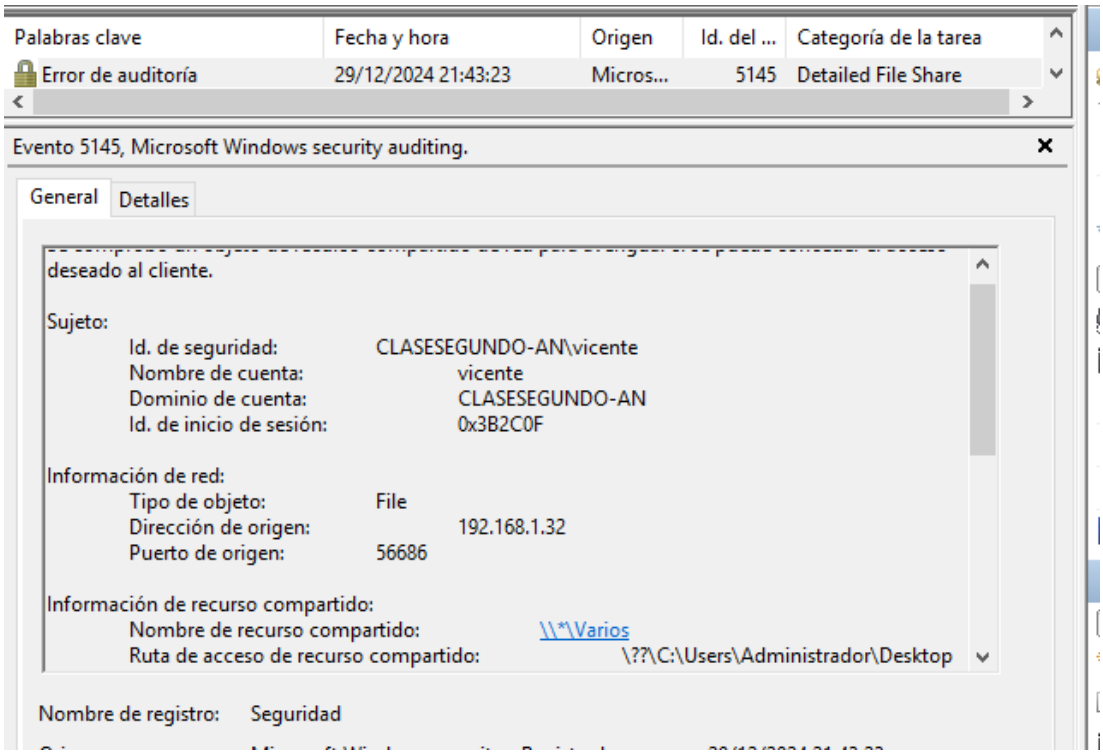
- Auditar todos los accesos erróneos para Vicente

Primero crearé esos errores para poder auditarlos:





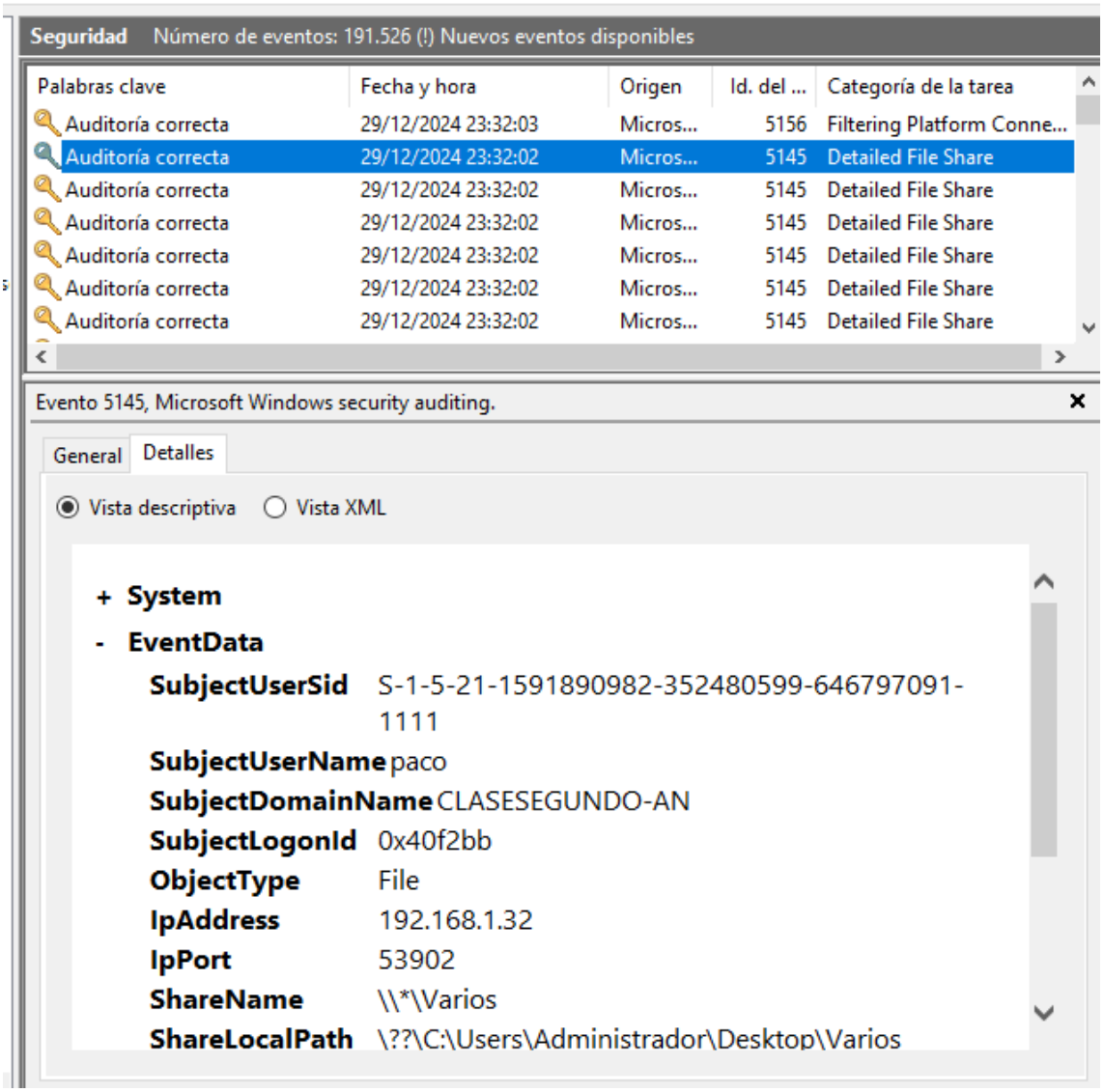
Ahora iré al visor de eventos en el servidor de Windows Server > Registros de Windows > Seguridad buscamos los que digan Vicente.



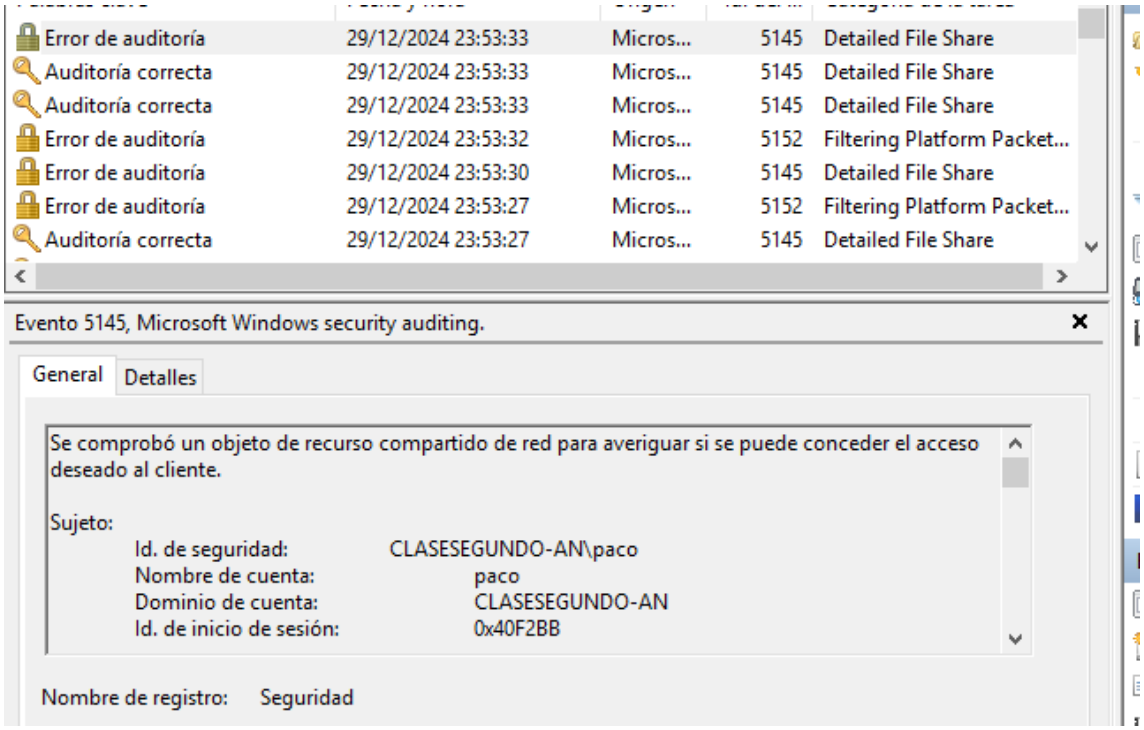
- Auditar todos los accesos correctos y erróneos para packomaster

Haré lo mismo con el usuario paco:

Auditoría correcta:

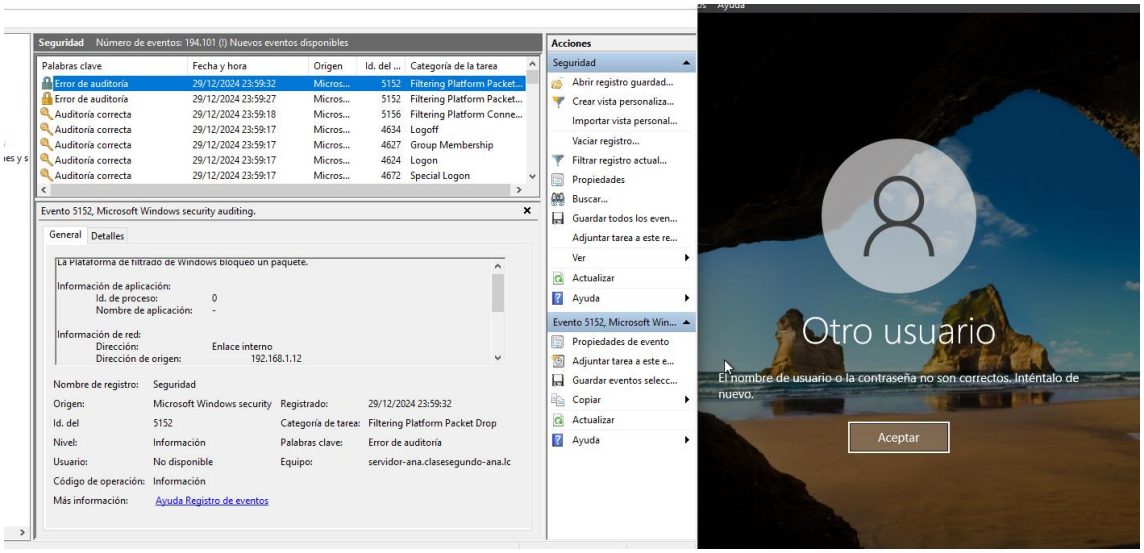


Error de auditoría:

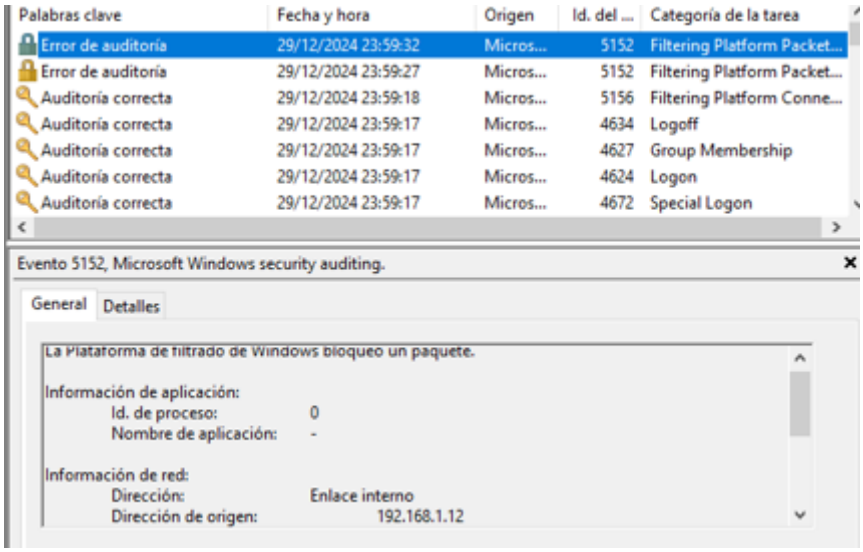


- Realizar varios accesos incorrectos desde un cliente:

- Accesos con usuarios existentes, pero contraseña incorrecta



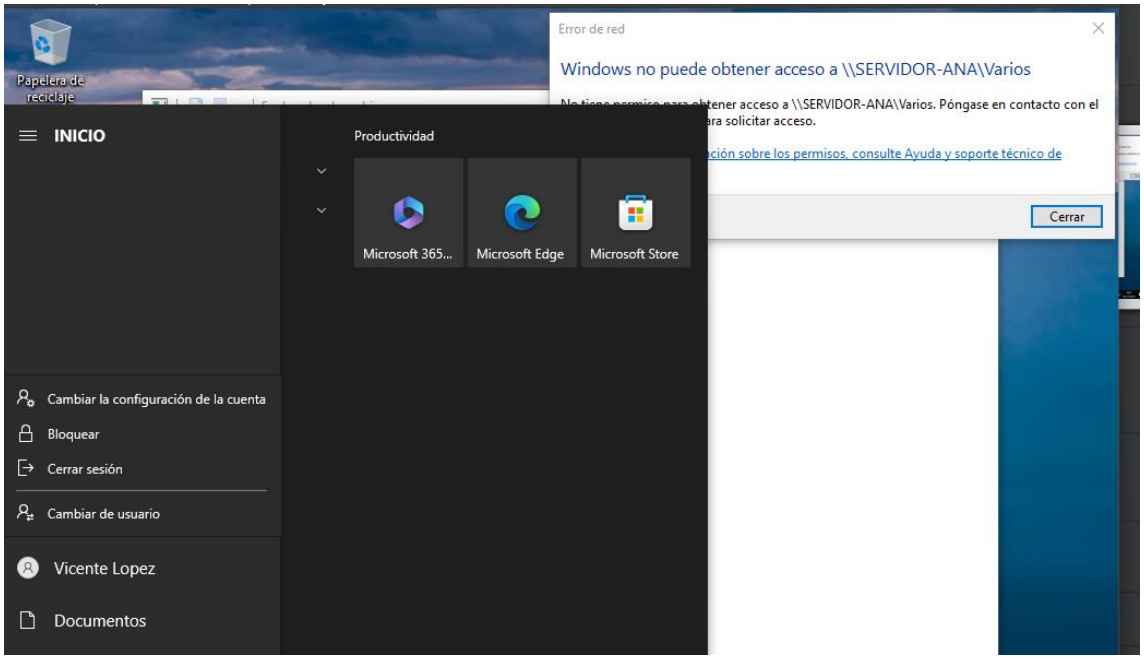
- Accesos con usuarios inexistentes

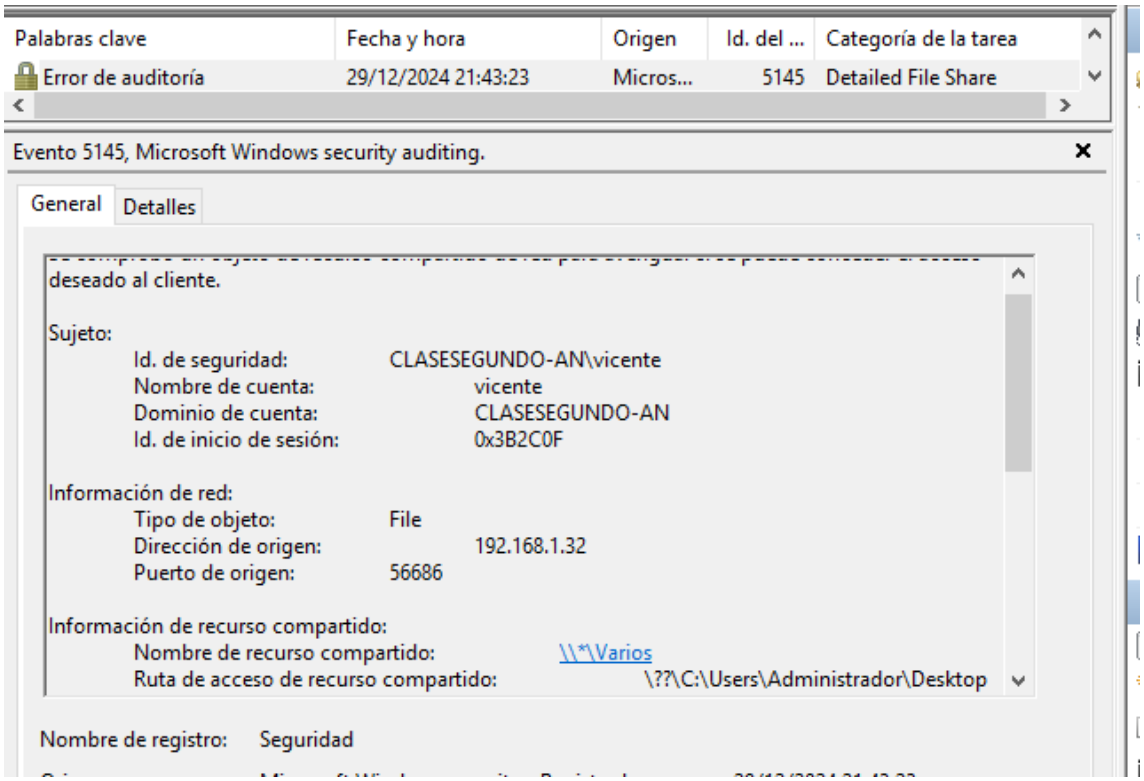


- Accesos con usuarios que no tengan permisos para utilizar el cliente desde el que se accede

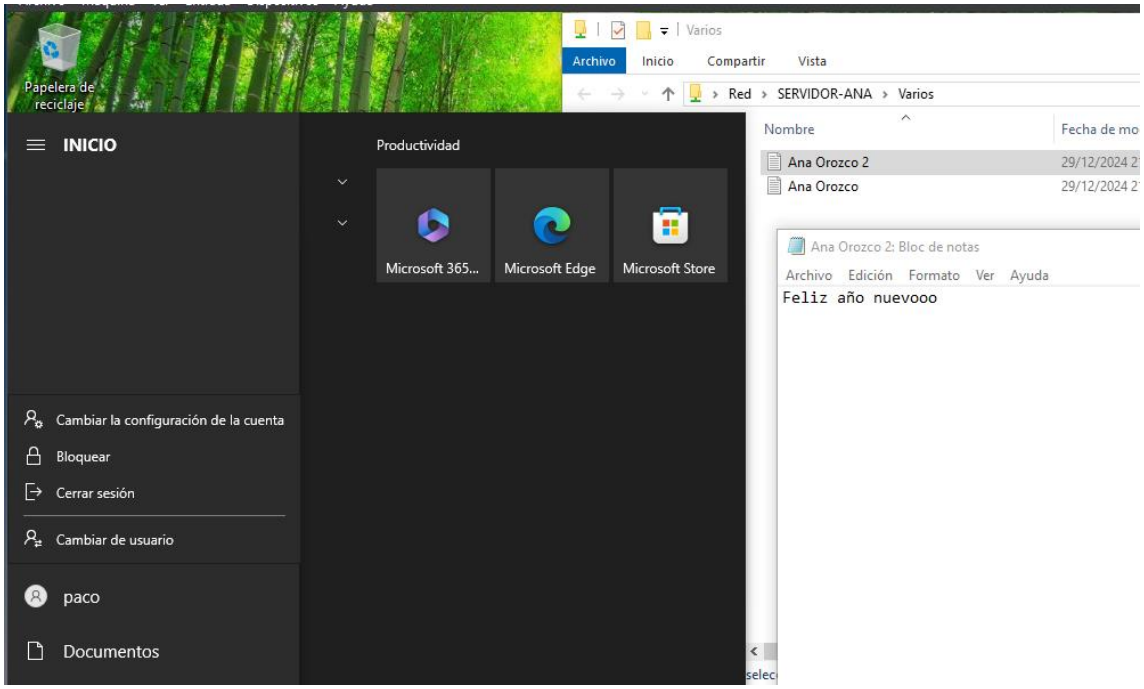
INCIDENCIA.

- Intentar acceder con el usuario Vicente a la carpeta compartida Varios.

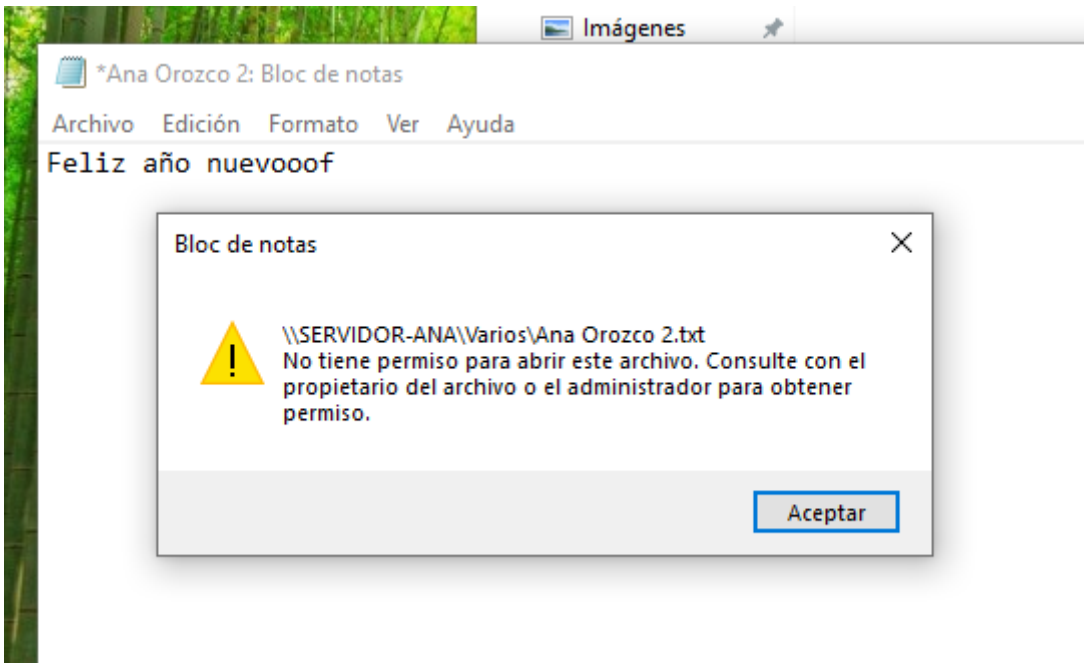


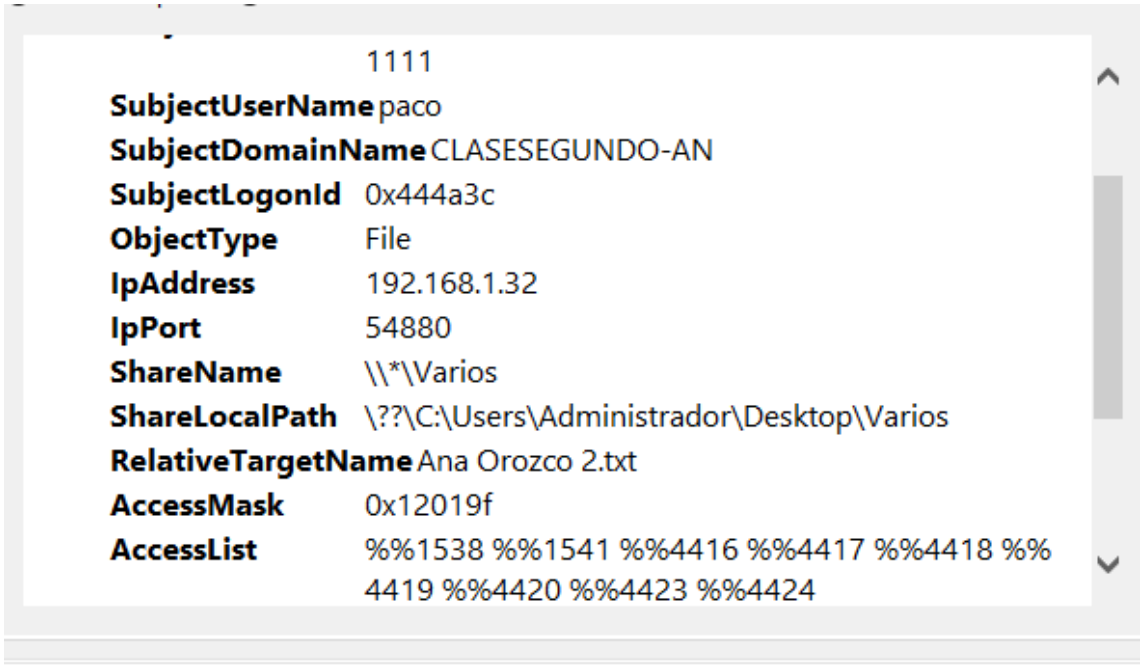


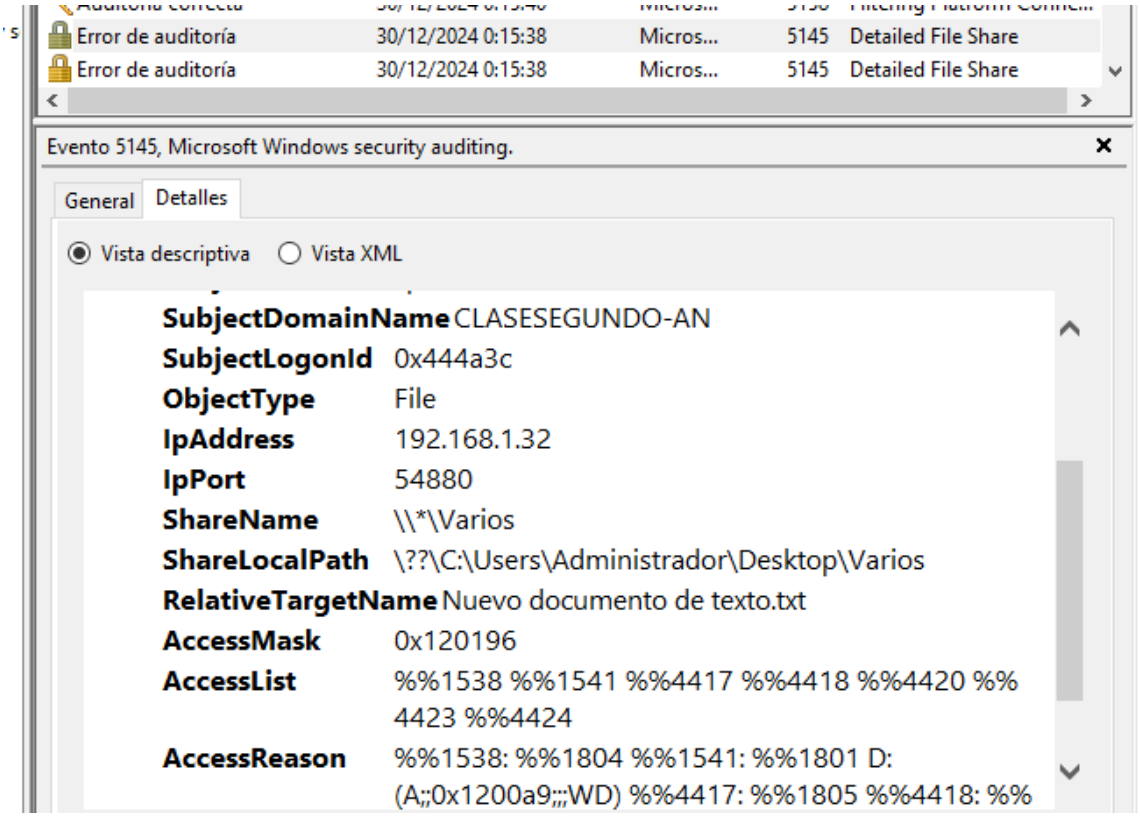
- Acceder con el usuario packomaster a la carpeta varios + Abrir alguno de los archivos que contiene la carpeta



- Intentar modificar alguno de ellos + Intentar crear un archivo en la carpeta







Al solo tener permisos de lectura, ni dos deja modificar el archivo existente ni dos deja crear un nuevo documento.

- Acceder al Visor de Sucesos del servidor y localizar los sucesos (correctos y errores) correspondientes a las operaciones realizadas.

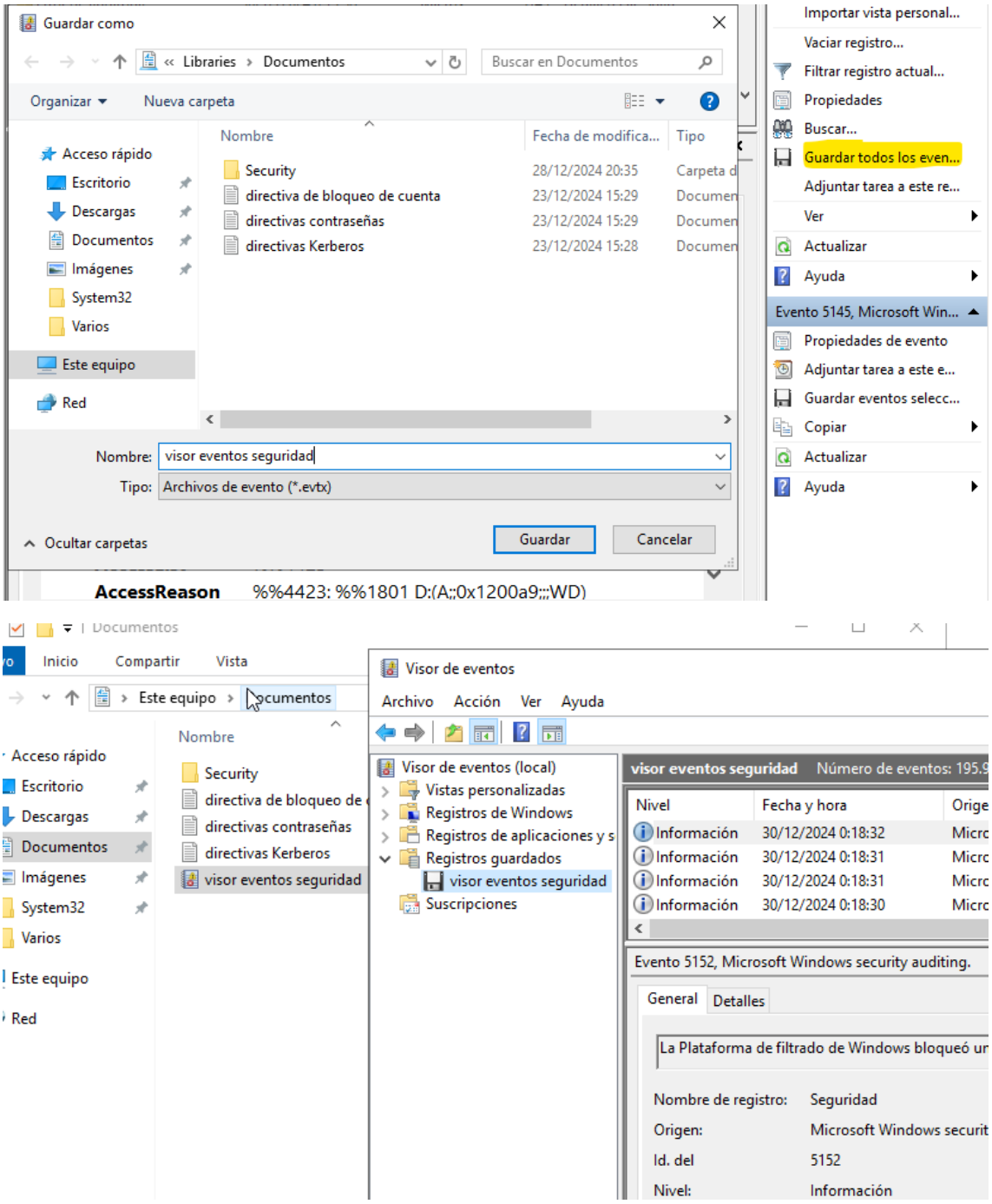
* Están las capturas en las operaciones realizadas.

- Buscar la ayuda de, al menos, un error de inicio de sesión y otro de acceso a la carpeta, indicando qué error se ha elegido.

* Están las capturas en las operaciones realizadas.

- Exportar a un archivo de texto los sucesos de seguridad para su posterior análisis.

En la barra derecha, pulsamos en “Guardar todos los...” con el nombre que le asignemos.


Guardar como
Libraries › Documentos
Buscar en Documentos
Organizar
Nueva carpeta
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
System32
Varios
Este equipo
Red
Nombre
Fecha de modifica...
Tipo
Security
28/12/2024 20:35
directiva de bloqueo de cuenta
23/12/2024 15:29
directivas contraseñas
23/12/2024 15:29
directivas Kerberos
23/12/2024 15:28
Nombre: visor eventos seguridad
Tipo: Archivos de evento (*.evtx)
Ocultar carpetas
Guardar
Cancelar
AccessReason %%4423: %%1801 D:(A;;0x1200a9;;;WD)
Importar vista personal...
Vaciar registro...
Filtrar registro actual...
Propiedades
Buscar...
Guardar todos los even...
Adjuntar tarea a este re...
Ver
Actualizar
Ayuda
Evento 5145, Microsoft Win...
Propiedades de evento
Adjuntar tarea a este e...
Guardar eventos selecc...
Copiar
Actualizar
Ayuda

Documentos
Inicio
Compartir
Vista
Este equipo › Documentos
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
System32
Varios
Este equipo
Red
Nombre
Security
directiva de bloqueo de
directivas contraseñas
directivas Kerberos
visor eventos seguridad
Visor de eventos
Archivo
Acción
Ver
Ayuda
Visor de eventos (local)
Vistas personalizadas
Registros de Windows
Registros de aplicaciones y s
Registros guardados
visor eventos seguridad
Suscripciones
visor eventos seguridad
Número de eventos: 195.9
Nivel
Fecha y hora
Orige
Información 30/12/2024 0:18:32 Micro
Información 30/12/2024 0:18:31 Micro
Información 30/12/2024 0:18:31 Micro
Información 30/12/2024 0:18:30 Micro
Evento 5152, Microsoft Windows security auditing.
General
Detalles
La Plataforma de filtrado de Windows bloqueó ur
Nombre de registro: Seguridad
Origen: Microsoft Windows securit
Id. del 5152
Nivel: Información

Incidencias

Tuve este fallo:

Y fue porque al hacer apt-get install libnss-ldap libpam-ldap ldap-utils -y no eliminé los caracteres sobrantes:

También tengo un error con juan que me ha creado carpeta con nombre de uid.

Además, el usuario ana es el mío y anag es el usuario de ana García.

He tenido incidencias de tonterías como nombres o ips mal puestas.

En el punto de auditorías, tuve una incidencia porque no aparece en las auditorías como un evento de error y por ello no puedo aportar una captura.

Valoración

Una práctica muy completa sobre seguridad en servidores Windows Server, la parte que más me ha gustado ver han sido las auditorías ya que aparece toda la información y me ha parecido curioso.

Ha sido una práctica larga aunque no difícil ya que eran muchos puntos que explicar, hacer capturas y documentar dichas capturas.