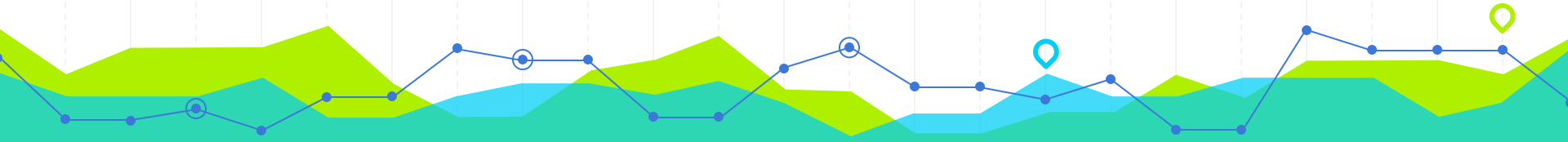


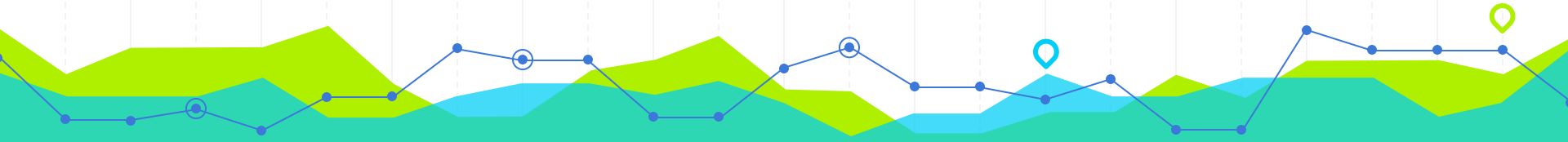
DIRECTIVAS DE SEGURIDAD Y AUDITORÍAS

Implantación de Sistemas Operativos – 1º ASIR

Profesora: Anabel Serradilla

CONTENIDOS

1. LAS DIRECTIVAS DE SEGURIDAD
2. LAS DIRECTIVAS DE GRUPO
3. LAS AUDITORÍAS



LAS DIRECTIVAS DE SEGURIDAD

1. LAS DIRECTIVAS DE SEGURIDAD

Definen el comportamiento del sistema en temas de seguridad.

Pueden ser de tres tipos:

- Directivas de seguridad local
- Directivas de seguridad de dominio
- Directivas de seguridad del controlador de dominio

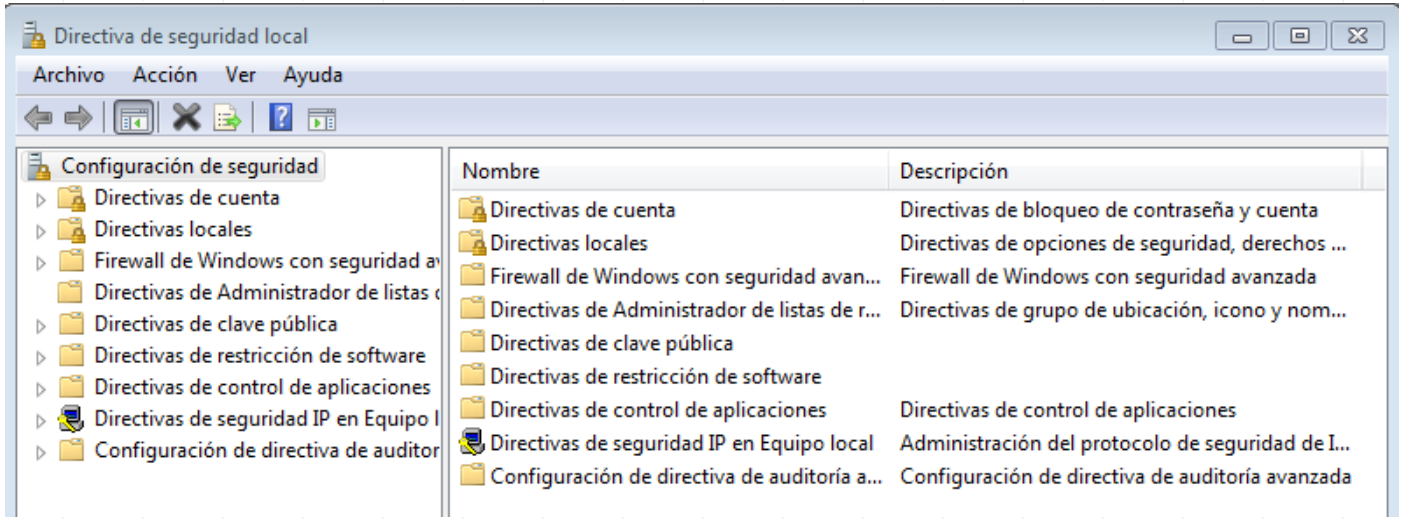
1. LAS DIRECTIVAS DE SEGURIDAD

Directivas de seguridad local

- Permiten configurar la seguridad de un equipo que no es un servidor Windows, o lo es pero no tiene instalado Active Directory.
- Inicio / Herramientas administrativas / Directiva de seguridad local
- secpol.msc

I. LAS DIRECTIVAS DE SEGURIDAD

Directivas de seguridad local



1. LAS DIRECTIVAS DE SEGURIDAD

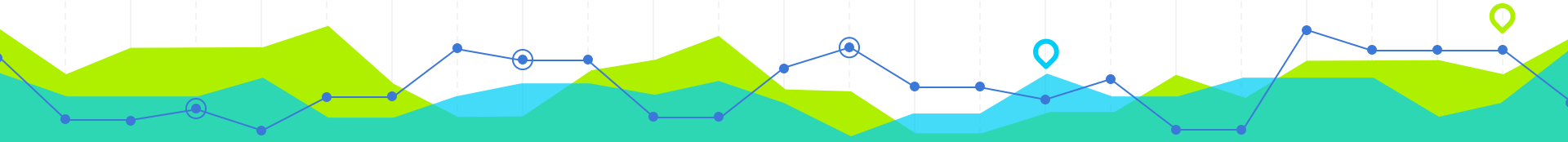
Directivas de seguridad de dominio

- Se utilizan en el caso de servidores de Windows como controladores de dominio.
- Con ellas se puede modificar la configuración de seguridad para todos los equipos miembros del dominio.
- Inicio / Herramientas administrativas / Administración de directivas de grupo
- gpedit.msc

1. LAS DIRECTIVAS DE SEGURIDAD

Directivas de seguridad del controlador del dominio

- Se utilizan también en el caso de servidores de Windows como controladores de dominio.
- A diferencia de las anteriores, solo modifican la configuración de seguridad para los equipos que sean controladores de dominio.
- Inicio / Herramientas administrativas / Administración de directivas de grupo
- gpedit.msc



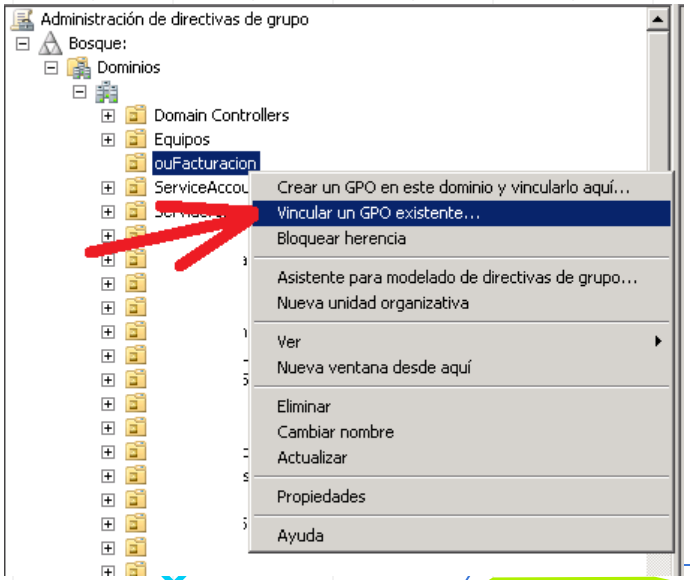
LAS DIRECTIVAS DE GRUPO 2

2. LAS DIRECTIVAS DE GRUPO

Las directivas de grupo (GPO) influyen en las cuentas de usuario, de grupo y de equipo.

Se pueden aplicar a sitios,

dominios o unidades organizativas.



2. LAS DIRECTIVAS DE GRUPO

Se aplican en el siguiente orden:

1. La directiva de equipo local
2. La directiva de usuario local
3. La directiva de grupo del sitio
4. La directiva de grupo del dominio
5. La directiva de grupo de la unidad organizativa
6. La directiva de grupo del controlador de dominio

2. LAS DIRECTIVAS DE GRUPO

Una directiva de grupo está constituida, entre otros, por los siguientes elementos:

- Configuración del equipo: se aplican cuando se inicia el equipo, independientemente del usuario que lo haga.

- Configuración de usuario: se aplica cuando un usuario inicia una sesión independientemente del equipo en el que lo haga.

2. LAS DIRECTIVAS DE GRUPO

Windows Server incorpora dos directivas de grupo por defecto (aparecen por defecto en el nodo del dominio). Ambas afectan tanto a la configuración de equipo como de usuario:

- Default Domain Policy: se aplica a todos los equipos del dominio
- Default Controller Domain Policy: se aplica a todos los equipos que sean controladores de dominio

2. LAS DIRECTIVAS DE GRUPO

Trabajar con directivas:

- Crear una nueva directiva de grupo
- Establecer la configuración que se quiera
- Vincular la directiva con un elemento del dominio (sitio, dominio, UO, …)
- Configurar el orden de aplicación

2. LAS DIRECTIVAS DE GRUPO

Trabajar con directivas:

- Configurar si se quiere impedir que otras directivas anulen la configuración de dicha directiva (Exigido)
- Configurar si se quiere impedir la herencia de directivas de dominios o unidades organizativas de nivel superior (Bloquear herencia)
- Editar las directivas que sea necesario

2. LAS DIRECTIVAS DE GRUPO

- Ficha Ámbito: dónde se aplica la directiva
- Ficha Detalles: información detallada y deshabilitación o no de la configuración de equipo, de usuario o de ambas
- Ficha Configuración: resumen de sus características
- Ficha Delegación: usuarios y grupos con permisos sobre la directiva

2. LAS DIRECTIVAS DE GRUPO

Comandos útiles con directivas

- gpupdate: se utiliza para forzar la actualización de la configuración de las directivas de grupo. Aplica solo las directivas cambiadas
- gpupdate /force: Vuelve a aplicar tanto las directivas nuevas como las antiguas

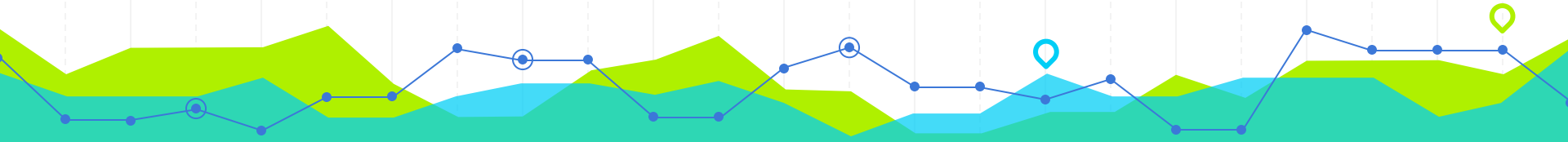
2. LAS DIRECTIVAS DE GRUPO

Comandos útiles con directivas

- gpresult: se utiliza para enumerar las políticas de grupo que se aplican actualmente al usuario o la computadora en cuestión

  Ejemplos: gpresult /s mi_equipo /user gandalf

  gpresult /user LOTR\frodo



LAS AUDITORÍAS 3

3. LAS AUDITORÍAS

Las auditorías permiten supervisar los sucesos relacionados con la seguridad del equipo.

Con cada uno de los sucesos auditados se generan registros que pueden ser consultados en el Visor de eventos.

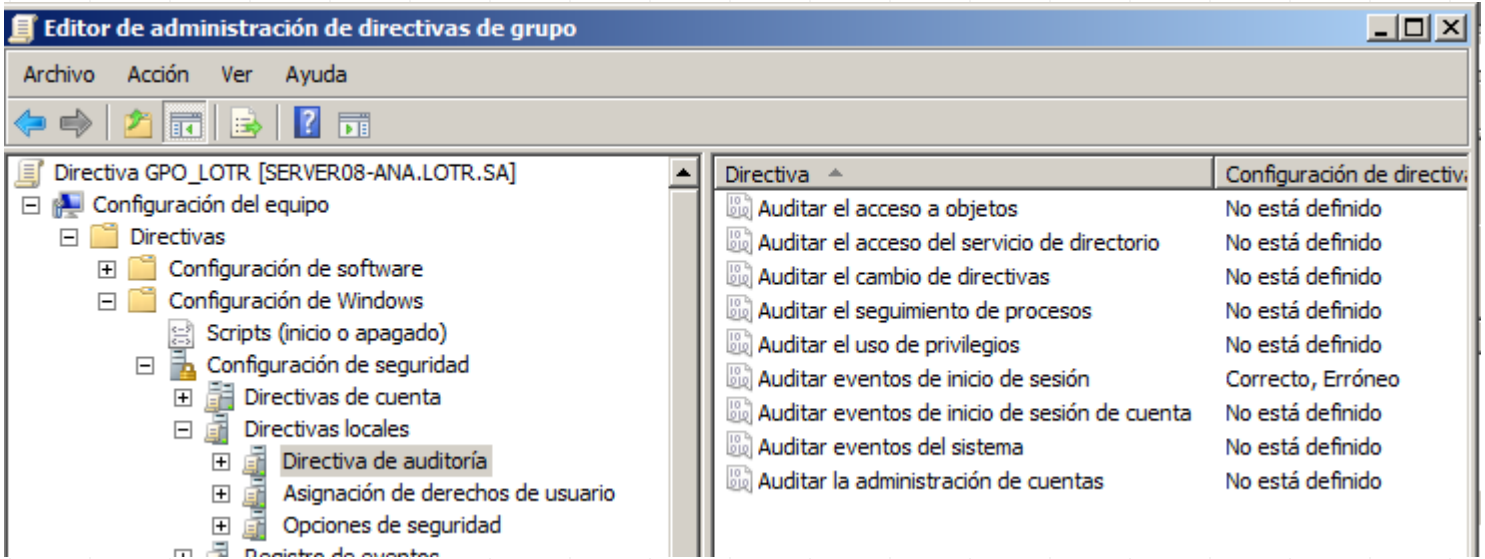
Al instalar Windows Server ya se activan varias categorías de auditoría

3. LAS AUDITORÍAS

Los tipos de sucesos más comunes que se pueden auditar son:

- Acceso a objetos, como archivos y carpetas
- Acceso al servicio de directorio
- Cambios de directivas
- Administración de cuentas de usuarios y grupos
- Inicio y finalización de sesiones de usuarios

3. LAS AUDITORÍAS



3. LAS AUDITORÍAS

Especificar las categorías de los sucesos que se quiere auditar

Definir el tamaño y el comportamiento del registro de seguridad

Si se audita el acceso a directorios u objetos, habrá que indicar sobre qué objetos se aplica

3. LAS AUDITORÍAS

Cada cierto tiempo conviene ver los sucesos que se han ido generando en el registro para ver los problemas que han podido surgir,
los intentos de entrada erróneos, …