ES-11 CONFIGURACIÓN SEGURIDAD SERVIDORES WINDOWS

1. Normatividad Relacionada

NO-07 Responsabilidad de Usuarios
NO-11 Administración de Cuentas
NO-13 Comandos Especiales y Administración de Componentes Tecnológicos
NO-14 Administración y Configuración de Parámetros de Seguridad
NO-15 Nombres de Usuario
NO-19 Administración de Accesos a Componentes Tecnológicos
NO-20 Claves de Acceso
NO-40 Software y Hardware Utilizado
ES-03 Contraseñas de Acceso
ES-04 Parámetros de Acceso
ES-05 Registro de Eventos

2. Objetivos

Establecer los parámetros básicos de seguridad que se deben configurar en los servidores con Sistema Operativo Microsoft Windows Server.

3. Componentes Tecnológicos Afectados

Servidores y Equipos con Sistema Operativo Microsoft Windows Server.

4. Descripción

- Parámetros de cuentas del sistema y auditoría:
  - ✓ Tamaño mínimo de contraseña: 10 caracteres
  - ✓ Intervalo mínimo de cambio de contraseña: 0 días
  - ✓ Intervalo máximo de cambio de contraseña: 30 días
  - ✓ Histórico de contraseñas: Mínimo las últimas 8 y máximo las últimas 15.
  - ✓ Tiempo de activación del protector de pantalla por inactividad: 5 minutos
  - ✓ Intentos de acceso fallido antes de bloquear la cuenta de usuario: 3.
  - ✓ Duración del bloqueo por intentos de acceso fallido a la cuenta de usuario: Hasta que el usuario solicite el desbloqueo.
  - ✓ Propiedades del usuario para compartir discos, carpetas o archivos: Deshabilitada

- ✓ Propiedades del usuario para instalar software: Deshabilitada
- ✓ Log de eventos de auditoría: Configurados y ajustados según el estándar ES-05 Registro Eventos

- Parámetros de configuración de seguridad:
  - ✓ Cuenta de invitado: Deshabilitada
  - ✓ Canal de datos: Cifrado cuando sea posible.
  - ✓ Permisos para usuarios anónimos: Ninguno.
  - ✓ Recursos compartidos: Solo para usuarios específicos o autorizados.
  - ✓ Servicios no utilizados: Desactivar o desinstalar.
  - ✓ Sistemas de archivos de usuario: Solo NTFS.
  - ✓ Sistemas de archivos: Cuando se crea o comparte un archivo o carpeta, no se deben dejar los valores por defecto en los permisos de Control Total, Modificación, Ejecución y Escritura.
  - ✓ Sincronización de hora y fecha: Servidor NTP autorizado.
  - ✓ Orden de arranque (boot): Configurar para evitar arranques no autorizados.
  - ✓ Remote Desktop Protocol: Si se utiliza se debe configurar nivel de encripción ALTO.
  - ✓ Software Antimalware: Instalado y Configurado.
  - ✓ Actualizaciones de Windows: Manual, previa verificación del impacto en ambiente de pruebas.
  - ✓ DNS: Debe estar configurado para Active Directory.
  - ✓ Cliente DHCP: Manual.
  - ✓ Firewall de Windows: Habilitado y Configurado.

- Descripciones y Valores de Derechos y Privilegios:

Grupos	Descripción	Valor
Administradores	Grupo global con privilegios de administrador de dominio o administrador local. Por defecto está el grupo Administradores. En los controladores de dominio no existe administrador local.	Este grupo debe contener solamente a los Administradores de Servidores Windows (personal autorizado para ejercer labores de administración de dominio Windows).
Operadores de Copia	Usuarios con privilegios de copia del sistema.	No debe contener ningún usuario.
Operadores de Cuenta	Grupo local en controladores de dominio con privilegios para crear, eliminar y modificar usuarios, grupos globales y grupos locales.	No debe contener ningún usuario.
Usuarios	Usuarios normales del sistema.	No debe contener ningún usuario.
Usuarios Avanzados	Usuarios con alguna capacidad administrativa.	No debe contener ningún usuario.

- ✓ Los privilegios del Grupo Administradores deben ser controlados y gestionados por el Grupo Soporte Informático, que es el responsable de administrar la infraestructura tecnológica informática y deben ser autorizados por el Grupo Seguridad de la Información.

- ✓ Los grupos locales en los controladores de dominio (Domain Controller) deben contener solamente usuarios y grupos autorizados. (Ej: Operadores de Impresión, Operadores de Servidores, Operadores de Cuentas).

- ✓ Los grupos locales en servidores miembros (Member Server) deben contener solamente usuarios autorizados.

- ✓ Los usuarios asignados a grupos privilegiados (Ej: Administradores de Dominio) deben ser mínimos y completamente justificados.

- ✓ Se debe habilitar la opción de fecha de expiración de cuentas de usuario.

- ✓ Se deben analizar periódicamente las cuentas deshabilitadas y determinar si deben ser eliminadas o no.

Derechos	Descripción	Valor
Hacer copias de seguridad de archivos y directorios.	Permite al usuario hacer copias de seguridad de archivos y directorios. Este permiso supera los permisos ya asignados sobre archivos y directorios.	Asignar solamente a Administradores y Operadores o Administradores de Copias de Respaldo y Recuperación.
Cambiar la hora del sistema	Permite cambiar la hora del sistema.	Asignar solamente a los Administradores.
Crear archivo de paginación	Permite la creación de un archivo de paginación	Asignar solamente a los Administradores.
Crear objetos compartidos permanentemente	Permite al usuario crear objetos especiales permanentes como \\Device.	No asignar a ningún usuario. Uso exclusivo para los Administradores.
Forzar apagado desde un sistema remoto	Permite a un usuario apagar el sistema usando una solicitud de red.	Asignar únicamente a los Administradores.
Incrementar cuotas	Permite aumentar la cuota asignada a un proceso	No asignar a ningún usuario.
Aumentar la prioridad de programación	Permite a los usuarios aumentar la prioridad de ejecución de un proceso	Asignar únicamente a los Administradores.
Cargar y descargar controladores	Permite al usuario instalar y remover controladores	Asignar únicamente a los Administradores.
Bloquear páginas en memoria	Permite a un usuario bloquear páginas en memoria para que no puedan ser paginadas al archivo de almacenamiento como Pagefile.sys.	No asignar a ningún usuario.
Acceder al sistema como un proceso “batch”	Permita al usuario acceder al sistema como un proceso “batch”.	No asignar a ningún usuario.
Acceder al sistema como un servicio	Permita al usuario acceder al sistema como un servicio.	No asignar a ningún usuario.

Derechos	Descripción	Valor
Acceder al sistema localmente	Permita al usuario acceder al computador desde el teclado	Para servidores y controladores de dominio asignar a los Administradores solamente.
Administra los registros de auditoría y seguridad	Permite al usuario administrar la auditoría de archivos, directorios y otros objetos. Un usuario con este permiso puede especificar opciones de auditoría para los objetos seleccionados usuarios, grupos y tipos de acceso.	Asignar únicamente a los Administradores.
Modificar los valores de ambiente de “Firmware”	Permite al usuario modificar la RAM no volátil de sistemas que usan este tipo de memoria para almacenar información de configuración.	Asignar únicamente a los Administradores.
Perfil de proceso único	Permite al usuario reunir la información de perfil de un proceso único.	Asignar únicamente a los Administradores.
Perfil de funcionamiento del sistema	Permite al usuario reunir la información de perfil (muestra de funcionamiento) para el sistema completo.	Asignar solamente a los Administradores.
Restaurar archivos y directorios	Permite al usuario restaurar copias de seguridad de archivos y directorios.	Asignar solamente a los Administradores.
Apagado del sistema	Permite a los usuarios apagar servidores con sistema operativo Microsoft Windows Server.	Asignar solamente a los Administradores para servidores y controladores de dominio. Para estaciones de trabajo puede asignarse a todos los usuarios.

Derechos	Descripción	Valor
Tomar propiedad de archivos u otros objetos	Permite al usuario tomar propiedad de archivos, directorios, impresoras y otros objetos del computador. Este permiso sobrepasa los permisos que protegen los objetos.	Asignar solamente a los Administradores.
Acceder al equipo desde la red	Permite o impide al usuario acceder al servidor desde la red.	Asignar solamente a los Administradores, para servidores y controladores de dominio. Para estaciones de trabajo puede asignarse a todos los usuarios.
Añadir estaciones al dominio	Permite al usuario añadir equipos al dominio actual.	Asignar solamente a los Administradores de Dominio.
Atravesar carpetas	Permite al usuario acceder archivos a los que tiene permisos a través de una ruta de directorios en los que no puede tener ningún permiso.	Asignar solamente a los Administradores.
Instalar manejadores de dispositivo	Permite al usuario instalar y desinstalar dispositivos plug and play.	Asignar solamente a los Administradores.
Asignación de roles para virtualización en Microsoft Windows Server	Provee los servicios que pueden ser usados para crear y gestionar máquinas virtuales y sus recursos.	Asignar solamente a los Administradores.