

The background of the entire page is a dense, close-up photograph of roses. The roses are primarily a pale yellow color, with some showing hints of light red or pink, especially towards the edges of the petals. The petals are tightly packed and layered, creating a complex, swirling pattern. The lighting is soft, highlighting the texture of the petals.

TEMA 8

directivas de seguridad y auditorias

MARTA GONZÁLEZ ARNAIZ

1º ASIR

IMPLANTACIÓN DE SISTEMAS OPERATIVOS

3º EVALUACIÓN

tabla de contenido

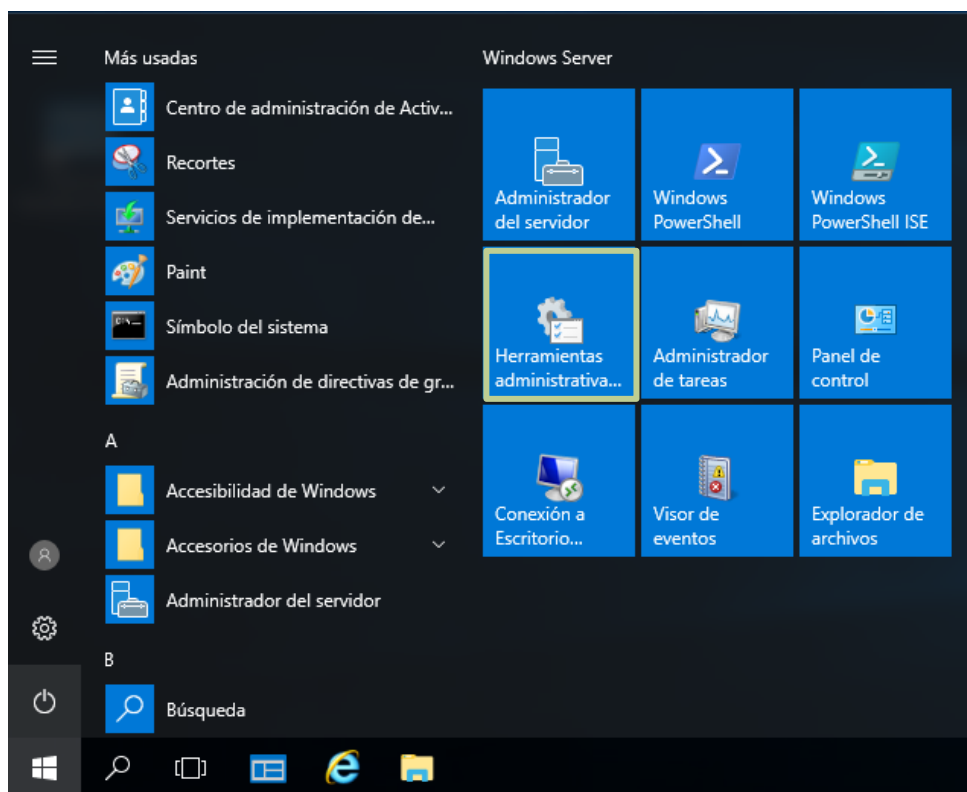
INTRODUCCIÓN	2
1. AUDITAR LOS INICIOS DE SESIÓN CORRECTOS Y ERRÓNEOS	3
2. AUDITAR LOS RECURSOS DEL SISTEMA	6
3. AUDITAR EL ACCESO A LOS OBJETOS.....	9
4. AUDITAR EL ACCESO A UNA CARPETA DEL EQUIPO PARA TODOS LOS USUARIOS.....	12
5. AUDITAR EL ACCESO A UNA CARPETA DEL EQUIPO PARA UN ÚNICO USUARIO	16
6. AUDITAR EL ACCESO A UN ARCHIVO DEL EQUIPO	21
7. CONSULTAR EL VISOR DE SUCESOS.....	25
CONCLUSIÓN	27
BIBLIOGRAFÍA.....	28

introducción

En esta práctica aprenderemos los tipos de directivas de seguridad, como establecerlas; a auditar todo tipo de sucesos u objetos y a manejar el Visor de eventos.

1. AUDITAR LOS INICIOS DE SESIÓN CORRECTOS Y ERRÓNEOS

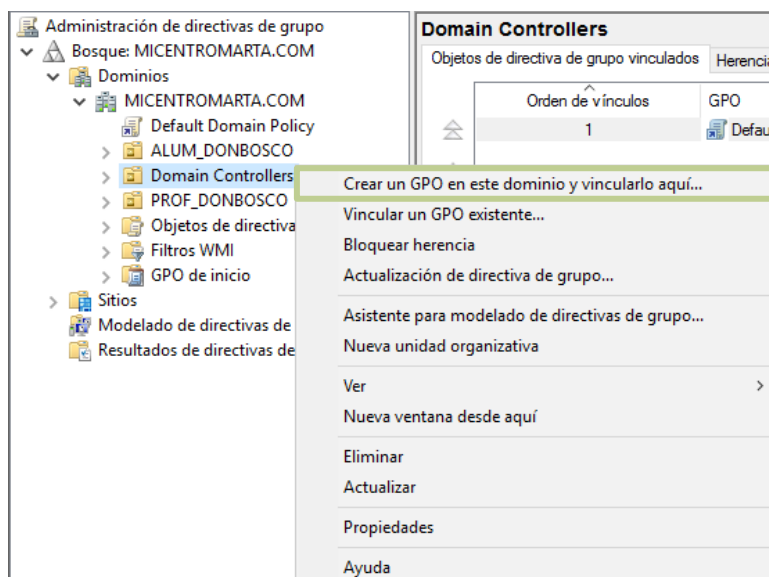
En Inicio seleccionamos "Herramientas administrativas"



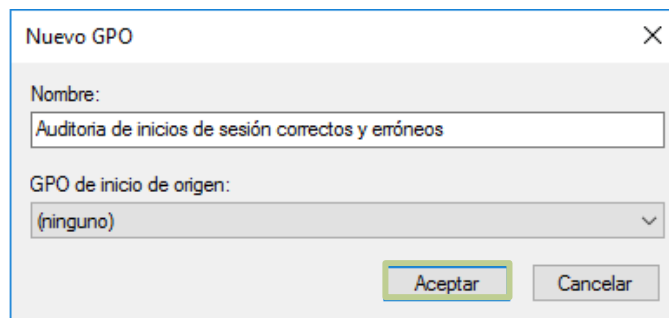
En la siguiente ventana seleccionaremos la opción "Administración de directivas de grupo"

Nombre	Fecha de modifica...	Tipo	Tamaño
Terminal Services	16/07/2016 15:23	Carpeta de archivos	
Administración de directivas de grupo	16/07/2016 15:19	Acceso directo	2 KB
Administración de equipos	16/07/2016 15:18	Acceso directo	2 KB
Administración de impresión	16/07/2016 15:19	Acceso directo	2 KB
Administrador del servidor	16/07/2016 15:19	Acceso directo	2 KB
Centro de administración de Active Direc...	16/07/2016 15:19	Acceso directo	2 KB

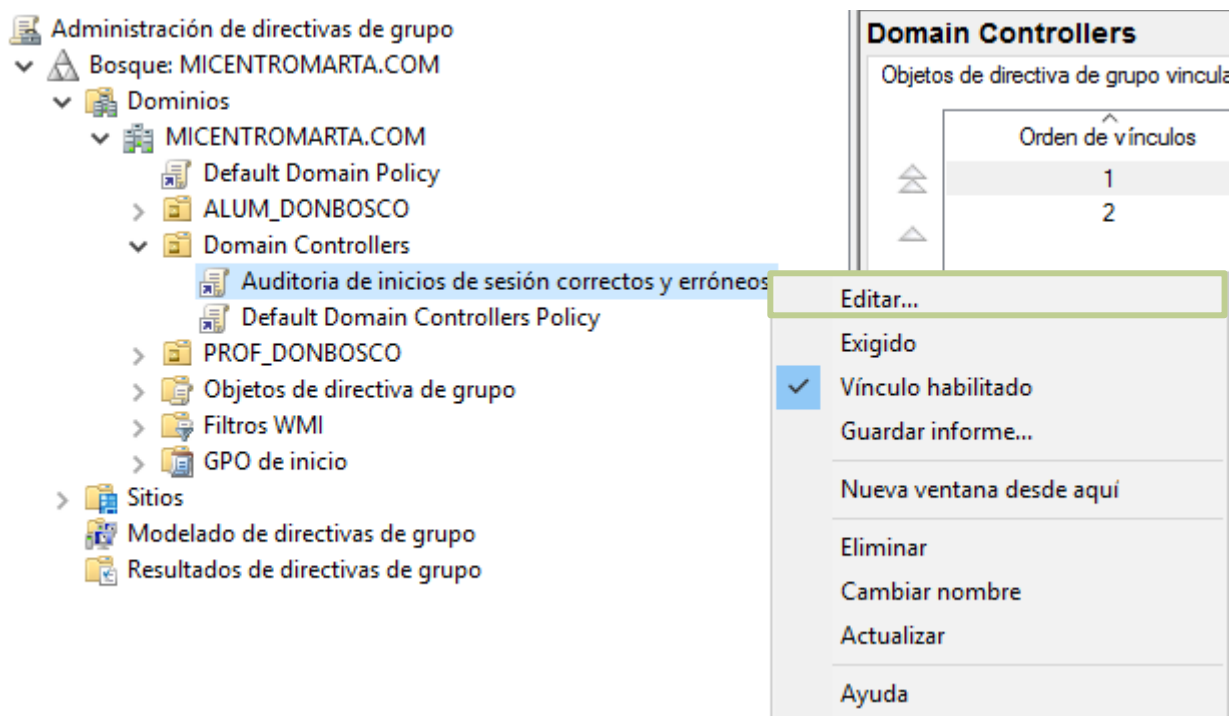
Dentro de ello seleccionamos "Dominios">"MICENTROMARTA.COM">"Domain Controllers", sobre esta última presionamos el botón derecho del ratón y seleccionamos "Crear un GPO en este dominio y vincularlo aquí..."



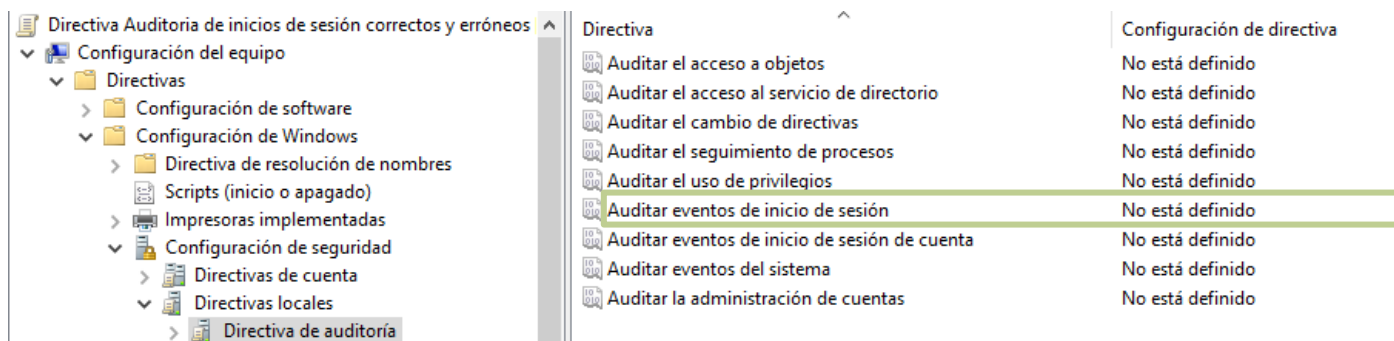
Introducimos el nombre que deseemos, en "GPO de inicio de origen:" seleccionamos "(ninguno)" y seleccionamos "Aceptar"



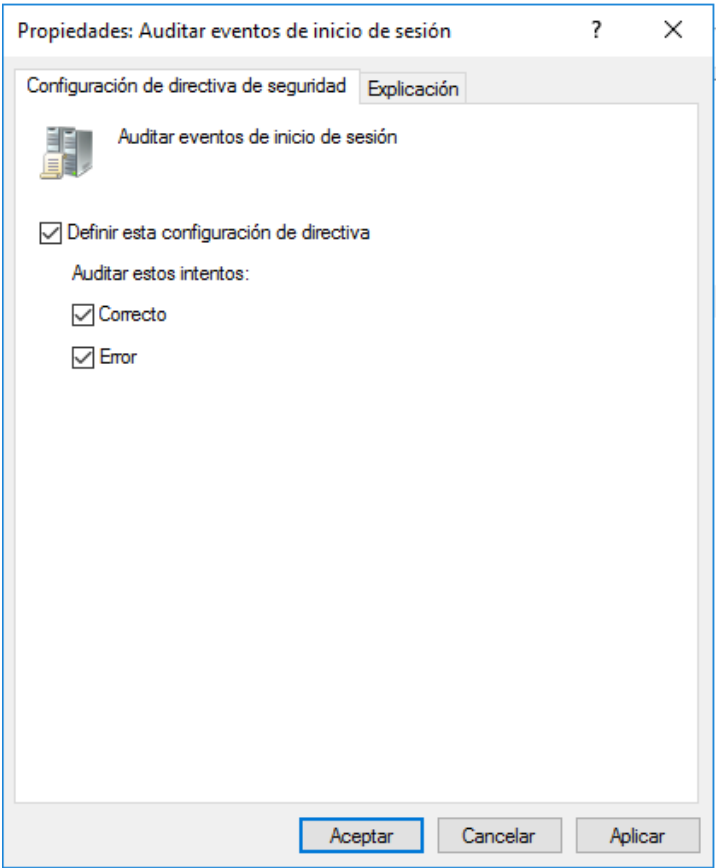
Desplegamos "Domain Controllers" y sobre la directiva que hemos creado presionamos el botón derecho del ratón y seleccionamos "Editar..."



Se abrirá la siguiente ventana en la que seleccionaremos "Configuración del equipo">"Directivas">"Configuración de Windows">"Configuración de seguridad">"Directivas locales">"Directiva de auditoria" y en las opciones que tenemos a la derecha seleccionamos "Auditar eventos de inicio de sesión"



Hacemos doble clic sobre ella y en la ventana a de "Propiedades" seleccionaremos las opciones "Definir esta configuración de directiva", "Correcto", "Error" y "Aceptar"

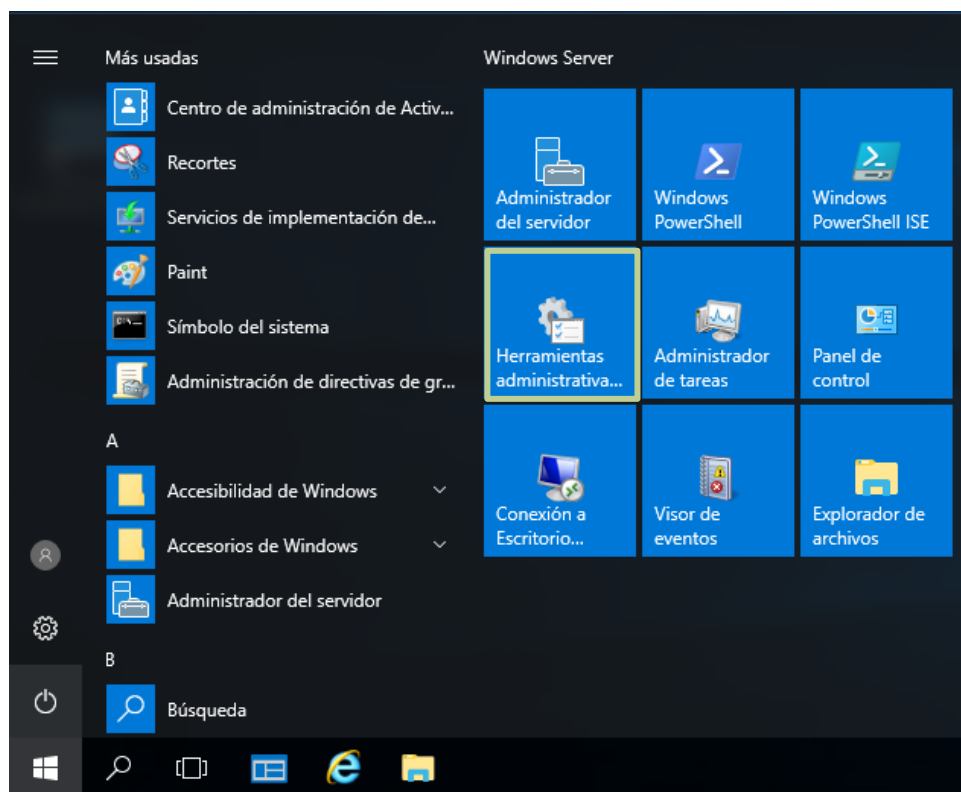


Este será el aspecto final:

Directiva	Configuración de directiva
Auditar el acceso a objetos	No está definido
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	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

2. AUDITAR LOS RECURSOS DEL SISTEMA

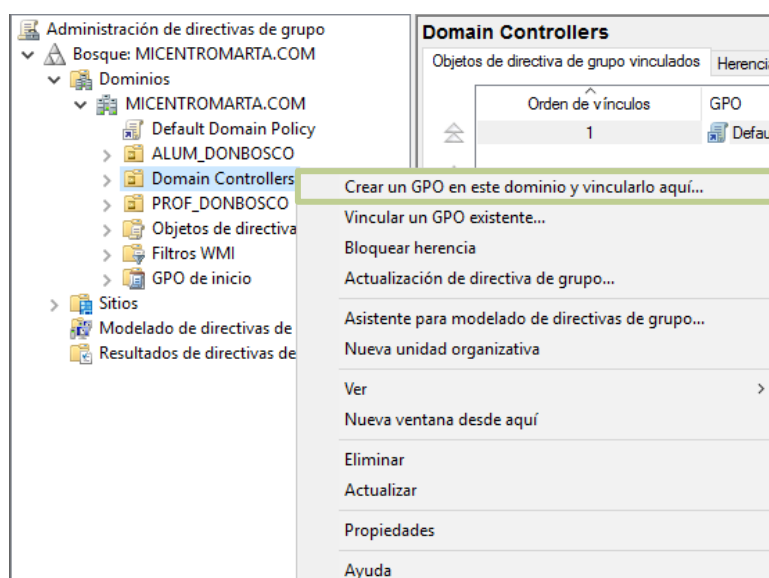
En Inicio seleccionamos "Herramientas administrativas"



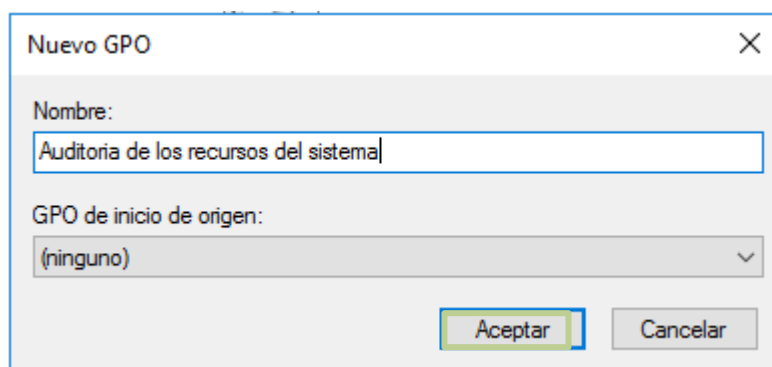
En la siguiente ventana seleccionaremos la opción "Administración de directivas de grupo"

Nombre	Fecha de modifica...	Tipo	Tamaño
Terminal Services	16/07/2016 15:23	Carpeta de archivos	
Administración de directivas de grupo	16/07/2016 15:19	Acceso directo	2 KB
Administración de equipos	16/07/2016 15:18	Acceso directo	2 KB
Administración de impresión	16/07/2016 15:19	Acceso directo	2 KB
Administrador del servidor	16/07/2016 15:19	Acceso directo	2 KB
Centro de administración de Active Direc...	16/07/2016 15:19	Acceso directo	2 KB

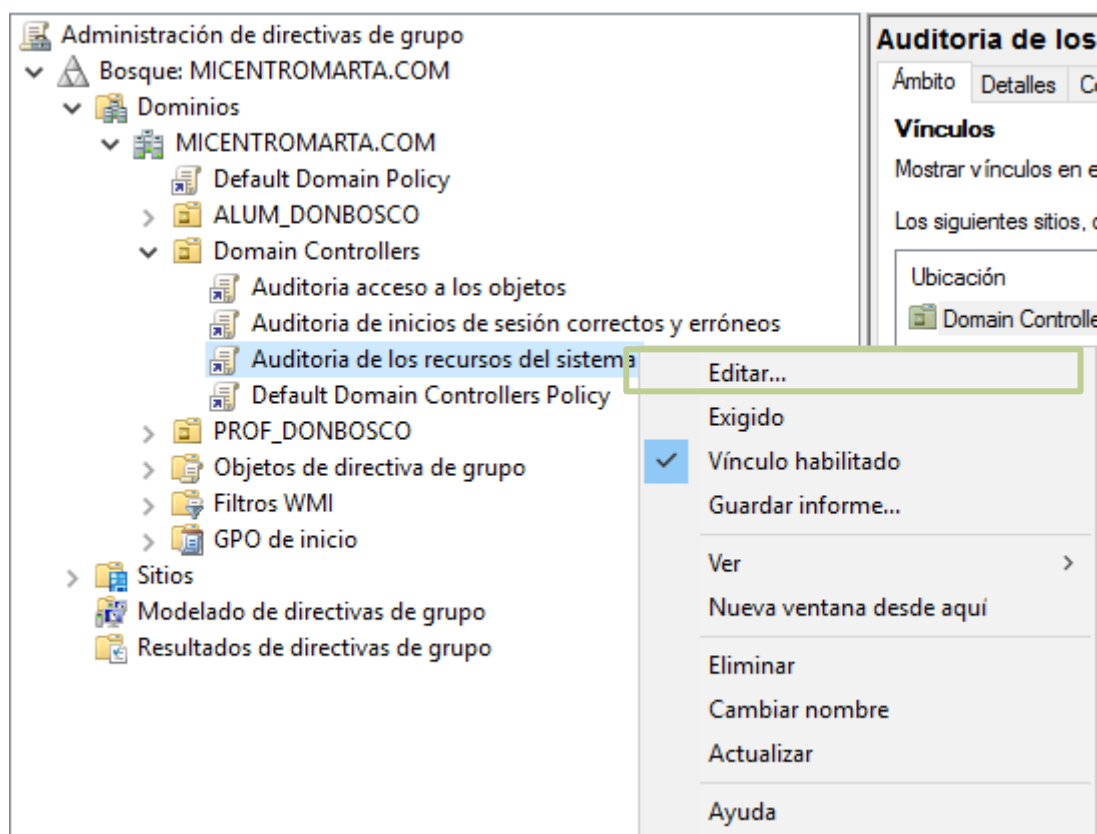
Dentro de ello seleccionamos "Dominios">"MICENTROMARTA.COM">"Domain Controllers", sobre esta última presionamos el botón derecho del ratón y seleccionamos "Crear un GPO en este dominio y vincularlo aquí..."



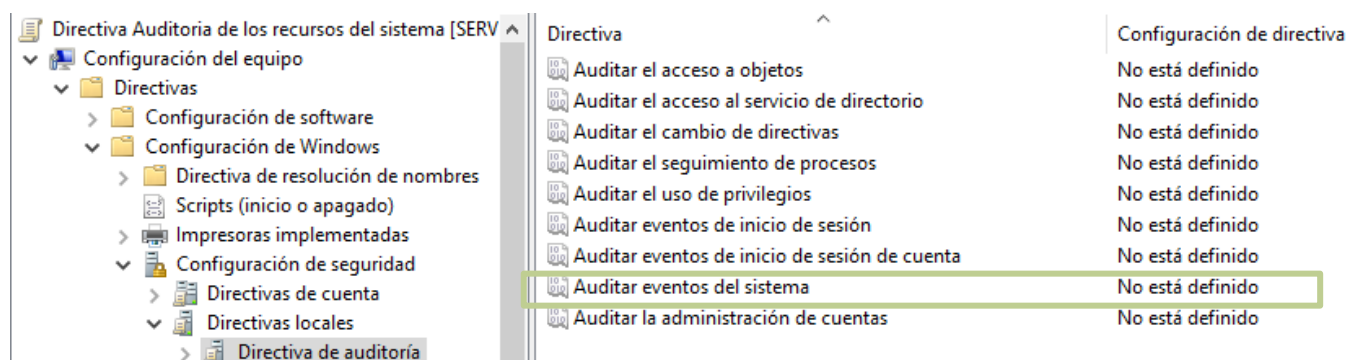
Introducimos el nombre que deseemos, en "GPO de inicio de origen:" seleccionamos "(ninguno)" y seleccionamos "Aceptar"



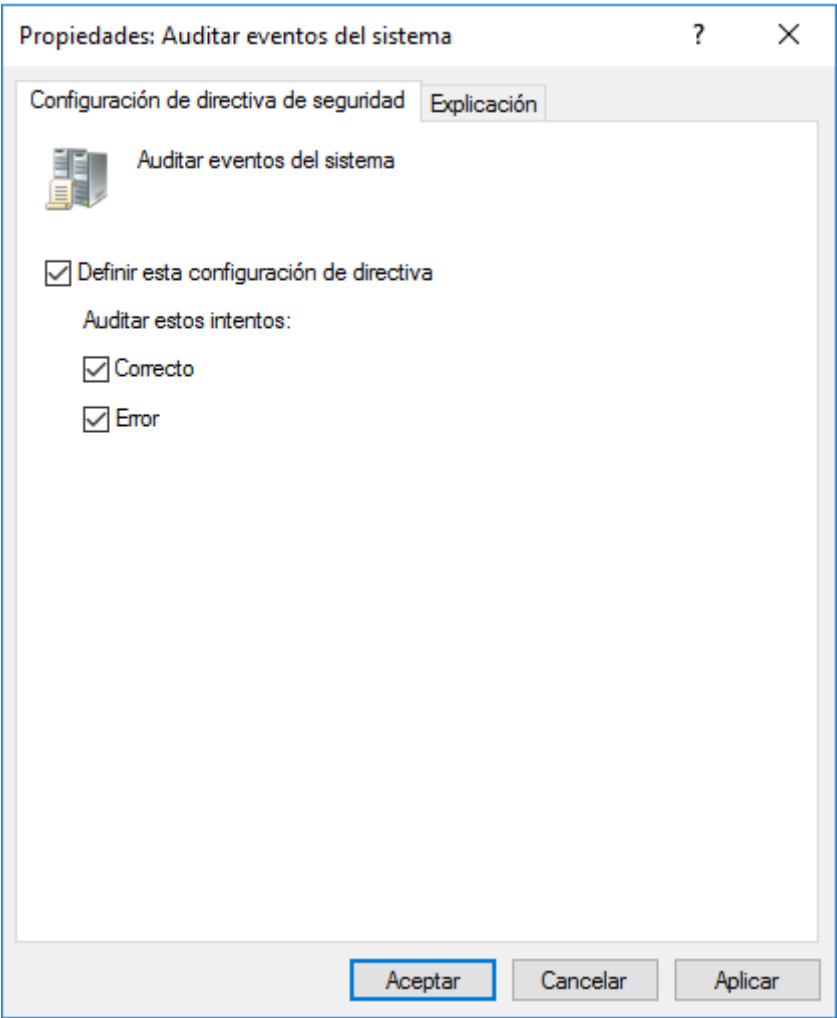
Desplegamos "Domain Controllers" y sobre la directiva que hemos creado presionamos el botón derecho del ratón y seleccionamos "Editar..."



Se abrirá la siguiente ventana en la que seleccionaremos "Configuración del equipo">"Directivas">"Configuración de Windows">"Configuración de seguridad">"Directivas locales">"Directiva de auditoria" y en las opciones que tenemos a la derecha seleccionamos "Auditar eventos del sistema"



Hacemos doble clic sobre ella y en la ventana a de "Propiedades" seleccionaremos las opciones "Definir esta configuración de directiva", "Correcto", "Error" y "Aceptar"

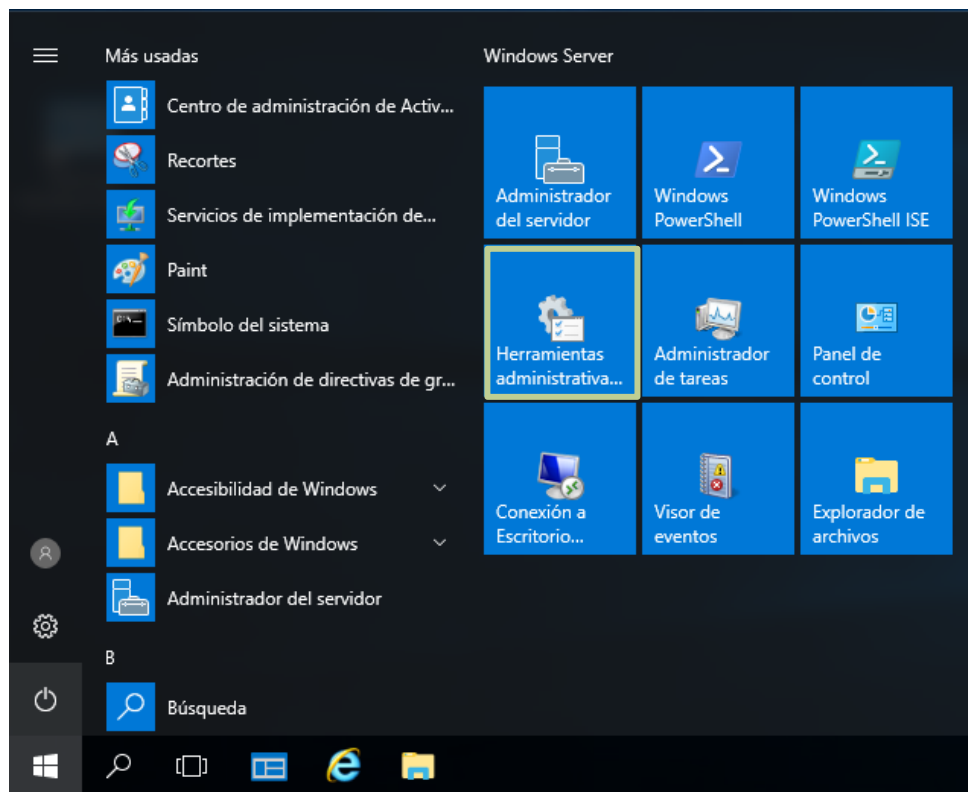


Este será el aspecto final:

Directiva	Configuración de directiva
Auditar el acceso a objetos	No está definido
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	Correcto, Erróneo
Auditar la administración de cuentas	No está definido

3. AUDITAR EL ACCESO A LOS OBJETOS

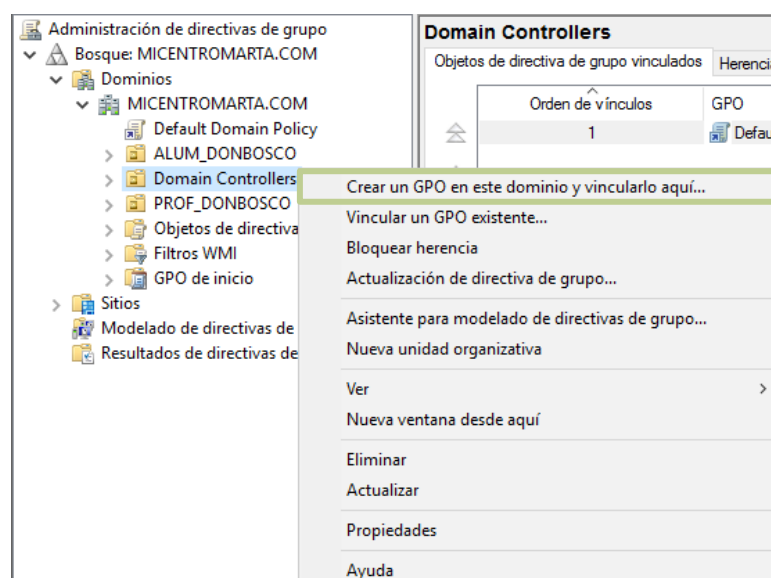
En Inicio seleccionamos "Herramientas administrativas"



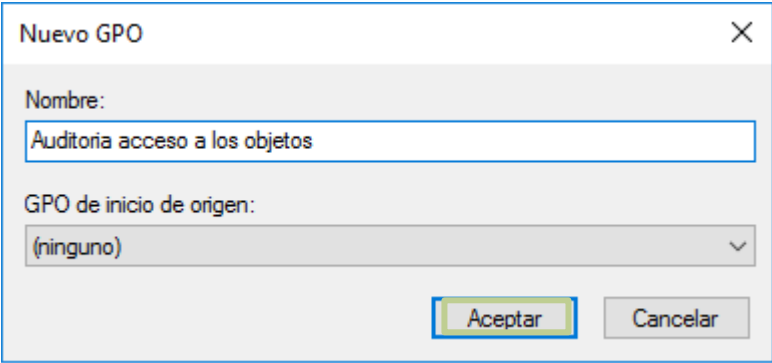
En la siguiente ventana seleccionaremos la opción "Administración de directivas de grupo"

Nombre	Fecha de modifica...	Tipo	Tamaño
Terminal Services	16/07/2016 15:23	Carpeta de archivos	
Administración de directivas de grupo	16/07/2016 15:19	Acceso directo	2 KB
Administración de equipos	16/07/2016 15:18	Acceso directo	2 KB
Administración de impresión	16/07/2016 15:19	Acceso directo	2 KB
Administrador del servidor	16/07/2016 15:19	Acceso directo	2 KB
Centro de administración de Active Direc...	16/07/2016 15:19	Acceso directo	2 KB

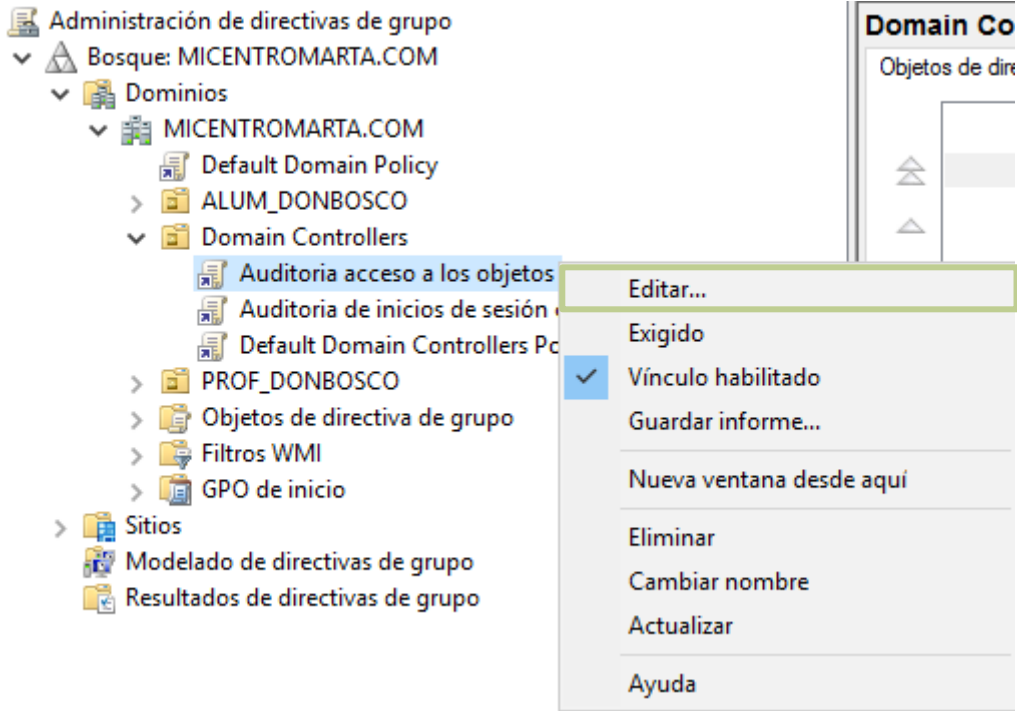
Dentro de ello seleccionamos "Dominios">"MICENTROMARTA.COM">"Domain Controllers", sobre esta última presionamos el botón derecho del ratón y seleccionamos "Crear un GPO en este dominio y vincularlo aquí..."



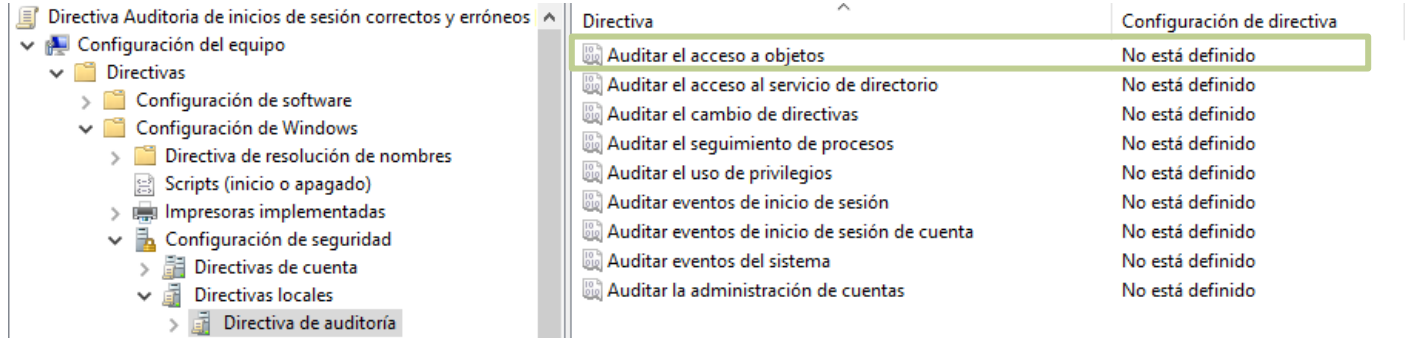
Introducimos el nombre que deseemos, en "GPO de inicio de origen:" seleccionamos "(ninguno)" y seleccionamos "Aceptar"



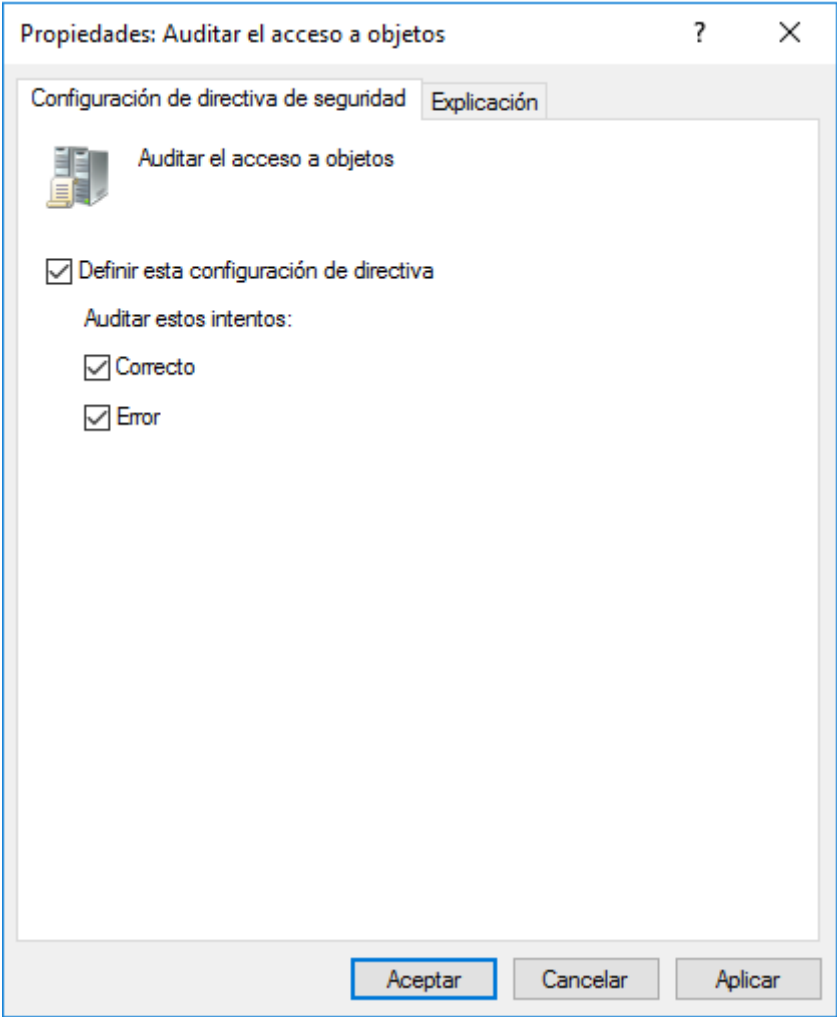
Desplegamos "Domain Controllers" y sobre la directiva que hemos creado presionamos el botón derecho del ratón y seleccionamos "Editar..."












Se abrirá la siguiente ventana en la que seleccionaremos "Configuración del equipo">"Directivas">"Configuración de Windows">"Configuración de seguridad">"Directivas locales">"Directiva de auditoria" y en las opciones que tenemos a la derecha seleccionamos "Auditar el acceso a objetos"



Hacemos doble clic sobre ella y en la ventana a de “Propiedades” seleccionaremos las opciones “Definir esta configuración de directiva”, “Correcto”, “Error” y “Aceptar”

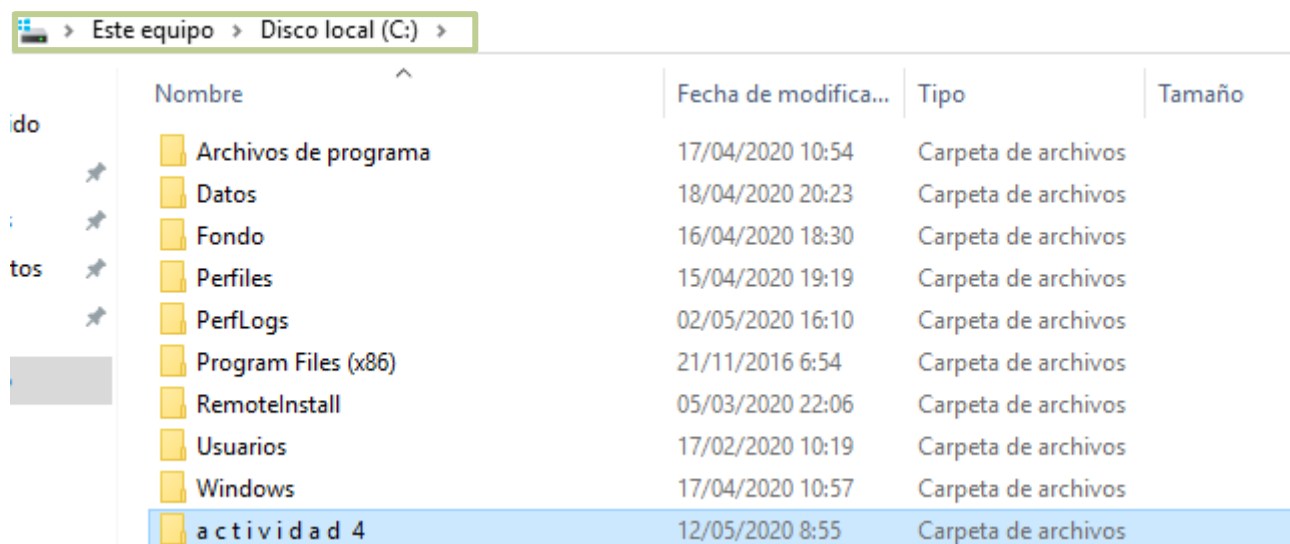


Este será el aspecto final:

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

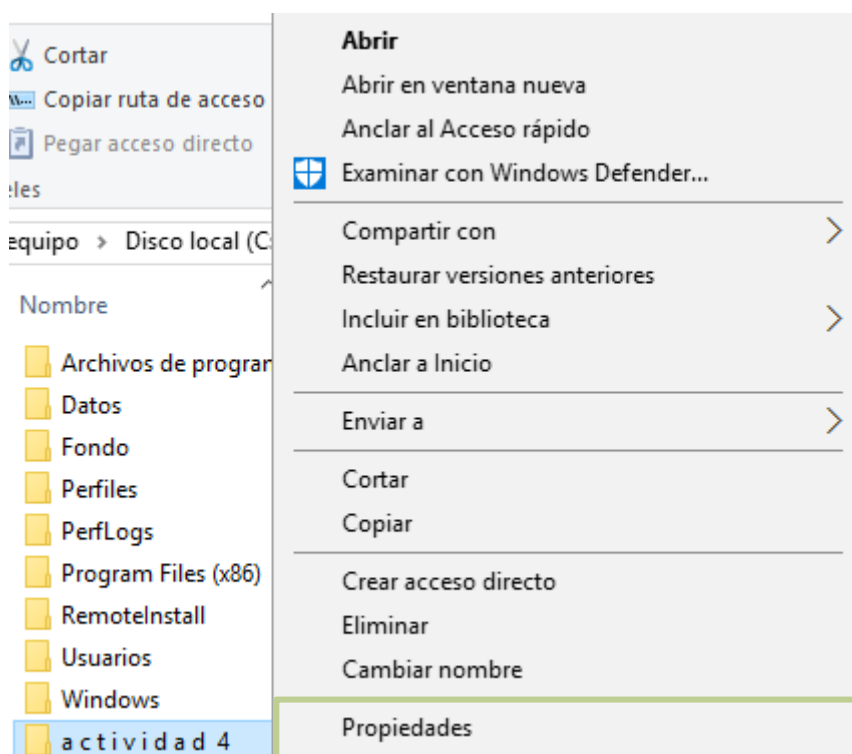
4. AUDITAR EL ACCESO A UNA CARPETA DEL EQUIPO PARA TODOS LOS USUARIOS

Creamos una carpeta en la ubicación que deseemos, en mi caso la he creado en el disco C: y la he llamado "actividad 4"

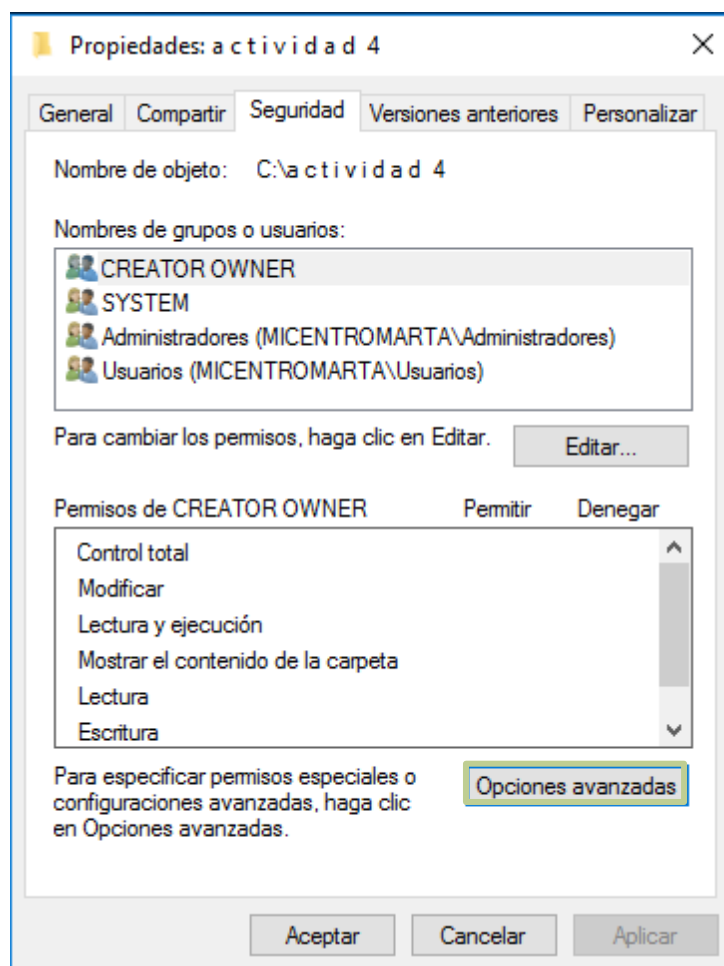


Este equipo > Disco local (C:) >				
	Nombre	Fecha de modifica...	Tipo	Tamaño
	Archivos de programa	17/04/2020 10:54	Carpeta de archivos	
	Datos	18/04/2020 20:23	Carpeta de archivos	
	Fondo	16/04/2020 18:30	Carpeta de archivos	
	Perfiles	15/04/2020 19:19	Carpeta de archivos	
	PerfLogs	02/05/2020 16:10	Carpeta de archivos	
	Program Files (x86)	21/11/2016 6:54	Carpeta de archivos	
	RemotelInstall	05/03/2020 22:06	Carpeta de archivos	
	Usuarios	17/02/2020 10:19	Carpeta de archivos	
	Windows	17/04/2020 10:57	Carpeta de archivos	
	actividad 4	12/05/2020 8:55	Carpeta de archivos	

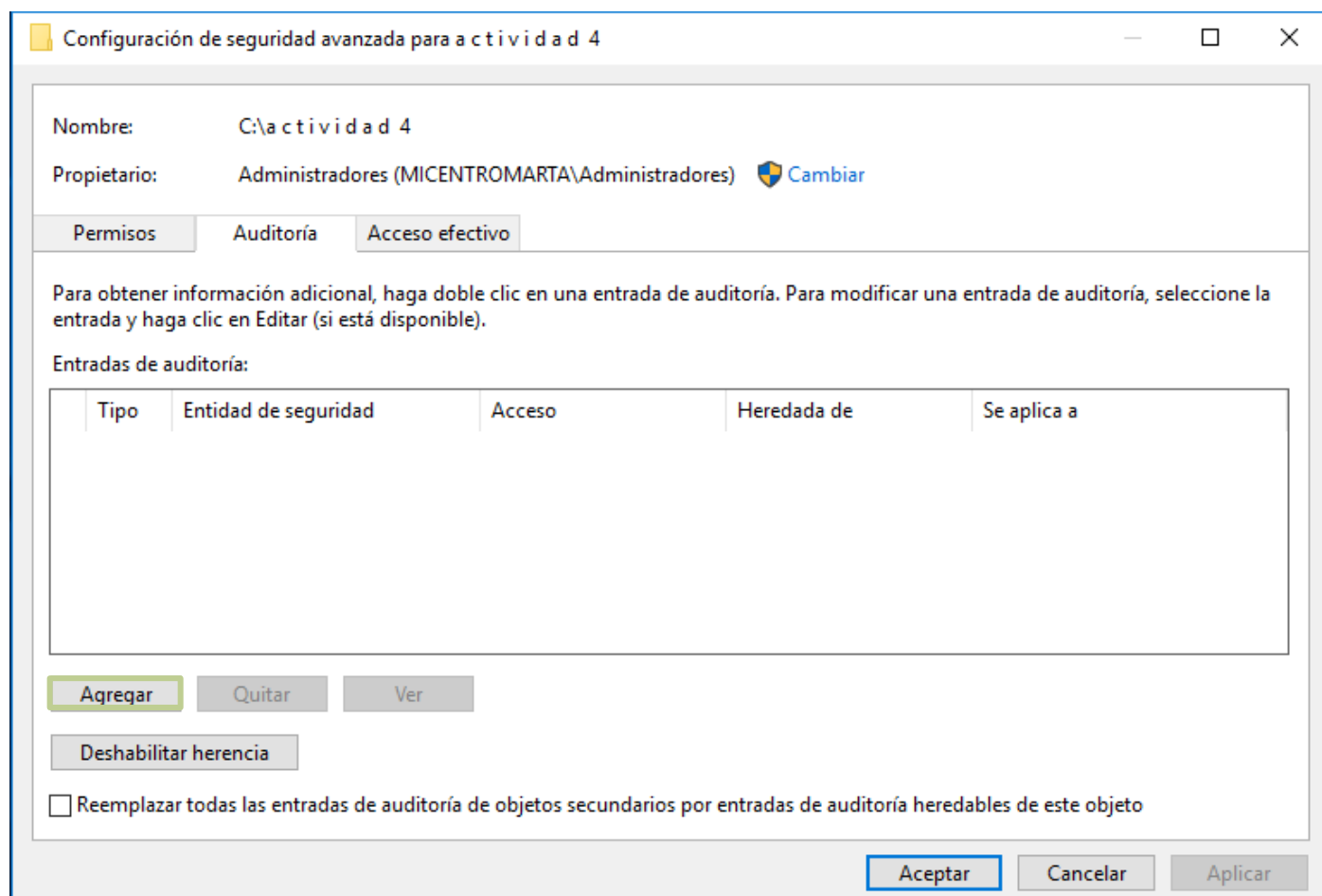
Presionamos el botón derecho del ratón y seleccionamos la opción "Propiedades"



En la ventana que se abrirá seleccionaremos "Seguridad">"Opciones avanzadas"



Seleccionamos "Auditoría">"Agregar"



Seleccionamos "Seleccionar una entidad de seguridad"

Entrada de auditoría para actividad 4

Entidad de seguridad: **Seleccionar una entidad de seguridad**

Tipo: Correcto

Se aplica a: Esta carpeta, subcarpetas y archivos

Permisos básicos: Mostrar permisos avanzados

- ☐ Control total
- ☐ Modificar
- ☒ Lectura y ejecución
- ☒ Mostrar el contenido de la carpeta
- ☒ Lectura
- ☐ Escritura
- ☐ Permisos especiales

☐ Aplicar esta configuración de auditoría solo a objetos y/o contenedores dentro de este contenedor Borrar todo

Agregue una condición para limitar el ámbito de esta entrada de auditoría. Los eventos de seguridad se registrarán únicamente si se cumplen las condiciones.

[Agregar una condición](#)

Aceptar Cancelar

Introducimos "Todos" y seleccionamos "Aceptar"

Seleccionar Usuario, Equipo, Cuenta de servicio o Grupo

Seleccionar este tipo de objeto:

Usuario, Grupo, o Entidad de seguridad integrada Tipos de objeto...

Desde esta ubicación:

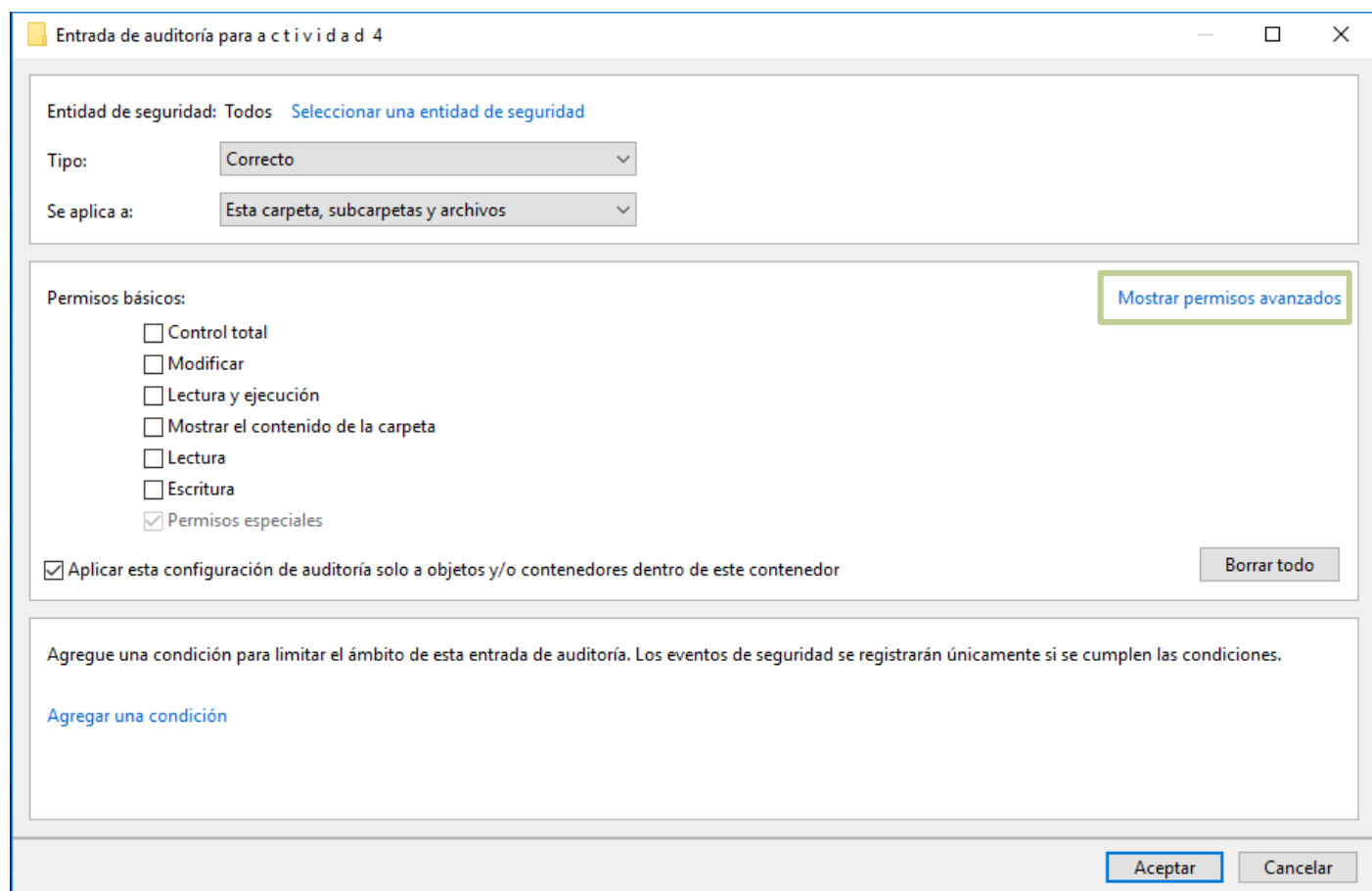
MICENTROMARTA.COM Ubicaciones...

Escriba el nombre de objeto para seleccionar (ejemplos):

Todos Comprobar nombres

Opciones avanzadas... Aceptar Cancelar

Seleccionamos "Mostrar permisos avanzados"



Entrada de auditoría para actividad 4

Entidad de seguridad: Todos [Seleccionar una entidad de seguridad](#)

Tipo:

Se aplica a:

Permisos básicos:

- ☐ Control total
- ☐ Modificar
- ☐ Lectura y ejecución
- ☐ Mostrar el contenido de la carpeta
- ☐ Lectura
- ☐ Escritura
- ☒ Permisos especiales

☒ Aplicar esta configuración de auditoría solo a objetos y/o contenedores dentro de este contenedor

[Mostrar permisos avanzados](#)

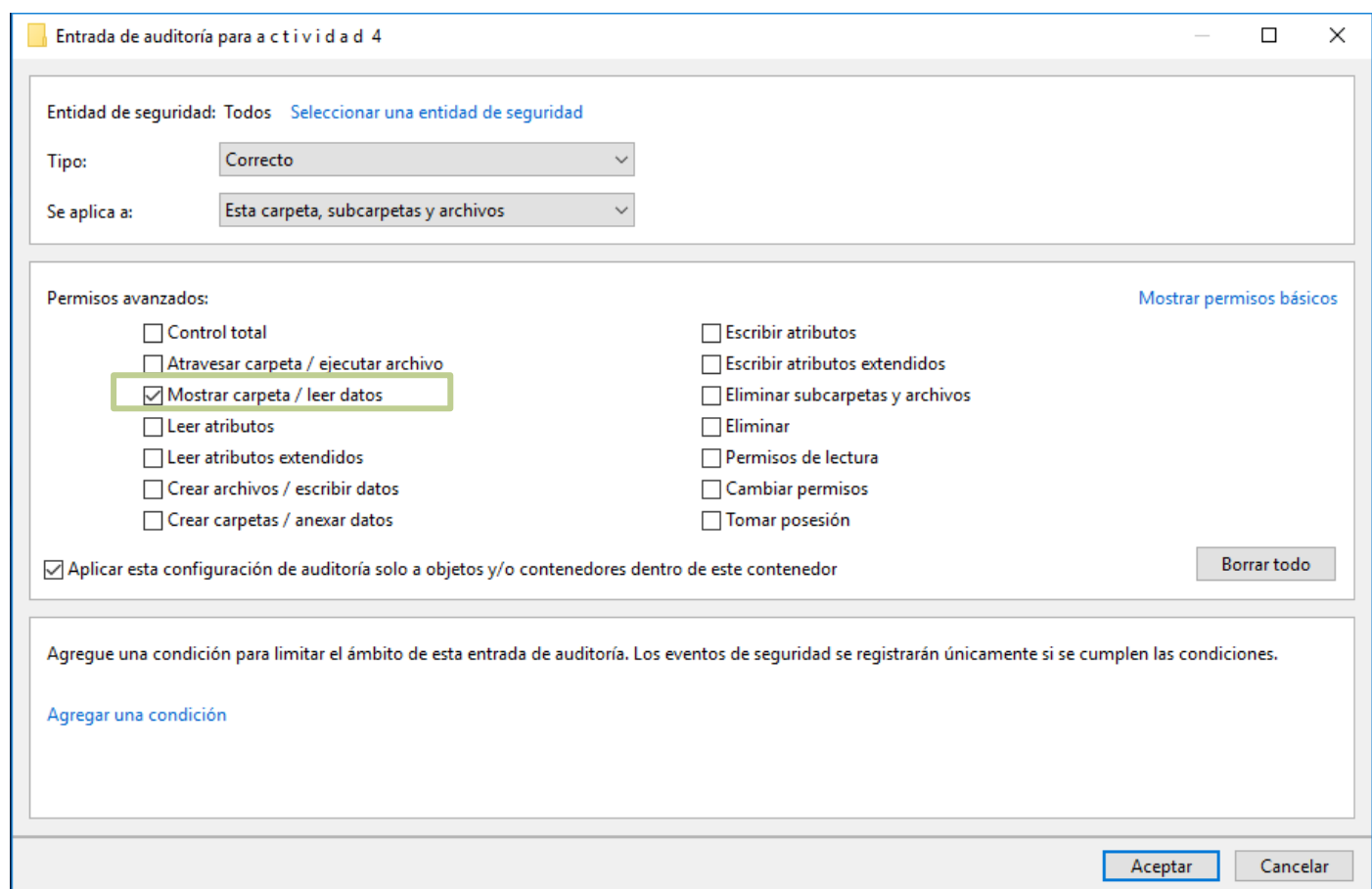
[Borrar todo](#)

Agregue una condición para limitar el ámbito de esta entrada de auditoría. Los eventos de seguridad se registrarán únicamente si se cumplen las condiciones.

[Agregar una condición](#)

[Aceptar](#) [Cancelar](#)

Seleccionamos "Mostrar carpeta/ leer datos", "Aplicar esta configuración de auditoria solo a objetos y/o contenedores dentro de este contenedor" y "Aceptar"



Entrada de auditoría para actividad 4

Entidad de seguridad: Todos [Seleccionar una entidad de seguridad](#)

Tipo:

Se aplica a:

Permisos avanzados:

- ☐ Control total
- ☐ Atravesar carpeta / ejecutar archivo
- ☒ Mostrar carpeta / leer datos
- ☐ Leer atributos
- ☐ Leer atributos extendidos
- ☐ Crear archivos / escribir datos
- ☐ Crear carpetas / anexar datos
- ☐ Escribir atributos
- ☐ Escribir atributos extendidos
- ☐ Eliminar subcarpetas y archivos
- ☐ Eliminar
- ☐ Permisos de lectura
- ☐ Cambiar permisos
- ☐ Tomar posesión

☒ Aplicar esta configuración de auditoría solo a objetos y/o contenedores dentro de este contenedor

[Mostrar permisos básicos](#)

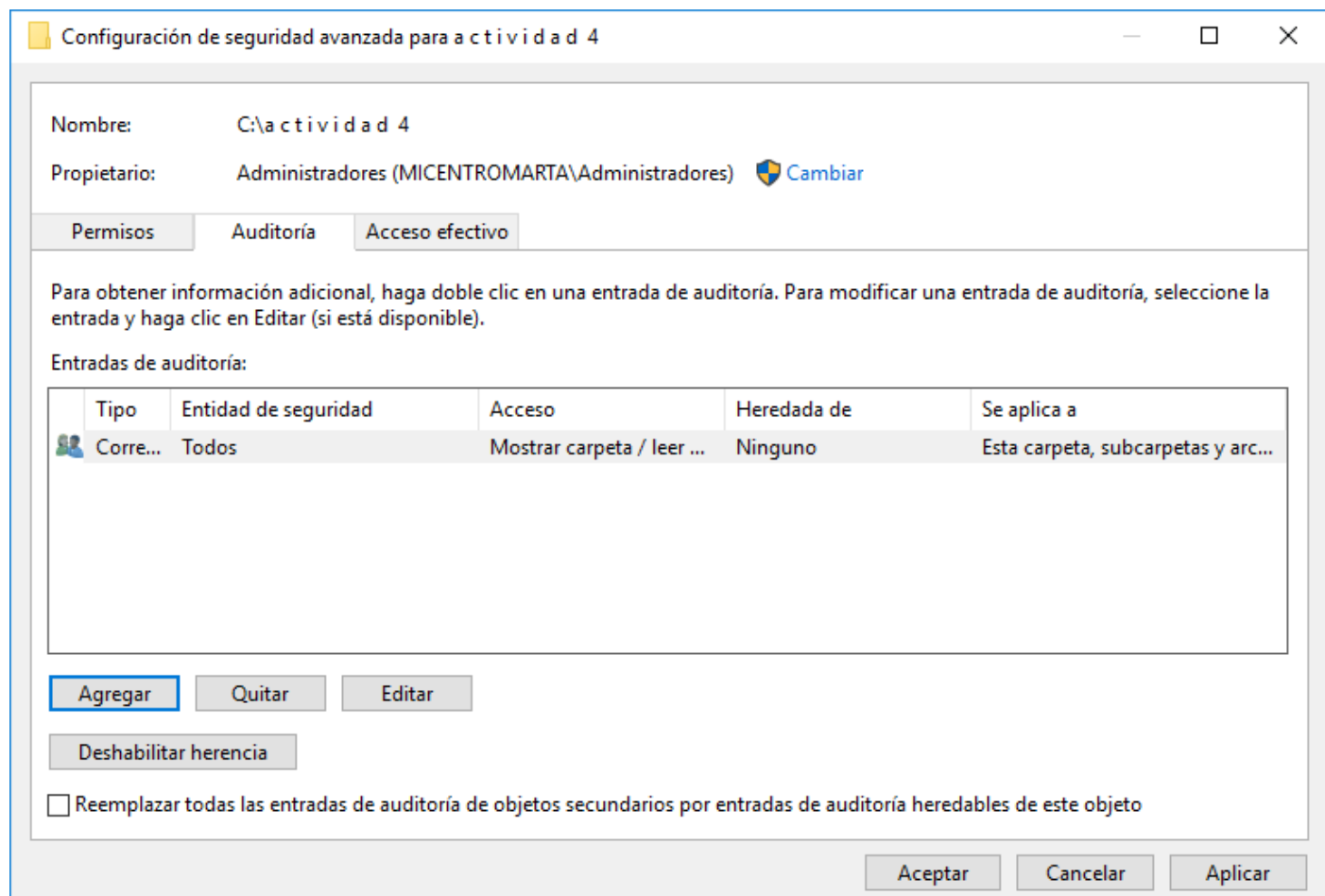
[Borrar todo](#)

Agregue una condición para limitar el ámbito de esta entrada de auditoría. Los eventos de seguridad se registrarán únicamente si se cumplen las condiciones.

[Agregar una condición](#)

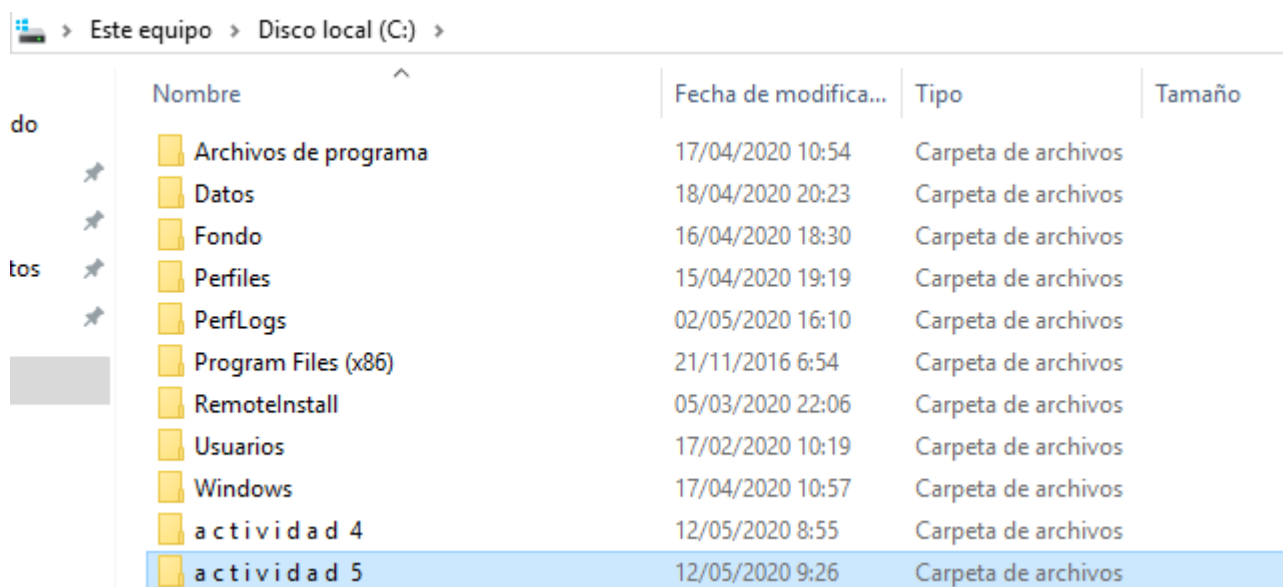
[Aceptar](#) [Cancelar](#)

Y este sería el aspecto final, para finalizar seleccionamos "Aceptar"

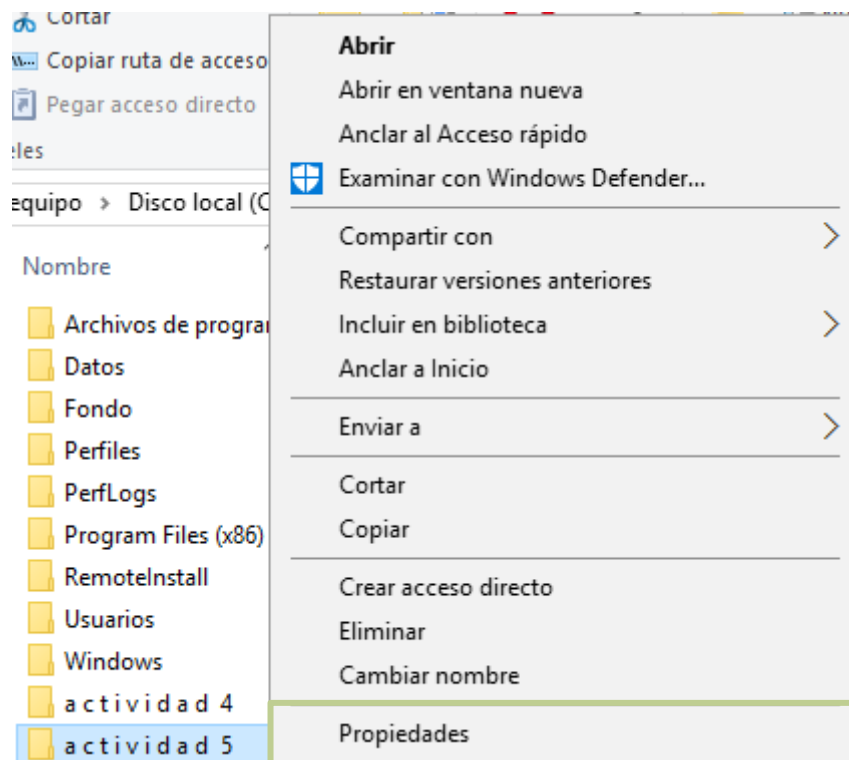


5. AUDITAR EL ACCESO A UNA CARPETA DEL EQUIPO PARA UN ÚNICO USUARIO

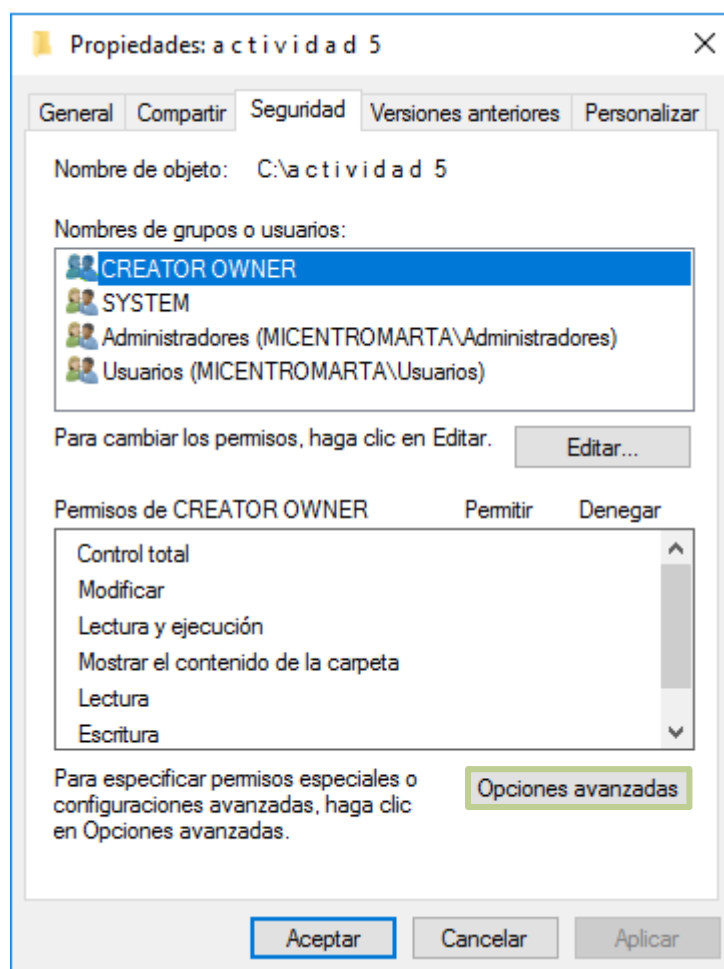
Creamos una carpeta en la ubicación que deseemos, en mi caso la he creado en el disco C: y la he llamado "a ct i v i d a d 5"



Presionamos el botón derecho del ratón y seleccionamos la opción "Propiedades"



En la ventana que se abrirá seleccionaremos "Seguridad">"Opciones avanzadas"



Seleccionamos "Auditoría">"Agregar"

Configuración de seguridad avanzada para actividad 5

Nombre: C:\actividad 5

Propietario: Administradores (MICENTROMARTA\Administradores) [Cambiar](#)

Permisos Auditoría Acceso efectivo

Para obtener información adicional, haga doble clic en una entrada de auditoría. Para modificar una entrada de auditoría, seleccione la entrada y haga clic en Editar (si está disponible).

Entradas de auditoría:

Tipo	Entidad de seguridad	Acceso	Heredada de	Se aplica a
------	----------------------	--------	-------------	-------------

[Agregar](#) [Quitar](#) [Ver](#)

[Deshabilitar herencia](#)

☐ Reemplazar todas las entradas de auditoría de objetos secundarios por entradas de auditoría heredables de este objeto

[Aceptar](#) [Cancelar](#) [Aplicar](#)

Seleccionamos "Seleccionar una entidad de seguridad"

Entrada de auditoría para actividad 5

Entidad de seguridad: [Seleccionar una entidad de seguridad](#)

Tipo: Correcto

Se aplica a: Esta carpeta, subcarpetas y archivos

Permisos básicos: [Mostrar permisos avanzados](#)

- ☐ Control total
- ☐ Modificar
- ☒ Lectura y ejecución
- ☒ Mostrar el contenido de la carpeta
- ☒ Lectura
- ☐ Escritura
- ☐ Permisos especiales

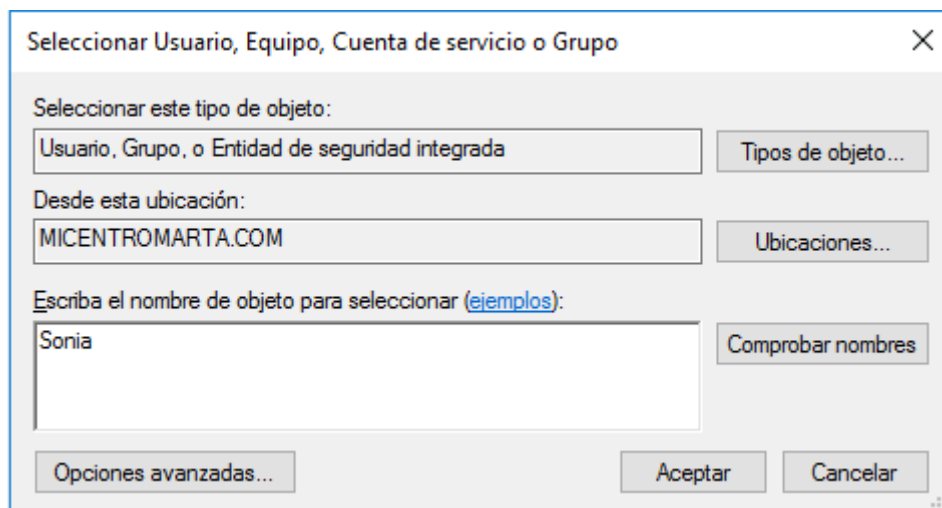
☐ Aplicar esta configuración de auditoría solo a objetos y/o contenedores dentro de este contenedor [Borrar todo](#)

Agregue una condición para limitar el ámbito de esta entrada de auditoría. Los eventos de seguridad se registrarán únicamente si se cumplen las condiciones.

[Agregar una condición](#)

[Aceptar](#) [Cancelar](#)

Introducimos "Sonia" y seleccionamos "Aceptar"



Seleccionar Usuario, Equipo, Cuenta de servicio o Grupo

Seleccionar este tipo de objeto:

Usuario, Grupo, o Entidad de seguridad integrada

Tipos de objeto...

Desde esta ubicación:

MICENTROMARTA.COM

Ubicaciones...

Escriba el nombre de objeto para seleccionar (ejemplos):

Sonia

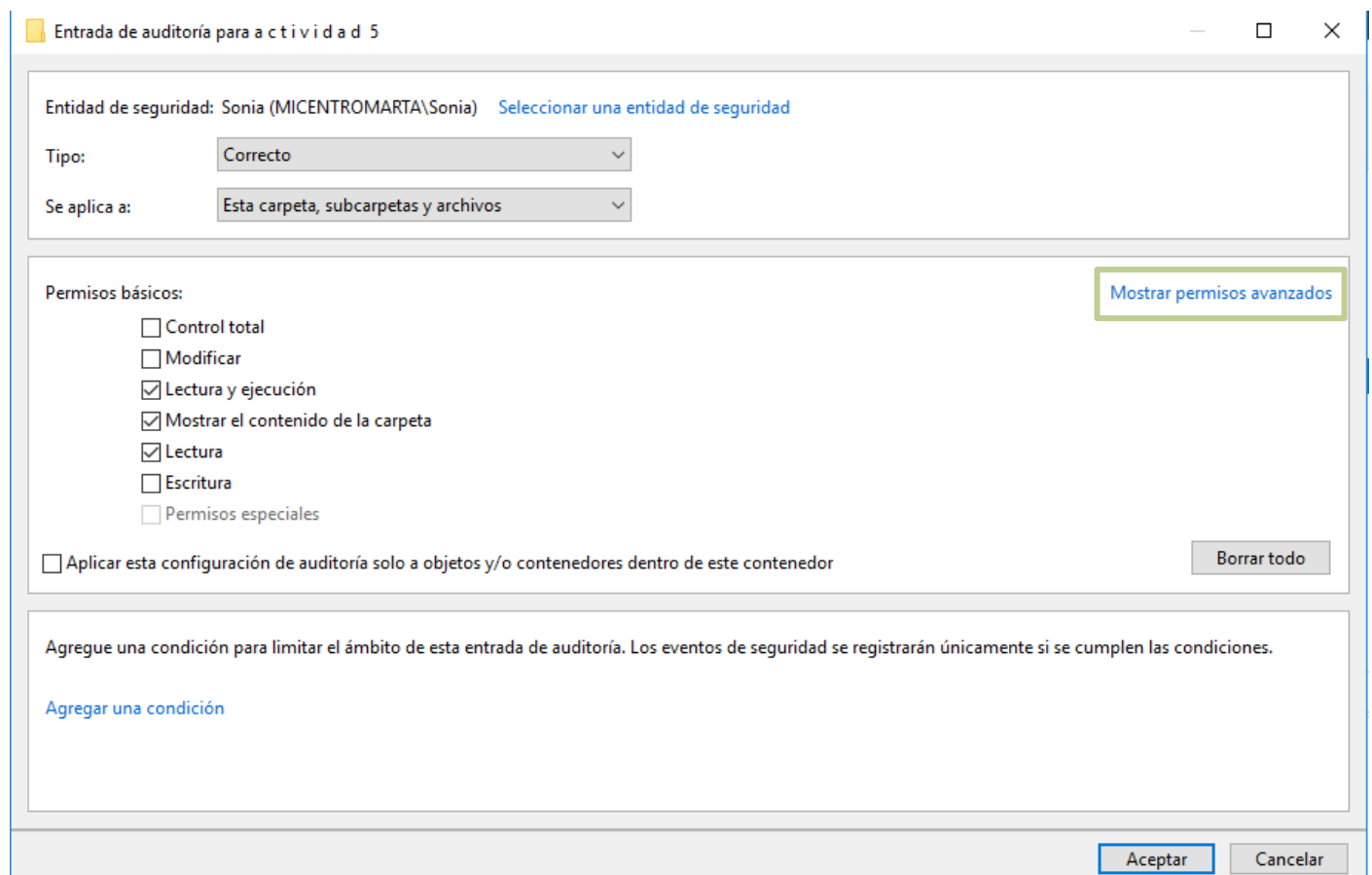
Comprobar nombres

Opciones avanzadas...

Aceptar

Cancelar

Seleccionamos "Mostrar permisos avanzados"



Entrada de auditoría para actividad 5

Entidad de seguridad: Sonia (MICENTROMARTA\Sonia) [Seleccionar una entidad de seguridad](#)

Tipo: Correcto

Se aplica a: Esta carpeta, subcarpetas y archivos

Permisos básicos:

- ☐ Control total
- ☐ Modificar
- ☒ Lectura y ejecución
- ☒ Mostrar el contenido de la carpeta
- ☒ Lectura
- ☐ Escritura
- ☐ Permisos especiales

[Mostrar permisos avanzados](#)

☐ Aplicar esta configuración de auditoría solo a objetos y/o contenedores dentro de este contenedor

Borrar todo

Agregue una condición para limitar el ámbito de esta entrada de auditoría. Los eventos de seguridad se registrarán únicamente si se cumplen las condiciones.

[Agregar una condición](#)

Aceptar

Cancelar

Seleccionamos "Mostrar carpeta/ leer datos", "Aplicar esta configuración de auditoria solo a objetos y/o contenedores dentro de este contenedor" y "Aceptar"

Entrada de auditoría para actividad 5

Entidad de seguridad: Sonia (MICENTROMARTA\Sonia) [Seleccionar una entidad de seguridad](#)

Tipo: Correcto

Se aplica a: Esta carpeta, subcarpetas y archivos

Permisos avanzados: [Mostrar permisos básicos](#)

- ☐ Control total
- ☐ Atravesar carpeta / ejecutar archivo
- ☒ Mostrar carpeta / leer datos
- ☐ Leer atributos
- ☐ Leer atributos extendidos
- ☐ Crear archivos / escribir datos
- ☐ Crear carpetas / anexar datos
- ☐ Escribir atributos
- ☐ Escribir atributos extendidos
- ☐ Eliminar subcarpetas y archivos
- ☐ Eliminar
- ☐ Permisos de lectura
- ☐ Cambiar permisos
- ☐ Tomar posesión

☒ Aplicar esta configuración de auditoría solo a objetos y/o contenedores dentro de este contenedor Borrar todo

Agregue una condición para limitar el ámbito de esta entrada de auditoría. Los eventos de seguridad se registrarán únicamente si se cumplen las condiciones.

[Agregar una condición](#)

Aceptar Cancelar

Y este sería el aspecto final, para finalizar seleccionamos "Aceptar"

Configuración de seguridad avanzada para actividad 5

Nombre: C:\actividad 5

Propietario: Administradores (MICENTROMARTA\Administradores) [Cambiar](#)

Permisos Auditoría **Acceso efectivo**

Para obtener información adicional, haga doble clic en una entrada de auditoría. Para modificar una entrada de auditoría, seleccione la entrada y haga clic en Editar (si está disponible).

Entradas de auditoría:

Tipo	Entidad de seguridad	Acceso	Heredada de	Se aplica a
Corre...	Sonia (MICENTROMARTA\Sonia)	Mostrar carpeta / leer ...	Ninguno	Esta carpeta, subcarpetas y arc...

Agregar Quitar Editar

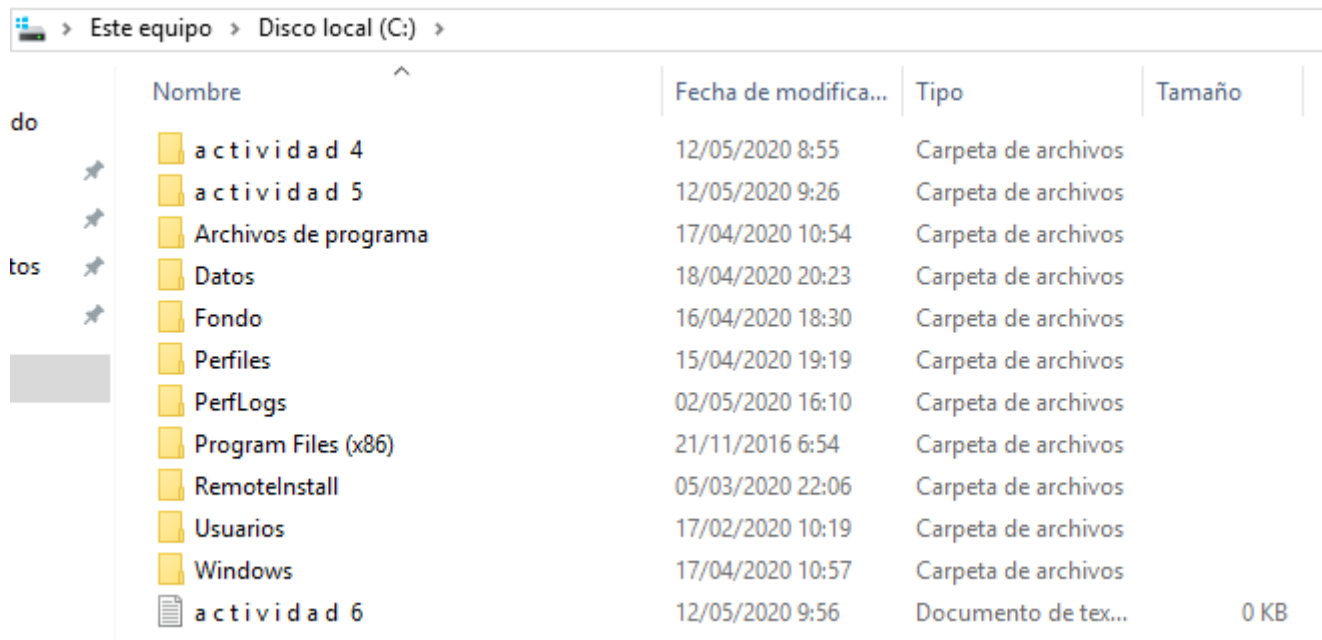
Deshabilitar herencia

☐ Reemplazar todas las entradas de auditoría de objetos secundarios por entradas de auditoría heredables de este objeto

Aceptar Cancelar Aplicar

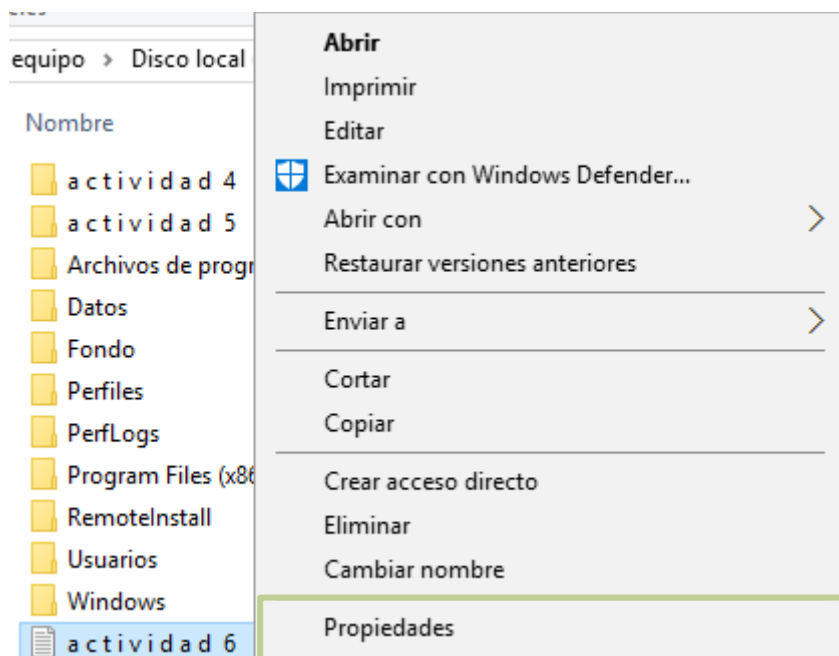
6. AUDITAR EL ACCESO A UN ARCHIVO DEL EQUIPO

Creamos un archivo de texto, en mi caso le he llamado "a c t i v i d a d 6"

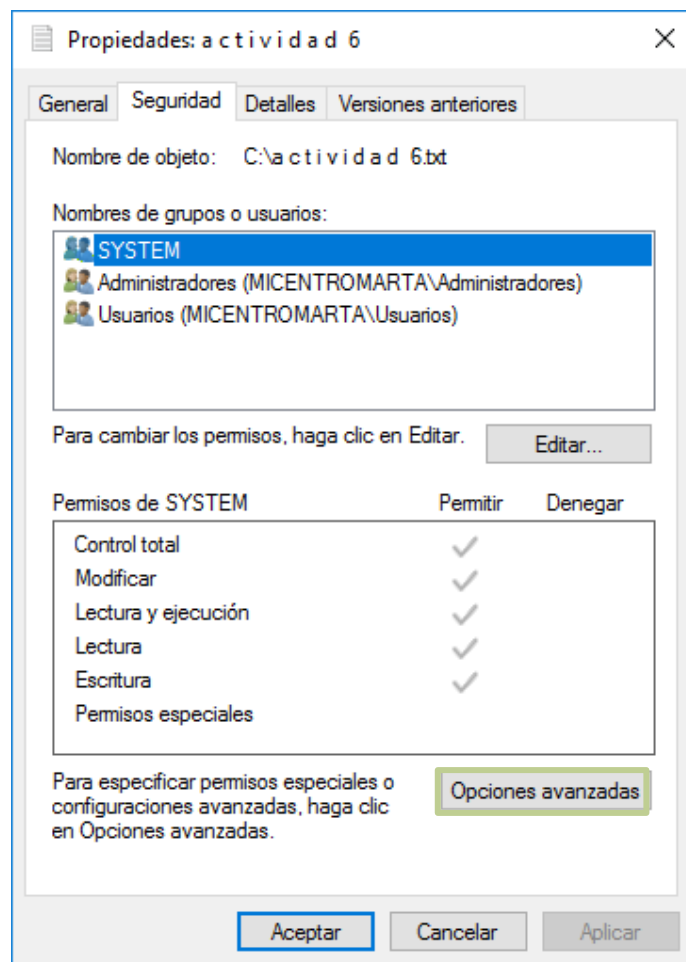


Este equipo > Disco local (C:) >				
	Nombre	Fecha de modifica...	Tipo	Tamaño
do	actividad 4	12/05/2020 8:55	Carpeta de archivos	
	actividad 5	12/05/2020 9:26	Carpeta de archivos	
tos	Archivos de programa	17/04/2020 10:54	Carpeta de archivos	
	Datos	18/04/2020 20:23	Carpeta de archivos	
	Fondo	16/04/2020 18:30	Carpeta de archivos	
	Perfiles	15/04/2020 19:19	Carpeta de archivos	
	PerfLogs	02/05/2020 16:10	Carpeta de archivos	
	Program Files (x86)	21/11/2016 6:54	Carpeta de archivos	
	RemoteInstall	05/03/2020 22:06	Carpeta de archivos	
	Usuarios	17/02/2020 10:19	Carpeta de archivos	
	Windows	17/04/2020 10:57	Carpeta de archivos	
	actividad 6	12/05/2020 9:56	Documento de tex...	0 KB

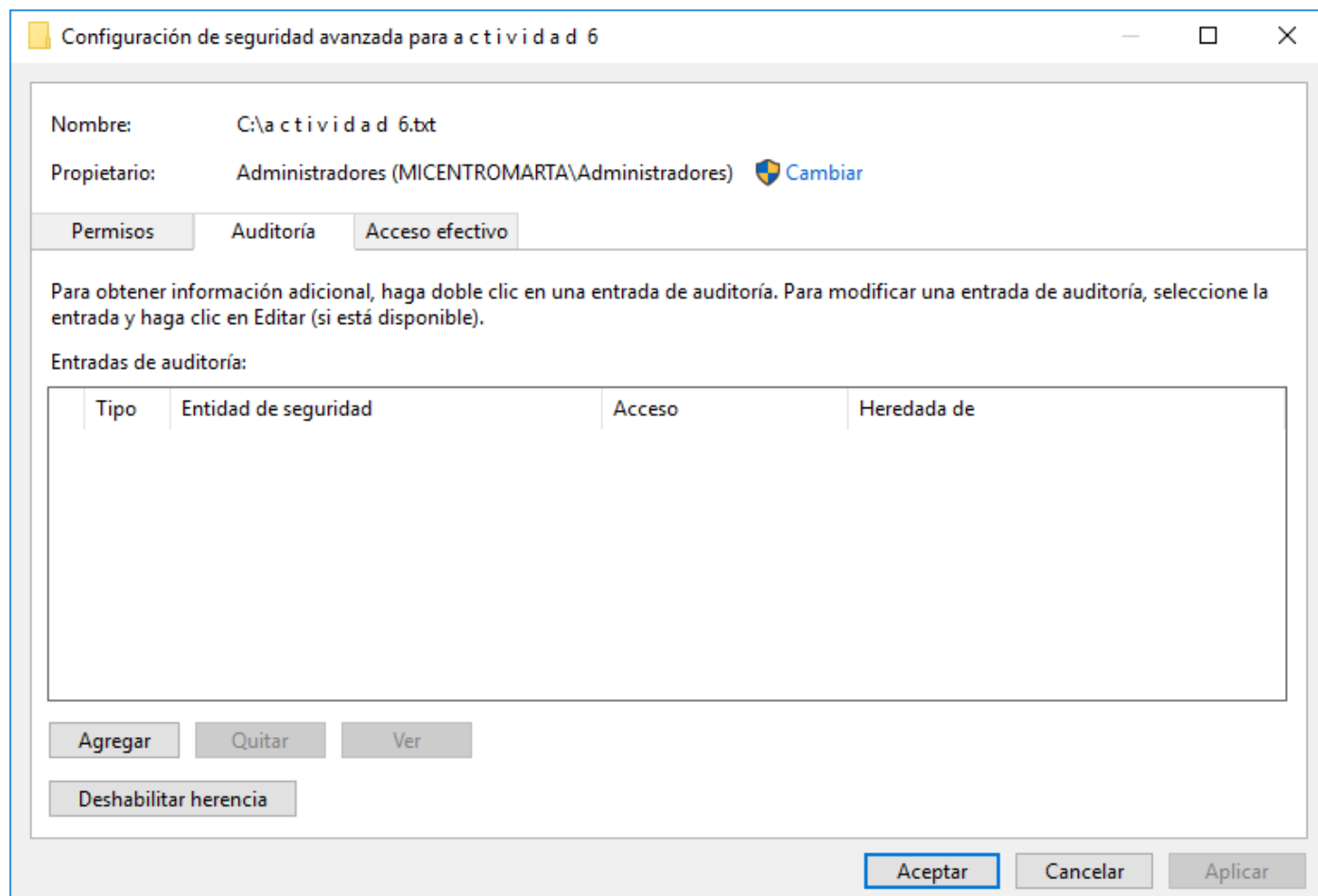
Presionamos el botón derecho del ratón y seleccionamos "Propiedades"



Seleccionamos "Seguridad">"Opciones avanzadas"



Seleccionamos "Auditoría">"Agregar"



Seleccionamos "Seleccionar una entidad de seguridad"

Entrada de auditoría para actividad 6

Entidad de seguridad: **Seleccionar una entidad de seguridad**

Tipo: Correcto

Permisos básicos: Mostrar permisos avanzados

- ☐ Control total
- ☐ Modificar
- ☒ Lectura y ejecución
- ☒ Lectura
- ☐ Escritura
- ☐ Permisos especiales

Borrar todo

Agregue una condición para limitar el ámbito de esta entrada de auditoría. Los eventos de seguridad se registrarán únicamente si se cumplen las condiciones.

[Agregar una condición](#)

Aceptar Cancelar

Introducimos "Todos" y "Aceptar"

Seleccionar Usuario, Equipo, Cuenta de servicio o Grupo

Seleccionar este tipo de objeto:
Usuario, Grupo, o Entidad de seguridad integrada Tipos de objeto...

Desde esta ubicación:
MICENTROMARTA.COM Ubicaciones...

Escriba el nombre de objeto para seleccionar (ejemplos):
Todos Comprobar nombres

Opciones avanzadas... Aceptar Cancelar

Seleccionamos en "Mostrar permisos avanzados" y en mi caso lo dejare por defecto y "Aceptar"

Entrada de auditoría para actividad 6

Entidad de seguridad: Todos [Seleccionar una entidad de seguridad](#)

Tipo: Correcto

Permisos avanzados:

- ☐ Control total
- ☒ Atravesar carpeta / ejecutar archivo
- ☒ Mostrar carpeta / leer datos
- ☒ Leer atributos
- ☒ Leer atributos extendidos
- ☐ Crear archivos / escribir datos
- ☐ Crear carpetas / anexar datos
- ☐ Escribir atributos
- ☐ Escribir atributos extendidos
- ☐ Eliminar
- ☒ Permisos de lectura
- ☐ Cambiar permisos
- ☐ Tomar posesión

[Mostrar permisos básicos](#)

Borrar todo

Agregue una condición para limitar el ámbito de esta entrada de auditoría. Los eventos de seguridad se registrarán únicamente si se cumplen las condiciones.

[Agregar una condición](#)

Aceptar Cancelar

Este seria el aspecto final, para finalizar seleccionamos "Aceptar"

Configuración de seguridad avanzada para actividad 6

Nombre: C:\actividad 6.txt

Propietario: Administradores (MICENTROMARTA\Administradores) [Cambiar](#)

Permisos Auditoría Acceso efectivo

Para obtener información adicional, haga doble clic en una entrada de auditoría. Para modificar una entrada de auditoría, seleccione la entrada y haga clic en Editar (si está disponible).

Entradas de auditoría:

Tipo	Entidad de seguridad	Acceso	Heredada de
Corre...	Todos	Lectura y ejecución	Ninguno

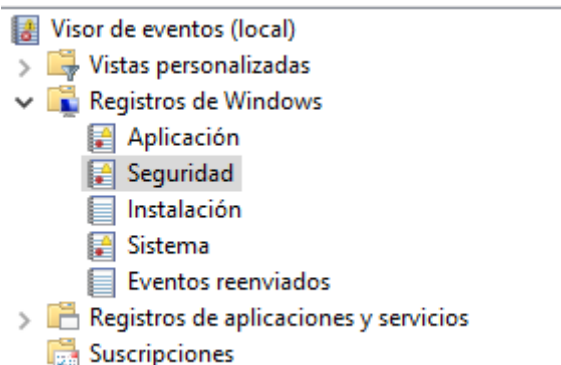
Agregar Quitar Editar

Deshabilitar herencia

Aceptar Cancelar Aplicar

7. CONSULTAR EL VISOR DE SUCESOS

Para ello he provocado todas las situaciones para poder visualizar las seis directivas. Para visualizar todos los eventos nos dirigimos a "Visor de eventos" y dentro de él seleccionamos en la barra lateral "Registros de Windows">"Seguridad"



Podemos observar que en el centro tenemos los eventos que han sucedido y en la parte inferior podemos ver los detalles de ese evento. En la siguiente imagen he escogido el evento seleccionado de azul que ha sido un error de auditoría ya que han intentado acceder con un nombre de usuario o contraseña incorrecta.

Seguridad Número de eventos: 248.725 (!) Nuevos eventos disponibles

Palabras clave	Fecha y hora	Origen
Auditoría correcta	14/05/2020 18:18:18	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:18:14	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:18:14	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:18:13	Microsoft Windows security auditing.
Error de auditoría	14/05/2020 18:18:13	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:18:13	Microsoft Windows security auditing.

Evento 4625, Microsoft Windows security auditing.

General Detalles

Cuenta con error de inicio de sesión:
Id. de seguridad: NULL SID
Nombre de cuenta: Administrador
Dominio de cuenta: MICENTROMARTA

Información de error:
Motivo del error: Nombre de usuario desconocido o contraseña incorrecta
Estado: 0xC000006D
Subestado: 0xC000006A

Nombre de registro: Seguridad

Origen: Microsoft Windows security Registrado: 14/05/2020 18:18:13

Id. del: 4625 Categoría de tarea: Inicio de sesión

Nivel: Información Palabras clave: Error de auditoría

Usuario: No disponible Equipo: Servidor-Martha.MICENTROMARTA.COM

Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

En la siguiente imagen hemos accedido a la carpeta "a c t i v i d a d 4" y como vemos la auditoria se ha realizado correctamente:

Seguridad

Número de eventos: 248.338 (!) Nuevos eventos disponibles

Palabras clave	Fecha y hora	Origen
Auditoría correcta	14/05/2020 18:26:10	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:26:10	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:26:10	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:26:10	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:26:10	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:26:10	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:26:10	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:26:10	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:26:10	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:26:10	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:26:10	Microsoft Windows security auditing.
Auditoría correcta	14/05/2020 18:26:10	Microsoft Windows security auditing.

Evento 4663, Microsoft Windows security auditing.

General

Detalles

☒ Vista descriptiva

☐ Vista XML

SubjectUserSid S-1-5-21-2835310881-3942032251-2157602538-500

SubjectUserName Administrador

SubjectDomainName MICENTROMARTA

SubjectLogonId 0x7e726

ObjectServer Security

ObjectType File

ObjectName C:\a c t i v i d a d 4

conclusión

En esta práctica aprenderemos los tipos de directivas de seguridad, como establecerlas; a auditar todo tipo de sucesos u objetos y a manejar el Visor de eventos en el cual hemos aprendido a interpretar los datos de las auditorías.

bibliografía

- Powerpoint "8 DIRECTIVAS DE SEGURIDAD Y AUDITORIAS"
- <https://www.youtube.com/watch?v=RDw1eA1esy8>