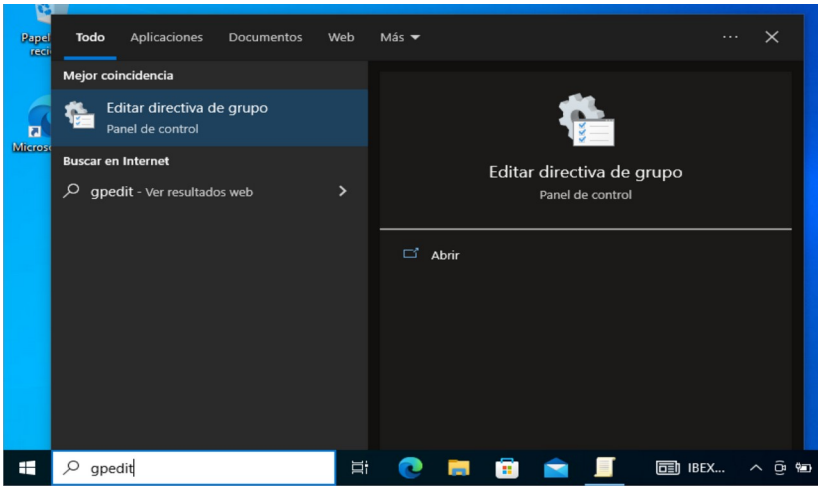
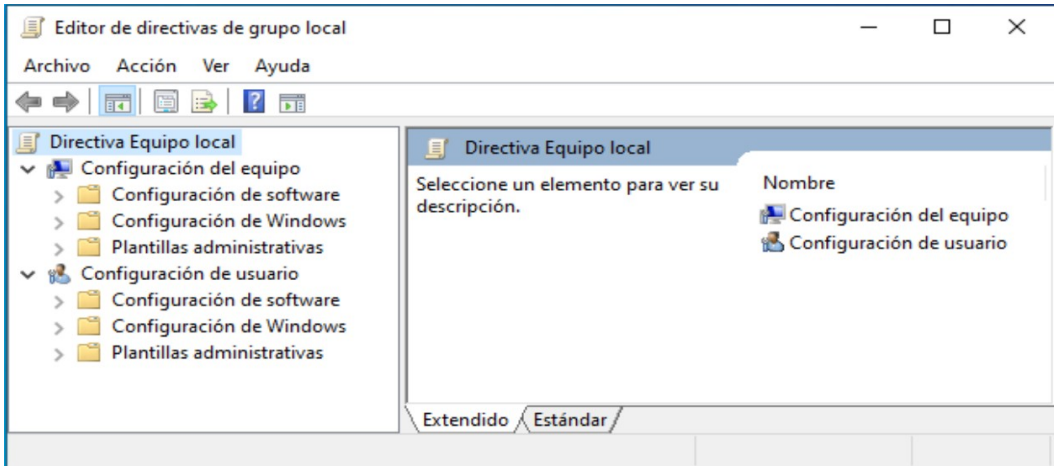
Directivas de Grupo

Iniciar el editor de directivas de grupo:

Se debe ejecutar la orden gpedit:



Con lo que se abrirá el editor de directivas de grupo donde se pueden observar dos tipos de directivas: **las de equipo y las de usuario**:



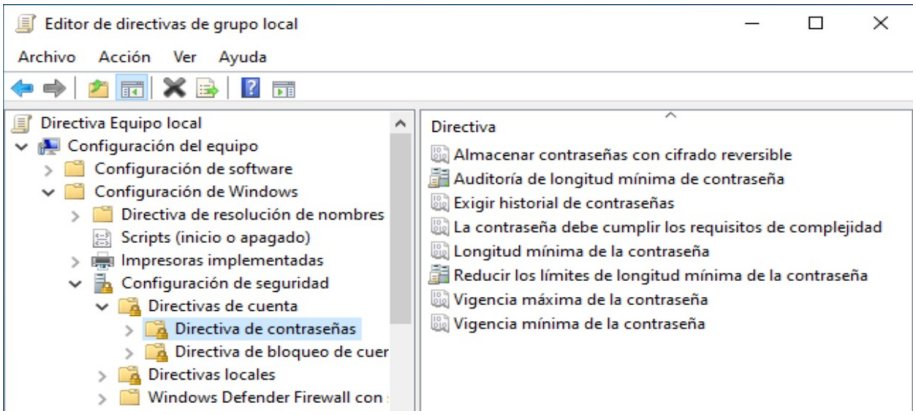
Con estas directivas se crean las reglas que controlan algunos aspectos de la configuración del sistema que nos interesan especialmente en las tareas de configuración de contraseñas y permisos de usuario.

Directivas sobre el uso de contraseñas

Desde el editor de directivas de grupo vamos a acceder a:

Configuración de Equipo → Configuración de Windows →Configuración de Seguridad

Dentro encontraremos la carpeta de Directivas de cuenta donde se halla la carpeta de las directivas de contraseña:



Entre las que se muestran en pantalla podemos destacar:

Exigir el historial de contraseñas para que el usuario no pueda repetir las últimas contraseñas empleadas en su cuenta.

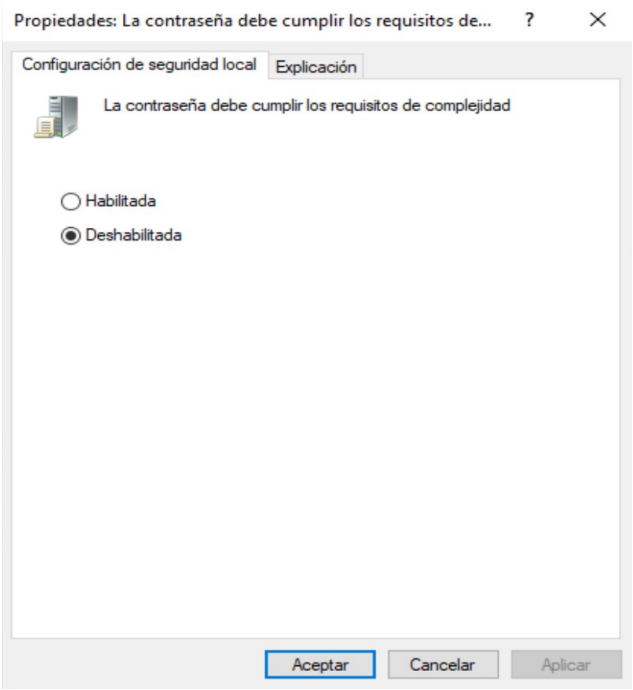
Cumplir requisitos de complejidad: obliga a los usuarios a poner contraseñas robustas, con letras, números y signos que no sean ni letras ni números.

Longitud mínima de la contraseña: establece el mínimo número de caracteres que debe tener una contraseña válida.

Vigencia máxima de la contraseña: Establece el número de días en los que la contraseña es válida. Dice cuando va a caducar la contraseña.

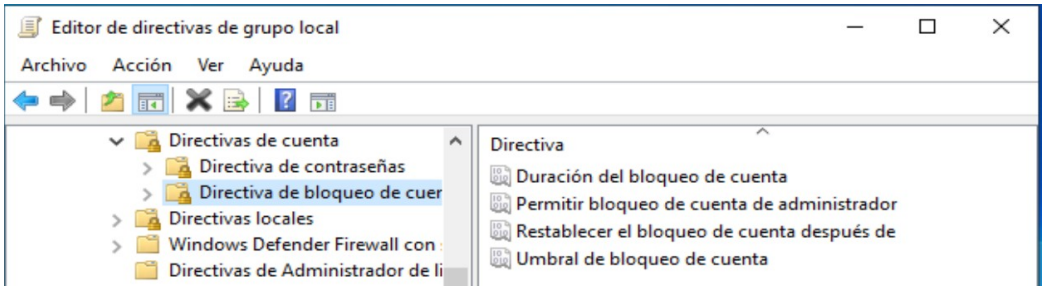
Vigencia mínima de la contraseña: Número de días que deben transcurrir hasta que se pueda cambiar la contraseña.

Para activar una directiva se puede hacer doble click sobre ella y se abrirá la ventana con sus propiedades:



Bloqueo de cuentas

Estas directivas permiten bloquear la cuenta de un usuario cuando se falla un determinado número de veces.



Umbral de bloqueo de cuentas: Número de intentos fallidos para que la cuenta quede bloqueada.

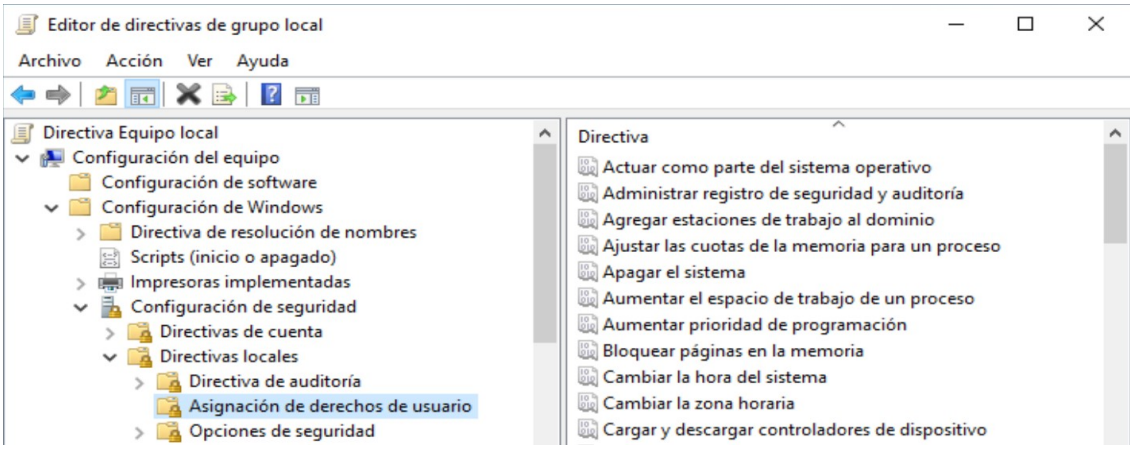
Duración del bloqueo: Tiempo que la cuenta quedará bloqueada.

Restablecer el bloqueo después de: Tiempo que tardará el contador de intentos fallidos en ponerse a cero.

Permitir el bloqueo de cuenta del administrador: Determina si a la cuenta integrada del Administrador se le aplicarán estas directivas.

Derechos de usuario

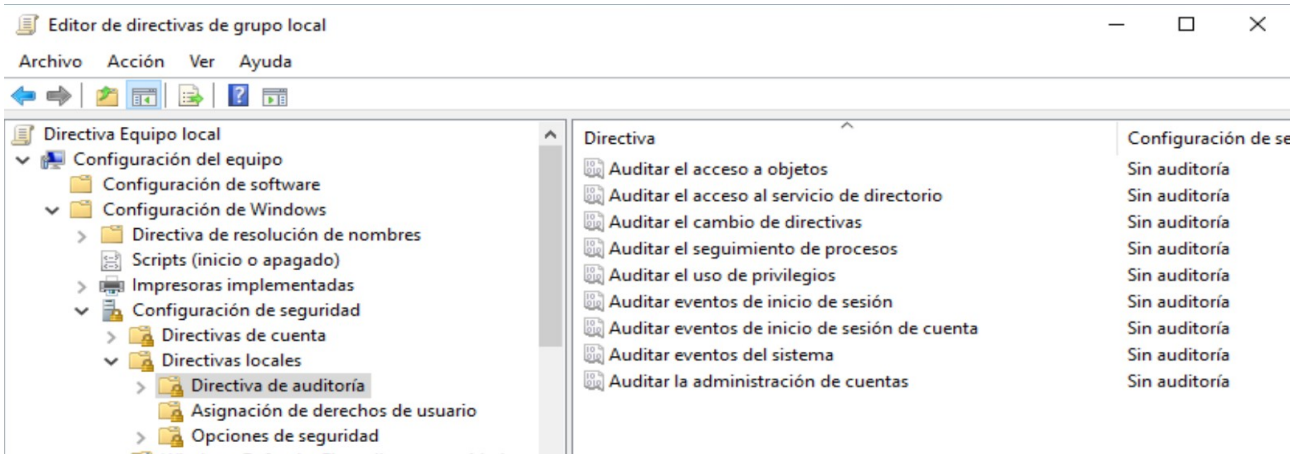
Estas directivas permiten establecer unos permisos especiales sobre usuarios o grupos que no sean Administradores



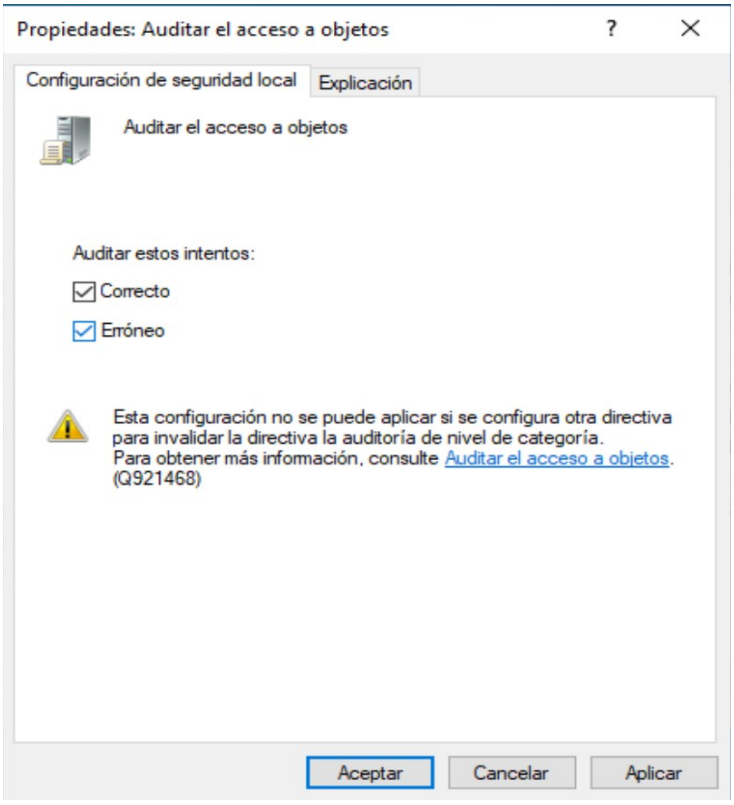
Permite a usuarios estándar realizar operaciones básicas de administración: cambiar la hora, la fecha, apagar el sistema...

Auditoría

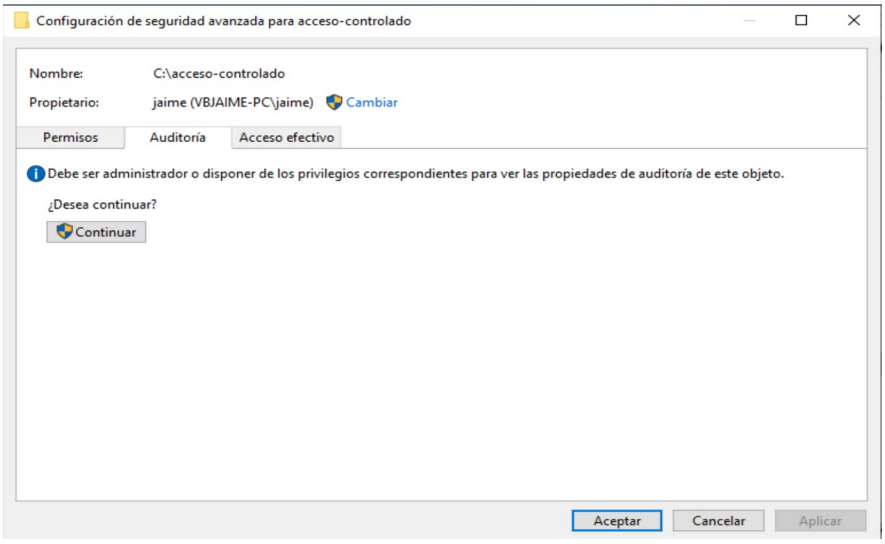
Permite que se registren eventos en el sistema cuando un usuario accede a carpetas o archivos, o cuando se inicia sesión en el sistema



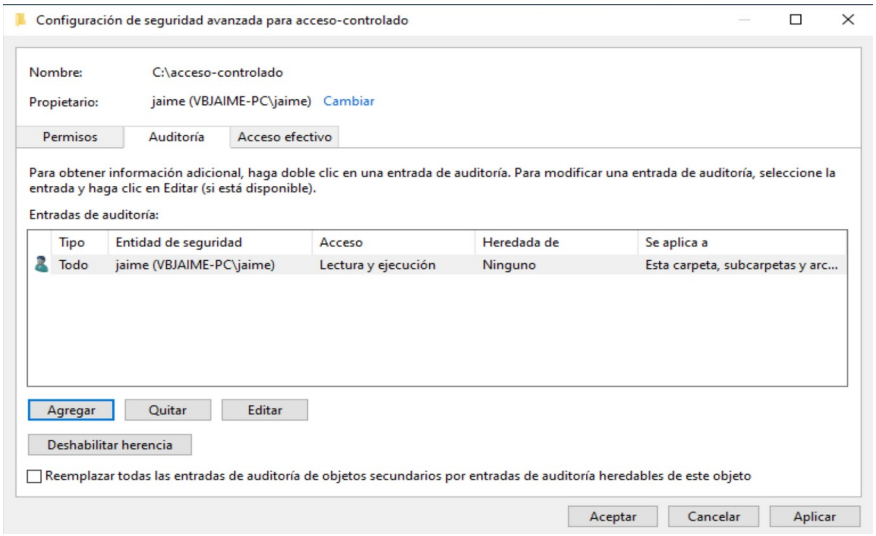
Para generar eventos de acceso a objetos del sistema de archivo se puede usar la pestaña de Seguridad de las propiedades del objeto y definir los tipos de eventos a generar:



En la pestaña seguridad de, por ejemplo, una carpeta encontraremos dentro de “opciones avanzadas” un apartado para configurar la auditoría sobre esta carpeta:



Si se tienen permisos de administrador se puede ver la configuración de auditoría de la carpeta llamada **acceso-controlado** y añadir a un usuario para que se registren los eventos correspondientes a los accesos realizados.



Los eventos se pueden visualizar en el visor de eventos del sistema: