

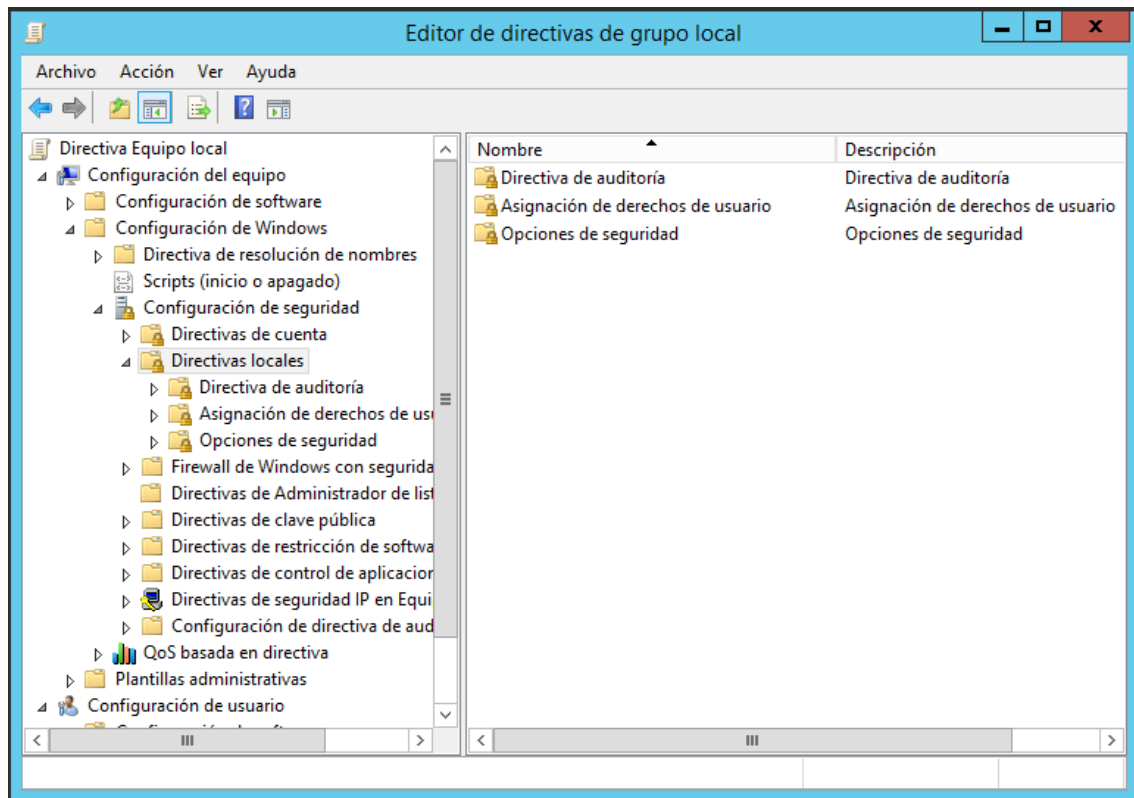


2017

Sistemas: Trabajo final

Directivas Locales de Seguridad

Andrei García Cuadra



INFORMACIÓN ÚTIL:

Directivas de auditoría: 9 Directivas.

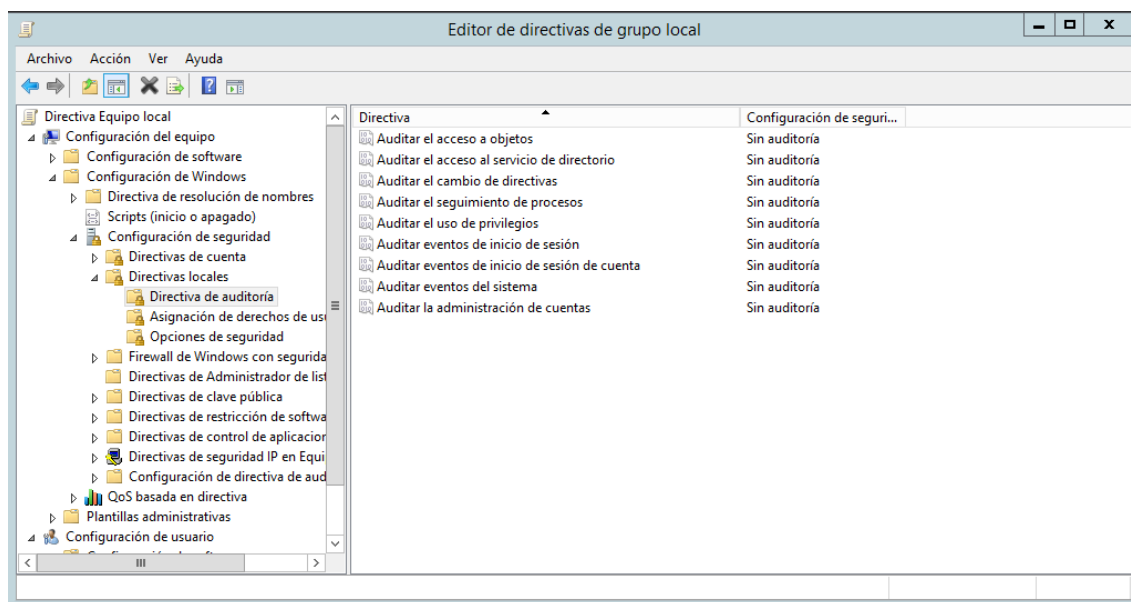
Asignación de derechos de usuario: 44 Directivas.

Opciones de seguridad: 95 Directivas.

Directivas totales: 148 Directivas.

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

1. DIRECTIVAS DE AUDITORÍA



1.1 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.

1.2 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.

1.3 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.

1.4 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.

1.5 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.

1.6 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.

1.7 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.

1.8 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.

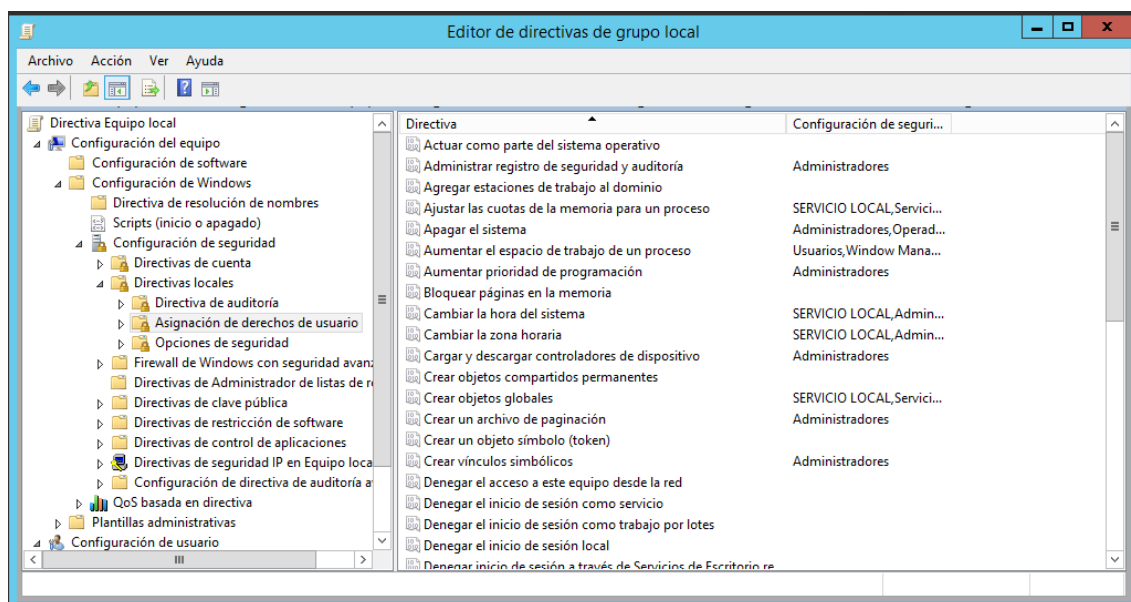
1.9 AUDITAR LA ADMINISTRACIÓN DE CUENTAS

Descripción: Guarda los cambios realizados en cuentas de usuario.

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

Valor predeterminado: Sin auditoría.

2. ASIGNACIÓN DE DERECHOS DE USUARIO



2.1 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.

2.2 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.

2.3 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.

2.4 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.

2.5 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.

2.6 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.

2.7 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.

2.8 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.

2.9 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.

2.10 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.

2.11 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.

2.12 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.

2.13 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.

2.14 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.

2.15 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.

2.16 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.

Sistemas: Trabajo final

2.17 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.

2.18 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.

2.19 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.

2.20 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.

2.21 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.

2.22 DEPURAR PROGRAMAS

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

Posibles valores: Cuentas de usuario o grupos.

Valor predeterminado: Administradores.

2.23 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.

2.24 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.

2.25 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.

2.26 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.

2.27 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.

2.28 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.

2.29 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.

2.30 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.

2.31 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.

2.32 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.

2.33 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.

2.34 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.

2.35 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.

2.36 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.

2.37 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.

2.38 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.

2.39 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.

2.40 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.

2.41 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.

2.42 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.

2.43 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.

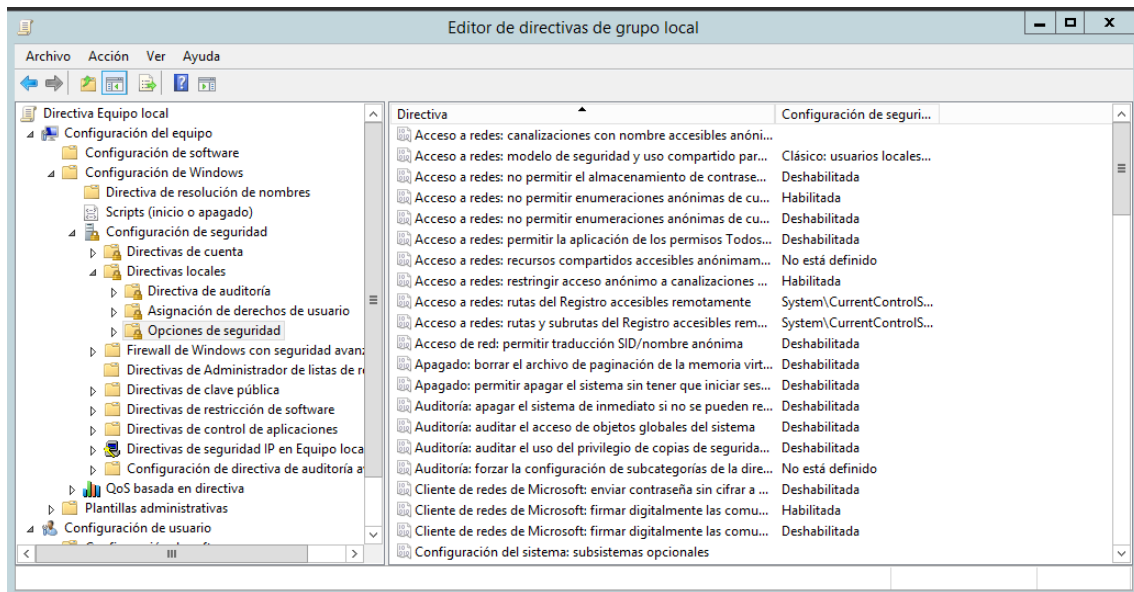
2.44 TOMAR POSESIÓN DE ARCHIVOS Y OTROS OBJETOS

Descripción: Determina quiénes pueden autoritarse cualquier objeto del sistema.

Posibles valores: Cuentas de usuario o grupos.

Valor predeterminado: Administradores.

3. OPCIONES DE SEGURIDAD



3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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.

3.8 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.

3.9 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

3.10 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

3.11 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.

3.12 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.

3.13 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.

3.14 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.

3.15 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.

3.16 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.

3.17 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.

3.18 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.

3.19 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.

Sistemas: Trabajo final

Posibles valores: Habilitado / Deshabilitado.

Valor predeterminado: Habilitado.

3.20 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.

3.21 CONFIGURACIÓN DEL SISTEMA: SUBSISTEMAS OPCIONALES

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

Posibles valores: Sistemas de compatibilidad.

Valor predeterminado: POSIX.

3.22 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.

3.23 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.

3.24 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.

3.25 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.

3.26 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.

3.27 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.

3.28 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.

3.29 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.

3.30 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.

3.31 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.

3.32 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.

3.33 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.

3.34 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.

3.35 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.

3.36 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.

3.37 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.

3.38 CRİPTOGRAFÍA 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.

3.39 CRİPTOGRAFÍA DE SISTEMA: USAR ALGORİTOS CRİPTOGRÁFICOS QUE CUMPLAN FIPS 140, INCLUIDOS ALGORİTOS CRİPTOGRÁFICOS, 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.

3.40 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.

3.41 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.

3.42 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.

3.43 CUENTAS: ESTADO DE LA CUENTA DE ADMINISTRADOR

Descripción: Determina si la cuenta Administrador está habilitada.

Posibles valores: Habilitado / Deshabilitado.

Valor predeterminado: Habilitado.

3.44 CUENTAS: ESTADO DE LA CUENTA DE INVITADO

Descripción: Determina si la cuenta Invitado está habilitada.

Posibles valores: Habilitado / Deshabilitado.

Valor predeterminado: Deshabilitado.

3.45 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.

3.46 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.

3.47 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.

3.48 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.

3.49 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.

3.50 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.

3.51 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.

3.52 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.

3.53 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

3.54 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.

3.55 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.

3.56 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.

3.57 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.

3.58 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.

3.59 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.

3.60 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.

3.61 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.

3.62 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.

3.63 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.

3.64 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.

3.65 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.

3.66 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.

3.67 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.

3.68 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.

3.69 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.

3.70 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.

3.71 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.

3.72 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.

3.73 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

3.74 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.

3.75 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.

3.76 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.

3.77 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.

3.78 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.

3.79 SEGURIDAD DE RED: PERMITIR SOLICITUDES DE AUTENTICACIÓN PKU2U A ESTE EQUIPO PARA USAR IDENTIDADES EN INTERNET.

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

Posibles valores: Habilitado / Deshabilitado.

Valor predeterminado: Deshabilitado.

3.80 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.

3.81 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.

3.82 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.

3.83 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.

3.84 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.

3.85 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.

3.86 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.

3.87 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.

3.88 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

3.89 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

3.90 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.

3.91 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.

3.92 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.

3.93 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.

3.94 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.

Sistemas: Trabajo final

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

Valor predeterminado: Sin definir.

3.95 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.