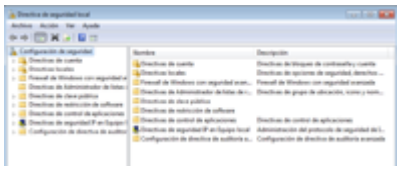
3.2.- Directivas de seguridad local y Directivas de grupo local.

Siempre desde una cuenta con privilegios de administrador Windows nos proporciona la posibilidad de gestionar de forma centralizada la configuración de la seguridad de nuestro sistema, a través de las **Directivas de seguridad local** y las **Directivas de grupo local**. Ambas opciones cuentan con consolas para facilitar la configuración de las directivas. Una directiva es un conjunto de reglas de seguridad que se pueden implementar en un sistema.

Con las **Directivas de seguridad local** veremos cómo aplicar distintas restricciones de seguridad sobre las cuentas de usuario y contraseñas. Por otro lado, las **Directivas de grupo local** nos permiten configurar equipos de forma local o remota, instalar o eliminar aplicaciones, restringir los derechos de los usuarios, entre otras acciones.

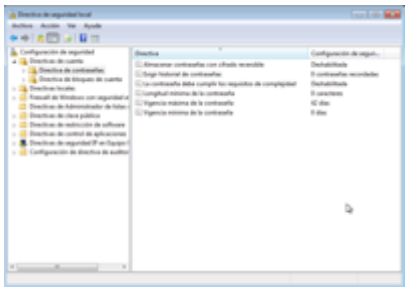
3.2.1.- Directivas de seguridad local.



Windows es un sistema operativo muy configurable por parte del usuario. Aunque estas configuraciones suelen estar algo ocultas para que no sean accesibles por los usuarios normales, y sólo pueden ser modificadas desde las consolas del sistema.

En concreto, desde la consola de Directiva de Seguridad Local, podemos gestionar varios aspectos sobre las cuentas y contraseñas. (Para acceder a la consola Directivas de Seguridad haremos: **Inicio - Ejecutar -** **SecPol.msc**

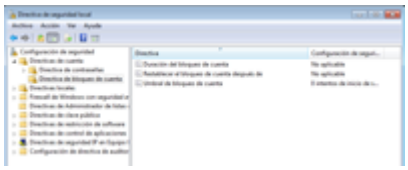
Una vez dentro podemos acceder a: **Configuración de Seguridad - Directivas de Cuenta - Directivas de Contraseñas**) o también se puede acceder a través de **Inicio - Panel de Control - Sistema y Seguridad - Herramientas administrativas - Directiva de seguridad local.**



Las **configuraciones** más útiles que podemos gestionar desde aquí son:

Forzar el historial de contraseñas. Impide que un usuario cambie su contraseña por una contraseña que haya usado anteriormente, el valor numérico indica cuantas contraseñas recordará Windows.
Las contraseñas deben cumplir los requerimientos de complejidad. Obliga a que las contraseñas deban cumplir ciertos requerimientos, como son mezclar letras mayúsculas, minúsculas y números, no parecerse al nombre de la cuenta, etc.
Longitud minina de la contraseña. Indica cuantos caracteres debe tener la contraseña como mínimo, un valor cero en este campo indica que pueden dejarse las contraseñas en blanco.
Vigencia máxima de la contraseña. Las contraseñas de los usuarios caducan y dejan de ser validas después del número de días indicados en esta configuración, y el sistema obligará al usuario a cambiarlas. (Recordemos que al crear una cuenta de usuario podemos indicar que la contraseña nunca caduca para esa cuenta).
Vigencia minina de la contraseña. Indica cuanto tiempo debe transcurrir desde que un usuario se cambia la contraseña, hasta que puede volver a cambiarla. Esta configuración de seguridad local se usa para evitar que un usuario cambie continuamente su contraseña a fin de volver a quedarse con su contraseña original caducada.

Bloqueo de las cuentas:



Desde **secpol.msc** también podemos gestionar un comportamiento de las cuentas de usuario relacionado con las contraseñas, y es el de bloquear las cuentas si se intenta acceder al sistema con las mismas pero usando contraseñas incorrectas. Esta configuración la encontramos en (**Inicio - Ejecutar -** **SecPol.msc** **- Configuración de Seguridad - Directivas de Cuenta - Directivas de Bloqueo de Cuentas**)

Aquí podemos **configurar**:

Duración del bloqueo de cuenta. (Durante cuanto tiempo permanecerá una cuenta bloqueada si se supera el umbral de bloqueo. Un valor cero indica que la cuenta se bloqueará hasta que un Administrador la desbloquee).
Restablecer la cuenta de bloqueos después de. (Indica cada cuanto tiempo se pone el contador de intentos erróneos a cero).
Umbral de bloqueo de la cuenta. (Indica cuantos intentos erróneos se permiten antes de bloquear la cuenta).

3.2.2. Directivas de grupo local.

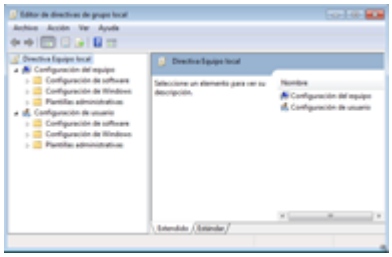
Las directivas de grupo es una característica de Windows XP, familia de sistemas operativos. Directiva de grupo es un conjunto de reglas que controlan el medio ambiente de trabajo de cuentas de usuario y cuentas de equipo. Las políticas de grupo son una herramienta muy poderosa que permite a los administradores configurar equipos de forma local o remota, instalando aplicaciones, restringiendo los derechos de los usuarios, eliminando aplicaciones, instalando y ejecutando scripts, y redirigiendo carpetas del sistema a red o viceversa. Pero también tienen utilidad las políticas de grupo en entornos pequeños, incluso en una sola maquina.

Usando las políticas de grupo en una maquina corriendo Windows, podemos:

Modificar políticas que se encuentran en el registro del sistema. El registro del sistema es una gran base de datos en la que se configuran cientos de comportamientos de Windows 7. Desde las políticas de grupo podemos acceder a estas características y modificarlas, de una forma mucho más simple que mediante la edición pura del registro.
Asignar scripts que se ejecutaran automáticamente cuando el sistema se encienda, se apague, un usuario inicie sesión o cierre sesión.
Especificar opciones especiales de seguridad.

Si estamos trabajando bajo un dominio (con un servidor en la red administrando dicho dominio) las políticas de grupo cobran mayor protagonismo. En un ambiente de grupo de trabajo, las políticas de grupo de cada máquina controlan los aspectos únicamente de dicha maquina, y en algunos casos es imposible sacarles el rendimiento esperado.

La consola desde donde podemos gestionar las directivas de grupo es el **gpedit.msc**. **(Inicio - Ejecutar - gpedit.msc)**.



Para poder trabajar con el **gpedit.msc** necesitamos estar usando una cuenta de usuario que pertenezca al grupo Administradores. Esta consola es muy configurable, permitiéndonos añadir y quitar opciones según deseemos. De momento, vamos a trabajar con las opciones que aparecen por defecto.

Si nuestro equipo está unido a un dominio, podemos configurar directivas del dominio completo, que afectaran a varias maquinas. Sin embargo, nos vamos a centrar aquí en las directivas locales, ya que no estamos trabajando en un dominio, de momento.

Principalmente veremos que dentro de las **directivas de grupo locales** tenemos dos **opciones**: **Configuración del equipo** y **Configuración del usuario**. En el caso de estar trabajando en grupo de trabajo es prácticamente indistinto trabajar con una opción u otra.

Para aprender más de una directiva en concreto, simplemente tendremos que seleccionarla con el ratón, y veremos una descripción detallada de dicha directiva en el panel central.

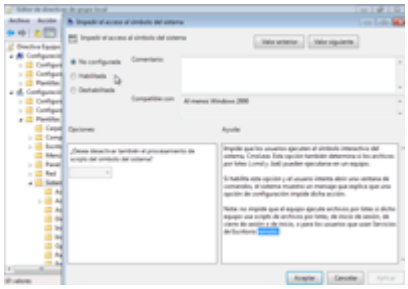
Algunas directivas aparecen tanto en la configuración del equipo como en la configuración del usuario. En caso de conflicto, la configuración del equipo siempre tiene preferencia.

Para modificar el estado o configuración de una directiva, simplemente tenemos que realizar doble click sobre dicha directiva para que nos aparezca el cuadro de dialogo que nos permite modificar dicha directiva. En dicho cuadro de dialogo nos mostrará una explicación de la funcionalidad de dicha directiva.

Respecto a la configuración, veremos que podemos:

No configurar la directiva, con lo que se comportará según el criterio por defecto para dicha directiva.
Habilitarla, con lo que la pondremos en marcha en el sistema.
Deshabilitarla, con lo que impediremos que se ponga en marcha dicha directiva.

Algunas directivas especiales permiten especificar otras informaciones.



Se recomienda leer cuidadosamente la explicación de cada directiva para entender sus efectos sobre el sistema y decidir habilitarla o no.

Probad a deshabilitar la directiva que hemos tomado como ejemplo (**gpedit.msc** - Configuración de Usuario - Plantillas Administrativas - Sistema - Impedir el acceso al símbolo del sistema) e intentad ejecutar una ventana de símbolo de comandos (**cmd.exe**)

Vemos como desde las directivas de grupo podemos modificar el comportamiento de Windows, dándonos una gran potencia en la administración del equipo.

Ejercicio:
Habilita las directivas de contraseña correspondientes para que el sistema
- Guarde registro de las 4 últimas contraseñas de usuario,
- Deben ser complejas,
- Ttener una vigencia máxima de 1 mes,
- Longitud mínima de 10 caracteres
- Permitir hasta 3 equivocaciones del usuario al iniciar sesión.
- Deniega el inicio de sesión local al usuario que creamos para escritorio remoto.
- Cambia el nombre de las cuentas de invitado y administradore desde aquí, y habilita/deshabilita las mismas.