



P05 WIN- SEGURIDAD EN ACTIVE DIRECTORY

ANA OROZCO ASENSIO



2ºASIR
I.E.S. ANTONIO MACHADO
ASO

Contenido

Contenido	2
1.Directivas de Seguridad.	5
Visualizar las directivas de seguridad local de un cliente 10 y las del Controlador del dominio. ¿Qué diferencias muestran?	5
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.	6
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?.....	7
¿Para qué sirve la exportación en formato .inf?¿En qué apartado (a qué nivel) se utiliza?	8
2.Directivas de Grupo.....	9
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.	9
Crear una nueva directiva de grupo para la Unidad organizativa que acabamos de crear, llamándola GPO práctica WIN05.	9
Modificar la directiva anterior con las siguientes características:	10
· Modifica las directivas de contraseñas y de bloqueo de cuentas para el equipo (con valores distintos a los especificados para el dominio).	10
· Accede desde un cliente con algunos de los usuarios del dominio. ¿Qué prevalecerá: las directivas del dominio o las de la unidad organizativa?	10
· Modifica el valor que prefieras del Panel de Control para el usuario.....	11
· Modifica las características de Internet Explorer de forma que el usuario no pueda tocar la configuración del Proxy.	12
· Accede desde cualquier cliente para comprobar los cambios.	12
Quita el vínculo de la directiva de grupo que acabas de crear con el contenedor.	
.....	13
Vuelve a establecer el vínculo con el contenedor.	14
Deshabilita únicamente la configuración del equipo de la directiva de grupo. ..	14
Crea una nueva Unidad Organizativa dentro de Unidad de prueba, llamándola Unidad hija.....	15
Bloquear la herencia de la Unidad hija. ¿Qué acabamos de hacer?	15

Vincular cualquiera de las directivas disponibles creadas anteriormente a la Unidad hija.....	16
Mirar ahora a qué Unidades Organizativas se está aplicando esta última directiva.....	16
Hacer que la directiva Default Domain Policy sea siempre heredable para todas las Unidades Organizativas del dominio.	17
Obtener el listado de todas las directivas definidas.....	17
Asignar la directiva de grupo Ocultar configuración de pantalla a los alumnos de segundo.....	18
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.	19
Crear una regla Hash para impedir el uso de la calculadora.	20
¿Cómo podemos saber que una Directiva de grupo está forzada?	21
¿Cómo podemos saber que se ha bloqueado la herencia de una Unidad Organizativa?.....	21
3. Plantillas de seguridad.....	22
Crear una consola, en el equipo servidor, llamada Consola de Seguridad e incorporarle los complementos Plantillas de Seguridad y Configuración y análisis de seguridad.	22
Crear con el complemento Plantillas de Seguridad una nueva plantilla llamada Práctica.	24
Configurar la plantilla creada modificando las directivas de contraseña y de bloqueo de cuenta de acuerdo con los criterios del alumno (hay que indicarlos).	25
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?.....	26
Crear con el complemento Configuración y análisis de Seguridad, una base de datos llamada BDSegLocal, e importar la plantilla Práctica.	27
Realiza la configuración local del equipo, modificando características de las contraseñas para que se provoquen errores.	29
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.	29
4.Ejecutar como.....	31

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).....	31
5.Auditorías.	32
Habilita las directivas Auditar el acceso a objetos y Auditar el acceso del servicio de directorio para todos los equipos del dominio.	32
Configurar el procesamiento de las directivas de seguridad con sus valores predeterminados por defecto para la sincronización de las directivas de grupo.	
.....	33
Auditar el acceso a objetos (correcto y errores) para el controlador de dominio.	
¿Qué conseguimos con ello?	33
Auditar los errores de inicio de sesión en el servidor.....	34
Crear una carpeta Varios en el directorio CFGS del servidor. Con ella:	35
- Crear algunos archivos de texto en su interior que contengan, al menos, una línea.	36
- Compartirla para todos los usuarios con permisos únicamente de lectura	37
- Quitar todos los permisos al usuario Vicente.....	37
- Auditar todos los accesos erróneos para Vicente.....	38
- Auditar todos los accesos correctos y erróneos para packomaster	39
- Realizar varios accesos incorrectos desde un cliente:	41
- Accesos con usuarios existentes, pero contraseña incorrecta	41
- Accesos con usuarios inexistentes	42
- Accesos con usuarios que no tengan permisos para utilizar el cliente desde el que se accede	42
- Intentar acceder con el usuario Vicente a la carpeta compartida Varios. ...	42
- Acceder con el usuario packomaster a la carpeta varios + Abrir alguno de los archivos que contiene la carpeta	43
- Intentar modificar alguno de ellos + Intentar crear un archivo en la carpeta	44
- Acceder al Visor de Sucesos del servidor y localizar los sucesos (correctos y errores) correspondientes a las operaciones realizadas.	45
- 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.	45
- Exportar a un archivo de texto los sucesos de seguridad para su posterior análisis.....	45
Incidencias.....	47
Valoración	47

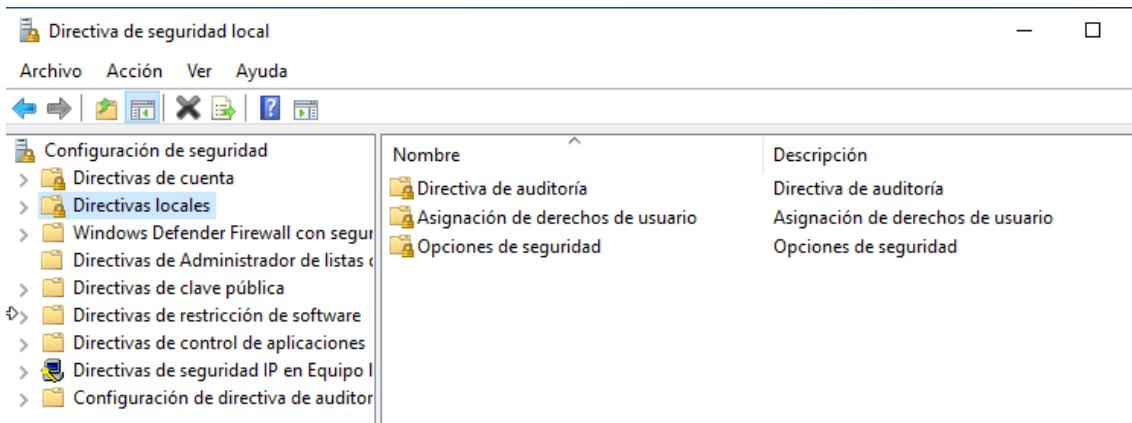
1. Directivas de Seguridad.

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

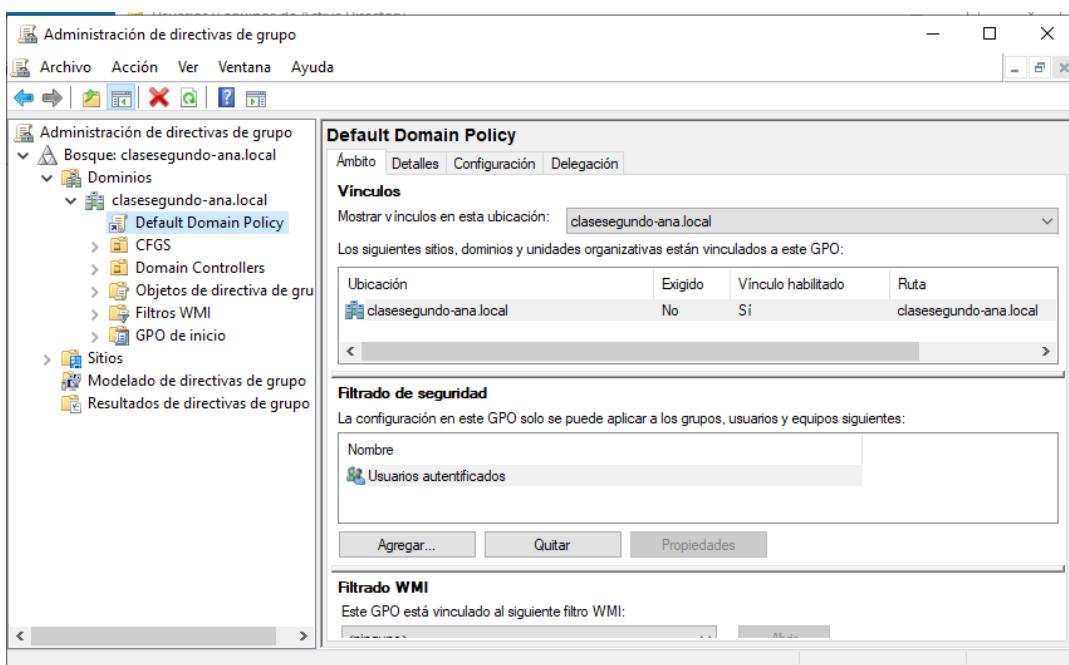
Las políticas de seguridad locales afectan únicamente a la máquina en la que se configuran, mientras que las establecidas en el controlador de dominio se extienden y aplican a todos los dispositivos que forman parte del dominio.

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:

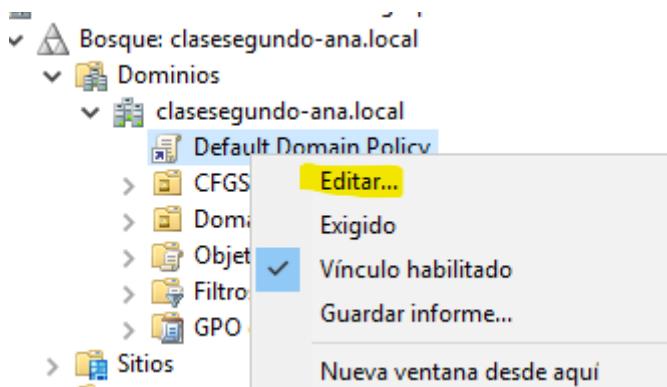


Dominio:



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.

A screenshot of the 'Editor de administración de directivas de grupo'. The left pane shows the navigation tree: 'Configuración del equipo' > 'Directivas' > 'Configuración de Windows' > 'Configuración de seguridad' > 'Directivas de cuenta' > 'Directiva de bloqueo de cuenta'. The right pane displays a table of policy settings. One row is selected, showing the 'Umbral de bloqueo de cuenta' setting with a value of '5 intentos de inicio de sesión no...'. Other settings shown include 'Duración del bloqueo de cuenta' (2880 minutos), 'Permitir bloqueo de cuenta de administrador' (Habilitada), and 'Restablecer el bloqueo de cuenta después de' (2880 minutos).

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.

The screenshot shows the Windows Group Policy Management console. On the left, the navigation pane displays the 'Directiva Default Domain Policy' under 'SERVIDOR-ANA.CLASESEGU'. In the center, the 'Directivas' (Policies) pane shows several policy items, including 'Aplicar restricciones de inicio de sesión de usuario' (Enabled), 'Tolerancia máxima para la sincronización de los relojes de los...', and 'Vigencia máxima del vale de servicio' (7 days). On the right, the 'Configuración de directiva' (Policy configuration) pane shows detailed settings for these policies. A context menu is open over the 'Directiva Kerberos' item, with 'Exportar lista...' highlighted. This menu also includes options like 'Abrir', 'Ver', 'Registro', 'Grupos de seguridad', 'Servicios', 'Registro de auditoría', and 'Ayuda'. A secondary window titled 'Exportar lista' is open, showing a list of save locations: 'Acceso rápido', 'Escritorio', 'Bibliotecas', 'Este equipo', and 'Red'. The 'Tipo:' dropdown menu at the bottom lists file formats: 'Texto (delimitado por tabuladores) (*.txt)', 'Texto (delimitado por tabuladores) (*.txt)' (selected), 'Texto (delimitado por comas) (*.csv)', 'Texto Unicode (delimitado por tabuladores) (*.txt)', and 'Texto Unicode (delimitado por comas) (*.csv)'.

Este equipo > Documentos			
	Nombre	Fecha de modifica...	Tipo
	directivas Kerberos	23/12/2024 15:28	Documento
	directivas contraseñas	23/12/2024 15:29	Documento
	directiva de bloqueo de cuenta	23/12/2024 15:29	Documento

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).

```

directiva de bloqueo de cuenta: Bloc de notas
Archivo Edición Formato Ver Ayuda
Directiva Configuración de directiva
Duración del bloqueo de cuenta 2880 minutos
Permitir bloqueo de cuenta de administrador Habilitada
Restablecer el bloqueo de cuenta después de 2880 minutos
Umbral de bloqueo de cuenta 5 intentos de inicio de sesión no válidos

directivas contraseñas: Bloc de notas
Archivo Edición Formato Ver Ayuda
Directiva Configuración de directiva
Almacenar contraseñas con cifrado reversible Deshabilitada
Auditoría de longitud mínima de contraseña No está definido
Exigir historial de contraseñas 24 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad Deshabilitada
Longitud mínima de la contraseña No está definido
Vigencia máxima de la contraseña 42 días
Vigencia mínima de la contraseña 1 días

directivas Kerberos: Bloc de notas
Archivo Edición Formato Ver Ayuda
Directiva Configuración de directiva
Aplicar restricciones de inicio de sesión de usuario Habilitada
Tolerancia máxima para la sincronización de los relojes de los equipos 5 minutos
Vigencia máxima de renovación de vales de usuario 7 días
Vigencia máxima del vale de servicio 600 minutos
Vigencia máxima del vale de usuario 10 horas

```

¿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.

The screenshot shows the 'Usuarios y equipos de Active Directory' (User and Computer) snap-in. On the left, the navigation pane displays the 'Users and Computers' tree under 'clasesegundo-ana.local'. Under 'Users', two users are listed: 'ana perez' and 'juan lopez', both categorized as 'Usuario'. The top menu bar includes 'Archivo', 'Acción', 'Ver', and 'Ayuda'. The toolbar below the menu contains various icons for file operations like New, Open, Save, Print, and Filter.

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.

The screenshot shows the 'Objetos de directiva de grupo vinculados' (Linked Group Policy Objects) dialog box. The 'Herencia de directivas de grupo' tab is selected. A table lists the linked GPOs:

Orden de vínculos	GPO	Exigido	Vínculo habilitado	Estado de GPO
1	GPO PWIN05	No	Sí	Habilitado

On the left, the 'Bosque: clasesegundo-ana.local' navigation pane shows the structure of the domain, including 'Dominios', 'clasesegundo-ana.local', 'Unidad de prueba', and 'GPO PWIN05'. There are also 'Objetos de directiva de grupo' and 'Filtros WMI' listed under '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:

The screenshot shows two separate Group Policy Objects (GPOs) named "Directiva GPO PWIN05 [SERVIDOR-ANA.CLASE]" and "Directiva GPO PWIN05 [SERVIDOR-ANA.CLASE]". Both are under the "Configuración del equipo" (Computer Configuration) node, specifically in the "Directivas" (Policies) section.

First GPO (Left):

Directiva	Configuración de directiva
Almacenar contraseñas con cifrado reversible	No está definido
Auditoría de longitud mínima de contraseña	6 caracteres
Exigir historial de contraseñas	3 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad	Habilitada
Longitud mínima de la contraseña	No está definido
Vigencia máxima de la contraseña	42 días
Vigencia mínima de la contraseña	3 días

Second GPO (Right):

Directiva	Configuración de directiva
Duración del bloqueo de cuenta	2 minutos
Permitir bloqueo de cuenta de administrador	No está definido
Restablecer el bloqueo de cuenta después de	2 minutos
Umbral de bloqueo de cuenta	5 intentos de inicio de sesi

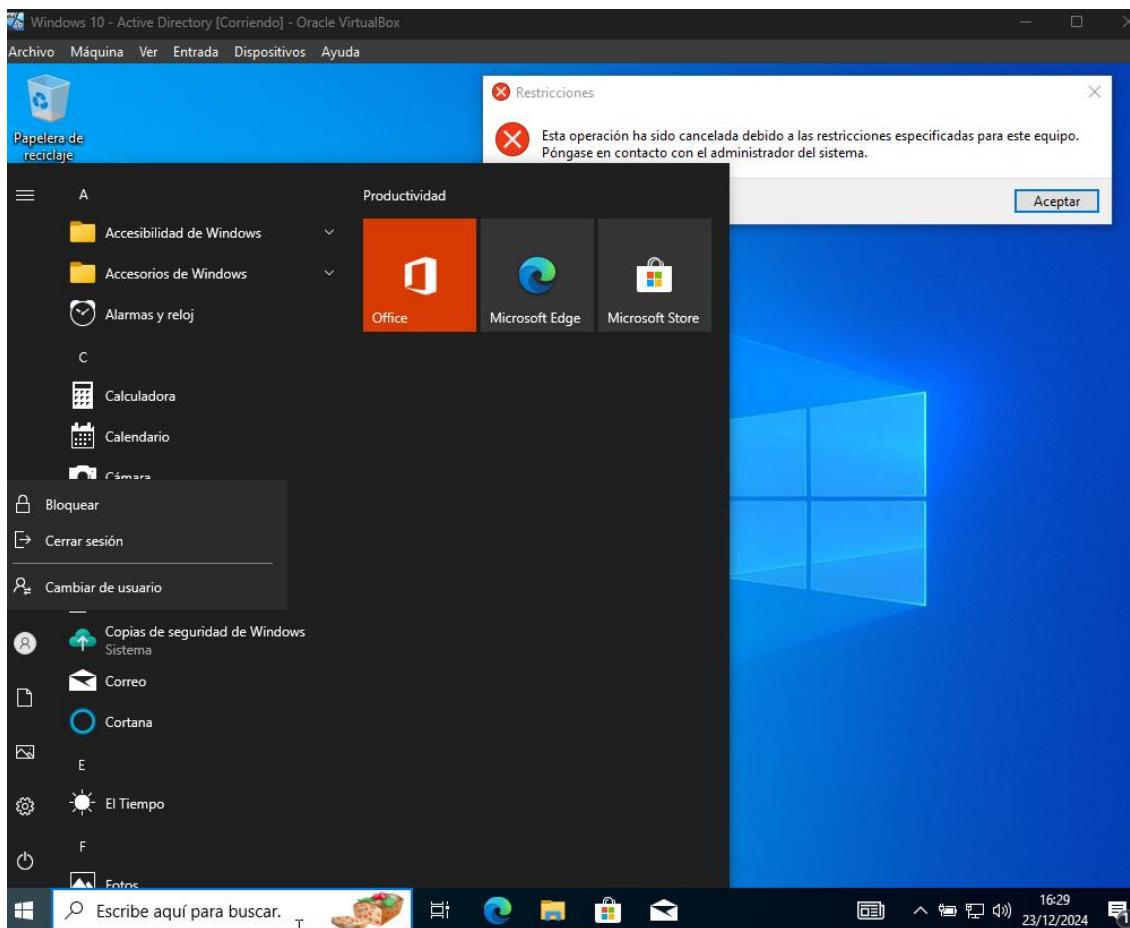
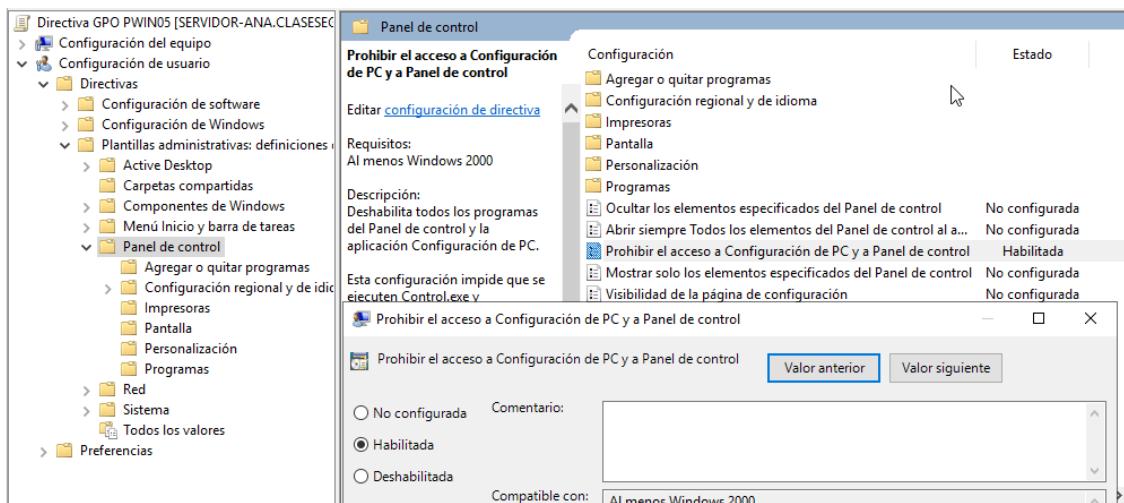
- Accede desde un cliente con algunos de los usuarios del dominio.

¿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.

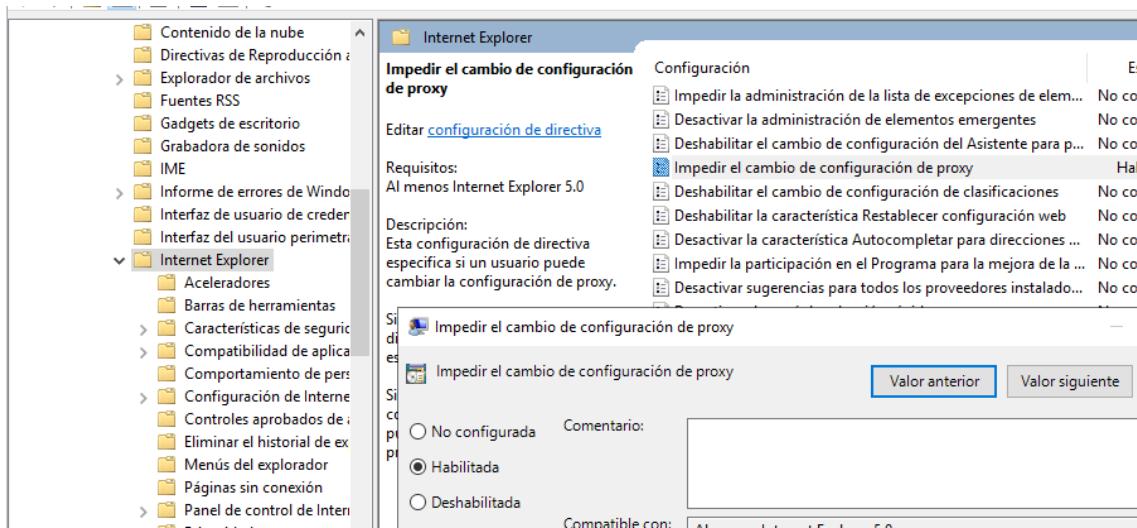
• Modifica el valor que prefieras del Panel de Control para el usuario.

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:

Configuración

Sistema - 1 resultado

Iniciar rápidamente

Acceda rápidamente a la exploración. Cuando esta opción está activada, ayuda a Microsoft Edge abrirse más rápido al iniciar el dispositivo. [Más información](#)

Seguir ejecutando extensiones y aplicaciones en segundo plano cuando Microsoft Edge está cerrado

Usar la aceleración de gráficos cuando esté disponible

Mejorar videos en Microsoft Edge

¿Está satisfecho con la mejora del video?

Mejore los videos y mejore el color, la iluminación y el contraste con la super resolución de los videos, cuando el dispositivo está conectado. No se mejorarán los videos protegidos y los videos que son pequeños en pantalla. Solo se mejorará el video reproducido más recientemente cuando haya varios videos activos en un sitio.

Método preferido de mejora de video: Super resolución

Edge usa una super resolución integrada para el escalado vertical de video en dispositivos compatibles. Se ofrecen técnicas de mejora, en función de las funcionalidades del dispositivo. La mejora del controlador de gráficos puede requerir una configuración adicional en el software de controlador.

Resolución máxima de video para la mejora: 1080p

La resolución máxima predeterminada para la mejora de video es de 1080p. Puede optar por reducir la resolución de video máxima admitida en función del rendimiento del dispositivo.

Abrir la configuración de proxy del equipo

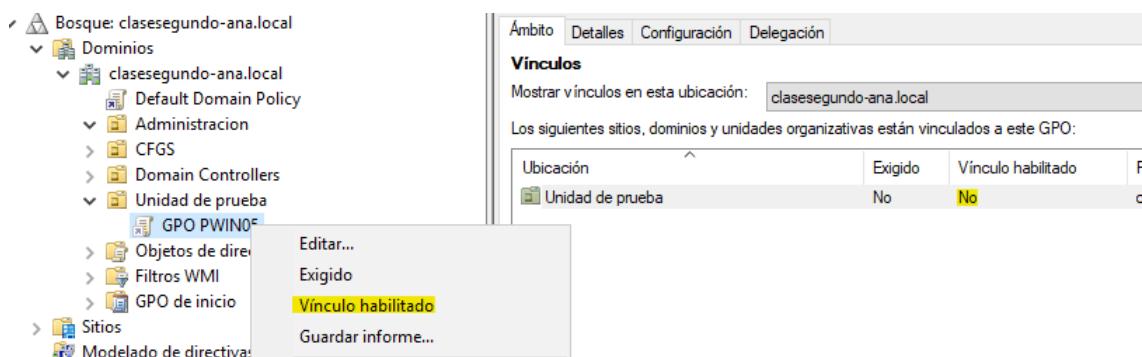
Proxy

*Algunas de estas opciones de configuración están ocultas o las administra la organización.

Configuración automática del proxy

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:

Proxy

Configuración automática del proxy

Usa un servidor proxy para conexiones Ethernet o Wi-Fi. Esta configuración no se aplica a conexiones VPN.

Detectar la configuración automáticamente

Activado

Usar script de configuración

Desactivado

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.

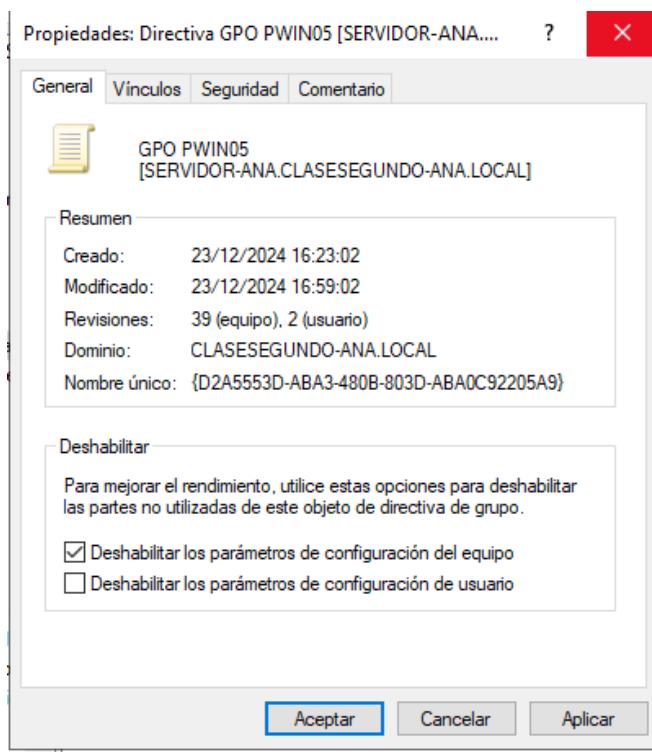
Proxy

*Algunas de estas opciones de configuración están ocultas o las administra la organización.

Configuración automática 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, llámándola Unidad hija.

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

The screenshot shows the 'Users and computers' section of Active Directory. On the left, there's a tree view of the domain 'clasesegundo-ana.local'. Under 'Unidad de prueba', a new folder named 'Unidad hija' is being created. On the right, a table lists the object details:

Nombre	Tipo
	No hay elem...

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

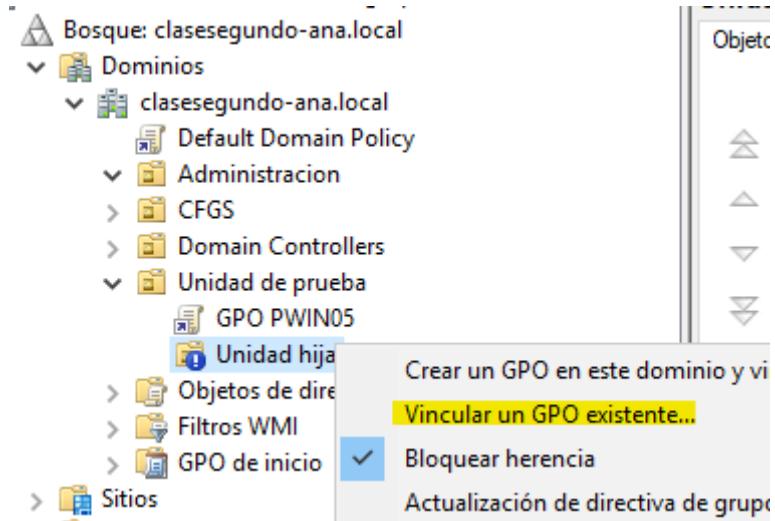
Esto garantiza que solo se apliquen las GPO creadas específicamente dentro de dicha unidad organizativa, evitando que se vean afectadas por otras directivas externas.

The screenshot shows the 'Group Policy Management' console. It displays the 'Default Domain Policy' for the 'clasesegundo-ana.local' domain. A context menu is open over the 'Unidad hija' GPO, with the 'Bloquear herencia' (Block inheritance) option highlighted with a yellow box. Other options in the menu include 'Crear un GPO en este dominio y vincularlo...' (Create a GPO in this domain and link it...), 'Vincular un GPO existente...' (Link an existing GPO...), and 'Actualizar directiva de grupo...' (Update group policy object...).

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.

The screenshot shows the 'Unidad hija' properties dialog. The left pane displays the 'Administración de directivas de grupo' tree, identical to the one in the previous screenshot. The right pane is titled 'Unidad hija' and contains tabs for 'Objetos de directiva de grupo vinculados', 'Herencia de directivas de grupo', and 'Delegación'. The 'Objetos de directiva de grupo vinculados' tab is selected, showing a table with one entry:

Orden de vínculos	GPO	Exigido	Vínculo heredado
1	GPO PWIN05	No	Si

Ubicación	Exigido	Vínculo habilitado	Ruta
Unidad de prueba	No	Si	clasesegundo-ana.local/Unidad de prueba
Unidad hija	No	Si	clasesegundo-ana.local/Unidad de prueba/Unidad hija

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.

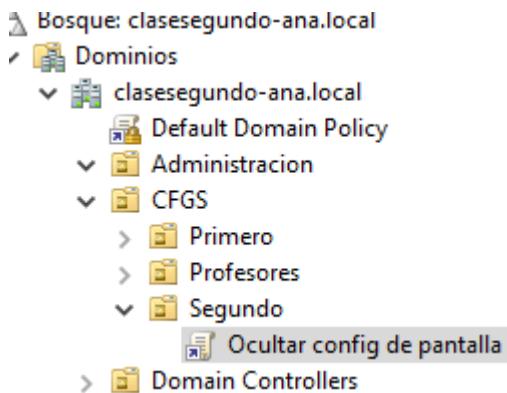
Cuando una directiva de grupo se configura como “Forzar”, tendrá prioridad sobre cualquier otra directiva que intente bloquear su herencia en una unidad organizativa (OU). Para establecer esta opción, simplemente hacemos clic derecho sobre la GPO y seleccionamos “Exigido”.

Obtener el listado de todas las directivas definidas.

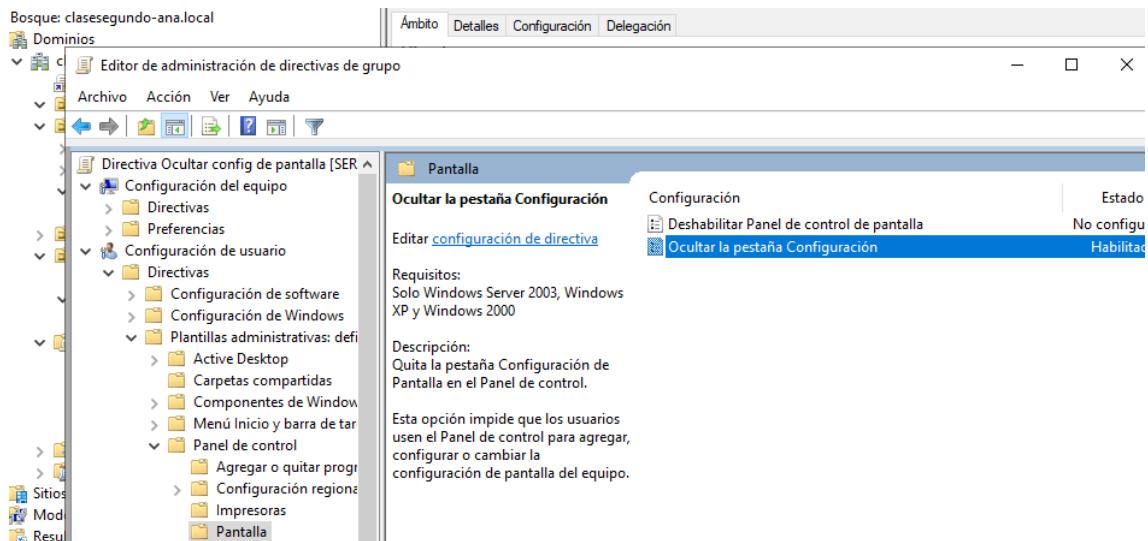
Podemos observar diferentes objetos de directiva de grupo, como los predefinidos, como Default Domain Policy, así como los personalizados, como Práctica WIN05.

Nombre	Estado de GPO	Filtro WMI	Modificado	Pri
Default Domain Controller Policy	Habilitado	Ninguno	26/09/2024 11:06...	A
Default Domain Policy	Habilitado	Ninguno	23/12/2024 15:21...	A
GPO PWIN05	Habilitado	Ninguno	23/12/2024 16:59...	A

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



Vamos a editar la GPO y accedemos a “Configuración 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 habilitaremos la opción de “no ejecutar aplicaciones de Windows especificadas”

The screenshot shows the Group Policy Management console. On the left, the navigation pane is open with the following structure:

- Configuración del equipo
- Directivas
- Preferencias
- Configuración de usuario
- Directivas (selected)
- Configuración de software
- Configuración de Windows
- Plantillas administrativas: definiciones de directivas (selected)
 - Active Desktop
 - Carpetas compartidas
 - Componentes de Windows
 - Menú Inicio y barra de tareas
 - Panel de control
 - Red
 - Sistema (selected)
 - Todos los valores
- Preferencias

The main pane displays the details for the selected policy:

No ejecutar aplicaciones de Windows especificadas

Requisitos: Al menos Windows 2000

Descripción: Impide que Windows ejecute los programas que usted especifique en esta configuración de directiva.

If you enable this configuration of the directive, users will not be able to run the programs that you specify in this configuration of the directive. Add them to the list of applications that are not permitted.

If you disable or do not define this configuration of the directive, users will be able to run any program.

On the right side, a list of other configuration options is visible, including:

- Configuración
- Directiva de grupo
- Inicio de sesión
- Instalación de controladores
- Opciones de Ctrl+Alt+Supr
- Opciones de mitigación
- Pantalla
- Perfiles de usuario
- Redirección de carpetas
- Scripts
- Servicios de configuración regional
- Descargar componentes COM que faltan
- Interpretación de siglo para el año 2000
- No permitir que estos programas se ejecuten
- No mostrar la pantalla de inicio de sesión
- Interfaz de usuario personalizada
- Impedir el acceso al símbolo del sistema
- Impedir el acceso a herramientas de edición
- No ejecutar aplicaciones de Windows

At the bottom, there is a configuration dialog for the policy:

No ejecutar aplicaciones de Windows especificadas

No configurada Comentario: _____

Habilitada

Deshabilitada

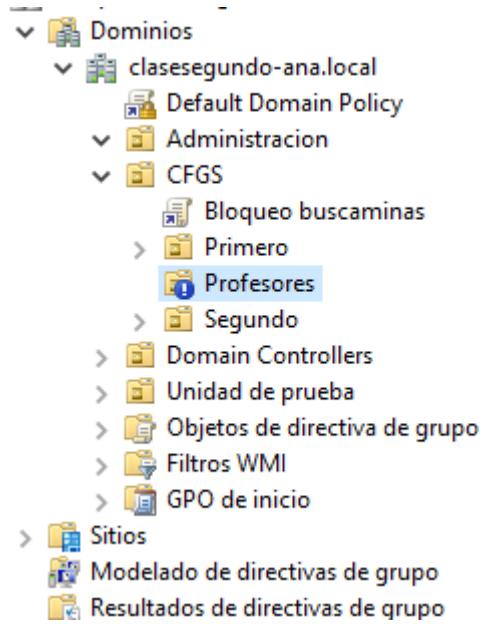
Valor anterior Valor siguiente

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

A table titled "Lista de aplicaciones no permitidas" (List of prohibited applications) is shown. It has two columns: "Nombre" (Name) and "Valor" (Value). The "Valor" column contains the value "winmine.exe".

Nombre	Valor
	winmine.exe

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.



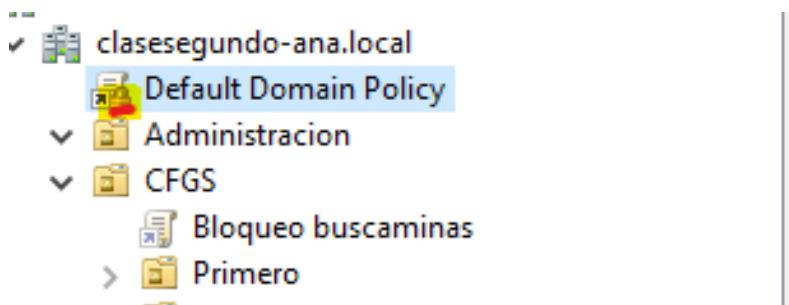
Crear una regla Hash para impedir el uso de la calculadora.

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:

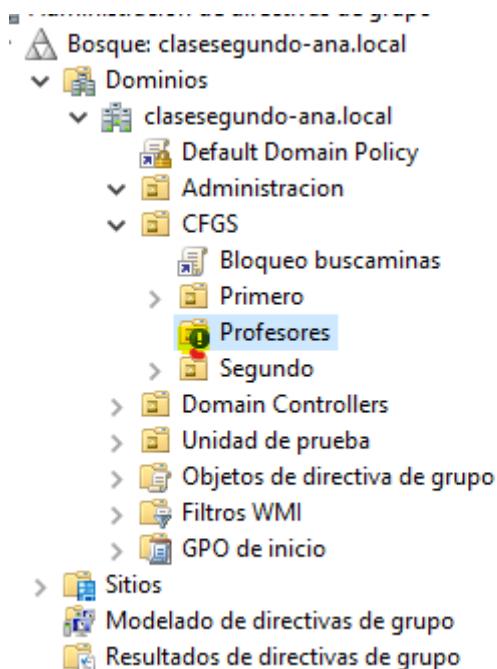
¿Cómo podemos saber que una Directiva de grupo está forzada?

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



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

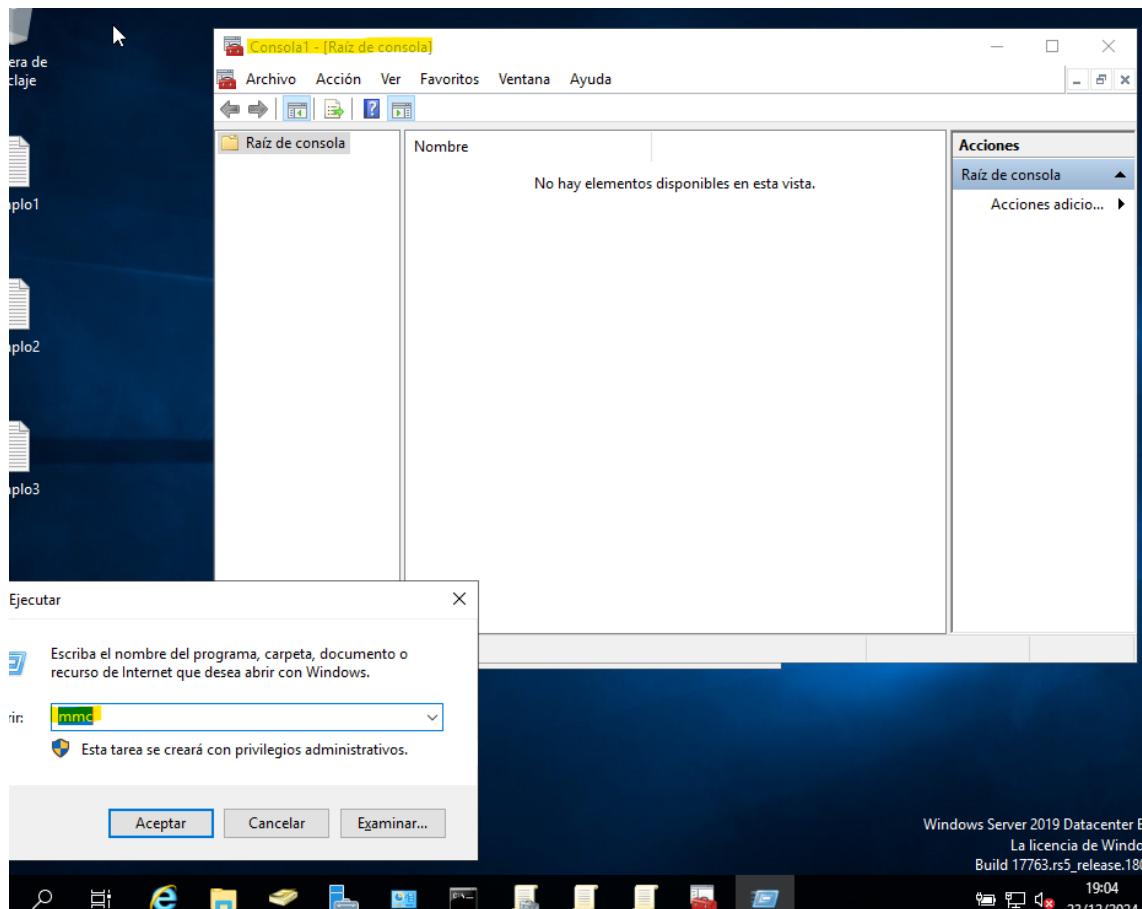
Porque aparecerá un círculo azul con una exclamación en su icono.



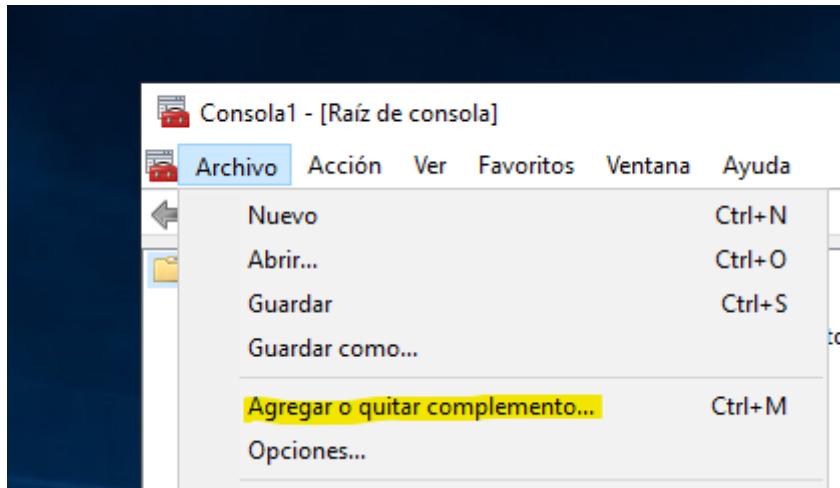
3. Plantillas de seguridad.

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

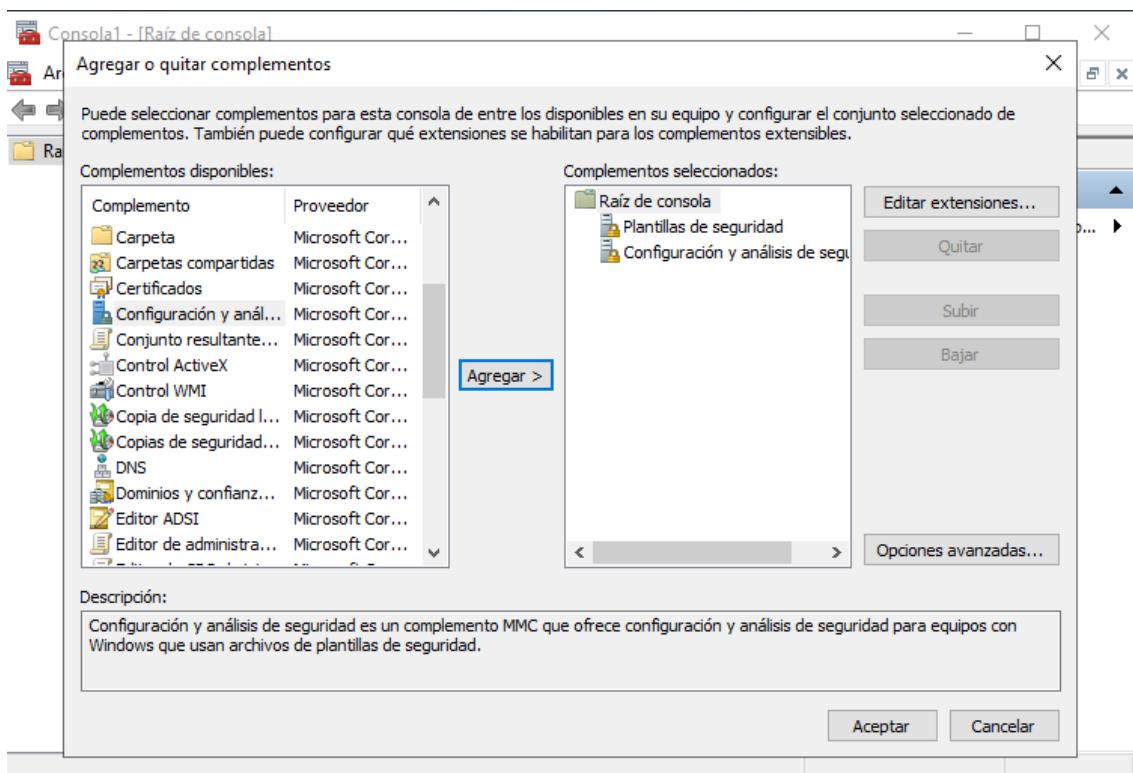
Para comenzar, presionaré Win + R para abrir el cuadro de ejecución y escribiré mmc.



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

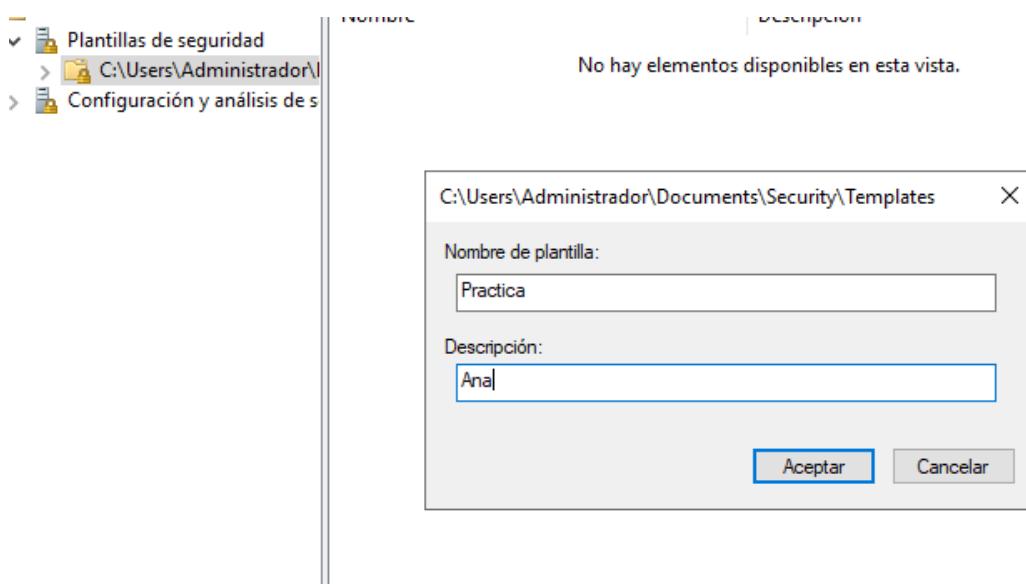
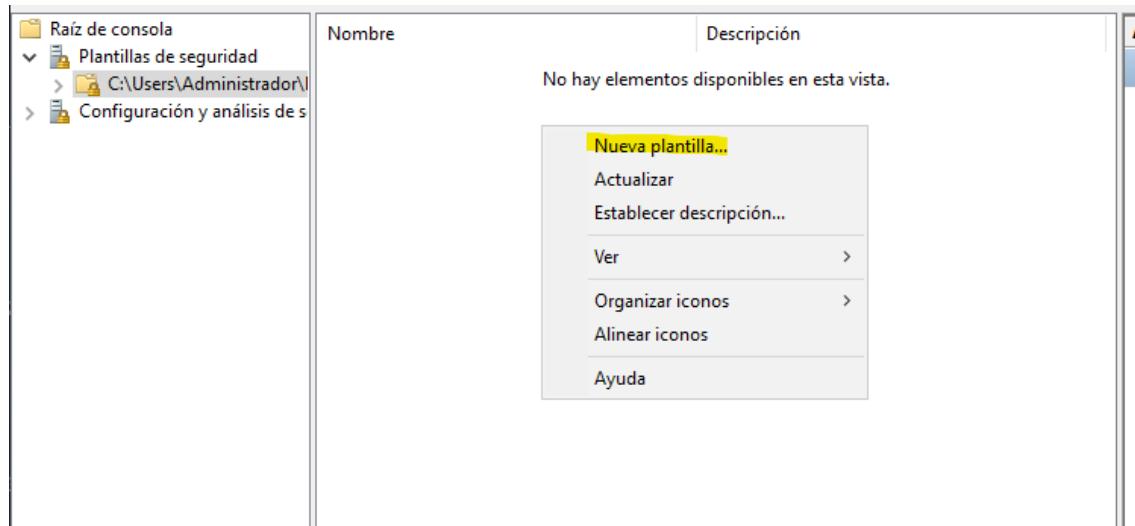


Ahora agregaremos “Plantillas de seguridad” y “Configuración y análisis de seguridad” y le daré a aceptar.



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.

The screenshot shows the Windows Security Policy Editor interface. The left pane displays a tree view of security templates, with 'Práctica' selected under 'C:\Users\Administrador\Documents\Security'. The right pane lists password-related directives:

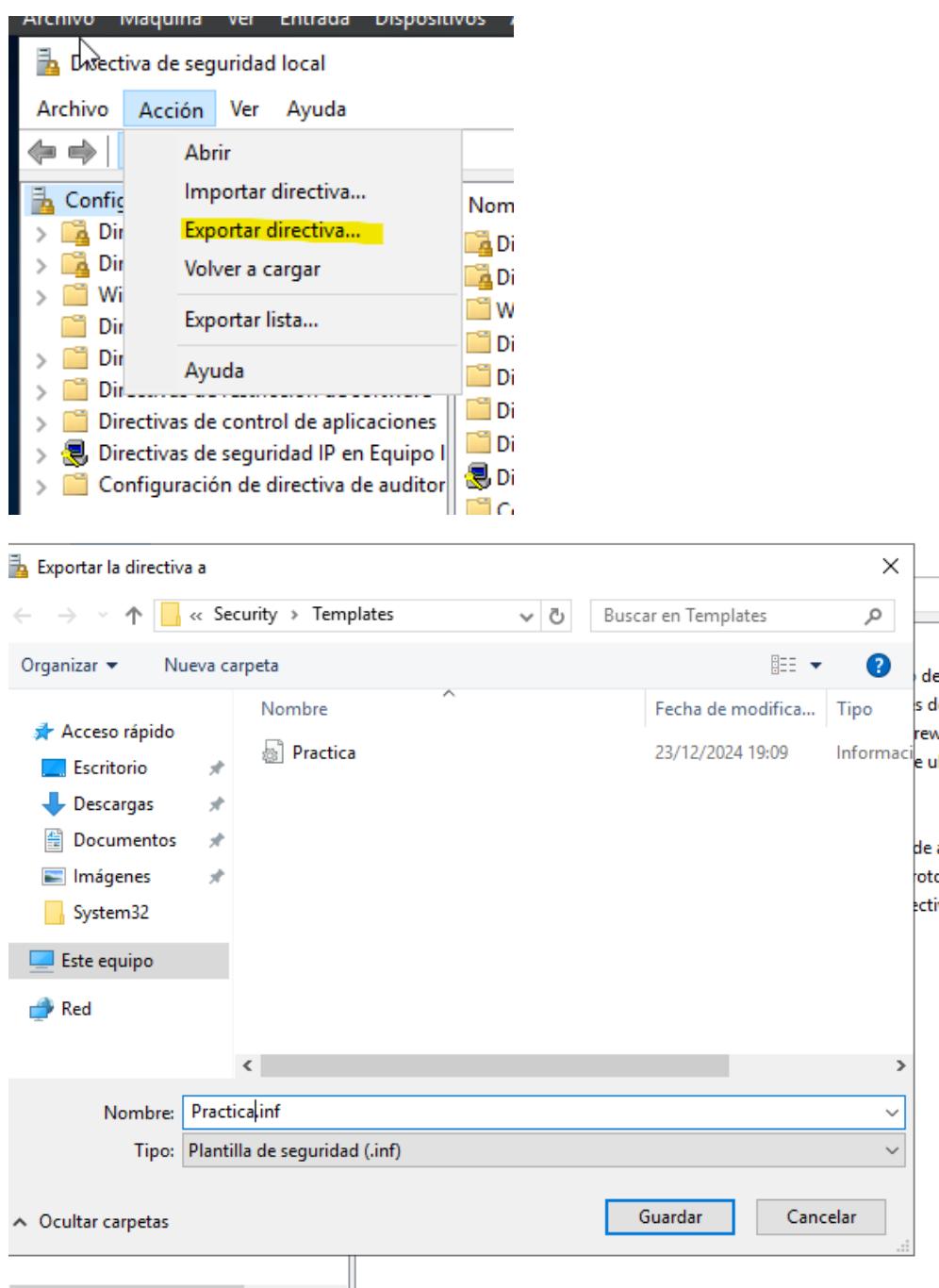
Directiva	Configuración del equipo
Almacenar contraseñas con cifrado reversible	No está definido
Auditoría de longitud mínima de contraseña	No está definido
Exigir historial de contraseñas	5 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad	No está definido
Longitud mínima de la contraseña	6 caracteres
Vigencia máxima de la contraseña	42 días
Vigencia mínima de la contraseña	30 días

The screenshot shows the Windows Security Policy Editor interface. The left pane displays a tree view of security templates, with 'Práctica' selected under 'C:\Users\Administrador\Documents\Security'. The right pane lists account lockout-related directives:

Directiva	Configuración del equipo
Duración del bloqueo de cuenta	10 minutos
Permitir bloqueo de cuenta de administrador	No está definido
Restablecer el bloqueo de cuenta después de	10 minutos
Umbral de bloqueo de cuenta	5 intentos de inicio de sesión no...

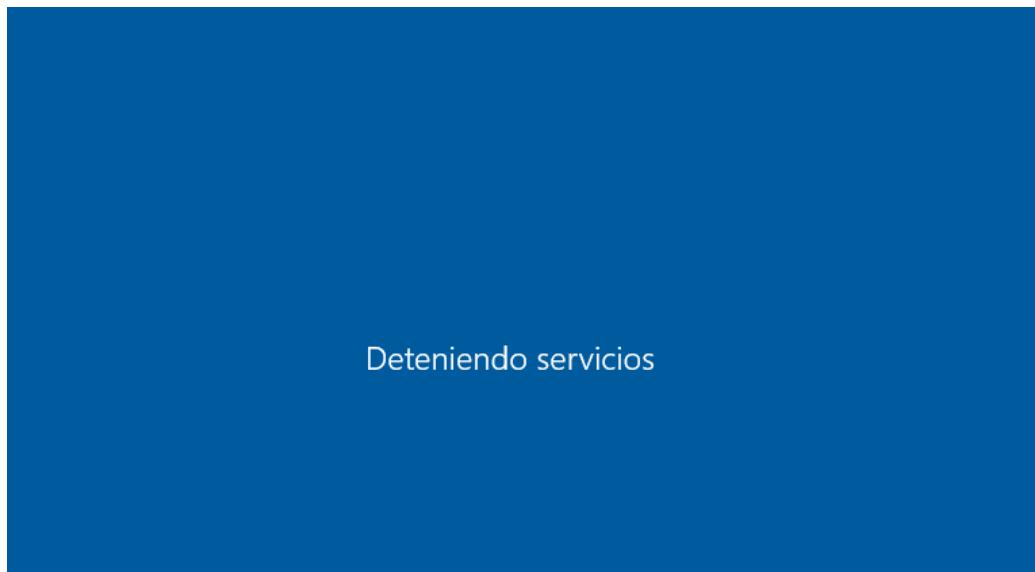
Exportar las características definidas en la plantilla a las Directivas de Seguridad del dominio. Hay que hacer una comparación mediante capturas de pantallas de la configuración de seguridad del dominio antes y después de la exportación. ¿Qué quiere decir lo que hemos hecho?

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



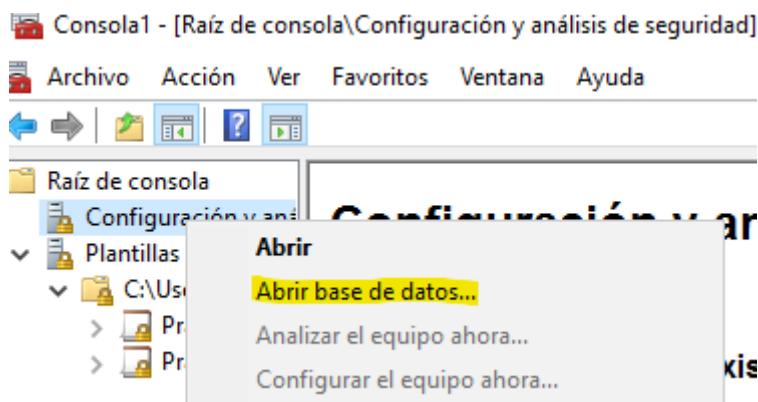
Haremos gpupdate /force para aplicar los cambios y reiniciará el servidor.

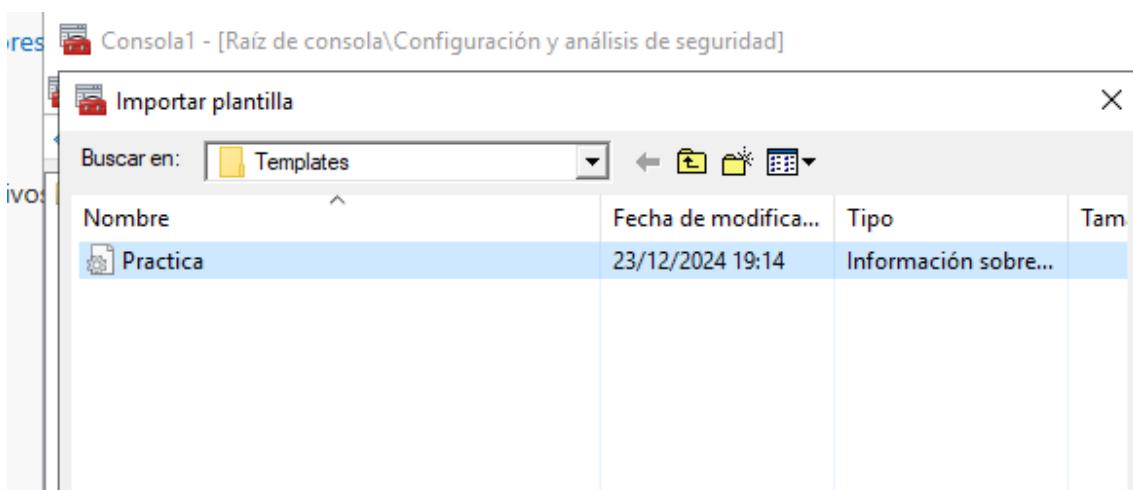
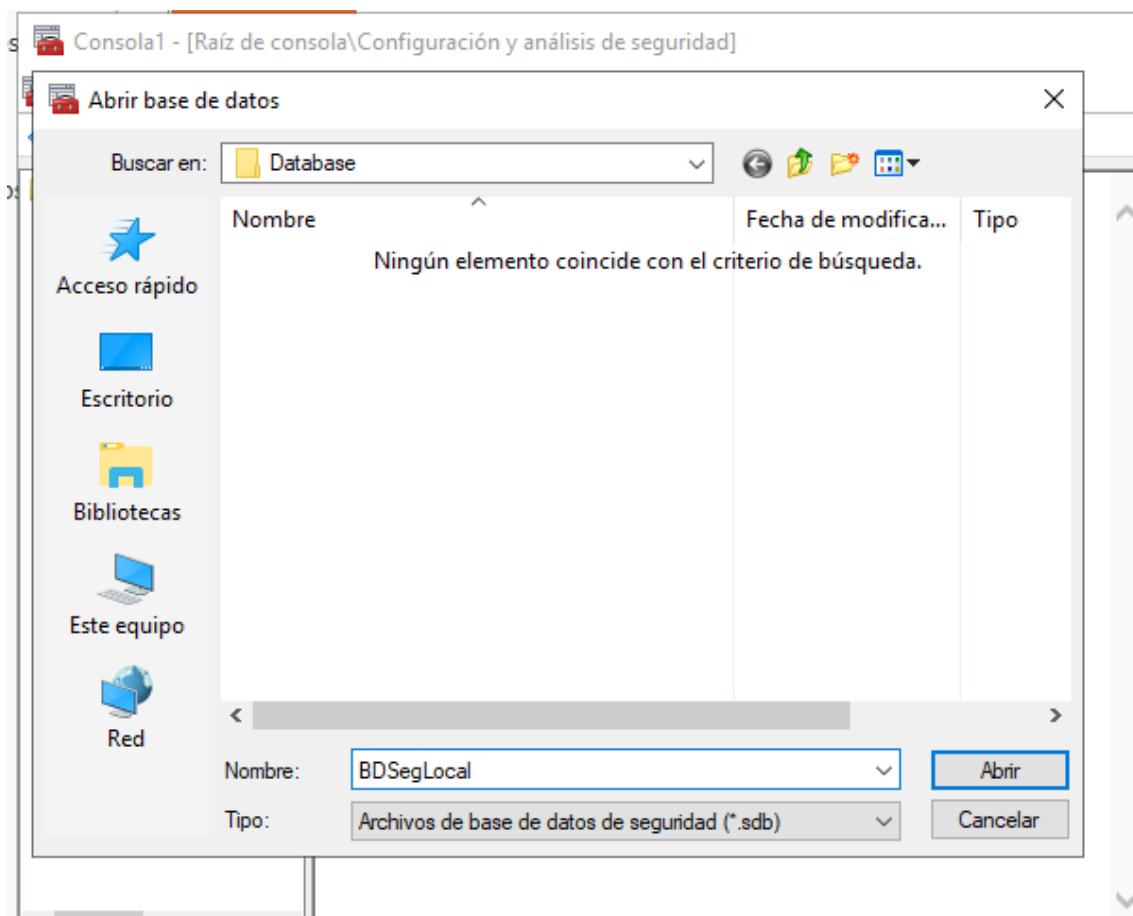
```
C:\Users\Administrador>gpupdate /force
Actualizando directiva...
La actualización de la directiva de equipo se completó correctamente.
→
```



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.





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

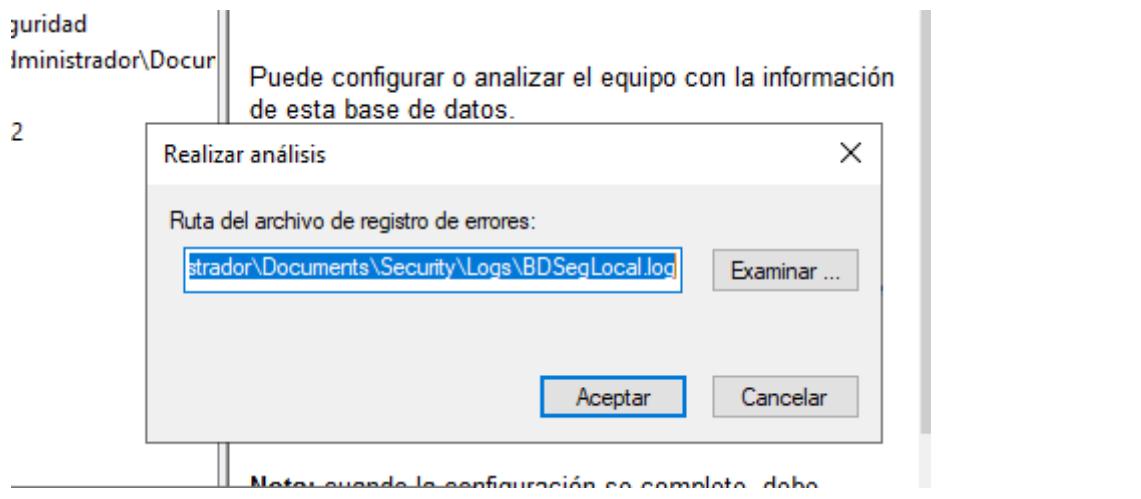
Lo modifco para que provoque algún error.

Directiva	Configuración de directiva
Almacenar contraseñas con cifrado reversible	Habilitada
Auditoría de longitud mínima de contraseña	No está definido
Exigir historial de contraseñas	24 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad	Habilitada
Longitud mínima de la contraseña	2 caracteres
Vigencia máxima de la contraseña	2 días
Vigencia mínima de la contraseña	1 días

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.

The screenshot shows the 'Configuración y análisis de seguridad' (Security Configuration and Analysis) interface. The left pane displays a tree structure with nodes like 'Raíz de consola', 'Configuración y análisis de seguridad', and 'Plantillas de seguimiento'. The right pane shows a context menu with several options: 'Abrir' (Open), 'Abrir base de datos...', 'Analizar el equipo ahora...' (highlighted in yellow), 'Configurar el equipo ahora...', 'Guardar', 'Importar plantilla...', 'Exportar plantilla...', 'Ver el archivo de registro', 'Ver', 'Nueva ventana desde aquí', 'Nueva vista del cuadro de tareas...', and 'Ayuda'. The path 'C:\Users\Administrador\Documentos' is visible at the top of the right pane.



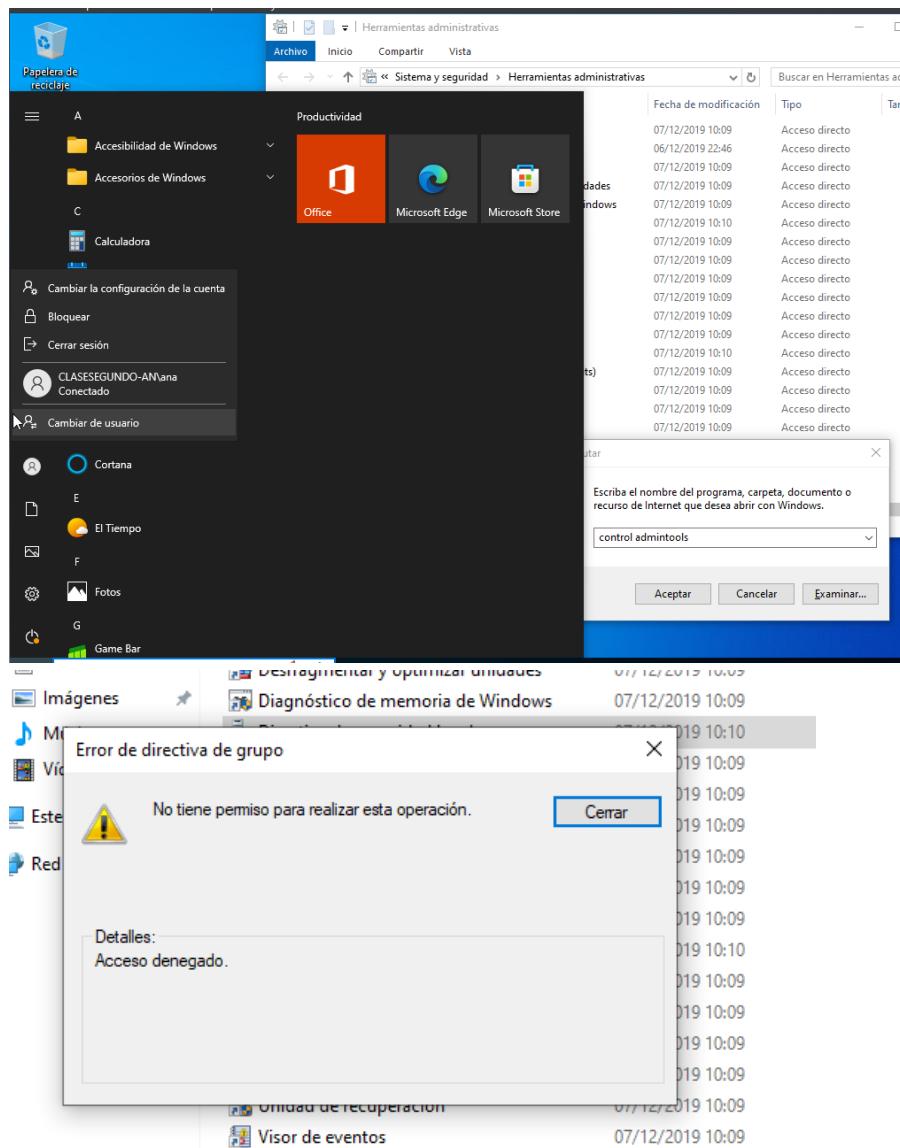
```
BDSegLocal: Bloc de notas
Archivo Edición Formato Ver Ayuda
-----
sábado, 28 de diciembre de 2024 20:36:15
----Se inicializó correctamente el motor de análisis.-----
----Leyendo información de configuración...

----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.



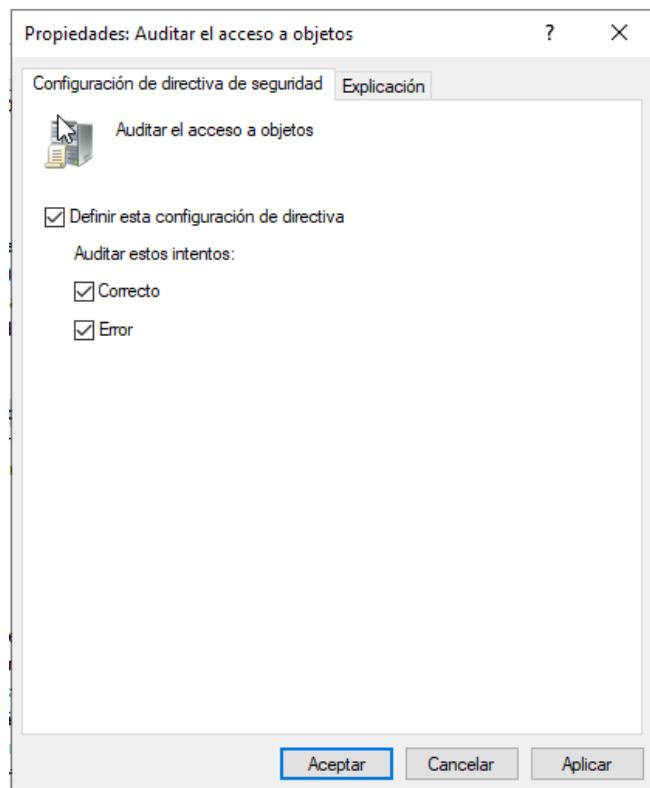
Al intentar acceder a algunas herramientas, aparecerá un error de permisos o se nos solicitará ingresar un usuario y contraseña con privilegios de administrador.

5. Auditorías.

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

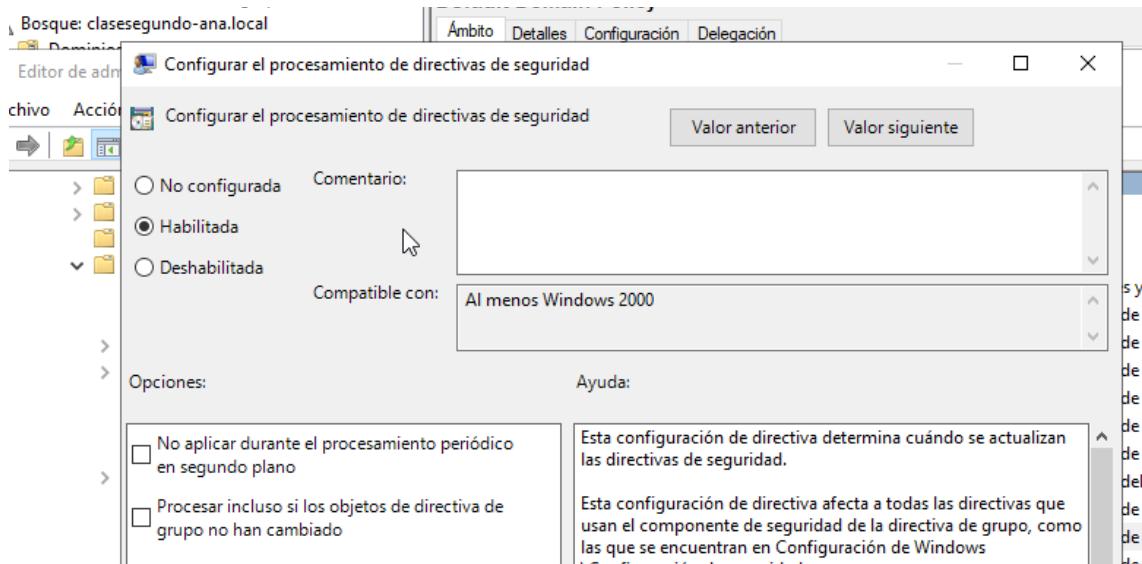
Para ello, modificamos la "Política de dominio predeterminada" y accedemos a la "Configuración del equipo", luego a "Configuración de Windows", después a "Configuración de seguridad", luego a "Directivas locales" y finalmente a "Directiva de auditorías". En este punto, habilitamos las opciones "Correcto"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

Directiva	Configuración de directiva
Auditar el acceso a objetos	Correcto, Erróneo
Auditar el acceso al servicio de directorio	Correcto, Erróneo
Auditar el cambio de directivas	No está definido
Auditar el seguimiento de procesos	No está definido
Auditar el uso de privilegios	No está definido
Auditar eventos de inicio de sesión	No está definido
Auditar eventos de inicio de sesión de cuenta	No está definido
Auditar eventos del sistema	No está definido
Auditar la administración de cuentas	No está definido



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.

Administración de directivas de grupo

Bosque: clasessegundo-ana.local

Domínicos

clasessegundo-ana.local

Editor de administración de directivas de grupo

Archivo Acción Ver Ayuda

Default Domain Controllers Policy

Ámbito Detalles Configuración Delegación

Vínculos

Directiva

Directiva	Configuración de directiva
Auditar el acceso a objetos	Correcto, Erróneo
Auditar el acceso al servicio de directorio	No está definido
Auditar el cambio de directivas	No está definido
Auditar el seguimiento de procesos	No está definido
Auditar el uso de privilegios	No está definido
Auditar eventos de inicio de sesión	No está definido
Auditar eventos de inicio de sesión de cuenta	No está definido
Auditar eventos del sistema	No está definido
Auditar la administración de cuentas	No está definido

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.

Administración de directivas de grupo

Bosque: clasessegundo-ana.local

Editor de administración de directivas de grupo

Archivo Acción Ver Ayuda

Default Domain Policy [SERVIDOR-AI]

Ámbito Detalles Configuración Delegación

Directiva

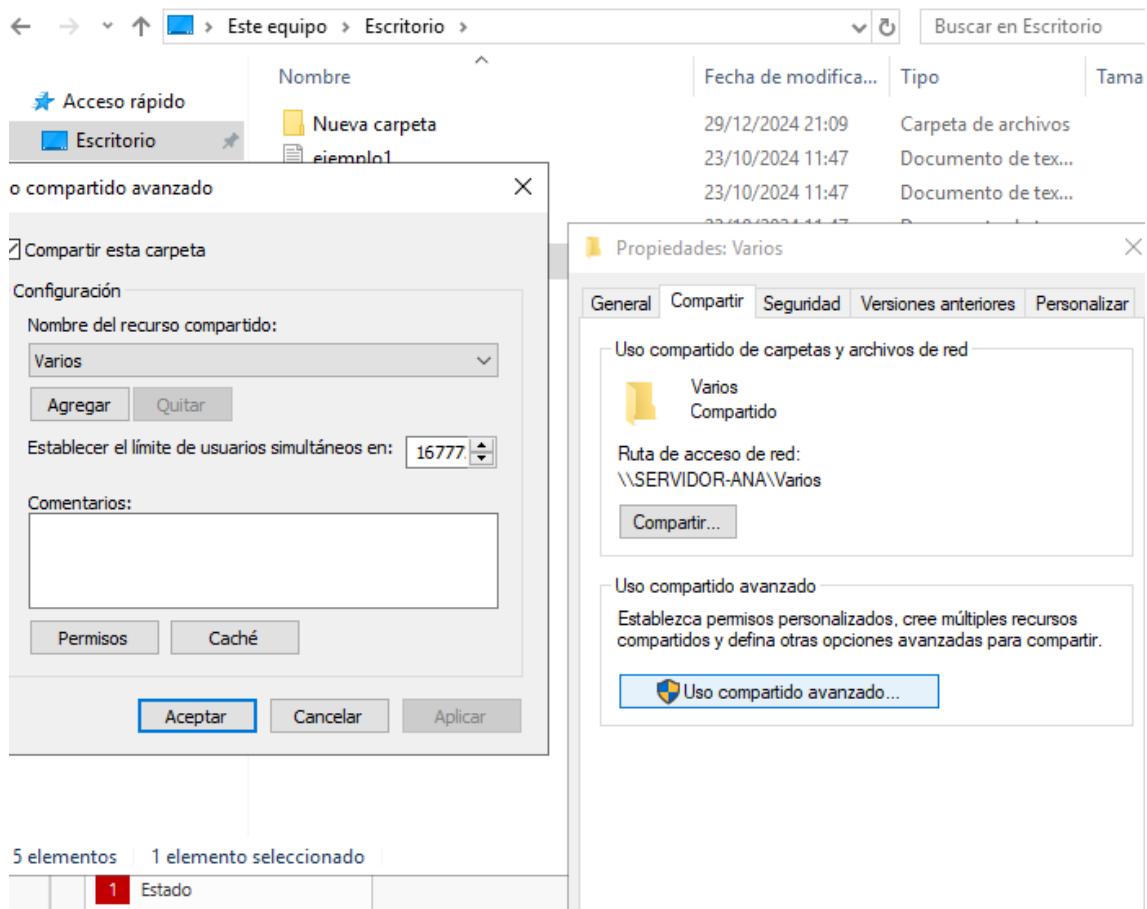
Directiva	Configuración de directiva
Auditar el acceso a objetos	Correcto, Erróneo
Auditar el acceso al servicio de directorio	Correcto, Erróneo
Auditar el cambio de directivas	No está definido
Auditar el seguimiento de procesos	No está definido
Auditar el uso de privilegios	No está definido
Auditar eventos de inicio de sesión	Correcto, Erróneo
Auditar eventos de inicio de sesión de cuenta	No está definido
Auditar eventos del sistema	No está definido
Auditar la administración de cuentas	No está definido

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

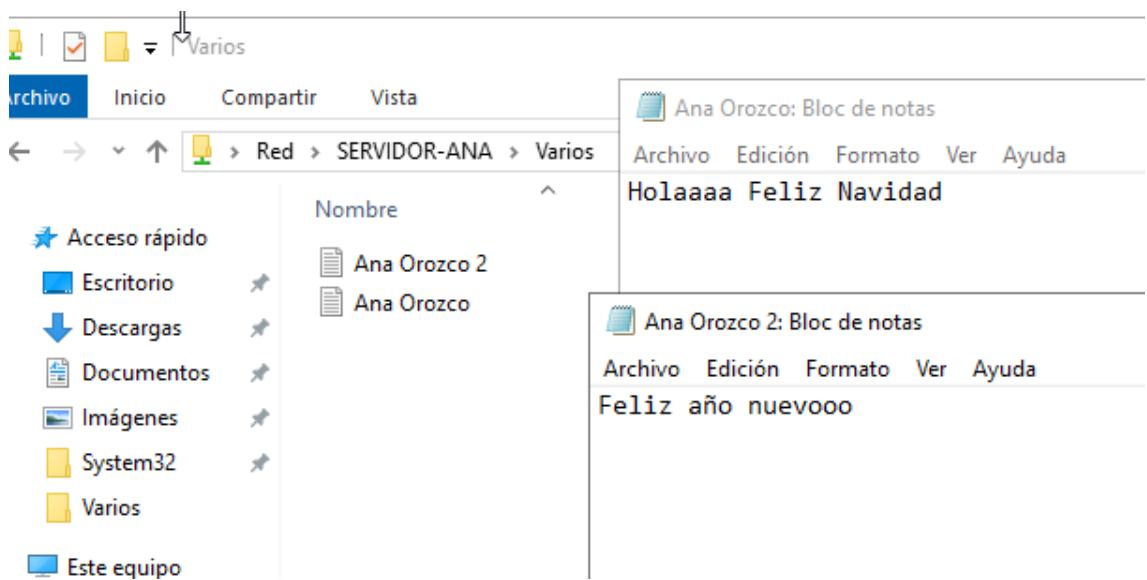
The screenshot shows the Windows Active Directory Users and Computers interface. On the left, a tree view shows the structure: 'Usuarios y equipos de Active Dir' > 'clasesegundo-ana.local' > 'Administracion' > 'CFGs'. Inside 'CFGs', there are three subfolders: 'Primero', 'Profesores', and 'Segundo'. A new folder named 'Varios' is being created. On the right, a table lists existing objects in the 'CFGs' container:

	Nombre	Tipo	Descripción
1	GrupoTodos	Grupo de segu...	
2	Primero	Unidad organi...	
3	Profesores	Unidad organi...	
4	Segundo	Unidad organi...	
5	Varios	Carpeta comp...	

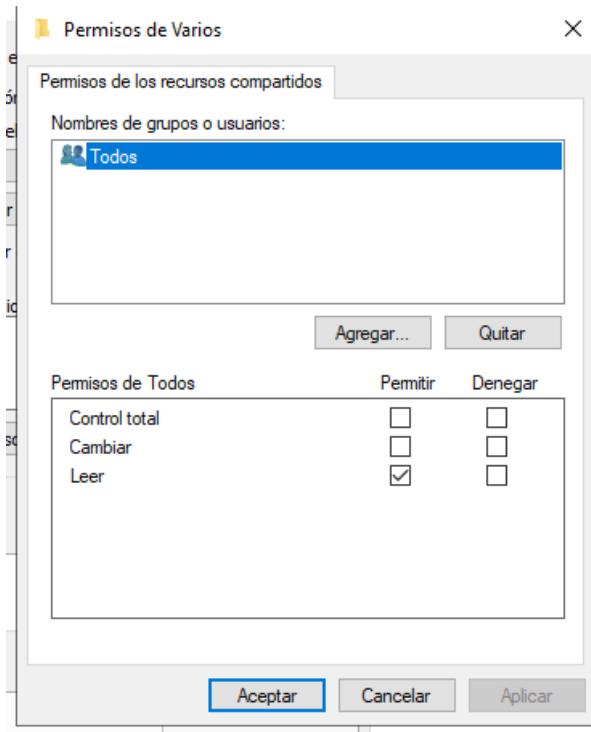
Below this, a 'Propiedades: Varios' dialog box is open. The 'General' tab is selected. It shows the folder icon and the name 'Varios'. The 'Descripción:' field is empty. The 'Nombre UNC:' field contains '\\SERVIDOR-ANA\Varios'. At the bottom, there are buttons for 'Aceptar', 'Cancelar', and 'Aplicar'.



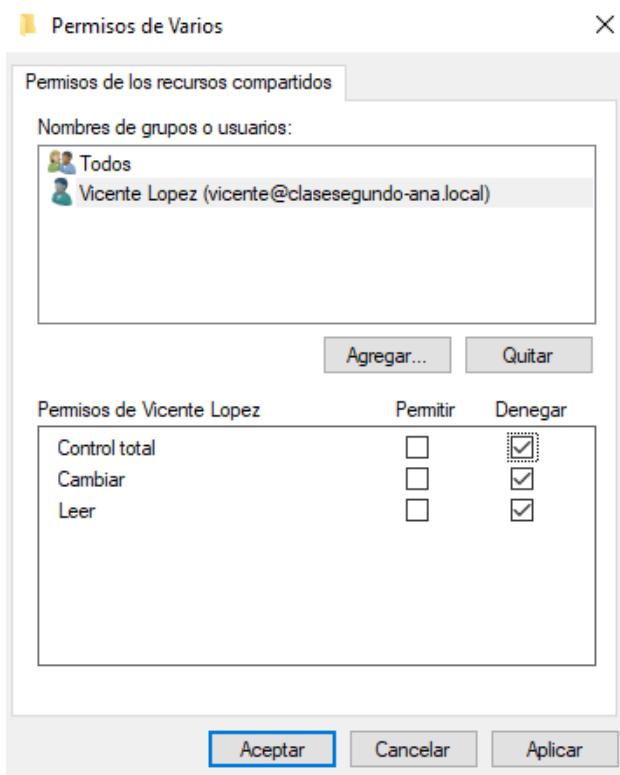
- Crear algunos archivos de texto en su interior que contengan, al menos, una línea.



- Compartirla para todos los usuarios con permisos únicamente de lectura

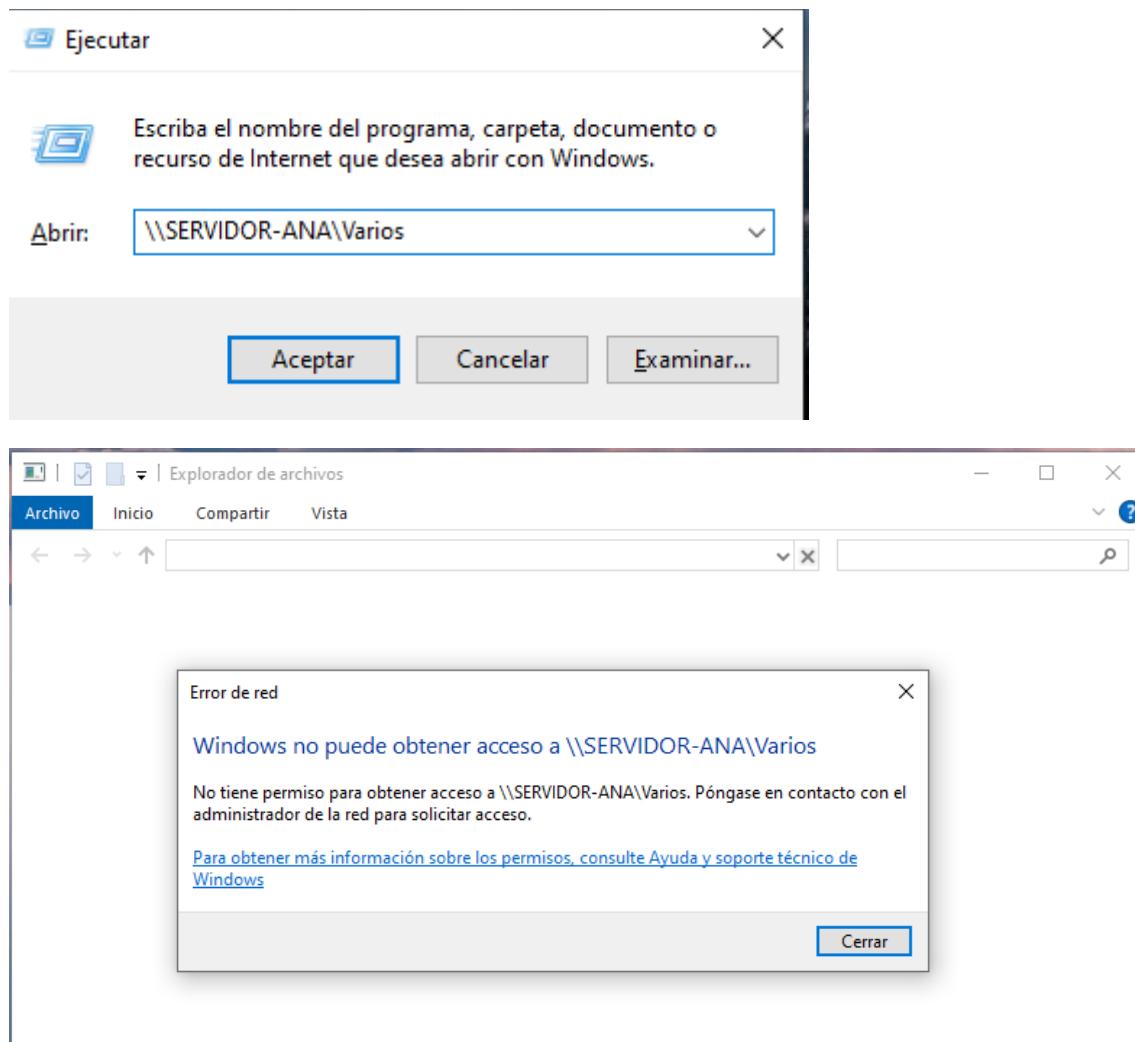


- Quitar todos los permisos al usuario Vicente



- Auditar todos los accesos erróneos para Vicente

Primero crearé esos errores para poder auditárslos:



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

The screenshot shows the Windows Event Viewer interface. At the top, there is a header with columns: Palabras clave, Fecha y hora, Origen, Id. del ..., and Categoría de la tarea. Below the header, a single event is listed:

Palabras clave	Fecha y hora	Origen	Id. del ...	Categoría de la tarea
>Error de auditoría	29/12/2024 21:43:23	Micros...	5145	Detailed File Share

The main pane displays the details of Event 5145, titled "Evento 5145, Microsoft Windows security auditing." It has two tabs: General and Detalles, with Detalles selected. The General tab contains a large amount of text describing the audit attempt, which is mostly illegible due to the small font size. The Detalles tab contains the following structured data:

Sujeto:

Id. de seguridad:	CLASESEGUNDO-AN\vicente
Nombre de cuenta:	vicente
Dominio de cuenta:	CLASESEGUNDO-AN
Id. de inicio de sesión:	0x3B2C0F

Información de red:

Tipo de objeto:	File
Dirección de origen:	192.168.1.32
Puerto de origen:	56686

Información de recurso compartido:

Nombre de recurso compartido:	*\Varios
Ruta de acceso de recurso compartido:	\??\C:\Users\Administrador\Desktop

Nombre de registro: Seguridad

- Auditar todos los accesos correctos y erróneos para packomaster

Haré lo mismo con el usuario paco:

Auditoría correcta:

Seguridad Número de eventos: 191.526 (!) Nuevos eventos disponibles

Palabras clave	Fecha y hora	Origen	Id. del ...	Categoría de la tarea
🔍 Auditoría correcta	29/12/2024 23:32:03	Micros...	5156	Filtering Platform Conne...
🔍 Auditoría correcta	29/12/2024 23:32:02	Micros...	5145	Detailed File Share
🔍 Auditoría correcta	29/12/2024 23:32:02	Micros...	5145	Detailed File Share
🔍 Auditoría correcta	29/12/2024 23:32:02	Micros...	5145	Detailed File Share
🔍 Auditoría correcta	29/12/2024 23:32:02	Micros...	5145	Detailed File Share
🔍 Auditoría correcta	29/12/2024 23:32:02	Micros...	5145	Detailed File Share
🔍 Auditoría correcta	29/12/2024 23:32:02	Micros...	5145	Detailed File Share
🔍 Auditoría correcta	29/12/2024 23:32:02	Micros...	5145	Detailed File Share

Evento 5145, Microsoft Windows security auditing.

General Detalles

Vista descriptiva Vista XML

+ System
- EventData

SubjectUserId S-1-5-21-1591890982-352480599-646797091-1111
SubjectUserName paco
SubjectDomainName CLASESEGUNDO-AN
SubjectLogonId 0x40f2bb
ObjectType File
IpAddress 192.168.1.32
IpPort 53902
ShareName *\Varios
ShareLocalPath \?\?C:\Users\Administrador\Desktop\Varios

Error de auditoría:

Evento 5145, Microsoft Windows security auditing.

Icono	Descripción	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
	Error de auditoría	29/12/2024 23:53:33	Micros...	5145	Detailed File Share
	Auditoría correcta	29/12/2024 23:53:33	Micros...	5145	Detailed File Share
	Auditoría correcta	29/12/2024 23:53:33	Micros...	5145	Detailed File Share
	Error de auditoría	29/12/2024 23:53:32	Micros...	5152	Filtering Platform Packet...
	Error de auditoría	29/12/2024 23:53:30	Micros...	5145	Detailed File Share
	Error de auditoría	29/12/2024 23:53:27	Micros...	5152	Filtering Platform Packet...
	Auditoría correcta	29/12/2024 23:53:27	Micros...	5145	Detailed File Share

Nombre de registro: Seguridad

- Realizar varios accesos incorrectos desde un cliente:
- Accesos con usuarios existentes, pero contraseña incorrecta

Seguridad Número de eventos: 194,101 (0) Nuevos eventos disponibles

Palabras clave	Fecha y hora	Origen	Id. del ...	Categoría de la tarea
	29/12/2024 23:59:32	Micros...	5152	Filtering Platform Packet...
	29/12/2024 23:59:27	Micros...	5152	Filtering Platform Packet...
	29/12/2024 23:59:18	Micros...	5156	Filtering Platform Conne...
	29/12/2024 23:59:17	Micros...	4634	Logoff
	29/12/2024 23:59:17	Micros...	4627	Group Membership
	29/12/2024 23:59:17	Micros...	4624	Logon
	29/12/2024 23:59:17	Micros...	4672	Special Logon

Evento 5152, Microsoft Windows security auditing.

General Detalles

La Plataforma de filtrado de Windows bloqueó un paquete.

Información de aplicación:
Id. de proceso: 0
Nombre de aplicación: -

Información de red:
Dirección: Enlace interno
Dirección de origen: 192.168.1.12

Nombre de registro: Seguridad
Origen: Microsoft Windows security Registrado: 29/12/2024 23:59:32
Id. del evento: 5152 Categoría de tarea: Filtering Platform Packet Drop
Nivel: Información Palabras clave: Error de auditoría
Usuario: No disponible Equipo: servidor-ana.clasesegundo-ana.lc
Código de operación: Información
Más información: Ayuda Registro de eventos

Acciones

- Seguridad
 - Abrir registro guardado...
 - Crear vista personalizada...
 - Importar vista personalizada...
 - Vaciar registro...
 - Filtrar registro actual...
 - Propiedades
 - Buscar...
 - Guardar todos los eventos...
 - Adjuntar tarea a este registro...
 - Ver
 - Actualizar
 - Ayuda
- Evento 5152, Microsoft Windows security
 - Propiedades de evento
 - Adjuntar tarea a este evento...
 - Guardar eventos seleccionados
 - Copiar
 - Actualizar
 - Ayuda

Otro usuario

El nombre de usuario o la contraseña no son correctos. Intentelo de nuevo.

Aceptar

- Accesos con usuarios inexistentes

The screenshot shows the Windows Event Viewer interface. At the top, there's a table with columns: Palabras clave, Fecha y hora, Origen, Id. del ..., and Categoría de la tarea. Below the table, a specific event is expanded:

Evento 5152, Microsoft Windows security auditing.

General tab selected.

Detalles pane content:

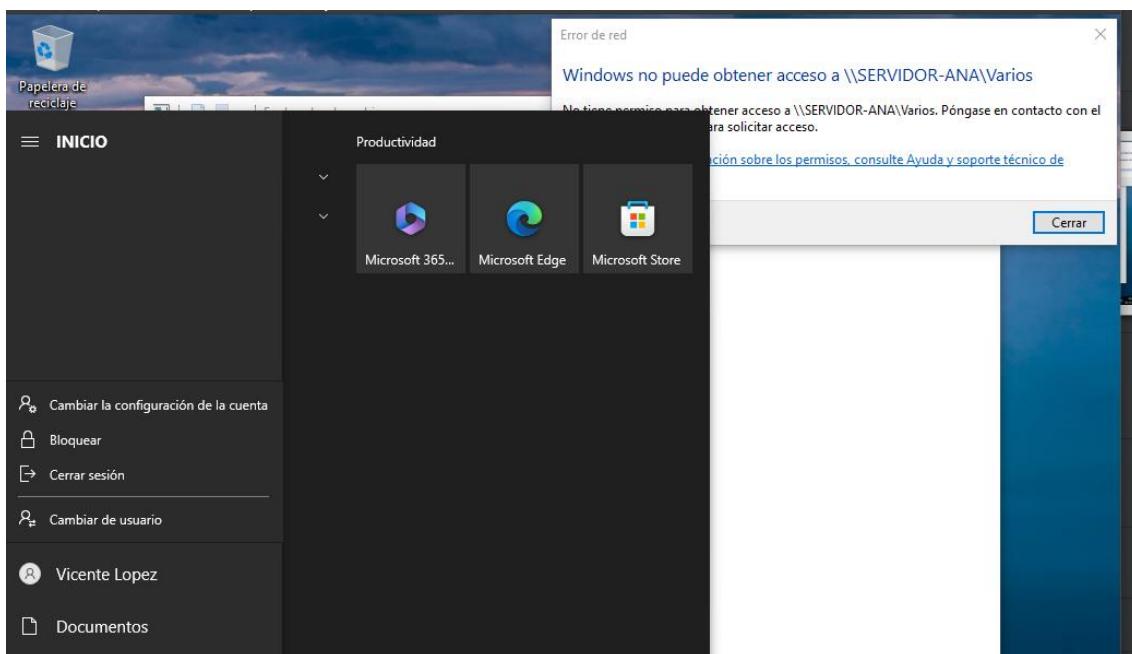
- La Plataforma de filtrado de Windows bloqeo un paquete.
- Información de aplicación:
 - Id. de proceso: 0
 - Nombre de aplicación: -
- Información de red:
 - Dirección: Enlace interno
 - Dirección de origen: 192.168.1.12

- 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.



Palabras clave | Fecha y hora | Origen | Id. del ... | Categoría de la tarea

Error de auditoría | 29/12/2024 21:43:23 | Micros... | 5145 | Detailed File Share

Evento 5145, Microsoft Windows security auditing.

General Detalles

deseado al cliente.

Sujeto:

Id. de seguridad:	CLASESEGUNDO-AN\vicente
Nombre de cuenta:	vicente
Dominio de cuenta:	CLASESEGUNDO-AN
Id. de inicio de sesión:	0x3B2C0F

Información de red:

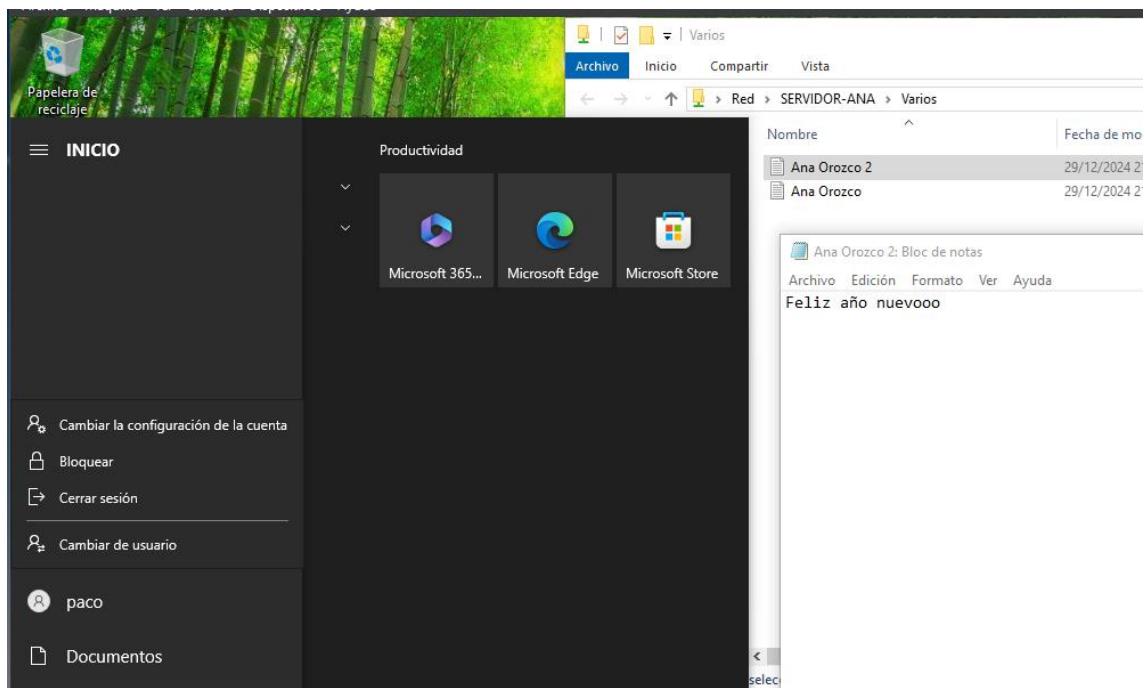
Tipo de objeto:	File
Dirección de origen:	192.168.1.32
Puerto de origen:	56686

Información de recurso compartido:

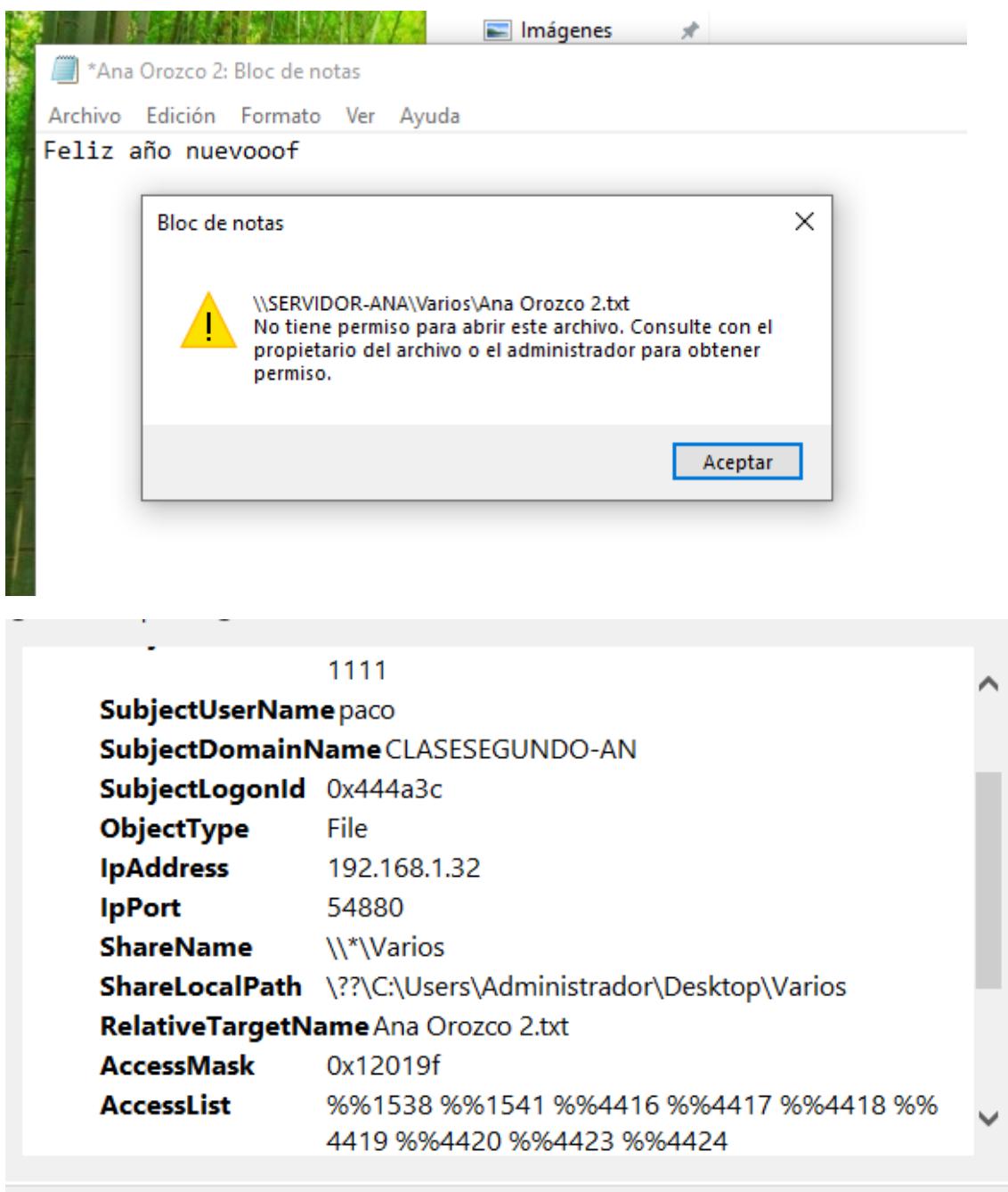
Nombre de recurso compartido:	***Varios
Ruta de acceso de recurso compartido:	\?\?C:\Users\Administrador\Desktop

Nombre de registro: Seguridad

- 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



Event 5145, Microsoft Windows security auditing.

General Detalles

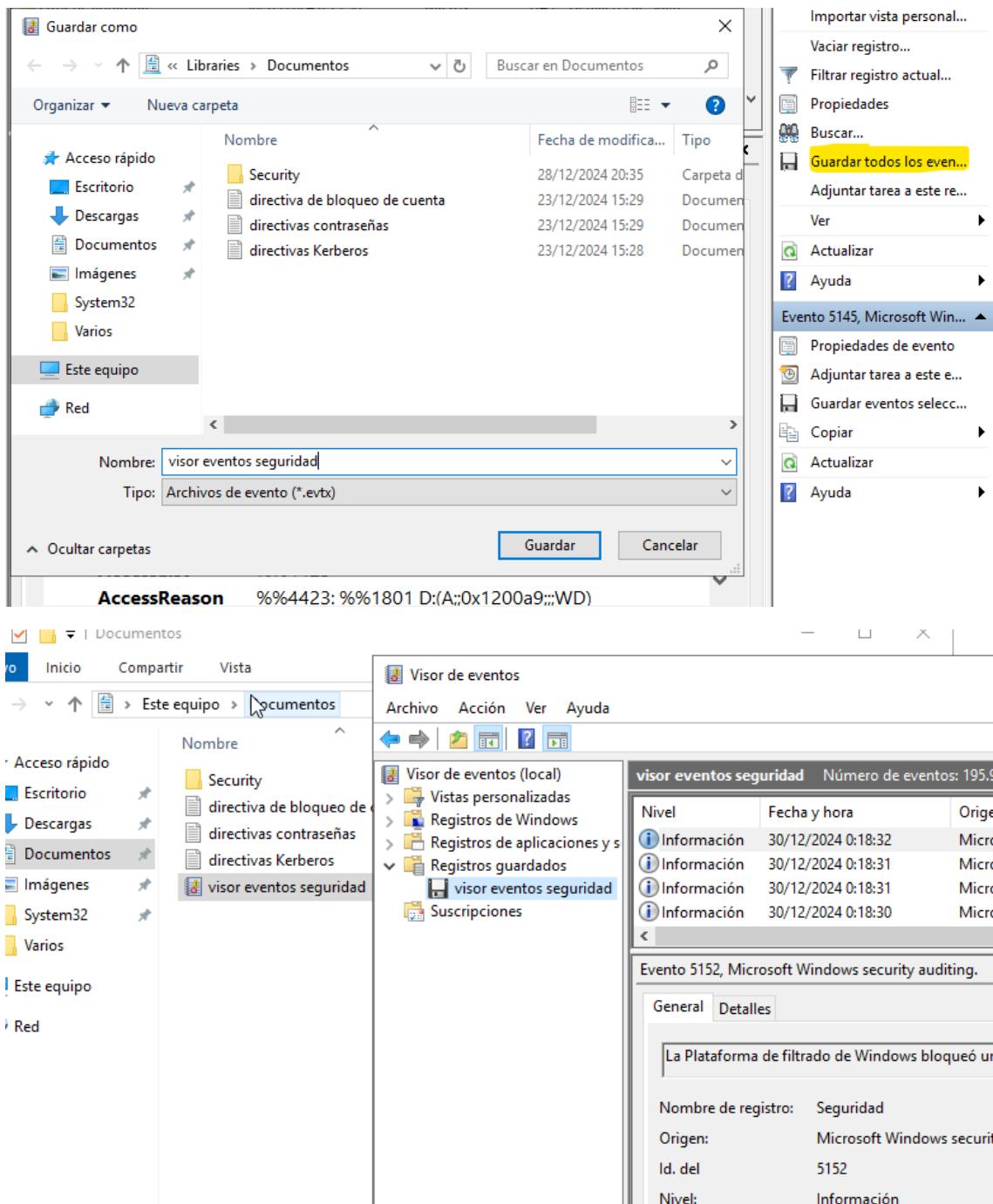
Vista descriptiva Vista XML

SubjectDomainName CLASESEGUNDO-AN
SubjectLogonId 0x444a3c
ObjectType File
IpAddress 192.168.1.32
IpPort 54880
ShareName *\Varios
ShareLocalPath \??\C:\Users\Administrador\Desktop\Varios
RelativeTargetName Nuevo documento de texto.txt
AccessMask 0x120196
AccessList %1538 %1541 %4417 %4418 %4420 %4423 %4424
AccessReason %1538: %1804 %1541: %1801 D: (A;;0x1200a9;;;WD) %4417: %1805 %4418: %

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.



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.