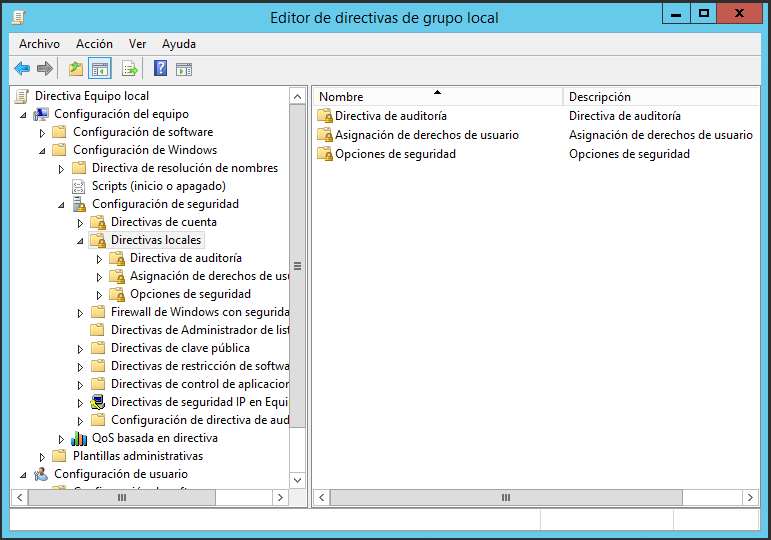
# https://3.bp.blogspot.com/-iC2m9Zv8TNg/Vtc7fgig9VI/AAAAAAAATp8/FmGfzRlcxxE/s1600/March-2016-Abstract-Wallpaper-Blank%2Bcopy.png

Sistemas: Trabajo final

Directivas Locales de Seguridad

**2017**

Andrei García Cuadra



# Información útil:

**Directivas de auditoría**: 9 Directivas.

**Asignación de derechos de usuario**: 44 Directivas.

**Opciones de seguridad**: 95 Directivas.

**Directiva de contraseñas**: 6 Directivas.

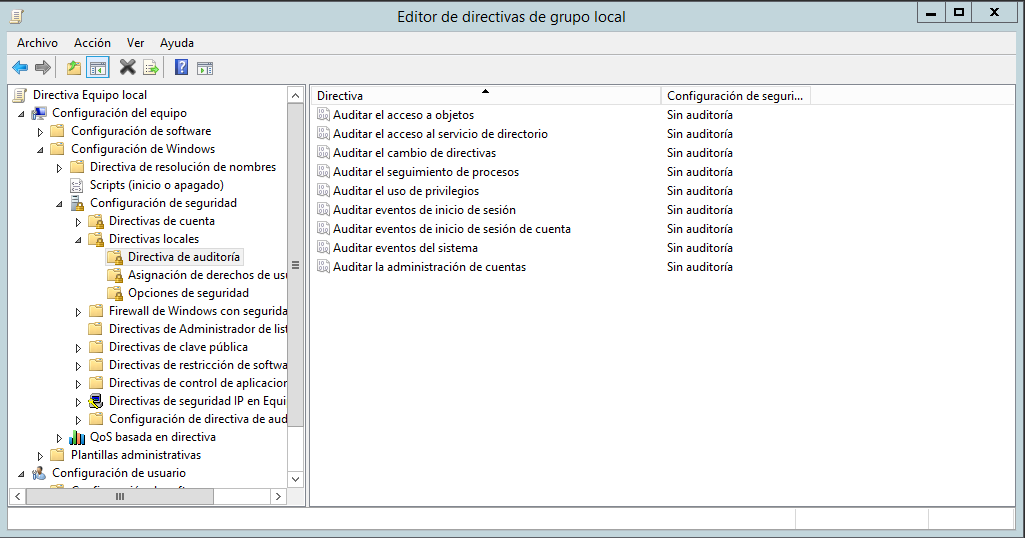
**Directiva de bloqueo de cuenta**: 3 Directivas.

**Directiva de Kerberos**: 5 Directivas.

**Directivas totales**: 162 Directivas.

Las directivas en verde son las más útiles, mientras que las directivas en rojo son las que expondrán a más riesgos al equipo.

# Directivas de auditoría



## Auditar el acceso a objetos

**Descripción**: Guarda los accesos válidos y fallidos a objetos ajenos a Active Directory.

**Posibles valores**: Auditar correcto, auditar erróneo, sin auditoría.

**Valor predeterminado**: Sin auditoría.

## auditar el acceso al servicio de directorio

**Descripción**: Guarda los accesos válidos y fallidos a objetos exclusivos de Active Directory.

**Posibles valores**: Auditar correcto, auditar erróneo, sin auditoría.

**Valor predeterminado**: Sin auditoría.

## auditar el cambio de directivas

**Descripción**: Guarda los accesos válidos y fallidos a cambios en directivas.

**Posibles valores**: Auditar correcto, auditar erróneo, sin auditoría.

**Valor predeterminado**: Sin auditoría.

## auditar el seguimiento de procesos

**Descripción**: Guarda inicio, errores y finalización de procesos.

**Posibles valores**: Auditar correcto, auditar erróneo, sin auditoría.

**Valor predeterminado**: Sin auditoría.

## auditar el uso de privilegios

**Descripción**: Guarda cada acción que requiera privilegios del usuario.

**Posibles valores**: Auditar correcto, auditar erróneo, sin auditoría.

**Valor predeterminado**: Sin auditoría.

## auditar eventos de inicio de sesión

**Descripción**: Guarda los inicios y cierres de sesión en el equipo actual.

**Posibles valores**: Auditar correcto, auditar erróneo, sin auditoría.

**Valor predeterminado**: Sin auditoría.

## auditar eventos de inicio de sesión de cuenta

**Descripción**: Guarda los inicios y cierres de sesión de un usuario determinado en el equipo actual.

**Posibles valores**: Auditar correcto, auditar erróneo, sin auditoría.

**Valor predeterminado**: Sin auditoría.

## auditar eventos del sistema

**Descripción**: Guarda los cambios internos en el equipo (Por ejemplo, el reloj, inicio o cierre del sistema de seguridad…).

**Posibles valores**: Auditar correcto, auditar erróneo, sin auditoría.

**Valor predeterminado**: Sin auditoría.

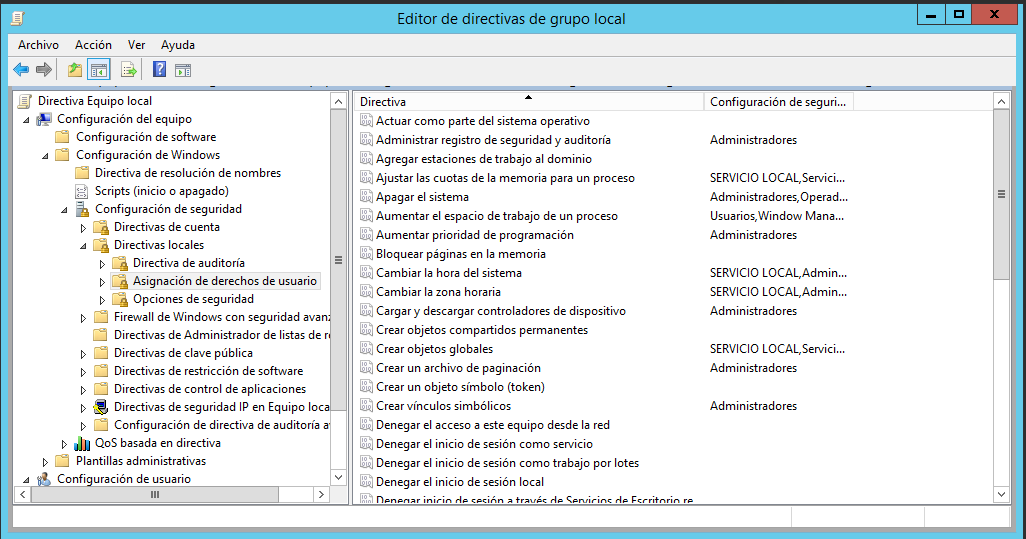
## auditar la administración de cuentas

**Descripción**: Guarda los cambios realizados en cuentas de usuario.

**Posibles valores**: Auditar correcto, auditar erróneo, sin auditoría.

**Valor predeterminado**: Sin auditoría.

# asignación de derechos de usuario



## actuar como parte del sistema operativo

**Descripción**: Permite a cualquier proceso suplantar a usuarios sin requerir autenticación.

**Posibles valores**: Cuentas de usuario.

**Valor predeterminado**: Sin cuentas de usuario.

## administrar registro de seguridad y auditoría

**Descripción**: Determina que usuarios pueden configurar opciones de auditoría de acceso a objetos y recursos de Active Directory.

**Posibles valores**: Cuentas de usuario.

**Valor predeterminado**: Sin cuentas de usuario.

## agregar estaciones de trabajo al dominio

**Descripción**: Determina que usuarios o grupos pueden agregar estaciones de trabajo a un dominio.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Sin cuentas de usuario.

## ajustar las cuotas de la memoria para un proceso

**Descripción**: Determina quién puede cambiar la memoria máxima que puede consumir un proceso.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores, Servicio de red, SERVICIO LOCAL.

## apagar sistema

**Descripción**: Determina qué usuarios pueden apagar el equipo.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores, Operadores de copia de seguridad.

## aumentar el espacio de trabajo de un proceso

**Descripción**: Determina que usuarios pueden aumentar o disminuir el tamaño del espacio de trabajo de un determinado proceso.

**Posibles valores**: Cuentas de usuario.

**Valor predeterminado**: Usuarios, Window Manager\Window Manager Group.

## aumentar prioridad de programación

**Descripción**: Determina que cuentas pueden cambiar la prioridad de programación de un proceso.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores.

## bloquear páginas en la memoria

**Descripción**: Determina que cuenta puede usar un proceso para mantener datos en la RAM.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Sin cuentas de usuario.

## cambiar la hora del sistema

**Descripción**: Determina que usuarios o grupos pueden modificar el reloj del sistema.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores, SERVICIO LOCAL.

## cambiar la zona horaria

**Descripción**: Determina que usuarios o grupos pueden modificar la zona horaria del reloj.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores, SERVICIO LOCAL.

## cargar y descargar controladores de dispositivo

**Descripción**: Determina quiénes pueden modificar los *drivers* del sistema.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores.

## crear objetos compartidos permanentes

**Descripción**: Determina quiénes pueden usar procesos para crear un objeto en la raíz del administrador de objetos.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Sin cuentas de usuario.

## crear objetos globales

**Descripción**: Determina quiénes pueden crear o modificar objetos globales.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL.

## crear un archivo de paginación

**Descripción**: Determina quiénes pueden usar la API del kernel de Windows.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores.

## crear un objeto símbolo (token)

**Descripción**: Determina quiénes pueden crear claves para poder usar la API del kernel de Windows.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Sin cuentas de usuario.

## crear vínculos simbólicos

**Descripción**: Determina si el usuario puede crear un vínculo simbólico desde el equipo en el que inició sesión.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores.

## denegar el acceso a este equipo desde la red

**Descripción**: Deniega el acceso a este equipo desde la red.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Invitado.

## denegar el inicio de sesión como servicio

**Descripción**: Determina que cuentas no pueden iniciar sesión como servicio.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Sin cuentas de usuario.

## denegar el inicio de sesión como trabajo por lotes

**Descripción**: Determina que cuentas no pueden iniciar sesión como trabajo por lotes (BAT).

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Sin cuentas de usuario.

## denegar el inicio de sesión local

**Descripción**: Determina que cuentas no pueden iniciar sesión en este equipo.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Sin cuentas de usuario.

## denegar el inicio de sesión a través de servicios de escritorio remoto

**Descripción**: Determina que cuentas no pueden iniciar sesión en este equipo a través de Escritorio Remoto.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Sin cuentas de usuario.

## depurar programas

**Descripción**: Determina quiénes podrán adjuntar un depurador a los procesos.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores.

## forzar cierre desde un sistema remoto

**Descripción**: Determina quiénes pueden apagar este equipo desde la red.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores.

## generar auditorías de seguridad

**Descripción**: Determina quiénes pueden usar un proceso para agregar entradas al registro.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Servicios de red, SERVICIO LOCAL.

## generar perfiles de un solo proceso

**Descripción**: Determina quiénes pueden supervisar el rendimiento de los procesos que no son internos del sistema.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores.

## generar perfiles del rendimiento del sistema

**Descripción**: Determina quiénes pueden supervisar el rendimiento de los procesos que son internos del sistema.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores, NT SERVICE\WdiServiceHost.

## habilitar confianza con el equipo y las cuentas de usuario para delegación

**Descripción**: Determina quiénes pueden delegar permisos.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores en controladores de dominio.

## hacer copias de seguridad de seguridad de archivos y directorios

**Descripción**: Determina quiénes pueden omitir los permisos de archivos y directorios para realizar copias de seguridad del sistema.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores, Operadores de copia de seguridad.

## iniciar sesión como proceso por lotes

**Descripción**: Permitir inicio de sesión de un usuario por archivo por lotes (BAT).

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores, Operadores de copia de seguridad, Usuarios del registro de rendimiento.

## iniciar sesión como servicio

**Descripción**: Permite el inicio de sesión de un usuario por un servicio.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: NT SERVICE\ALL SERVICES.

## modificar la etiqueta de un objeto

**Descripción**: Determina quiénes pueden cambiar el nombre de un objeto del registro, archivos…

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Sin cuentas de usuario.

## modificar valores de entorno firmware

**Descripción**: Determina quiénes pueden modificar las variables de entorno para equipos X86 (32 bits).

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores.

## obtener acceso al administrador de credenciales como un llamador de confianza

**Descripción**: Delegar permisos para administrar todas las credenciales en las operaciones de copia de seguridad.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Sin cuentas de usuario.

## omitir comprobación de recorrido

**Descripción**: Determina quiénes pueden recorrer árboles de directorios aunque no se disponga de permisos en el directorio recorrido.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Todos, Administradores, Operadores de copia de seguridad, Servicio de red, SERVICIO LOCAL, Usuarios, Window Manager\Window Manager Group.

## permitir el inicio de sesión local

**Descripción**: Determina que usuarios pueden iniciar sesión en este equipo.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores, Operadores de copia de seguridad, Usuarios.

## permitir el inicio de sesión a través de servicios de escritorio remoto

**Descripción**: Permitir que usuarios inicien sesión a través de Escritorio Remoto.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores, Usuarios de escritorio remoto.

## quitar equipo de la estación de acoplamiento

**Descripción**: Determina quiénes pueden mover físicamente un equipo portátil sin iniciar sesión.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores.

## realizar tareas de mantenimiento del volumen

**Descripción**: Determina quiénes pueden realizar operaciones sobre el volumen.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores.

## reemplazar un símbolo (token) de nivel de proceso

**Descripción**: Determina que usuarios pueden realizar llamadas a la API del kernel para que un servicio pueda iniciar otro.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Servicio de red, SERVICIO LOCAL.

## restaurar archivos y directorios

**Descripción**: Determina qué usuarios pueden omitir los permisos sobre ficheros y directorios.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores, Operadores de copia de seguridad.

## sincronizar los datos del servicio de directorio

**Descripción**: Determina quiénes disponen de privilegios para sincronizar todos los datos de Active Directory.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Sin cuentas de usuario.

## suplantar a un cliente tras la autenticación

**Descripción**: Permitir que a un determinado usuario se le permita ejecutar programas de control remoto sin autorización previa.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL.

## tener acceso a este equipo desde la red

**Descripción**: Permitir a cierto usuario acceder a este equipo desde la red.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Todos, Administradores, Operadores de copia de seguridad, Usuarios.

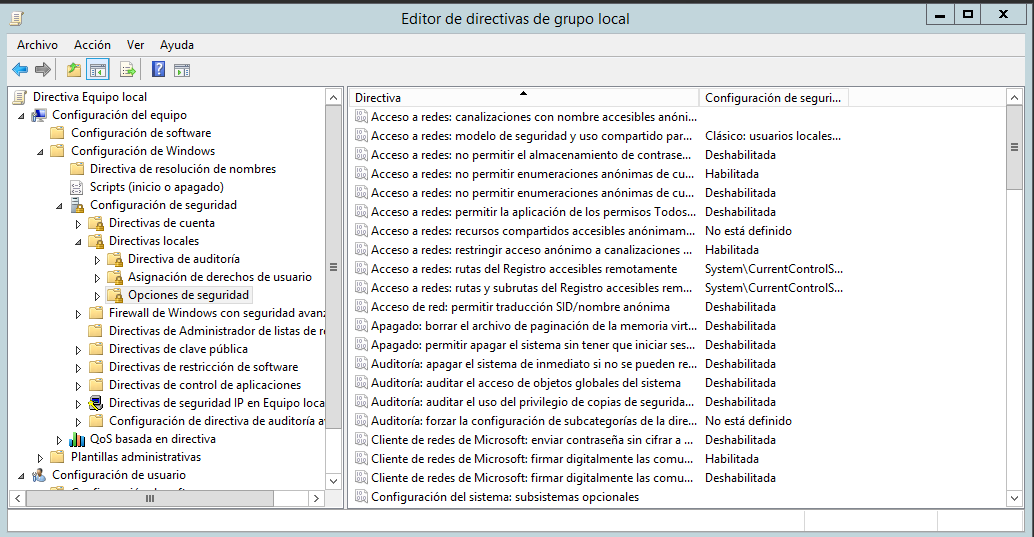
## tomar posesión de archivos y otros objetos

**Descripción**: Determina quiénes pueden autoritarse cualquier objeto del sistema.

**Posibles valores**: Cuentas de usuario o grupos.

**Valor predeterminado**: Administradores.

# opciones de seguridad



## Acceso a redes: canalizaciones con nombre accesibles anónimamente

**Descripción**: Esta configuración de seguridad determina las sesiones de comunicación (canalizaciones) que tendrán atributos y permisos que permitan el acceso anónimo.

**Posibles valores**: Nombres accesibles anónimamente.

**Valor predeterminado**: Ninguno.

## Acceso a redes: modelo de seguridad y uso compartido para cuentas locales

**Descripción**: Determina como se ha de iniciar sesión para conectarse a una red.

**Posibles valores**: Clásico: usuarios locales se autentican con credenciales propias, Sólo invitado: los usuarios locales se autentican como invitados.

**Valor predeterminado**: Clásico.

## Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red

**Descripción**: Determina si se posibilita guardar las credenciales de sesión o no.

**Posibles valores**: Habilitada / Deshabilitada.

**Valor predeterminado**: Deshabilitada.

## Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM

**Descripción**: Determina los permisos adicionales que se concederán para las conexiones anónimas al equipo.

**Posibles valores**: Habilitada / Deshabilitada.

**Valor predeterminado**: Habilitada.

## Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM

**Descripción**: Determina si se pueden numerar cuentas de SAM.

**Posibles valores**: Habilitada / Deshabilitada.

**Valor predeterminado**: Deshabilitada.

## Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos

**Descripción**: Seguridad determina los permisos adicionales que se conceden para conexiones anónimas al equipo.

**Posibles valores**: Habilitada / Deshabilitada.

**Valor predeterminado**: Deshabilitada.

## Acceso a redes: recursos compartidos accesibles anónimamente

**Descripción**: Indica qué recursos pueden ser accesibles sin autenticación desde la red.

**Posibles valores**: Recurso.

**Valor predeterminado**: Ninguno especificado.

## Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos

**Descripción**: Prohíbe el acceso a los recursos compartidos a usuarios sin autenticar.

**Posibles valores**: Habilitada / Deshabilitada.

**Valor predeterminado**: Habilitada.

## Acceso a redes: rutas del Registro accesibles remotamente

**Descripción**: Especifica línea por línea que rutas del registro pueden ser accedidas remotamente sin incluir en la ACL.

**Posibles valores**: Rutas del registro de Windows.

**Valor predeterminado**: System\CurrentControlSet\Control\ProductOptions

System\CurrentControlSet\Control\Server Applications

Software\Microsoft\Windows NT\CurrentVersion

## Acceso de red: rutas y subrutas de Registro accesibles remotamente

**Descripción**: Especifica línea por línea que rutas del registro pueden ser accedidas remotamente incluidos en la ACL.

**Posibles valores**: Rutas del registro de Windows.

**Valor predeterminado**: System\CurrentControlSet\Control\Print\Printers

System\CurrentControlSet\Services\Eventlog

Software\Microsoft\OLAP Server

Software\Microsoft\Windows NT\CurrentVersion\Print

Software\Microsoft\Windows NT\CurrentVersion\Windows

System\CurrentControlSet\Control\ContentIndex

System\CurrentControlSet\Control\Terminal Server

System\CurrentControlSet\Control\Terminal Server\UserConfig

System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration

Software\Microsoft\Windows NT\CurrentVersion\Perflib

System\CurrentControlSet\Services\SysmonLog

## Acceso de red: permitir traducción SID-nombre anónima

**Descripción**: Determina si un usuario anónimo puede solicitar el SID de otro usuario.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Apagado: borrar el archivo de paginación de la memoria virtual

**Descripción**: Determina si se borra el archivo de paginación del sistema al apagar el mismo.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Apagado: permitir apagar el sistema sin tener que iniciar sesión

**Descripción**: Especifica si se puede apagar el sistema sin iniciar sesión.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad

**Descripción**: Determina si el sistema fuerza el apagado cuando no se pueden registrar las auditorías de seguridad.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Auditoría: auditar el acceso de objetos globales del sistema

**Descripción**: Determina si se audita el acceso a objetos globales.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Auditoría: auditar el uso del privilegio de copias de seguridad y restauración

**Descripción**: Determina si se va a auditar los archivos restaurados o copias de seguridad.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Auditoría: forzar que la configuración de subcategoría de directiva de auditoría (Windows Vista o posterior) invalide la configuración de categoría de directiva de auditoría.

**Descripción**: Determina si se usarán directivas de uso específico en las auditorías en Windows Vista y posterior.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Ninguna especificada.

## Cliente de redes de Microsoft: enviar contraseña sin cifrar para conectar con servidores SMB de terceros

**Descripción**: Permitir compartir contraseñas sin cifrar con servidores SMB (INSEGURO).

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)

**Descripción**: Determina si el cliente SMB intentará negociar la firma de todos los paquetes de SMB.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)

**Descripción**: Determina si el cliente CMB requiere la firma digital de paquetes.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Configuración del sistema: subsistemas opcionales

**Descripción**: Determina los subsistemas disponibles para la compatibilidad de aplicaciones.

**Posibles valores**: Sistemas de compatibilidad.

**Valor predeterminado**: POSIX.

## Configuración del sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software

**Descripción**: Determina si se procesan los certificados de seguridad en cada aplicación .exe.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Consola de recuperación: permitir el inicio de sesión administrativo automático

**Descripción**: Determina si se ha de proporcionar la contraseña de Administrador para tener acceso al sistema independientemente del usuario actual.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas

**Descripción**: Activa el comando SET (Registro) en la consola de recuperación.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación

**Descripción**: Determina si las solicitudes de permisos ubicadas en el escritorio son permitidas o no.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador

**Descripción**: Controla el comportamiento de la petición de permisos de los Administradores.

**Posibles valores**: Elevar sin preguntar, Pedir credenciales en el escritorio seguro, Pedir consentimiento en el escritorio seguro, Pedir credenciales, Pedir consentimiento, Pedir consentimiento para binarios que no son de Windows.

**Valor predeterminado**: Pedir consentimiento para binarios que no son de Windows.

## Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar

**Descripción**: Controla la elevación de permisos para usuarios estándar.

**Posibles valores**: Rechazar solicitudes de elevación de permisos automáticamente, Pedir credenciales en el escritorio seguro, Pedir credenciales.

**Valor predeterminado**: Pedir credenciales.

## Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación

**Descripción**: Controla el comportamiento de instalación de aplicaciones.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Control de cuentas de usuario: activar el Modo de aprobación de administrador.

**Descripción**: Establece si UAC está activado.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Control de cuentas de usuario: elevar solo aplicaciones UIAccess instaladas en ubicaciones seguras

**Descripción**: Determina si las aplicaciones ejecutadas deben encontrarse en una ruta del sistema segura.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Control de cuentas de usuario: elevar solo los archivos ejecutables firmados y validados

**Descripción**: Determina si se requieren claves PKI para las aplicaciones interactivas ejecutadas con privilegios elevados.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Control de cuentas de usuario: usar Modo de aprobación de administrador para la cuenta predefinida Administrador

**Descripción**: Determina el modo de aprobación para UAC.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro.

**Descripción**: Determina si los programas UIA pueden deshabilitar automáticamente el escritorio seguro.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Control de cuentas de usuario: virtualizar los errores de escritura de archivo y del Registro a ubicaciones por usuario

**Descripción**: Determina si se redireccionan los errores de escritura de programas a ubicaciones definidas en el registro.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo

**Descripción**: Determina si los controladores de dominio rechazarán las solicitudes realizadas por los equipos que han de cambiar sus contraseñas.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Sin valor.

## Controlador de dominio: permitir a los operadores de servidor programar tareas

**Descripción**: Determina si los operadores de servidor pueden enviar tareas mediante AT.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Sin valor.

## Controlador de dominio: requisitos de firma de servidor LDAP

**Descripción**: Determina el modo de negociación de la firma de LDAP.

**Posibles valores**: Ninguno, Requerir firma.

**Valor predeterminado**: Sin valor.

## Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo

**Descripción**: Determina si las claves privadas del usuario requieren el uso de contraseña.

**Posibles valores**: No es necesaria la intervención del usuario al guardar y usar claves nuevas, Se preguntará al usuario cuando se use la clave por primera vez., El usuario debe escribir una contraseña cada vez que use una clave.

**Valor predeterminado**: Sin definir.

## Criptografía de sistema: usar algoritmos criptográficos que cumplan FIPS 140, incluidos algoritmos criptográficos, hash y de firma

**Descripción**: Define si se ha de usar la criptografía FIPS 140 para protocolos seguros.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Cuentas: bloquear cuentas Microsoft

**Descripción**: Evita que los usuarios agreguen nuevas cuentas al equipo.

**Posibles valores**: Esta directiva está deshabilitada, Los usuarios no pueden agregar cuentas Microsoft, Los usuarios no pueden agregar cuentas Microsoft ni iniciar sesión con ellas.

**Valor predeterminado**: Sin definir.

## Cuentas: cambiar el nombre de cuenta de invitado

**Descripción**: Determina si hay otro SID asociado a la cuenta Invitado.

**Posibles valores**: Cuenta de usuario.

**Valor predeterminado**: Invitado.

## Cuentas: cambiar el nombre de la cuenta de administrador

**Descripción**: Determina si hay otro SID asociado a la cuenta Administrador.

**Posibles valores**: Cuenta de usuario.

**Valor predeterminado**: Administrador.

## Cuentas: estado de la cuenta de administrador

**Descripción**: Determina si la cuenta Administrador está habilitada.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Cuentas: estado de la cuenta de invitado

**Descripción**: Determina si la cuenta Invitado está habilitada.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Cuentas: limitar el uso de cuentas locales con contraseña en blanco solo para iniciar sesión en la consola

**Descripción**: Determina si las cuentas locales sin contraseña se pueden usar fuera de la consola.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## DCOM: restricciones de acceso al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)

**Descripción**: Determina los usuarios o grupos que pueden tener acceso a la aplicación DCOM.

**Posibles valores**: Usuario o grupo.

**Valor predeterminado**: Sin definir.

## DCOM: restricciones de inicio de equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)

**Descripción**: Determina si se puede utilizar la aplicación DCOM local o remotamente.

**Posibles valores**: Usuario o grupo.

**Valor predeterminado**: Sin definir.

## Dispositivos: impedir que los usuarios instalen controladores de impresora cuando se conecten a impresoras compartidas

**Descripción**: Determina si se requiere el controlador específico de una impresora para poder proceder a la impresión.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Dispositivos: permitir desacoplamiento sin tener que iniciar sesión

**Descripción**: Determina si un equipo portátil se puede acoplar sin tener que iniciar sesión.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Dispositivos: permitir formatear y expulsar medios extraíbles

**Descripción**: Determina quién puede formatear y expulsar medios NTFS.

**Posibles valores**: Administradores, Administradores y usuarios avanzados, Administradores y usuarios interactivos.

**Valor predeterminado**: Sin definir.

## Dispositivos: restringir el acceso a disquetes solo al usuario con sesión iniciada localmente

**Descripción**: Determina si tanto los usuarios locales como los remotos pueden tener acceso a los medios de disquete extraíble simultáneamente.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Sin definir.

## Dispositivos: restringir el acceso al CD-ROM solo al usuario con sesión iniciada localmente

**Descripción**: Determina si tanto los usuarios locales como los remotos pueden tener acceso al CD-ROM simultáneamente.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Sin definir.

## Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente

**Descripción**: Determina qué hacer cuando se desconecta la tarjeta inteligente de un usuario que inició sesión con la misma.

**Posibles valores**: Ninguna acción, Bloquear estación de trabajo, Forzar cierre sesión, Desconectar si es una sesión de Servicios de Escritorio remoto.

**Valor predeterminado**: Ninguna acción

## Inicio de sesión interactivo: límite de inactividad de equipo.

**Descripción**: Establecer el límite de inactividad de la sesión.

**Posibles valores**: Segundos para bloquear sesión.

**Valor predeterminado**: Sin definir.

## Inicio de sesión interactivo: mostrar información de usuario cuando se bloquee la sesión

**Descripción**: Determina si se muestra información de la sesión anterior cuando se llegue al límite de inactividad del equipo.

**Posibles valores**: Nombre para mostrar del usuario y nombres de dominio y usuario, Sólo nombre para mostrar del usuario, No mostrar la información del usuario.

**Valor predeterminado**: Sin definir.

## Inicio de sesión interactivo: no mostrar el último nombre de usuario

**Descripción**: Determina si se muestra el nombre del último usuario que inicio sesión en el equipo en la pantalla de inicio de sesión.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr

**Descripción**: Determina si no se requiere presionar CTRL+ALT+SUPR antes de iniciar sesión.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Inicio de sesión interactivo: número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible)

**Descripción**: Determina el número de veces que se almacenará en caché el inicio de sesión cuando el controlador del dominio no esté disponible.

**Posibles valores**: Número de inicios de sesión.

**Valor predeterminado**: 10 inicios de sesión.

## Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire

**Descripción**: Determina los días de antelación en los que se comenzará a avisar al usuario de que su contraseña está a punto de expirar.

**Posibles valores**: Número de días.

**Valor predeterminado**: 5 días.

## Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear la estación de trabajo

**Descripción**: Determina si es necesario autenticarse como controlador de dominio en un equipo para desbloquearlo.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Inicio de sesión interactivo: requerir tarjeta inteligente

**Descripción**: Determina si es obligatorio el inicio de sesión con tarjeta inteligente.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión

**Descripción**: Muestra un texto al usuario al iniciar sesión (si es que hay texto para mostrar).

**Posibles valores**: Mensaje al iniciar sesión.

**Valor predeterminado**: Ningún mensaje.

## Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión

**Descripción**: Muestra un texto al usuario al mostrar el panel de conexión (si es que hay texto para mostrar).

**Posibles valores**: Mensaje para el panel de conexión.

**Valor predeterminado**: Ningún mensaje.

## Inicio de sesión interactivo: umbral de cuentas del equipo.

**Descripción**: Determina el número de veces que un usuario puede equivocarse en la conexión antes de que se le bloquee el equipo.

**Posibles valores**: Número de intentos de inicio de sesión válidos.

**Valor predeterminado**: No definido.

## Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)

**Descripción**: Determina si es necesario forzar un protocolo seguro en todas las acciones de un equipo.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)

**Descripción**: Determina si todo el tráfico en protocolo seguro ha de estar firmado digitalmente.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo

**Descripción**: Determina si un usuario ha de cambiar periódicamente su contraseña.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Miembro de dominio: duración máxima de contraseña de cuenta de equipo

**Descripción**: Determina cada cuánto tiempo ha de cambiar su contraseña el usuario.

**Posibles valores**: Número de días.

**Valor predeterminado**: 30 Días.

## Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)

**Descripción**: Determina si un usuario ha de firmar digitalmente sus acciones cuando sea posible.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)

**Descripción**: Determina si se requiere cifrado de 128 bits para el canal seguro.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)

**Descripción**: Determina si los usuarios no administradores pueden leer objetos compartidos (pero no modificar los que no crearon).

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows

**Descripción**: Fuerza a sistemas POSIX a que no se distinga entre mayúsculas y minúsculas.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Seguridad de red: configurar tipos de cifrado permitidos para Kerberos

**Descripción**: Determina las opciones de cifrado disponibles para KERBEROS.

**Posibles valores**: DES\_CBC\_CRC -> ON/OFF

DES\_CBC\_MD5 -> ON/OFF

RC4\_HMAC\_MD5 -> ON/OFF

AES128\_HMAC\_SHA1 -> ON/OFF

AES256\_HMAC\_SHA1 -> ON/OFF

Tipos de cifrado futuros -> ON/OFF

**Valor predeterminado**: DES\_CBC\_CRC -> OFF

DES\_CBC\_MD5 -> OFF

RC4\_HMAC\_MD5 -> OFF

AES128\_HMAC\_SHA1 -> OFF

AES256\_HMAC\_SHA1 -> OFF

Tipos de cifrado futuros -> OFF

## Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión

**Descripción**: Determina si los usuarios que estén conectados cuando expiren en sus horas de inicio de sesión han de ser expulsados del sistema.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Seguridad de red: nivel de autenticación de LAN Manager

**Descripción**: Determina el protocolo de autenticación en red.

**Posibles valores**: Enviar respuestas LM y NTLM, Enviar LM y NTLM, Enviar solo respuesta NTLM, Enviar solo respuesta NTLMv2, Enviar solo respuesta NTLMv2 y rechazar LM, Enviar solo respuesta NTLMv2 y rechazar LM y NTLM.

**Valor predeterminado**: Sin definir.

## Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña

**Descripción**: Determina si en el próximo cambio de contraseña se ha de almacenar usando el cifrado de Lan Manager.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM

**Descripción**: Determina si los servicios de sistema local que negocien la autenticación NTLM usen la identidad del equipo.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Sin definir.

## Seguridad de red: permitir retroceso a sesión NULL de LocalSystem

**Descripción**: Permitir el valor NULL en NTML cuando se usa en el sistema local.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Sin definir.

## Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidades en Internet.

**Descripción**: Permitir que equipos en internet se autentiquen como un equipo unido al dominio.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Seguridad de red: requisitos de firma de cliente LDAP

**Descripción**: Determina el nivel de seguridad de la firma de datos que se solicita en nombres de clientes que emiten solicitudes para LDAP.

**Posibles valores**: Ninguno, Negociar firma, Requerir firma.

**Valor predeterminado**: Negociar firma.

## Seguridad de red: restringir NTLM: agregar excepciones de servidor en este dominio

**Descripción**: Determina los equipos excluidos en los que se puede usar la autenticación de acceso directo NTLM.

**Posibles valores**: Equipos.

**Valor predeterminado**: Sin definir.

## Seguridad de red: restringir NTLM: agregar excepciones de servidor remoto para autenticación NTLM

**Descripción**: Permite crear una lista de excepciones de servidores remotos en los que los clientes pueden usar la autenticación NTLM.

**Posibles valores**: Equipos.

**Valor predeterminado**: Sin definir.

## Seguridad de red: restringir NTLM: auditar tráfico NTLM entrante

**Descripción**: Audita el tráfico NTLM entrante.

**Posibles valores**: Deshabilitar, Habilitar la auditoría para cuentas de dominio, Habilitar la auditoría para todas las cuentas.

**Valor predeterminado**: Sin definir.

## Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio

**Descripción**: Permite auditar la autenticación NTLM en un dominio desde este controlador de dominio.

**Posibles valores**: Deshabilitar, Habilitar para cuentas de dominio en servidores de dominio, Habilitar para cuentas de dominio, Habilitar para servidores de dominio, Habilitar todo.

**Valor predeterminado**: Sin definir.

## Seguridad de red: restringir NTLM: autenticación NTLM en este dominio

**Descripción**: Permite denegar o permitir la autenticación NTLM en un dominio de este controlador de dominio.

**Posibles valores**: Deshabilitar, Denegar para cuentas de dominio en servidores de dominio, Denegar para cuentas de dominio, Denegar para servidores de dominio, Denegar todo.

**Valor predeterminado**: Sin definir.

## Seguridad de red: restringir NTLM: tráfico NTLM entrante

**Descripción**: Esta configuración de directiva permite denegar o permitir el tráfico NTLM entrante.

**Posibles valores**: Permitir todo, denegar todas las cuentas de dominio, Denegar todas las cuentas.

**Valor predeterminado**: Sin definir.

## Seguridad de red: restringir NTLM: tráfico NTLM saliente hacia servidores remotos

**Descripción**: Permite denegar o auditar el tráfico NTLM saliente de este equipo hacia cualquier servidor remoto Windows.

**Posibles valores**: Permitir todo, Auditar todo, Denegar todo.

**Valor predeterminado**: Sin auditar.

## Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)

**Descripción**: Permite a un cliente requerir la negociación del cifrado de 128 bits y/o la seguridad de sesión NTLMv2.

**Posibles valores**: Requerir seguridad de sesión NTLMv2 -> ON/OFF

Requerir cifrado de 128 bits -> ON/OFF

**Valor predeterminado**: Requerir seguridad de sesión NTLMv2 -> OFF

Requerir cifrado de 128 bits -> ON

## Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)

**Descripción**: Permite a un servidor requerir la negociación del cifrado de 128 bits y/o la seguridad de sesión NTLMv2.

**Posibles valores**: Requerir seguridad de sesión NTLMv2 -> ON/OFF

Requerir cifrado de 128 bits -> ON/OFF

**Valor predeterminado**: Requerir seguridad de sesión NTLMv2 -> OFF

Requerir cifrado de 128 bits -> ON

## Servidor de red Microsoft: intentar S4U2Self para obtener información de notificaciones

**Descripción**: Permite admitir clientes que ejecuten una versión de Windows anterior a Windows 8 y que intentan acceder a un recurso compartido de archivos que requiere funcionalidades de Windows 8 o superior.

**Posibles valores**: Valor predeterminado, Habilitado, Deshabilitado.

**Valor predeterminado**: Automático.

## Servidor de red Microsoft: desconectar a los clientes cuando expiren las horas de inicio de sesión

**Descripción**: Determina si se va a desconectar a los usuarios conectados mediante SMB al equipo local fuera de las horas de inicio de sesión válidas de su cuenta de usuario.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)

**Descripción**: Determina si el servidor SMB negociará la firma de paquetes SMB con los clientes que lo soliciten.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)

**Descripción**: Determina si el componente de servidor SMB requiere la firma de los paquetes.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor

**Descripción**: Controla el nivel de validación que realiza el equipo con carpetas o impresoras compartidas.

**Posibles valores**: Desactivado, Aceptar si lo proporciona el cliente, Requerido del cliente.

**Valor predeterminado**: Sin definir.

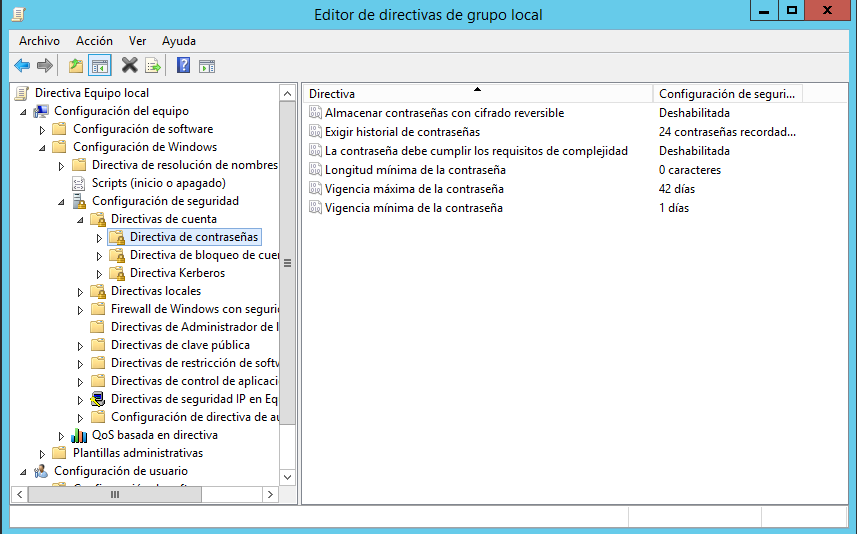
## Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión

**Descripción**: Determina el tiempo que ha de pasar hasta que se marque como inactivo en una sesión.

**Posibles valores**: Número de minutos.

**Valor predeterminado**: 15 Minutos.

# Directiva de contraseñas



## Almacenar contraseñas con cifrado reversible

**Descripción**: Almacena las contraseñas de modo que pueden ser leídas en texto plano si se decodifican correctamente.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Deshabilitado.

## Exigir historial de contraseñas

**Descripción**: Guardar contraseñas anteriores para reforzar la complejidad de contraseñas.

**Posibles valores**: Número de días.

**Valor predeterminado**: 24 Días.

## La contraseña debe cumplir con los requisitos de complejidad

**Descripción**: Forzar las contraseñas a ser complejas.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Sin definir.

## Longitud mínima de la contraseña

**Descripción**: Longitud mínima de la contraseña del usuario.

**Posibles valores**: Número de caracteres mínimos.

**Valor predeterminado**: Sin definir.

## Vigencia máxima de la contraseña

**Descripción**: Período máximo de tiempo que puede permanecer un usuario sin cambiar su contraseña.

**Posibles valores**: Duración en días.

**Valor predeterminado**: 42 Días.

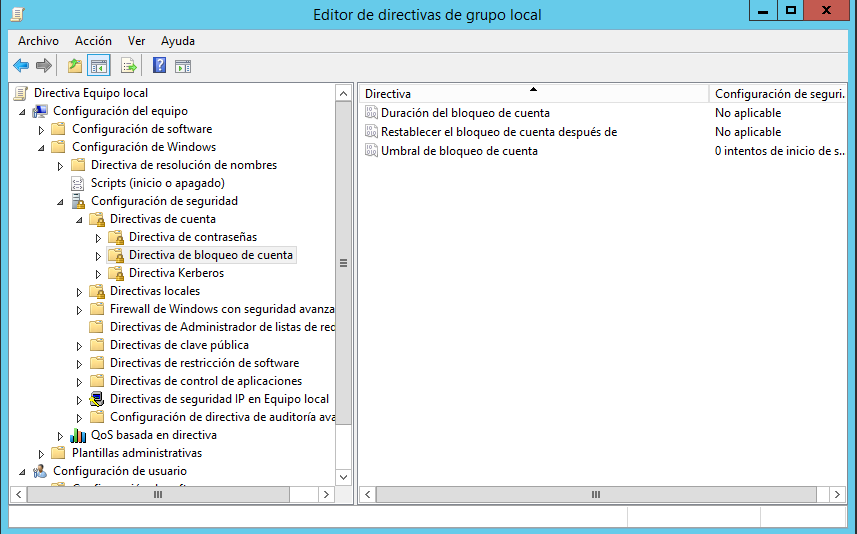
## Vigencia mínima de la contraseña

**Descripción**: Período mínimo de tiempo que puede permanecer un usuario sin cambiar su contraseña.

**Posibles valores**: Duración en días.

**Valor predeterminado**: 1 Día.

# Directiva de bloqueo de cuenta



## Duración del bloqueo de cuenta

**Descripción**: Duración del bloqueo de cuenta en días.

**Posibles valores**: Número de días.

**Valor predeterminado**: Sin definir.

## Restablecer el bloqueo de cuenta después de

**Descripción**: Tiempo desde que se bloquea la cuenta hasta que se vuelve a habilitar.

**Posibles valores**: Número de días.

**Valor predeterminado**: Sin definir.

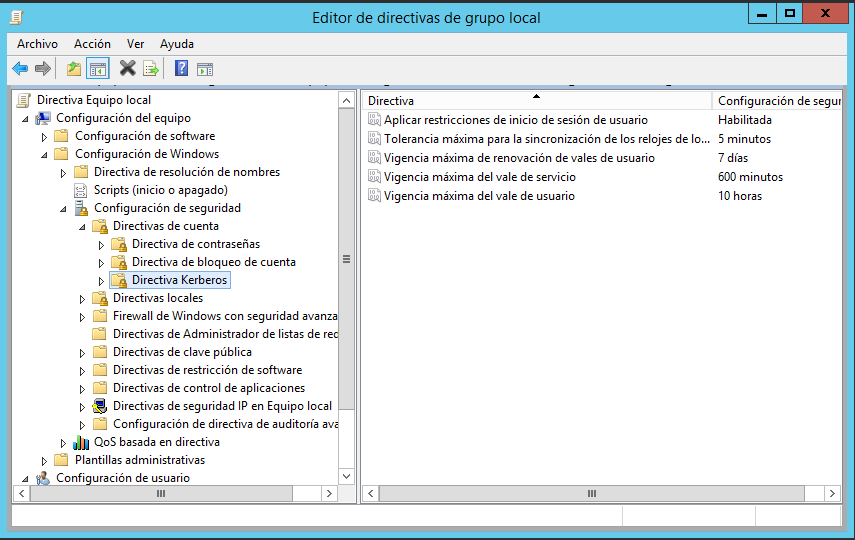
## Umbral de bloqueo de cuenta

**Descripción**: Número de intentos de inicio de sesión máximos, a partir de los cuales se bloqueará la cuenta.

**Posibles valores**: Número de intentos.

**Valor predeterminado**: Sin definir.

# Directiva Kerberos



## aplicar restricciones de inicio de sesión de usuario

**Descripción**: Determina si el centro Kerberos validará todas las solicitudes de inicio de sesión.

**Posibles valores**: Habilitado / Deshabilitado.

**Valor predeterminado**: Habilitado.

## tolerancia máxima para la sincronización de los relojes de los usuarios

**Descripción**: Determina el intervalo máximo en el cual se sincronizarán los relojes de los usuarios.

**Posibles valores**: Tiempo en minutos.

**Valor predeterminado**: 5 Minutos.

## vigencia máxima de renovación de vales de usuario

**Descripción**: Determina el tiempo de renovación de vales TGT para los usuarios.

**Posibles valores**: Número de días.

**Valor predeterminado**: 7 Días.

## vigencia máxima del vale de servicio

**Descripción**: Determina el tiempo máximo de validez para un vale concedido a un servicio.

**Posibles valores**: Número de minutos.

**Valor predeterminado**: 600 minutos.

## vigencia máxima del vale de usuario

**Descripción**: Determina el tiempo máximo de validez para un vale concedido a un usuario.

**Posibles valores**: Número de horas.

**Valor predeterminado**: 10 Horas.