Versión: 01
Vigencia: 25 / Junio / 2021
Documento Controlado

1. OBJETIVO

Gestionar un servicio de directorio activo para centralizar la administración de los recursos de red sobre sistemas Linux compatible con Windows utilizando Active Directory.

2. ALCANCE

Aplica para toda la plataforma de tecnología del directorio activo en los ambientes tales como; productivos, como contingentes.

3. DEFINICIONES

Kernel: es la base fundamental del sistema operativo, es el encargado de toda la comunicación entre el hardware y el software, así como de la administración del mismo.

LDAP: permite delegar con seguridad la lectura y modificación basada en autorizaciones según las necesidades, mediante una lista de control de acceso (ACL).

ACL: Es una lista secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior.

NTP: es un protocolo que permite una precisión de milisegundos en equipos de cómputo ya que obtiene la hora de relojes atómicos.

Root: Usuario administrador en sistemas Linux. Como tal, tiene acceso a los datos de todos los usuarios y a los recursos del ordenar, puede instalar y desinstalar programas, gestionar usuarios y grupos.

DOMINIO DE DIRECTORIO ACTIVO: El directorio activo es el servicio de directorio que permite que las aplicaciones encuentren, utilicen y administren recursos de la Organización.

Versión: 01
Vigencia: 25 / Junio / 2021
Documento Controlado

4. CONDICIONES GENERALES

4. 1. Directivas de contraseñas y cuentas.

Directivas de contraseñas

- ✓ Cambio de contraseña en el primer Login
- ✓ Longitud mínima de la contraseña: 8 caracteres
- ✓ Requerimientos de construcción: Mínimo una mayúscula y dos números.
- ✓ Forzar el historial de contraseñas: 4 contraseñas recordadas
- ✓ Forzar el cambio de contraseña: cada 30 días
- ✓ Historial de No uso de las ultimas 2 contraseñas

Directiva de bloqueo de cuentas

- ✓ Umbral de bloqueos de la cuenta: 5 intentos fallidos
- ✓ Duración del bloqueo de cuenta:5 minutos
- ✓ Restablecer la cuenta de bloqueos después de: 5 minutos
- ✓ Cierre de sesión por inactividad después de 1 Minuto
- ✓ Vencimiento automático de cuenta por inactividad: 3 meses

4. 1.1. UNIDADES ORGANIZATIVAS

Se deben tener presente la creación de una directiva de grupo que abarque todos los servidores y que asegure, al mismo tiempo, que los que residan dentro del servicio de directorio satisfagan los estándares de seguridad de su entorno. Con este diseño, cada servidor recibirá las configuraciones de seguridad a través de directivas de grupo en los tres niveles jerárquicos siguientes:

a) Nivel de Dominio. Para cumplir los requisitos comunes de seguridad, tales como directivas de cuenta y de contraseñas que deben ejecutarse en todos los servidores del dominio.

b) Nivel de Referencia. Para cumplir los requisitos de seguridad específicos del servidor que son comunes a todos los servidores miembros del dominio.

c) Nivel de Rol. Para cumplir los requisitos de seguridad de los roles específicos del servidor. Por ejemplo, los requisitos de seguridad de los servidores de infraestructura son distintos de los de los servidores que ejecutan Internet

4.1.2. SERVICIOS DE ARQUITECTUTA Y RED

Se deben establecer los servicios de Red y arquitectura tales como;

- Servicios de resolución de nombres de dominio (DNS)
- Servicio de sincronización de hora (NTP)
- Servicio de configuración de red (DHCP)
- Autoridad de certificación (CA)
- Servicio de red privada virtual (VPN) con openVPN
- Cortafuegos (Firewall interno)
- Enrutamiento
- Reglas de control de acceso (ACLs)
- Limitación de ancho de banda
- Políticas de Grupo (GPO)
- Sistema de detección de intrusos (IDS/IPS)
- Servicio de Impresión
- Directivas de Grupo y usuarios
- Desactivación de actualizaciones automáticas
- Activación de Security-Enhanced Linux, o SELinux
- Deshabilitar el usuario root, utilizando solo los privilegios Sudoer para la administración del servidor
- Actualizaciones de parches
- Ultima versión liberada del sistema operativo Linux para tener actualizaciones recientes
- Integración de con otros sistemas para el cambio de contraseña
- Realizar Hardening al servidor (Bloqueo de puertos abiertos no necesarios, protocolos seguros, deshabilitar servicios innecesarios en segundo plano, separar partición de discos., entre otros)
- Carpetas compartidas
- Deshabilitar puertos USB

Versión: 01
Vigencia: 25 / Junio / 2021
Documento Controlado

4.1.3. RESPALDO Y RECUPERACION

Directrices para la creación y actualización de respaldos;

- Copias de seguridad periódicas (Medios y Configuración)
- Arquitectura de respaldo para contingencia
- Elaboración y ejecución de pruebas de respaldo
- Implementación de Clouster o replica.

5. RESPONSABILIDADES

Área de Tecnología

Implementar, analizar, planificar y gestionar los parámetros de seguridad para la instalación de los sistemas tecnológicos de IGS.

Gerencia de tecnología

Planificar las actividades de trabajo a realizar para la instalación de seguridad en los sistemas.

Gerencia de tecnología

Ejecutar e instalar las medidas de seguridad en los sistemas.

6. DOCUMENTOS DE REFERENCIA

- Política Seguridad de la Informacion.
- Política de control de acceso
- Política de gestión de usuario

Versión: 01
Vigencia: 25 / Junio / 2021
Documento Controlado

7. HISTORIAL DE CAMBIOS

FECHA	VERSION	NATURALEZA DEL CAMBIO
25-06-2021	1.0	➢ Creación del documento.