educación IT
CODE YOUR FUTURE

Introducción a la Ciberseguridad

Módulo 4

Directiva de Seguridad Local

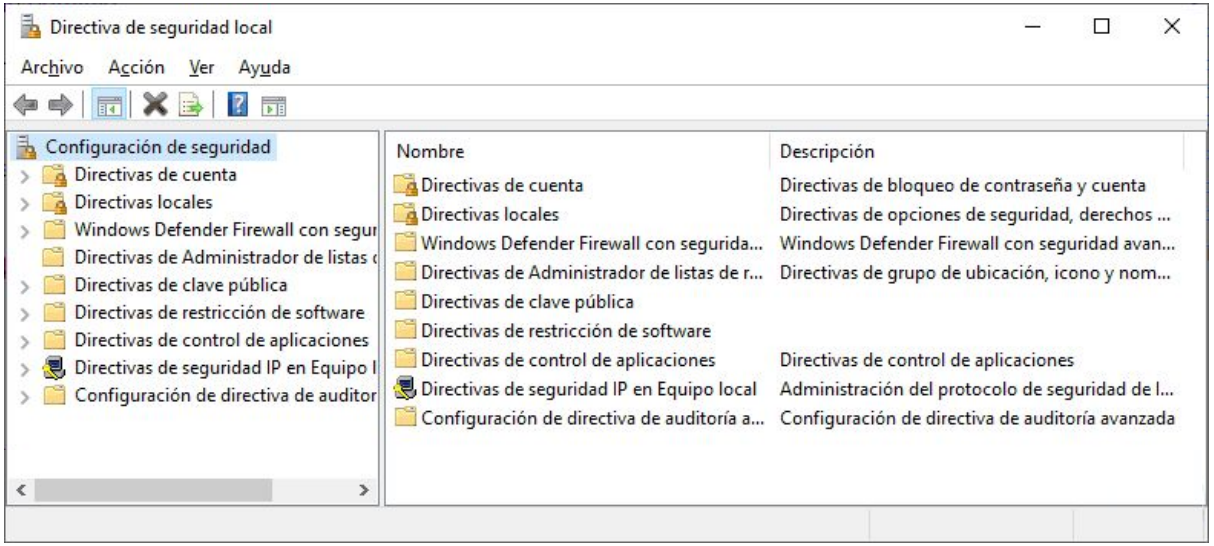
Directiva de Seguridad Local

La **directiva de seguridad local** nos permite definir muchísimos aspectos del sistema relacionados con la seguridad. Es muy similar al concepto de directivas de grupo *(Group Policies)* que se utiliza en *Active Directory*, con la diferencia de que **esta es únicamente local y no se aplica a través de la red.**

Para abrir la herramienta de administración de la directiva de seguridad local, podemos ejecutar el siguiente comando:

```
secpol.msc
```

A continuación podemos ver una captura de pantalla de la interfaz:



Una vez dentro de la interfaz gráfica, veremos que existen **varias categorías** para los distintos aspectos de c**onfiguración del sistema.**

A continuación, haremos un repaso por los parámetros más significativos:

Account Policies

Permite definir parámetros acerca de las cuentas de usuario local.

Password Policy

- ***Enforce Password History***

  Permite definir un historial de contraseñas para que los usuarios no puedan repetir las últimas N cantidad de contraseñas al realizar el cambio de la misma.

- ***Maximum Password Age***

  Permite definir cuál es el tiempo máximo de vida de una contraseña. Transcurrido este tiempo, el usuario se verá obligado a modificar su contraseña.

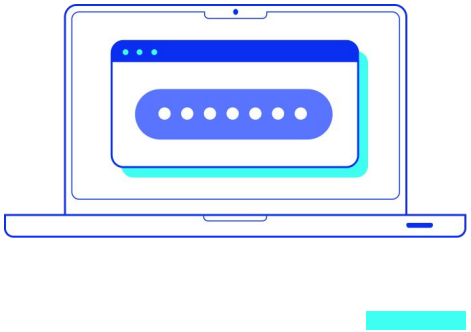
- ***Minimum Password Length***

  Permite definir cuál es la cantidad mínima de caracteres con los que debe contar una contraseña.

- ***Password Must Meet Complexity Requirements***

  Si está habilitada, obliga a que las contraseñas cumplan con los siguientes requerimientos:

  - No contener el nombre de usuario o parte del nombre completo.
  - Tener, como mínimo, seis caracteres de longitud.
  - Tener, por lo menos, tres de las siguientes categorías de caracteres:
    - Mayúsculas (A – Z).
    - Minúsculas (a – z).
    - Números (0 al 9).
    - Caracteres no alfanuméricos (ejemplos: , !, $, #, %).



Account Lockout Policy

- ***Account Lockout Threshold:*** después de qué cantidad de intentos de acceso fallidos se va a bloquear una cuenta de usuario.
- ***Account Lockout Duration:*** cuánto tiempo debe transcurrir para que una cuenta se desbloquee automáticamente.

Local Policies

User Rights Assignment

- ***Act as part of the operating system:*** las cuentas de usuario listadas aquí podrán ejecutar procesos en nombre de cualquier usuario del sistema sin que se les requiera autenticación.

  > **Nota:** esto representa un riesgo de seguridad y no se recomienda.

- ***Allow logon through Remote Desktop Services:*** las cuentas de usuario listadas aquí podrán acceder al equipo a través de RDP *(Remote Desktop Protocol).*

- ***Load and unload device drivers:*** los usuarios listados aquí podrán cargar y descargar controladores de dispositivos y otro tipo de códigos en el núcleo.

  > **Nota:** no aplica para los dispositivos Plug & Play y no se recomienda modificar esta política por motivos de seguridad.

- ***Take ownership of files or other objects:*** estos usuarios podrán modificar quién es el dueño de archivos, directorios y otros objetos.

  > **Nota:** no se recomienda modificar esta política.

Security Options

- ***Accounts: Administrator account status:*** por defecto, la cuenta de administrador local se encuentra deshabilitada en Windows 7. Modificando esto, podemos habilitarla.

  > **Nota:** esto no se recomienda.

- ***Accounts: Guest account status:*** por defecto, la cuenta de invitado se encuentra deshabilitada en Windows 7. Modificando esto, podemos habilitarla.

  > **Nota:** esto no se recomienda.

- ***Interactive Logon: Display user information when the session is locked:*** define si se van a mostrar o no los datos del usuario que se encuentra logueado cuando la sesión está bloqueada.

  > **Nota:** es recomendable definir esta política en “No mostrar información del usuario”.

- ***Interactive Logon: Do not display last user name:*** define si se va a mostrar cuál fue la última cuenta en acceder al sistema.

  > **Nota:** es recomendable habilitar esta política, para no mostrar el nombre del último usuario que accedió al sistema.

- ***Interactive Logon: Do not require CTRL+ALT+DEL:*** define si los usuarios están obligados a utilizar la combinación de teclas CTRL+ALT+DEL antes de poder iniciar sesión en el equipo.

  > **Nota:** se recomienda deshabilitar esta política para obligar a los usuarios a utilizar esta combinación, lo que puede prevenir cierto tipo de ataques.

- ***Network Access: Do not allow anonymous enumeration of SAM accounts:*** si está habilitada, no permite que se puedan conocer los nombres de usuario válidos a través de conexiones anónimas.

  > **Nota:** es recomendable habilitar esta política.

- ***Network Security: Do not store LAN Manager Hash value on next password change:*** hace que no se almacene el *hash* LM de la contraseña de los usuarios a partir del próximo cambio de contraseña.

  > **Nota:** como los hashes LM han demostrado ser muy débiles, es recomendable habilitar esta política.

¡Sigamos trabajando!