Unidad 8

Directivas de seguridad y auditorías

Implantación de sistemas operativos

Índice

Introducción

En las unidades anteriores se han ido viendo los objetos del AD y como trabajar con ellos, como se limita a los usuarios en temas de trabajo con carpetas, etc.

Pero, hay otro aspecto que puede que sea necesario limitar para otros usuarios, que no es simplemente el acceso a archivos, sino el poder o no usar ciertas utilidades del sistema o incluso predefinir y establecer cierto uso de aplicaciones.

Para esto, nacen las directivas de seguridad de un equipo, que también se gestionan desde el controlador de dominio y que a lo largo de esta unidad vamos a ver como funcionan y en que consisten, al igual que aprenderemos como manejarlas.

Por último, si se crean restricciones, hay que saber quién las incumple o controlar si ciertas restricciones no se han tomado y se deberían de tomar. Para esto, es necesario que se controle o monitoricen una serie de actividades en el equipo, aquí nacen las auditorías.

Veremos también como trabajan las auditorías y sabremos como crearlas y en que consisten dependiendo del tipo de auditoría que se use.

Al finalizar esta unidad

- Conoceremos lo que son las directivas de seguridad.
- Sabremos lo que son las directivas de grupo.
- Seremos capaces de identificar las distintas directivas de grupo que puede haber en el dominio.
- Podremos crear una nueva directiva de grupo.
- Sabremos como modificar la configuración de las directivas y la forma de aplicarla.
- Conoceremos como ejecutar una aplicación como otro usuario.
- Sabemos lo que son las auditorías.
- Seremos capaces de establecer una configuración de auditoría.
- Podremos ver los distintos sucesos generados por la auditoría.

8.1. Las directivas de seguridad

Las **directivas de seguridad** en Windows son una serie de normas donde se refleja el comportamiento que debe de tener el equipo en lo referente a la seguridad.

Existen dos tipos principales:

- **Directivas de seguridad local.** Son las usadas cuando lo que tenemos es un equipo con sistema operativo Windows, pero no tienen un Directorio Activo instalado (Windows 10 o Windows Server sin AD). Los nodos de configuración son menores que en otros casos. Si queremos configurarlas, debemos de hacer lo siguiente:

  Menú de Inicio → Herramientas administrativas → Directivas de seguridad local

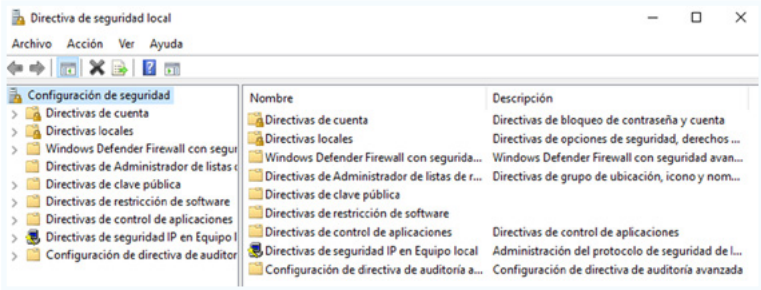

Imagen 1. Directivas de seguridad local.

- **Directiva de seguridad de dominio.** Son las directivas que tenemos en un sistema Windows Server que tiene un Active Directory instalado, es decir, querer modificar la configuración de seguridad para los equipos dentro del dominio. Si queremos configurar estas directivas, debemos de hacer lo siguiente:

  Inicio → Herramientas administrativas → Administración de directivas de grupo

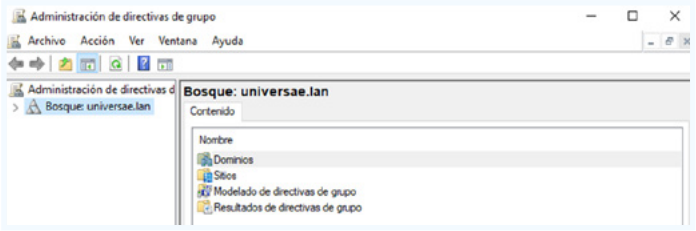

Imagen 2. Administración de directivas de grupo

Dentro de estas últimas, además, tenemos las **directivas de seguridad del controlador de dominio**. Funcionan como las últimas en todo, pero en este caso, la configuración que se modifica es para otros controladores de dominio.

También albergan aquí directivas de seguridad para objetos del AD, como pueden ser las Unidades organizativas.

8.2. Las directivas de grupo

Las directivas de grupo son también conocidas como GPO y nos ayudan a identificar una serie de normas hacer la seguridad del equipo y del usuario. Su influencia pasa por usuarios, grupos, sitios, dominios, o unidades organizativas.

Por eso, su orden de aplicación es el siguiente:

- **Directiva de equipo local.**
- **Directiva de usuario local.**
- **Directiva de grupo del sitio.**
- **Directiva de grupo del dominio.**
- **Directiva de grupo de la unidad organizativa.**
- **Directiva de grupo del controlador de dominio**

Si le damos a editar la directiva de grupo por defecto, podemos ver, que se divide principalmente en dos sectores:

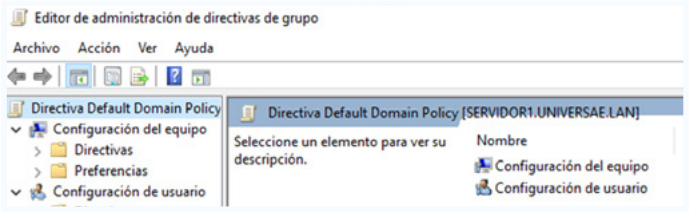

Imagen 3. Editor de administración de directivas de grupo

Configuración del equipo

Los cambios que se realizan en las directivas afectan cada vez que se inicia el equipo, no importa que usuario lo inicie. Se suelen conformar por:

- **Directivas:**
  - **Configuración de software:**
    - Instalación de software.
  - **Configuración de Windows:**
    - Scripts (inicio o apagado).
    - Directiva de resolución de nombres.
    - Impresoras implementadas.
    - Configuración de seguridad:
      - Directivas de cuenta:
        - Directivas de contraseñas.
        - Directiva de bloqueo de cuenta.
        - Directiva Kerberos.

- Directivas locales:
  - Directiva de auditoría.
  - Asignación de derechos de usuario.
  - Opciones de seguridad.
- Registro de eventos.
- Grupos restringidos.
- Servicios del sistema.
- Registro.
- Sistema de archivos:
  - Directiva de acceso central.
- Directivas de red cableada (IEEE 802.3).
- Windows defender Firewall con seguridad avanzada.
- Directivas de Administrador de listas de redes.
- Directivas de red inalámbrica (IEEE 802.11).
- Directivas de clave pública:
  - Sistema de cifrado de archivos (EFS).
  - Protección de datos.
  - Cifrado de unidad BitLocker.
  - Certificado de desbloqueo en red de Cifrado de unidad BitLocker.
  - Configuración de la solicitud de certificados automática.
  - Entidades de certificación raíz de confianza.
  - Confianza empresarial.
  - Entidades de certificación intermedias.
  - Editores de confianza.
  - Certificados en los que no se confía.
  - Personas de confianza.
- Directivas de restricción de software.
- Directivas de control de aplicaciones:
  - AppLocker.
- Directivas de seguridad IP en Active Directory.
- Configuración de directiva de auditoría avanzada:
  - Directivas de auditoría.

- QoS basada en directiva.

» **Plantillas administrativas:** definiciones de directiva recuperadas del equipo local:

- Componentes de Windows:
  - Administración de derechos digitales de Windows Media.
  - Administración remota de Windows.
  - Administración de ventanas del escritorio.
  - Agregar características a Windows 10.
  - Antivirus de Windows Defender.
  - Asistencia en línea.
  - Buscar.
  - Cámara.
  - Carpetas de trabajo.
  - Centro de movilidad de Windows.
  - Centro de seguridad.
  - Cifrado de unidad Bitlocker.
  - Compatibilidad de aplicaciones.
  - Compatibilidad de dispositivos y controladores.
  - Contenido de la nube.
  - Cuenta de Microsoft.
  - Entrada de texto.
  - Explorador de archivos.
  - Factor de autenticación secundario de Microsoft.
  - Historial de archivos.
  - Informe de errores de Windows.
  - Interfaz de usuario de credenciales.
  - Internet Information Services.
  - OneDrive.
  - Opciones de apagado.
  - Opciones de inicio de sesión de Windows.
  - Programador de tareas.
  - Registro de eventos.
  - Seguridad de Windows.
  - Servicios de Escritorio Remoto.
  - Tiempo de ejecución de la aplicación.
  - Visor de eventos.
  - Windows PowerShell.
  - Windows Update.

- Impresoras.
- Menú inicio y barra de tareas:
  - Notificaciones.
- Panel de control:
  - Configuración regional y de idioma:
    - Personalización de escritura a mano.
  - Cuentas de usuario.
  - Personalización.
- Red:
  - Administrador de conexiones de Windows.
  - Aislamiento de red.
  - Archivos sin conexión.
  - Cliente DNS.
  - Conexiones de red.
  - Configuración de TCP/IP.
  - Opciones de configuración SSL.
  - Servicio WLAN.
  - SNMP.
- Servidor.
- Sistema:
  - Acceso de almacenamiento extraíble.
  - Administración de comunicaciones de Internet.
  - Administración de energía.
  - Administrador del servidor.
  - Apagado.
  - Asistencia remota.
  - Cuotas de disco.
  - Directiva de grupo.
  - Directivas del sistema operativo.
  - Estado del almacenamiento.
  - Inicio de sesión.
  - Instalación de controladores.
  - Instalación de dispositivos.
  - Kerberos.
  - Net Logon.
  - Opciones de apagado.
  - Pantalla.
  - Perfiles de usuario.
  - Restaurar sistema.
  - Sistema de archivos.
  - Solución de problemas y diagnósticos.

Configuración de usuario

Este tipo de configuración se va a aplicar cada vez que un usuario inicie sesión. Sea en el equipo que sea. Los principales elementos son los siguientes:

- **Directivas:**
  - **Configuración de software:**
    - Instalación de Software.
  - **Configuración de Windows:**
    - Scripts.
    - Configuración de seguridad:
      - Directivas de clave pública:
        - Confianza empresarial.
        - Personas de confianza.
      - Directivas de restricción de software.
      - Redirección de carpetas.
      - Impresoras implementadas.
  - **Plantillas administrativas:**
    - Carpetas compartidas.
    - Componentes de Windows:
      - Administrador de ventanas del escritorio.
      - Agregar características a Windows 10.
      - Buscar.
      - Carpetas de trabajo.
      - Compatibilidad de aplicaciones.
      - Explorador de archivos:
        - Versiones anteriores.
      - Informe de errores de Windows.
      - Opciones de inicio de sesión de Windows.
      - Programador de tareas.
      - Reproductor de Windows Media.
      - Servicios de escritorio remoto:
        - Cliente de conexión a Escritorio Remoto.
        - Puerta de enlace del Escritorio Remoto.
      - Tiempo de ejecución de la aplicación.
      - Windows PowerShell.
      - Windows Update.
      - Menú de Inicio y barra de tareas;
        - Notificaciones
      - Panel de control:
        - Agregar o quitar programas.
        - Configuración regional y de idioma.
        - Impresoras.
        - Pantalla.
        - Programas.
      - Red:
        - Archivos sin conexión.
        - Conexiones de red.
      - Sistema:
        - Acceso de almacenamiento extraíble.
        - Administración de energía.
        - Directiva de grupo.
        - Inicio de sesión.
        - Instalación de controladores.
        - Opciones de Ctrl+Alt+Supr.
        - Perfiles de usuario.
        - Redirección de carpetas.
        - Servicios de configuración regional.

PARA TENER EN CUENTA

Para poder realizar cambios en las **GPO** es necesario tener los permisos de administrador sobre el equipo.

8.2.1. Las directivas de grupo incorporadas por defecto

En Windows Server, vienen dos directivas de grupo por defecto:

- **Default Domain Policy.** Si usamos esta directiva, sus cambios se aplican a todos los equipos que haya en el dominio y afectará tanto a la configuración del equipo de usuario.
- **Default Controller Domain Policy.** Se aplica a todos los servidores que actúen como controladores de dominio, afectando a configuración de equipo y de usuario.

Para acceder a ellas, seguimos los siguientes pasos:

1. Abrimos Administración de directivas de grupo.
2. Dentro de estas, escalamos del siguiente modo:
   a. Bosque
   b. Dominios
   c. Seleccionamos nuestro dominio
   d. Vamos a la sección Objetos de directiva de grupo
   e. Aquí podemos ver que ya se nos muestran las dos directivas predefinidas.

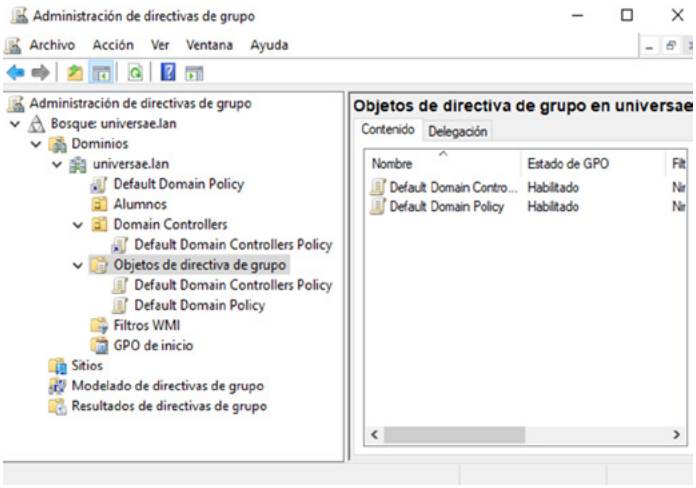

Imagen 4. Default Domain Controller Policy & Delfaut Domain Policy

PARA TENER EN CUENTA

En la imagen anterior podemos observar que hay varios Default Domain Controllers Policy, pero estos solo son un acceso directo del que en este apartado se ha introducido.

8.2.2. Como crear una directiva de grupo vinculada automáticamente

Vamos a ver en este momento como crear una directiva de grupo.

Aunque hay varios modos de crear las GPO, lo primero que vamos a ver es como crear una que automáticamente se vincule con una Unidad Organizativa.

Para desarrollar este tema, lo que vamos a hacer es mediante la GPO, deshabilitar las opciones de apagar, o reiniciar para todos los usuarios contenidos en la UO Alumnos que creamos en temas anteriores. El proceso que seguir es el siguiente:

1. Lo primero que debemos hacer es abrir Administración de directivas de grupo como hemos visto en el punto anterior.
2. Una vez aquí, seleccionamos la UO sobre la que queremos crear la GPO y hacemos clic derecho.
3. Elegimos la primera de las opciones que se nos presentan: Crear un GPO en este dominio y vincularlo aquí…

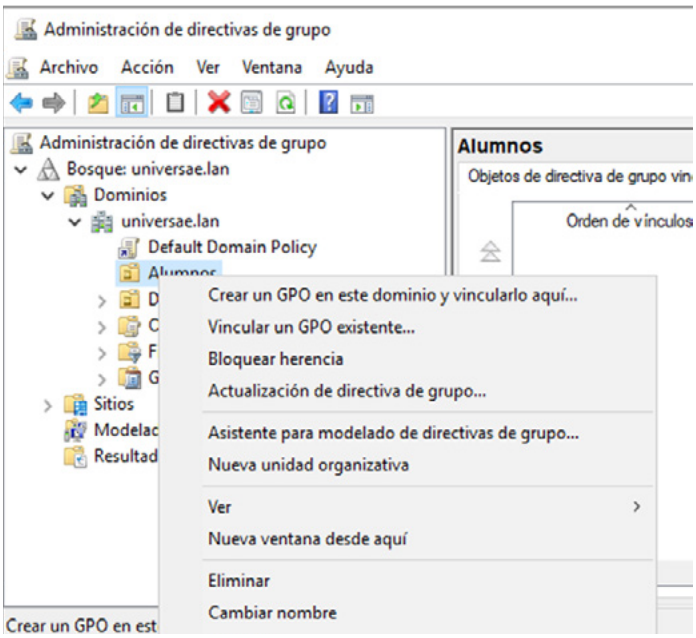

Imagen 5. Creación de GPO 1

4. Le damos un nombre a la GPO.

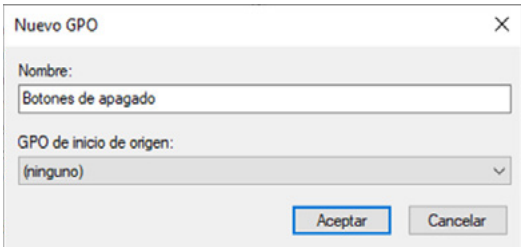

Imagen 6. Creación GPO 2

5. Podemos ver que ya aparece la GPO vinculada a la Unidad Organizativa.

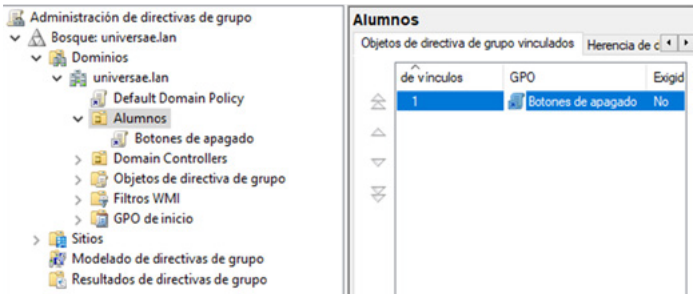

Imagen 7. Creación GPO 3

6. Nos posicionamos sobre la GPO y hacemos clic derecho.

7. Seleccionamos la primera opción, que nos dice Editar...

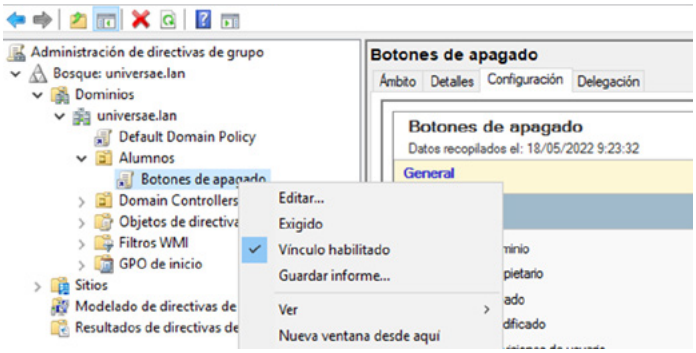

Imagen 8. Creación GPO 4

8. Se nos abre una consola de edición de las directivas como vimos anteriormente.

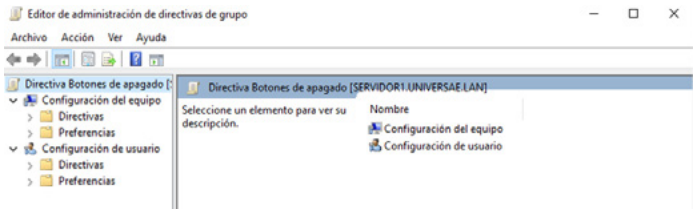

Imagen 9. Creación GPO 5

9. Seguimos el siguiente orden para llegar a la directiva que deseamos:

   a. Configuración de usuario

   b. Directivas

   c. Plantillas Administrativas

   d. Menú Inicio y barra de tareas

10. Una vez aquí, buscamos hasta encontrar la directiva Quitar y evitar el acceso a los comandos Apagar, Reiniciar, Suspender e Hibernar.

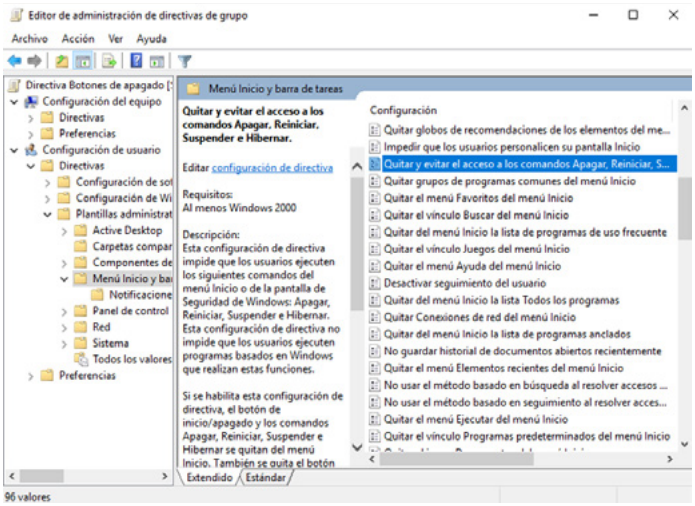

Imagen 10. Creación GPO 6

11. Clicamos sobre la directiva y se nos abre el cuadro de edición.

12. En este cuadro, Habilitamos la directiva, damos a Aplicar y a Aceptar.

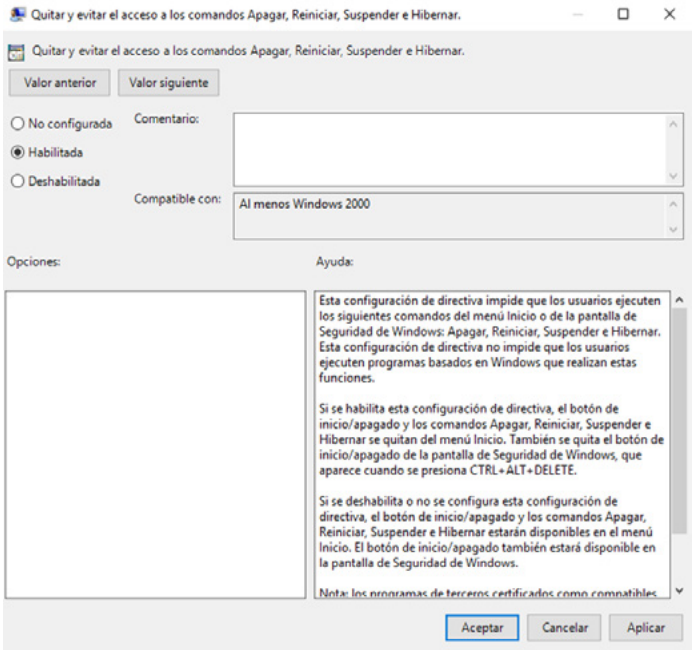

Imagen 11. Creación GPO 7

13. Si ahora iniciásemos sesión con cualquiera de los usuarios que se alojan en esa unidad organizativa, no podríamos apagar o reiniciar el ordenador desde los botones como se puede ver en la siguiente imagen.

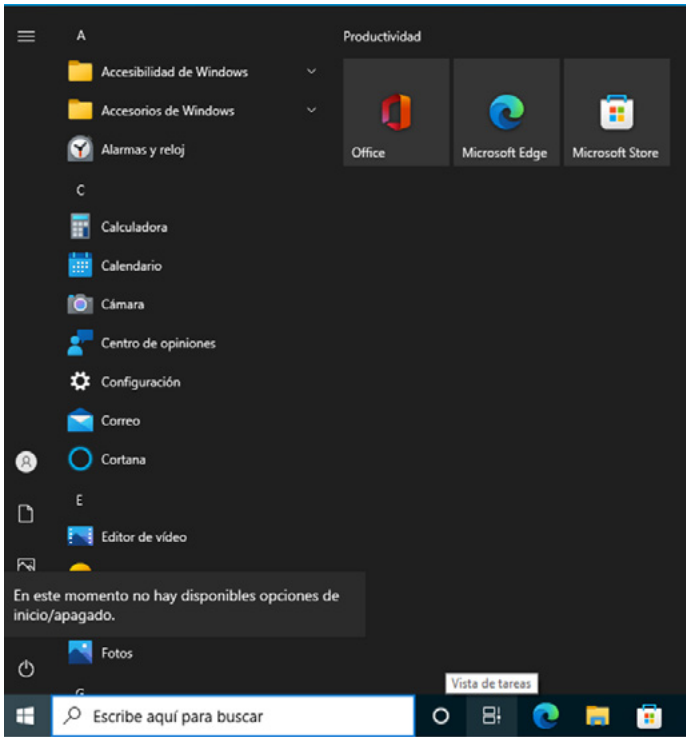

Imagen 12.Comprobación de la GPO, sin los botones de apagado

8.2.3. Como trabajar con las directivas en Windows Server

Hemos como se crea una directiva en Windows Server, y como vincularla directamente, pero se pueden hacer más cosas con una directiva de grupo.

Vamos a hacer un repaso por la consola **Administración de directivas de grupo**:

- Si nos posicionamos sobre la Unidad Organizativa con varias directivas, tenemos al lado derecho un panel con unas flechas que nos ayudan a **cambiar el orden de actuación de cada GPO**, para que, si hay contradicciones entre ellas, saber cuál se aplica primero.

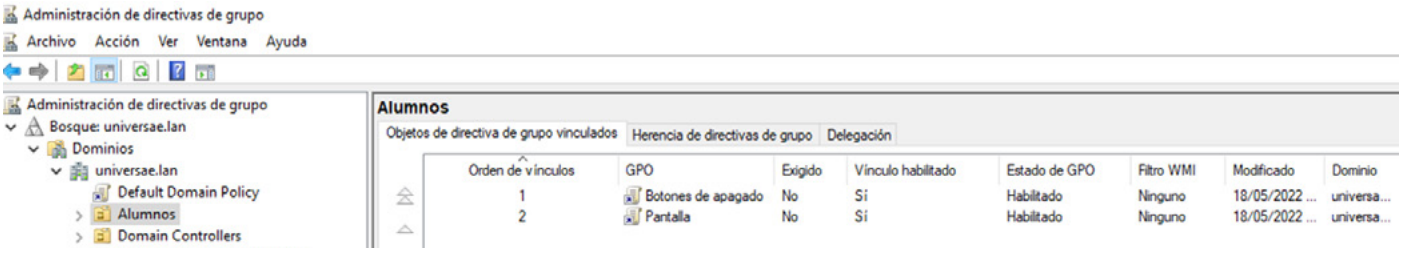

Imagen 13. Directivas en Windows Server 1

- Para que no se **anulen las peticiones de una directiva por otras**, hay que exigirla. Para esto lo que hacemos es clic derecho sobre la que deseamos y marcamos la opción Exigido.

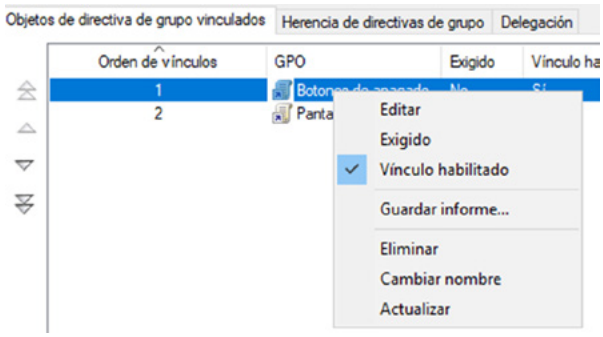

Imagen 14. Directivas en Windows Server 2

- Si queremos **modificar los permisos de alguna de las directivas de grupo**, lo que debemos de hacer es editar la GPO.
- Una vez dentro del editor, seleccionamos la pestaña Acción y Propiedades.

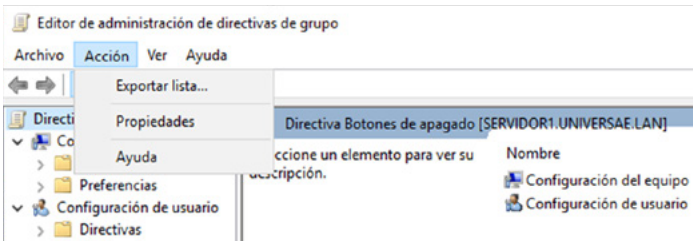

Imagen 15. Directivas en Windows Server 3

- Dentro de las propiedades podemos elegir Seguridad y ahí editamos los permisos como si de un archivo se tratase. (Esto se vio en unidades anteriores).

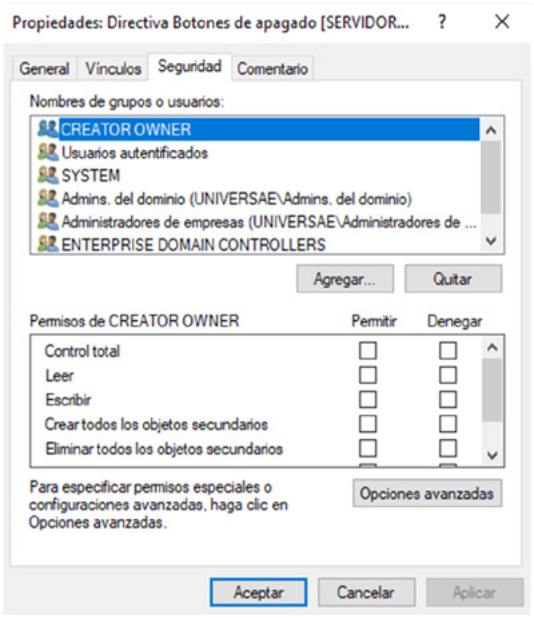

Imagen 16. Directivas en Windows Server 4

- Por último, en la Administración de directivas de grupo, lo que podemos hacer es posicionarnos sobre la GPO que queramos y visualizamos todas sus propiedades:
  - Ámbito: Dentro de esta sección tenemos:
    - Vínculo.
    - Filtrado de seguridad.
    - Filtrado WMI.

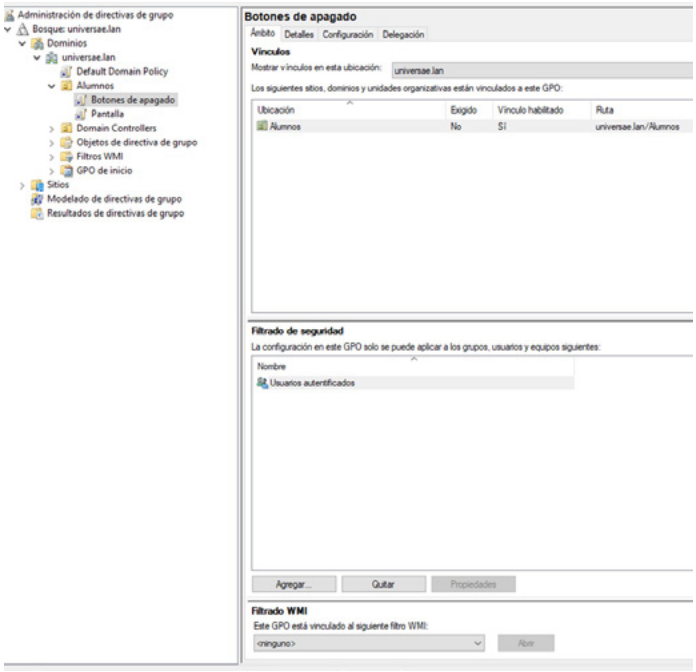

Imagen 17. Ámbito

» Detalles.

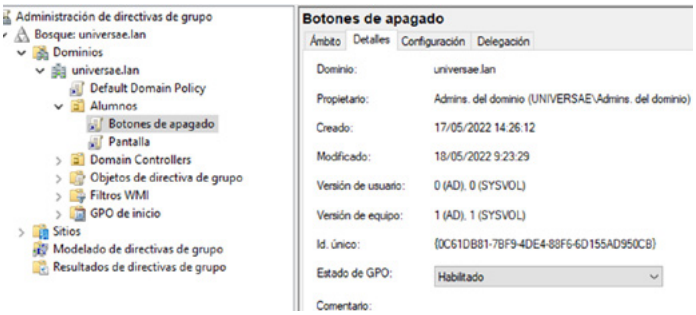

Imagen 18. Detalles

> Configuración.

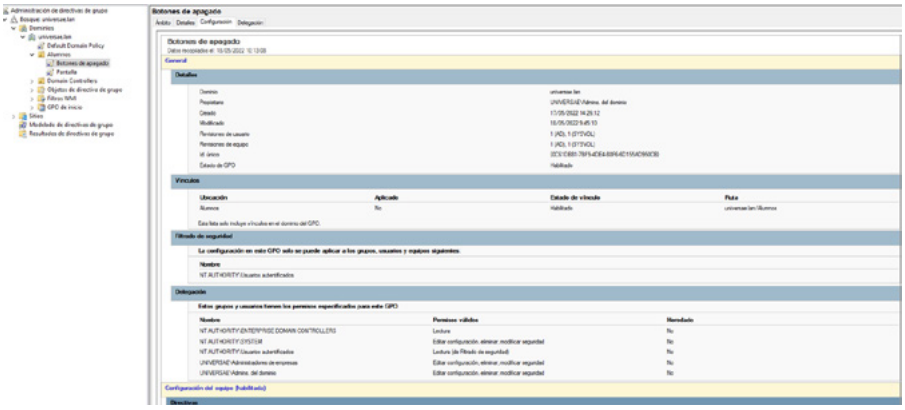

Imagen 19. Configuración

> Delegación.

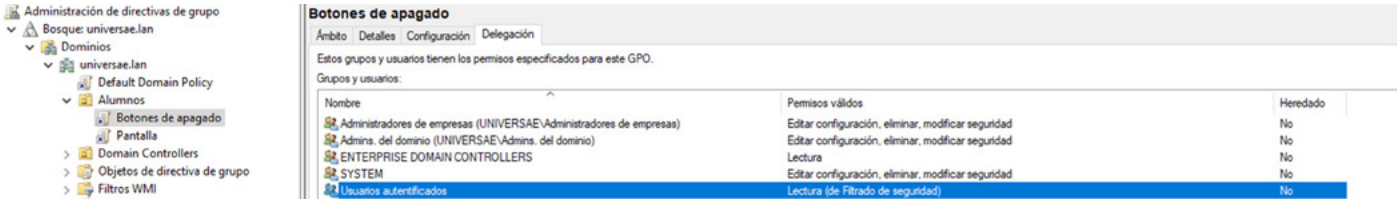

Imagen 20. Delegación

8.3. Las auditorías

Una **auditoría** se usa para poder monitorizar los sucesos en relación con la seguridad de nuestro sistema.

Los sucesos que más se suelen auditar son:

- El acceso a objetos del sistema.
- La administración de cuentas de usuarios y grupos.
- El inicio y fin de una sesión de usuario.

En un subapartado más hacia el final, veremos que cada uno de los sucesos que se auditen generaran una entrada en el registro de Windows, que se verá en el visor de eventos.

8.3.1. Auditar sucesos de seguridad

Es importante que existan auditorías en un sistema que ayuden a supervisar todo lo que antes hemos nombrado para que se obligue a tener una responsabilidad y en caso de incumplimiento, haya pruebas de lo sucedido.

Si queremos implementar una auditoría de seguridad, se deben de seguir los siguientes pasos en un primer instante:

1. Especificar las categorías de los sucesos que se desean auditar.
2. Definir el tamaño y como se va a comportar el registro de seguridad.
3. Para las auditorías destinadas a controlar el acceso a objetos, debemos de seleccionar y predefinir los objetos susceptibles de ser auditados, modificando los descriptores de seguridad que correspondan.

8.3.2. La directiva de auditoría

La **directiva de auditoría** nos indica sobre que sucesos de seguridad van a actuar ciertas auditorías. Por defecto al instalar Windows Server, se activan algunas categorías.

En Windows Server, tenemos las siguientes directivas de auditoría:

- Auditar el acceso a objetos.
- Auditar el acceso al servicio de directorio.
- Auditar el cambio de directivas.
- Auditar el seguimiento de procesos.
- Auditar el uso de privilegios.
- Auditar eventos de inicio de sesión de cuenta.
- Auditar eventos del sistema.
- Auditar la administración de cuentas.

8.3.3. Como establecer una directiva de auditoría

Si queremos establecer una directiva de auditoría lo primero que tenemos que hacer es irnos a la directiva que deseamos supervisar, y editarla. En nuestro ejemplo, vamos a usar la que hemos creado anterior mente, Botones de apagado.

1. Una vez en la edición de la directiva, seguimos el siguiente orden:
   a. Configuración del equipo
   b. Directivas
   c. Configuración de Windows
   d. Configuración de seguridad
   e. Directivas locales
   f. Directiva de auditoría

2. Podemos ver que, en la parte derecha, aparecen todos los elementos que son susceptibles de ser auditados.

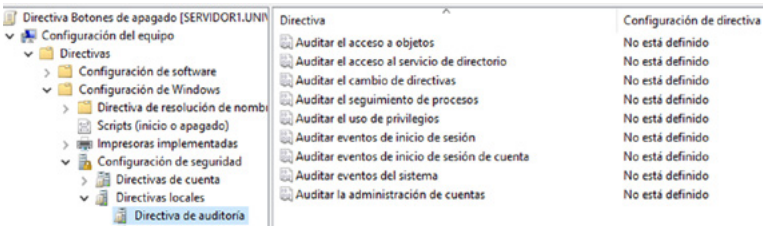

Imagen 21. Directivas de auditorías 1

3. Seleccionamos la auditoría correspondiente que tenemos, hacemos clic derecho sobre ella y elegimos Propiedades.

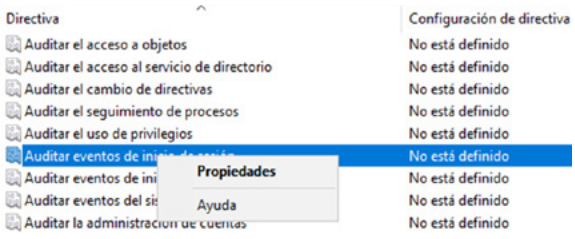

Imagen 22. Directivas de auditorías 2

4. En las propiedades de la auditoria debemos de hacer lo siguiente:
   a. Seleccionamos la opción Definir esta configuración de directiva.
   b. Más abajo tenemos dos opciones, en Auditar estos intentos:
      + Correcto, si queremos que se guarde cuando es correcto el suceso.
      + Error, si queremos que se guarde cuando sucede un error en el suceso.
5. Una vez que lo tenemos, damos a Aplicar y Aceptar.
6. Podemos ver fuera, que ahora, a la derecha de la auditoría el estado aparece como Correcto.

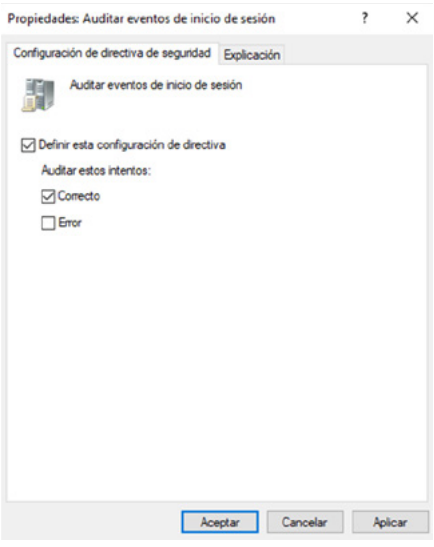

Imagen 23. Directivas de auditorías 3

8.3.4. Como configurar el procesamiento de una directiva

El siguiente procedimiento que vamos a ver es como configurar el procesamiento de una directiva.

Esto quiere decir, el modo en que la directiva de auditoría se va a ejecutar, en varios equipos, cada cierto tiempo, etc. Esto se hace debido a que, si la directiva se ejecutara en todo momento, sería un problema de recursos para el equipo y en muchas ocasiones no va a ser necesario.

Antes de comenzar con el procedimiento, cabe destacar que este procesamiento necesita de conocimiento extenso por parte del administrador sobre los usuarios susceptibles de ejecutar la auditoría y sobre como puede afectar. Vamos con el procedimiento:

1. Lo primero que debemos hacer, como siempre, es entrar en Editor de administración de directivas de grupo.
2. Ahora, seguimos el siguiente recorrido:
    a. Configuración del equipo
    b. Plantillas administrativas
    c. Sistema
    d. Directiva de grupo
3. Una vez aquí, debemos de seleccionar, en las directivas mostradas a la derecha, la opción Configurar el procesamiento de directivas de seguridad.

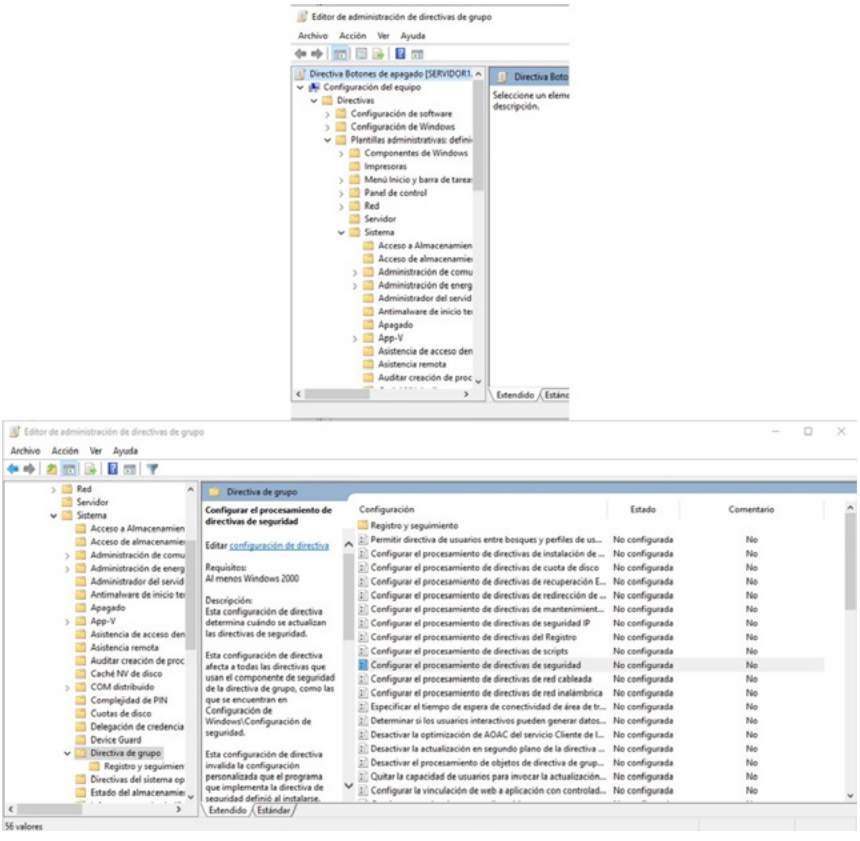

Imagen 24. Procesamiento de directivas 1

4. Habilitamos la directiva y vemos que tenemos dos opciones:

   a. No aplicar durante el procesamiento periódico en segundo plano: si activamos esta casilla, impediremos que el sistema actualice las directivas en segundo plano mientras que usamos el equipo, por tanto, se actualizarán cada vez que sincronicemos con el dominio, casi siempre, al iniciar sesión.

   b. Procesar incluso si los objetos de directiva de grupo no han cambiado: si activamos esta casilla, se hará una actualización continua de la directiva.

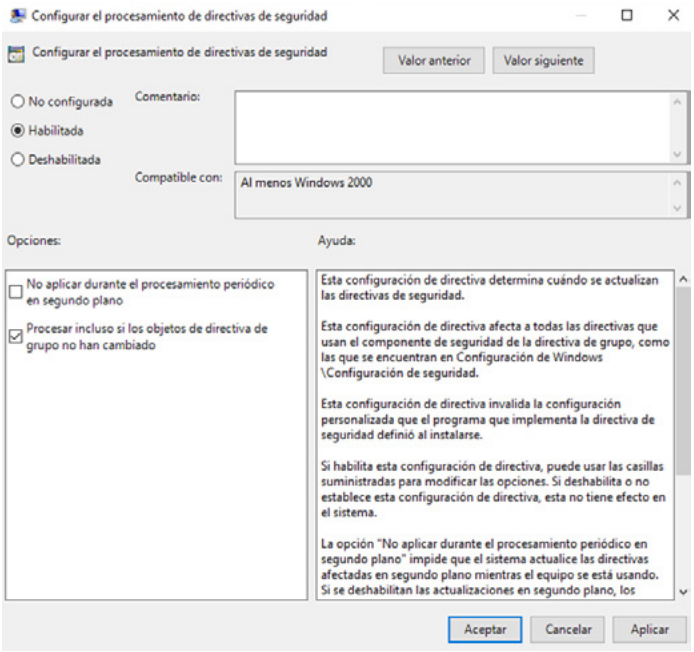

Imagen 25. Procesamiento de directivas 2

5. Podemos comprobar que la directiva se encuentra habilitada.

Imagen 26. Procesamiento de directivas 3

6. Ahora seleccionamos en el mismo sitio, la directiva siguiente: Establecer el intervalo de actualización de la directiva de grupo para controladores de dominio.

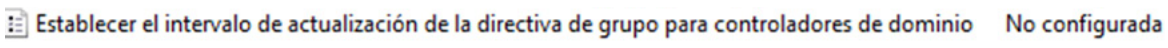

Imagen 27. Procesamiento de directivas 4

7. Habilitamos dicha directiva y de nuevo tenemos dos opciones, pero no para elegir una o la otra, sino para rellenar la que nosotros veamos conveniente:

   a. La primera opción indica con qué frecuencia se va a actualizar la directiva de grupo en el controlador de dominio, en segundo plano.

   b. La segunda opción se puede usar para añadir una variación del intervalo en caso de que requiramos que no sea exacto.

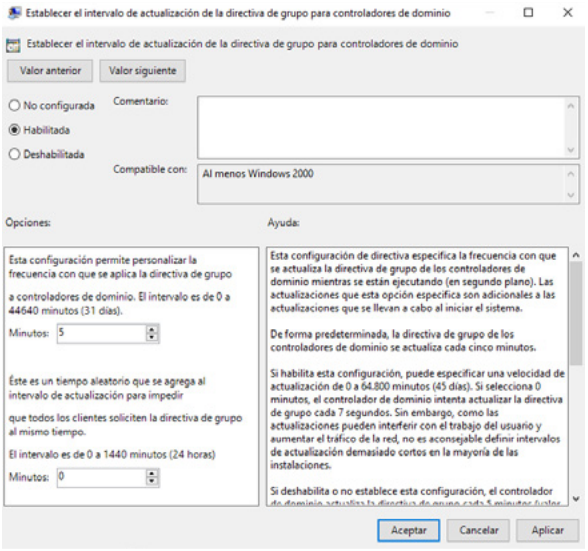

Imagen 28. Procesamiento de directivas 5

8. De nuevo debemos de modificar otra directiva, de igual modo, esta vez, será la directiva Establecer el intervalo de actualización de la directiva de grupo para equipos.

9. Esta directiva cuenta con los mismos parámetros que la anterior, su configuración es similar.

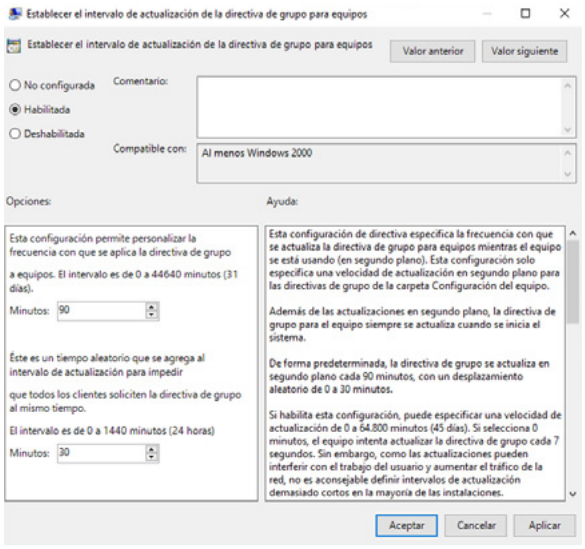

Imagen 29. Procesamiento de directivas 6

10. Una vez que tenemos todo lo relacionado con auditorías y su procesamiento configurado, vamos a forzar la actualización de políticas:

    a. Ejecutamos PowerShell en modo administrador.

    b. Lanzamos el siguiente comando:

```
gpudate /force
```

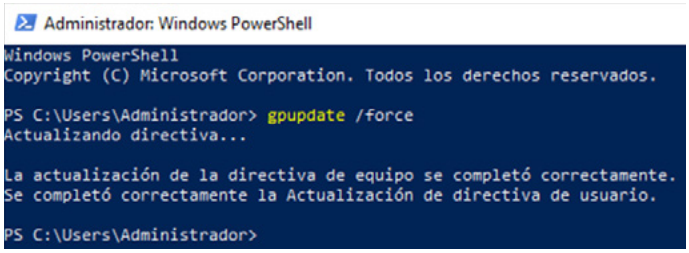

Imagen 30. gpupdate /force

DATE CUENTA

Establecer los intervalos de tiempo para el procesamiento en segundo plano de las auditorias solo tiene sentido si se ha permitido que se ejecuten en segundo plano.

8.3.5. Auditar el acceso a objetos

Cada uno de los objetos del sistema cuentan con un sistema de almacenamiento de información referente a seguridad que se llama descriptor de seguridad. Hay una parte del descriptor de seguridad que son las listas de control de acceso discrecional (DACL) que se vio en unidades anteriores.

Pero, en este descriptor, además de las DACL, también tenemos la información acerca de los sucesos que se auditan. La información de auditoría es llamada lista de control de acceso al sistema, SACL, donde indicamos lo siguiente:

- Las cuentas del sistema susceptibles de ser auditadas con respecto a su acceso a un objeto.
- Los sucesos que se van a tener en cuenta a la hora de auditar cada cuenta del sistema.
- El atributo Acierto o Error para cada uno de los sucesos de acceso, que trabajan en función de los permisos del objeto y de las DACL.

El modo de auditoría dependerá de si se audita el acceso a los objetos del explorador de archivos o a objetos del AD.

Establecer estas auditorías se realizarían desde la directiva correspondiente de las que vimos al principio de estos apartados.

8.3.6. Auditar el acceso a archivos y carpetas

Como vimos al principio de este apartado, uno de los tipos de auditoría más usados es la auditoría a objetos de explorar de archivos, es decir a volúmenes NTFS con la intención de saber quien a accedido a los objetos y que acciones ha realizado.

En el siguiente cuadro vemos un recuerdo de los tipos de acceso a carpetas y archivos que tenemos:

Tipos de accesos a objetos del explorador de archivos	
Tipos de acceso a carpetas	**Tipos de acceso a archivos**
Recorrer carpeta	Ejecutar archivo
Mostrar carpeta	Leer datos
Leer atributos	Leer atributos
Leer atributos extendidos	Leer atributos extendidos
Crear archivos	Escribir datos
Crear carpetas	Anexar datos
Escribir atributos	Escribir atributos
Escribir atributos extendidos	Escribir atributos extendidos
Eliminar	Eliminar
Permisos de lectura	Permisos de lectura
Cambiar permisos	Cambiar permisos
Tomar posesión	Tomar posesión

Vamos ahora a ver como se auditaría, por ejemplo, el acceso del usuario Alumno 1 a todo el disco duro de nuestro servidor:

1. Lo primero que debemos de hacer es habilitar las siguientes directivas de auditoría:
   a. Auditar el acceso a objetos
   b. Auditar el acceso al servicio de directorio

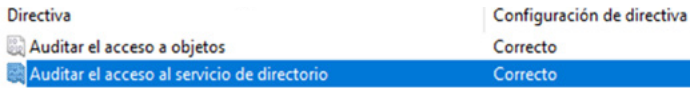

Imagen 31. Auditoría de objetos del explorador de archivos 1

2. Una vez que tenemos las dos directivas habilitadas, nos desplazamos hasta el explorador de archivos.
3. Abrimos las propiedades del volumen o unidad que queramos auditar y nos vamos a la pestaña Seguridad.
4. En esta pestaña, pulsamos Opciones avanzadas.

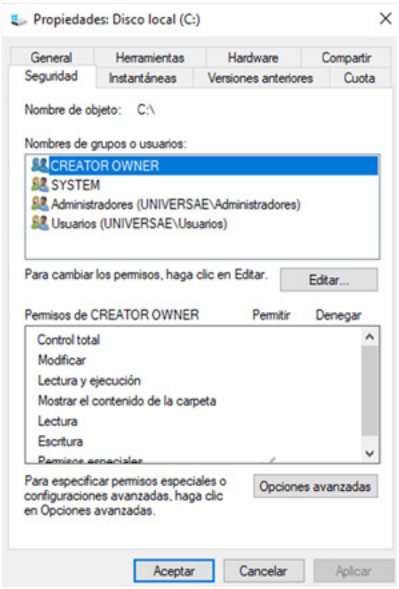

Imagen 32. Auditoría de objetos del explorador de archivos 2

5. Una vez en las opciones avanzadas, lo que debemos de hacer es dirigirnos a la pestaña Auditoría.
6. En esta pestaña, como cuando añadíamos usuarios en los permisos, seleccionamos Agregar.

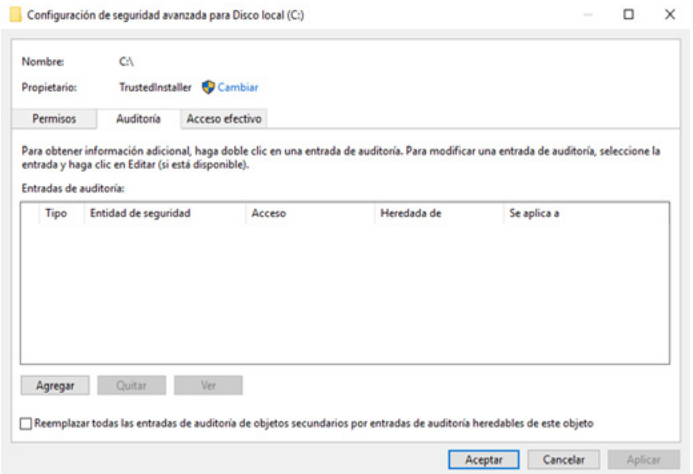

Imagen 33. Auditoría de objetos del explorador de archivos 3

7. Agregamos el usuario que queramos, seleccionamos que permisos queremos que se auditen y como, y aceptamos.

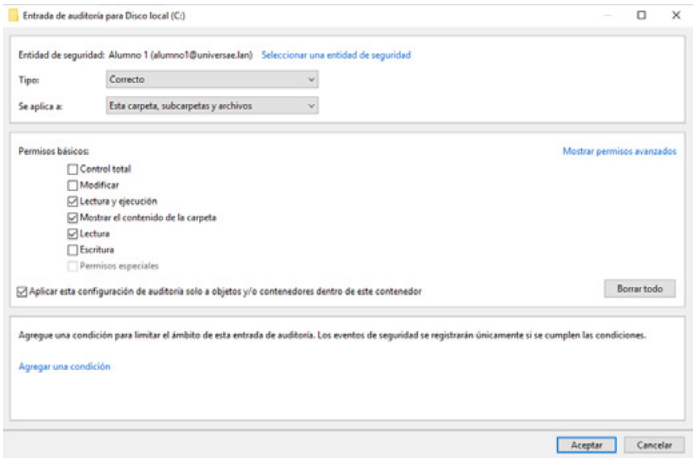

Imagen 34. Auditoría de objetos del explorador de archivos 4

8. Podemos ver que se ha quedado reflejada la configuración en la pestaña de Auditoría.

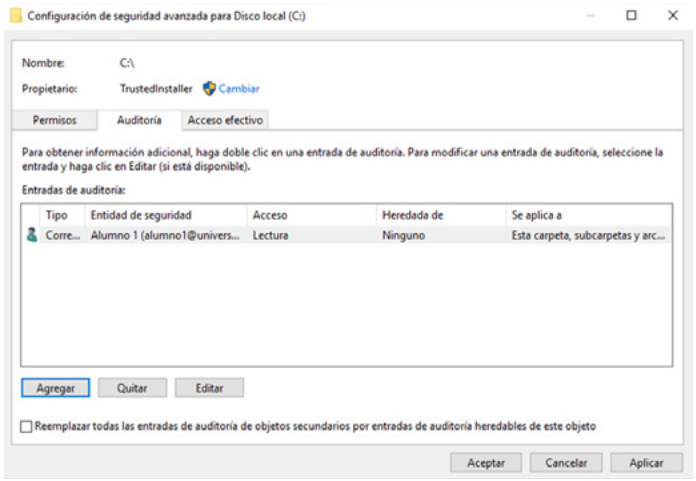

Imagen 35. Auditoría de objetos del explorador de archivos 5

PARA TENER EN CUENTA

Si queremos modificar o eliminar alguna de estas directivas, se realizaría igual que cuando realizábamos cambios en los permisos, seleccionando Editar sobre esta en la anterior imagen.

8.3.7. Como ver los registros de seguridad

Si queremos auditar algunos sucesos, lógicamente, tendremos que revisar estas auditorías cada cierto espacio en el tiempo para asegurarnos de que todo va como debe de ir, y para esto, recurrimos al **Visor de eventos**. (También está disponible en Windows 10, no solo en la versión de servidor.

Para visualizar los eventos, realizamos lo siguiente:

1. Abrimos desde las herramientas administrativas, o directamente buscándolo en el Inicio, la utilidad nativa de Windows, Visor de eventos.
2. Tenemos una serie de eventos o registros en la parte izquierda que se podrían comprobar.

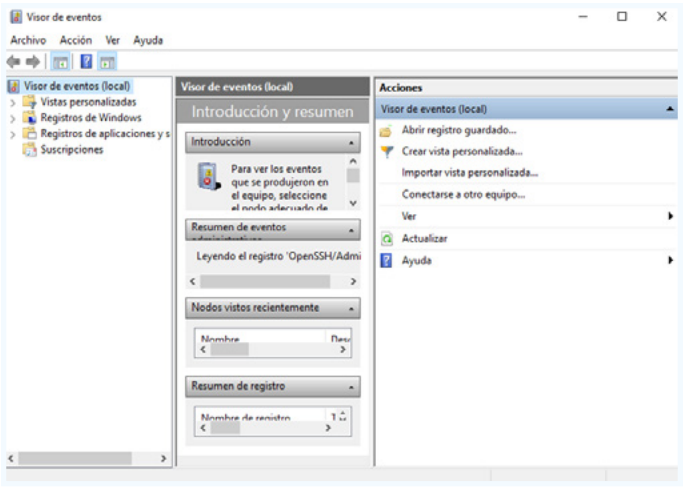

Imagen 36. Registros de seguridad en Windows 1

3. Ahora, nos desplazamos del siguiente modo:
   a. Registros de Windows.
   b. Seguridad.
4. Vemos que, a la derecha, nos aparecen todos los eventos que se han registrado, y más a la derecha aún, tenemos un menú de opciones.

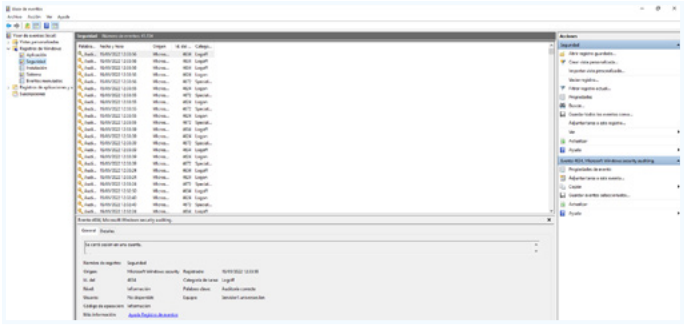

Imagen 37. Registro de seguridad en Windows 2

5. Por último, si abrimos cualquiera de ellos, podemos ver que se ha registrado en la parte de abajo, en nuestro caso, como creamos antes esa directiva, se ha registrado el cierre de sesión de una cuenta.

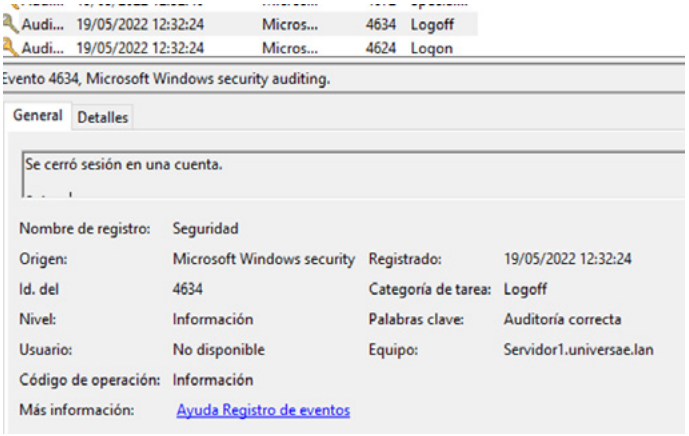

Imagen 38. Registros de seguridad en Windows 3

www.universae.com