unir
LA UNIVERSIDAD DE INTERNET

FORMACIÓN PROFESIONAL

MP0483.
Sistemas informáticos

UF6. Gestión de recursos en una red

6.2. Directivas de seguridad

Índice

Objetivos

Para avanzar un poco más en el conocimiento de cómo gestionar la seguridad de nuestro equipo, vamos a conocer qué son las directivas de seguridad y cómo utilizarlas, al menos de forma básica, para llevar un control sobre los componentes del sistema operativo, los recursos de la red, y el entorno de trabajo de los usuarios.

En esta unidad perseguimos los siguientes objetivos:

1. Saber qué son las directivas de seguridad y para qué que sirven.
2. Conocer los principales tipos de directivas, así como su ámbito de aplicación.
3. Aprender a implementar algunos de los principales mecanismos basados en directivas y relacionados con la seguridad del sistema.

Qué son las directivas de grupo

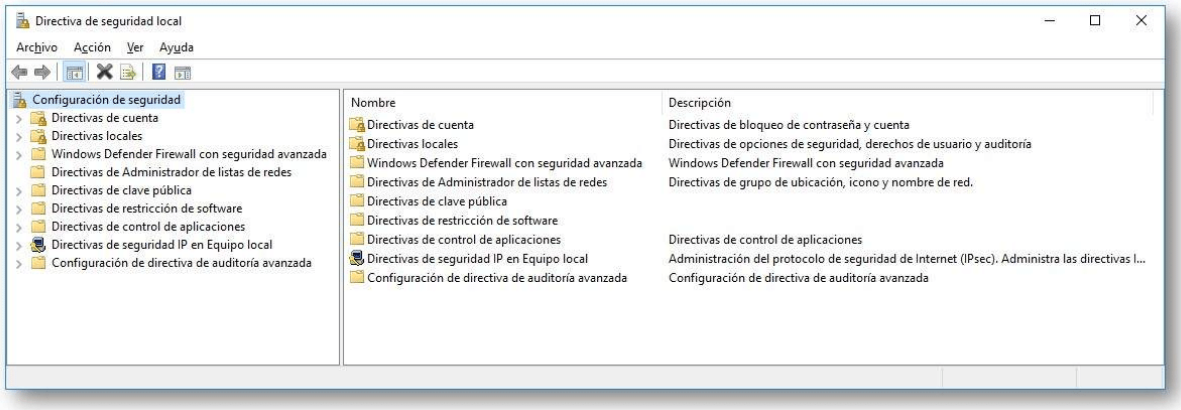
Las directivas de grupo son herramientas formadas por reglas y parámetros de control sobre los privilegios y permisos de los usuarios.

Las directivas se utilizan también para definir configuraciones particulares y opciones de inicio y final de sesión y, por supuesto, opciones de seguridad.

Entre otras cosas, estas directivas pueden proporcionar:

- Un **control sobre los componentes** del sistema operativo, los recursos de la red, y el entorno de trabajo de los usuarios.
- Programar el **bloqueo de cuentas** de usuario, permisos de acceso, perfiles de seguridad, etc.

Según el sistema, la forma de aplicar las directivas puede variar. Por ejemplo, en el caso de Windows las directivas se pueden aplicar a sitios, dominios, unidades organizativas... y disponemos de una **"Consola de administración de directivas de grupo" (GPMC)**. Si el equipo no está en una red y no pertenece a un dominio, entonces las directivas a aplicar serán locales, y se guardarán en el propio equipo.



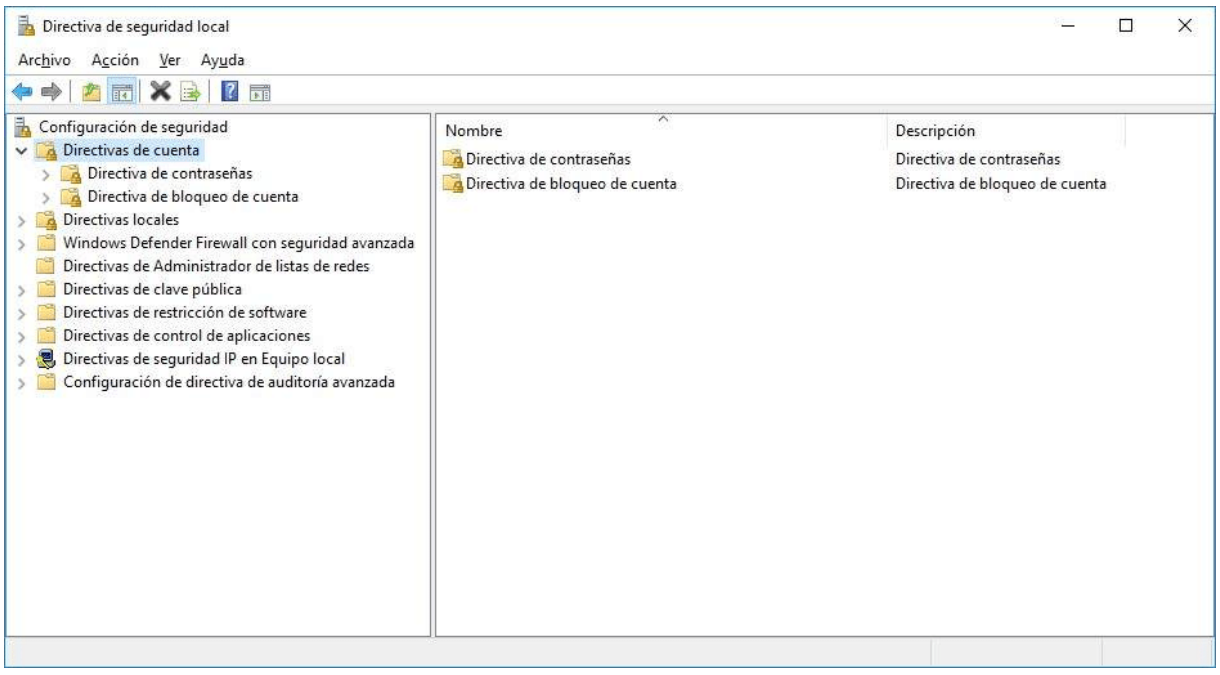
Directivas locales en Windows 10.

Algunos tipos de directivas

Dentro de las directivas de seguridad, y antes de entrar a describirlas, podemos hacer una primera división en:

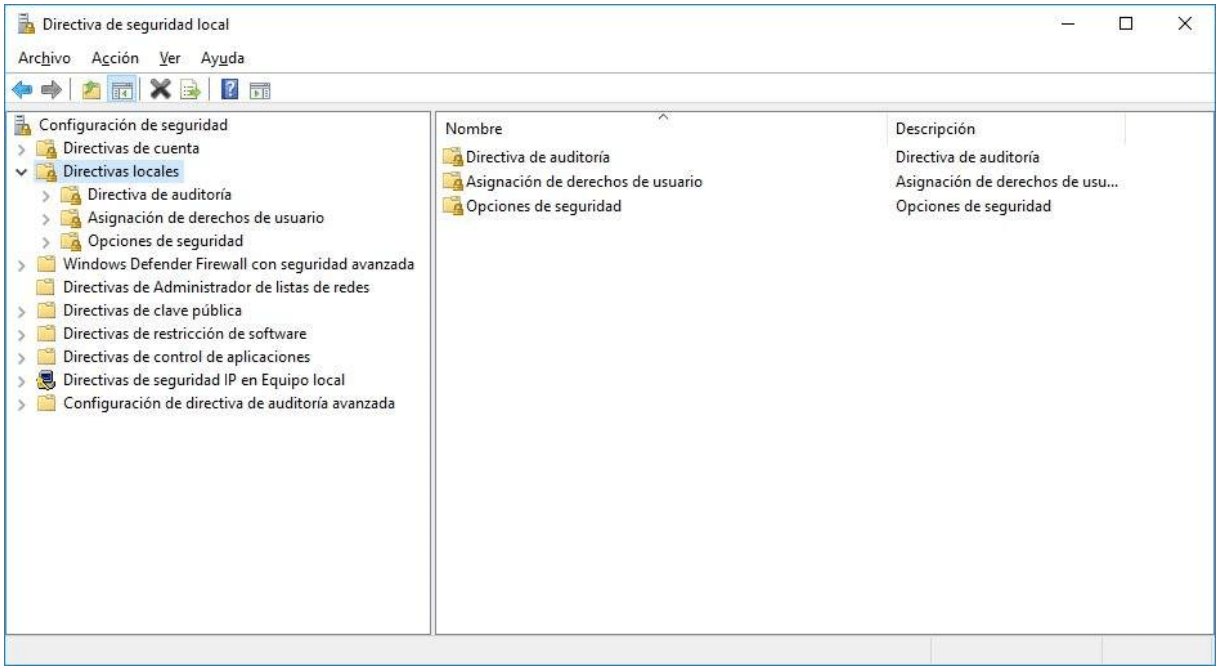
Directivas de cuentas

- **Directiva de contraseña:** restricciones relacionadas con las contraseñas de la cuenta.
- **Directiva de bloqueo de cuenta:** comportamiento (duraciones) relacionado con el bloqueo de la cuenta.



Directivas locales

- **Directivas de auditoría:** parámetros de monitorización del sistema y registro de eventos.
- **Asignación de derechos al usuario:** definiendo lo que el usuario puede o no puede hacer (p. ej. iniciar sesión en red).
- **Opciones de seguridad:** parámetros relacionados con la seguridad y el comportamiento ante eventos peligrosos.



Ámbito de las directivas

Las directivas de grupo pueden aplicarse tanto a la configuración relacionada con la cuenta de usuario, como al propio equipo.

Debes tener en cuenta que una misma directiva puede existir tanto para el equipo como para el usuario con los parámetros correspondientes.

Una **directiva de grupo** puede a su vez referirse a:

- La instalación y configuración del software.
- La configuración de los parámetros del sistema operativo.

Las aplicación de directivas permite realizar una gestión muy potente de los recursos de la organización, pero el elevado número de opciones disponibles, la posibilidad de interacción entre distintas directivas, las opciones de herencia, etc., pueden hacer muy compleja la configuración del sistema.

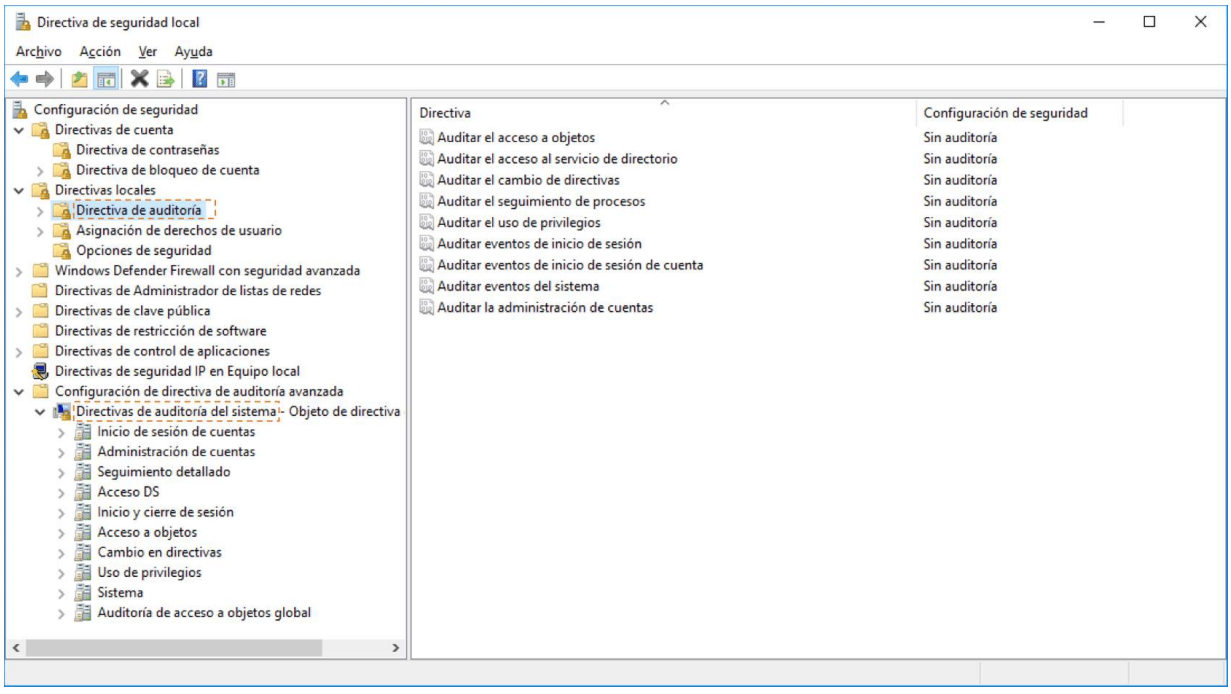
El administrador deberá estudiar bien los requisitos de las operaciones y el funcionamiento de la organización, **planificar y diseñar cuidadosamente la política de directivas** a implementar y, por supuesto, comprobar que la solución adoptada cumple con la funcionalidad deseada.

Además, según el sistema sobre el que estemos trabajando, pueden existir directivas ya predefinidas (**directivas por defecto**), que seguramente podremos modificar o bien crear otras nuevas.

Directivas de auditoría

Podemos configurar el almacenamiento y auditar diferentes tipos de eventos, como por ejemplo:

- **Eventos de inicio de sesión:** cada conexión y desconexión de un usuario o un equipo.
- **Acciones de administración:** la propia administración de una cuenta en un equipo genera un evento que permite luego saber quién ha realizado las acciones (creación, modificación o eliminación de usuarios, etc.).
- **Acceso a un determinado servicio u objeto/recurso:** por ejemplo, podemos auditar el acceso de un usuario a un determinado objeto, que a su vez tendrá asociada una lista de control de acceso de sistema (ACL) que puede tener definidas qué acciones hay que registrar y cuáles no.



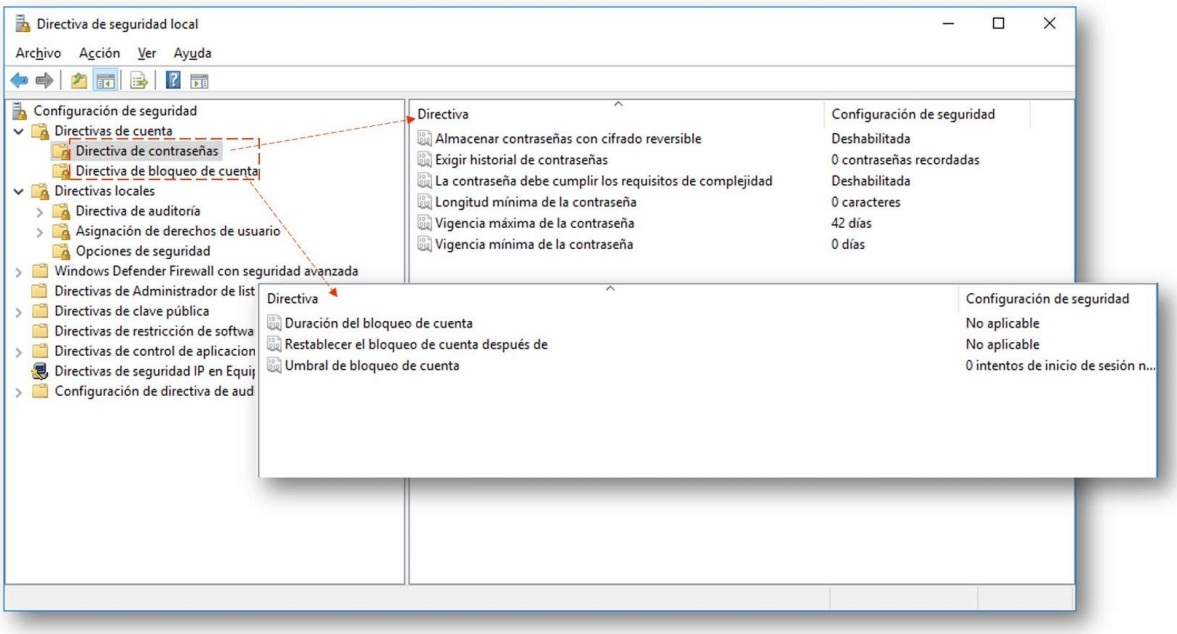
Las directivas de auditoría nos permitirán almacenar en un **registro de eventos** las acciones realizadas por los usuarios (guardando por supuesto la identidad del usuario que la ha realizado y el tipo de acción), y saber si una determinada acción ha tenido éxito o no.

Directivas de seguridad

Las directivas de seguridad contienen **parámetros relativos a la política de contraseñas y bloqueo de cuentas**.

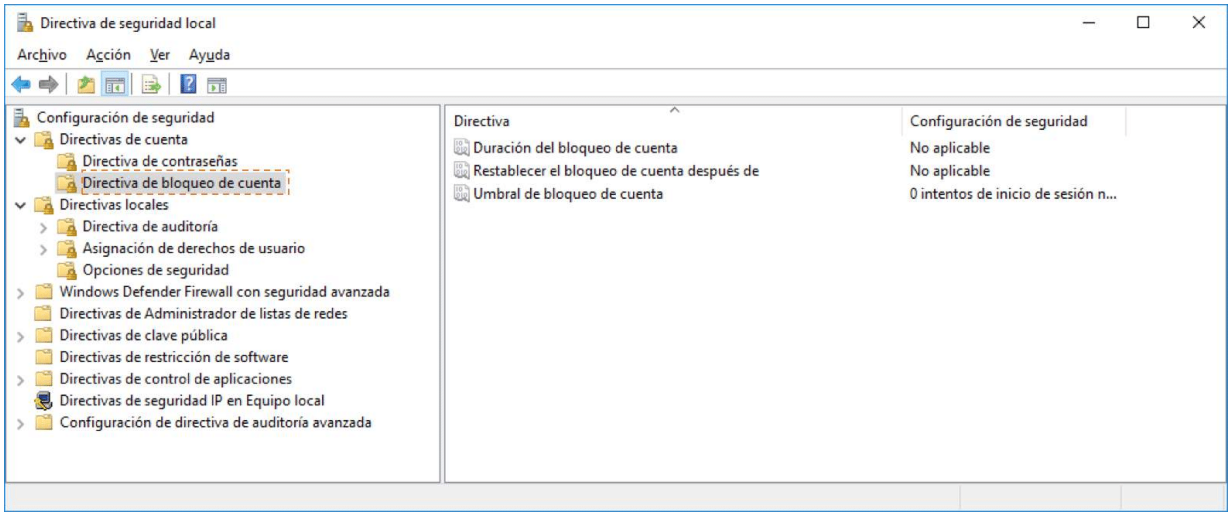
Algunas de las opciones que podemos controlar a través de las **directivas de contraseñas** pueden ser:

- **Exigir historial de contraseñas:** cuántas nuevas se exigen antes de poder repetir una contraseña usada.
- **Duración máxima:** tiempo hasta que el sistema obliga a cambiarla.
- **Vigencia mínima de contraseña:** tiempo que ha de pasar antes de permitir volver a cambiarla.
- **Longitud mínima de contraseña:** número mínimo de caracteres de la clave.
- **Requisitos de complejidad para la contraseña:** tipos de caracteres especiales que debe contener, etc.
- **Cifrado reversible al almacenar las contraseñas:** para permitir que algunas aplicaciones puedan utilizarla. No se recomienda esta opción a no ser que sea absolutamente necesaria.



A su vez, para las **directivas de bloqueo de cuentas**, los parámetros a configurar podrían ser, por ejemplo:

- **Duración del bloqueo de la cuenta:** definimos el tiempo en minutos que estará bloqueada la cuenta (si se produce el bloqueo).
- **Restablecer recuentos de bloqueo de cuenta atrás:** especifica el tiempo (en minutos) tras el cual el contador de bloqueo (p. ej. intentos fallidos) se vuelve a poner a cero.
- **Umbral de bloqueo de cuenta:** aquí se configura el número de intentos erróneos que se permiten en el inicio de sesión, tras los cuales se bloquea la cuenta.



Objetos de directiva

En algunos sistemas se habla de "objetos de directiva", en Windows se conocen como "objetos de directiva de grupo – GPO" y son elementos que contienen configuraciones de directiva. Un GPO es como si fuera un **"*documento*" que contiene la información de la directiva** y la aplica a los equipos y usuarios sobre los que se asigna.

No es nuestro objetivo entrar al detalle de configuración de todos los parámetros. Recuerda que, tanto estos como la forma en la que se configura la directiva, puede variar de un sistema operativo a otro, o tener varias opciones dentro del mismo sistema.

Plantillas de seguridad

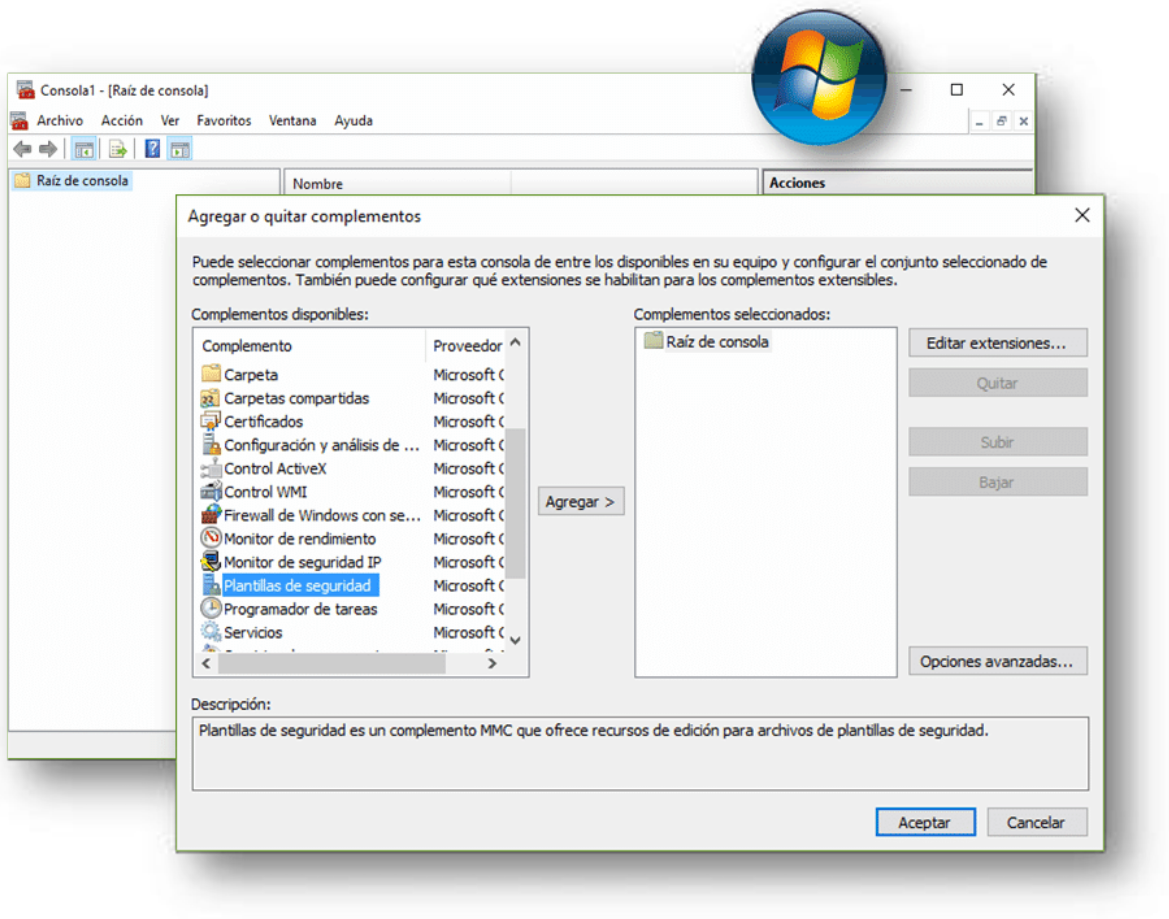
Una **plantilla de seguridad** (o administrativa) es un archivo que contiene la configuración de las políticas y directivas a emplear.

Una **plantilla de seguridad** contiene la configuración de las políticas y directivas a emplear. **Puede ser importado en una directiva de grupo**, de forma que usándolo como modelo podemos generalizar la política de directivas de seguridad en varios sistemas de la organización.

En ese archivo, que se puede agregar, modificar o eliminar en función de las necesidades que surjan, se configurarán todos los parámetros que deben formar parte de la directiva sobre la que vayamos a aplicar la plantilla.

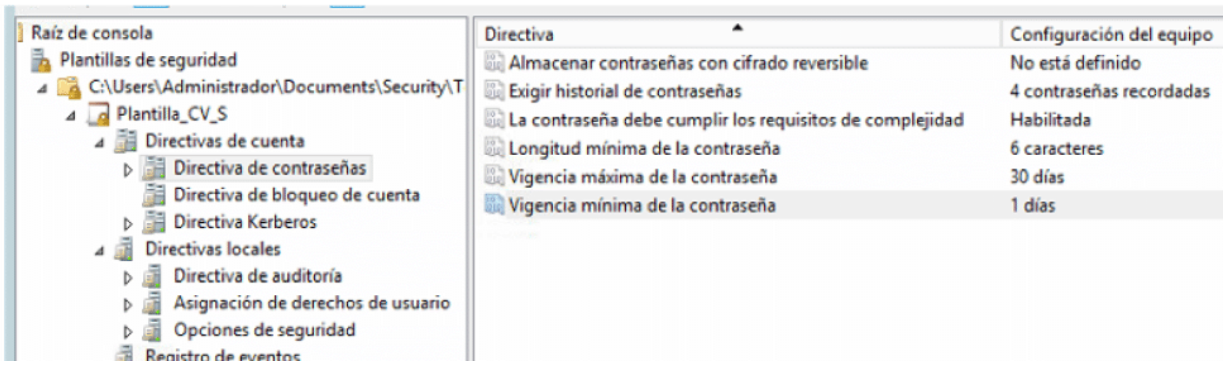
Se puede **crear el archivo plantilla en sistemas Windows a través de una consola de gestión**. Para abrirla teclearemos "**mmc**" en el cuadro de diálogo de "Ejecutar" (tecla Windows+R) o en una consola de comandos normal. Una vez creado y seleccionado el archivo, podremos configurar las directivas de contraseñas (salen en el menú), la directiva de bloqueo de cuenta y las opciones de seguridad en las directivas locales.

Windows nos permite realizar un análisis de seguridad para saber si existen directivas presentes que no coinciden con la configuración de la plantilla y, en ese caso, aplicar la plantilla creada, sustituyéndolas.



Creación de una plantilla de seguridad en una ventana de consola.

En general, podemos tener plantillas para administrar una gran variedad de opciones en nuestros sistemas y, como hemos dicho, siempre debemos estudiar qué posibilidades nos ofrece un sistema concreto, pues aunque puedan ser parecidas, seguramente no serán iguales en Windows, Unix,...



Por ejemplo, podemos tener plantillas para:

Configuración del equipo

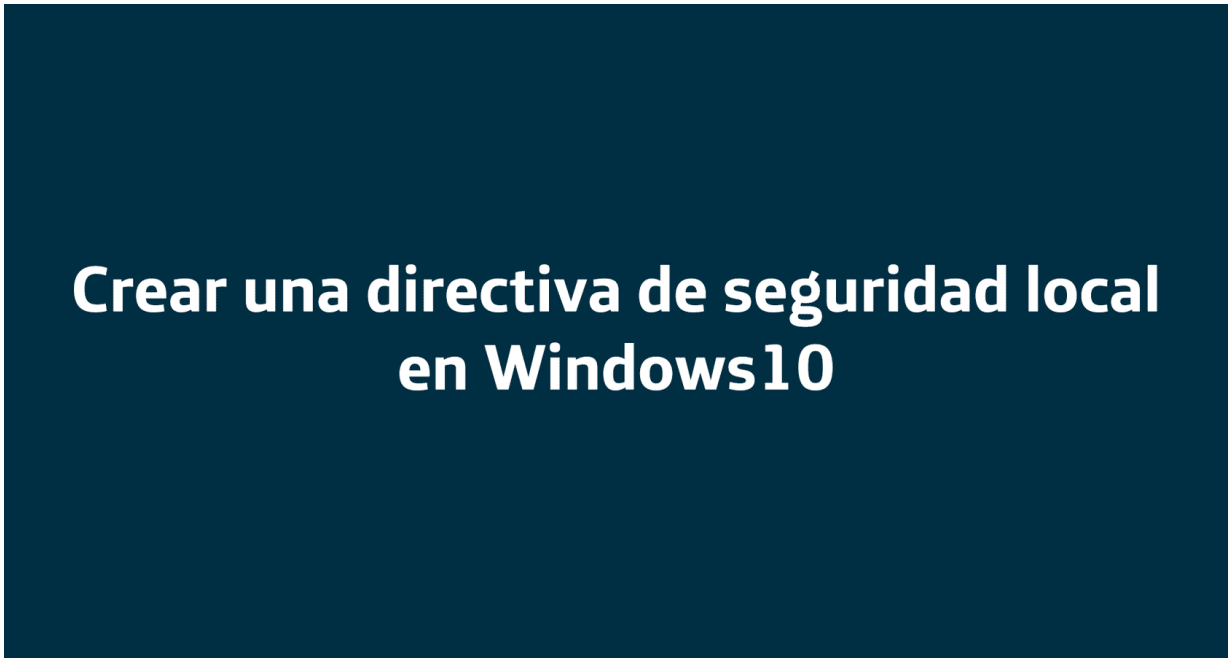
- Configurar los componentes del sistema operativo.
- Controlar la funcionalidad del sistema (perfiles de usuario, derechos, etc.).
- Cómo se comportan los componentes de conexión a la red y cuando no están conectados.
- Configuración de conexiones de periféricos en red como impresoras, etc.

Configuración del usuario

- Componentes del sistema que interactúan con el usuario.
- Configuración de los menús que se ofrecen y las barras de tareas.
- Opciones ofrecidas dentro del panel de control o administración.
- Control del comportamiento del sistema con respecto a las opciones de los perfiles de usuario, comandos y opciones ofrecidas, etc.

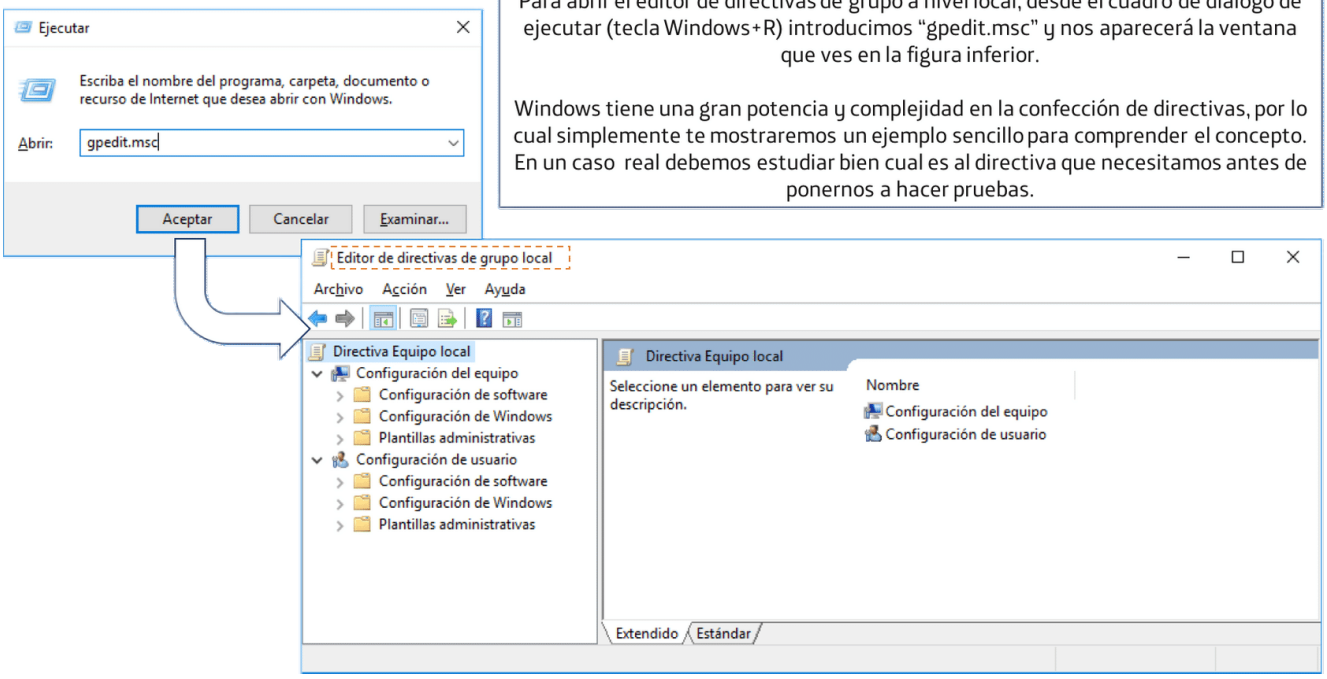
Ejemplo: crear una directiva local en Windows

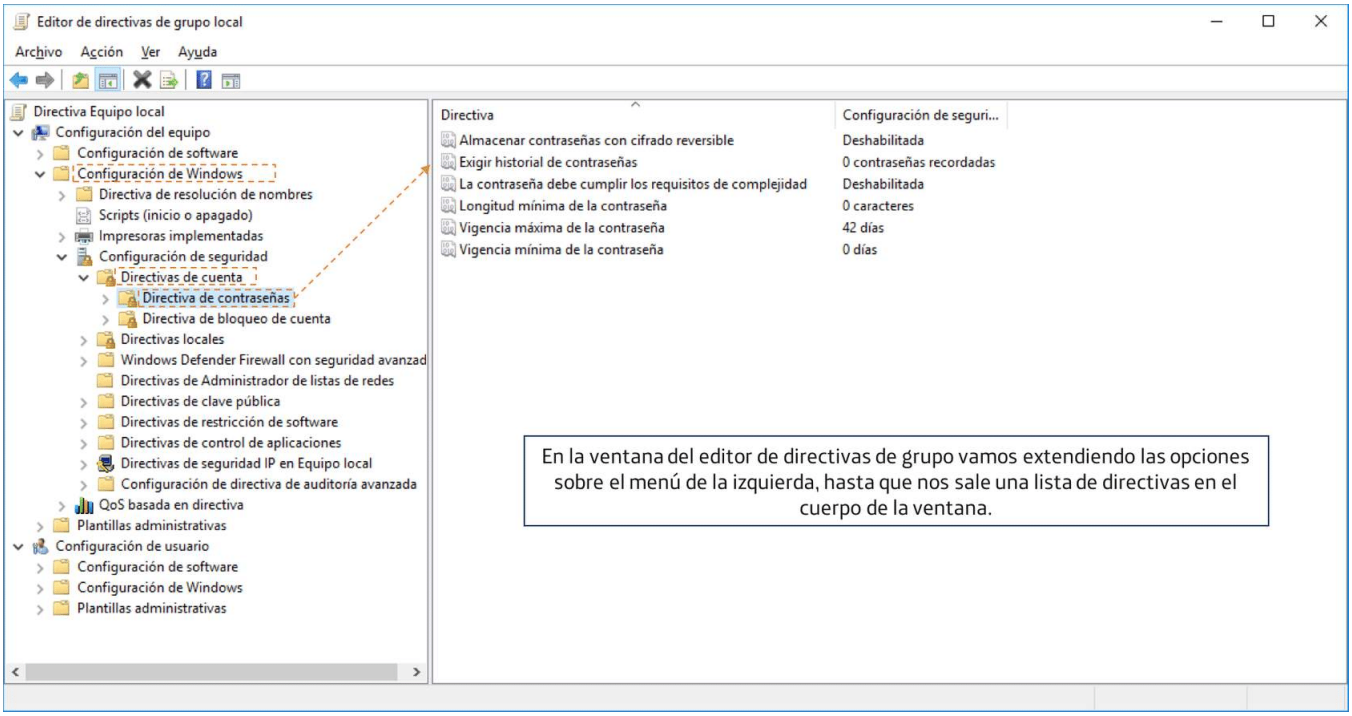
Aunque el tema es complejo y solamente deseamos que te quedes con el concepto, te mostraremos en las siguientes imágenes cómo se crearía una directiva local en la máquina virtual de Windows10, por ejemplo para variar los requisitos de las contraseñas de los usuarios.



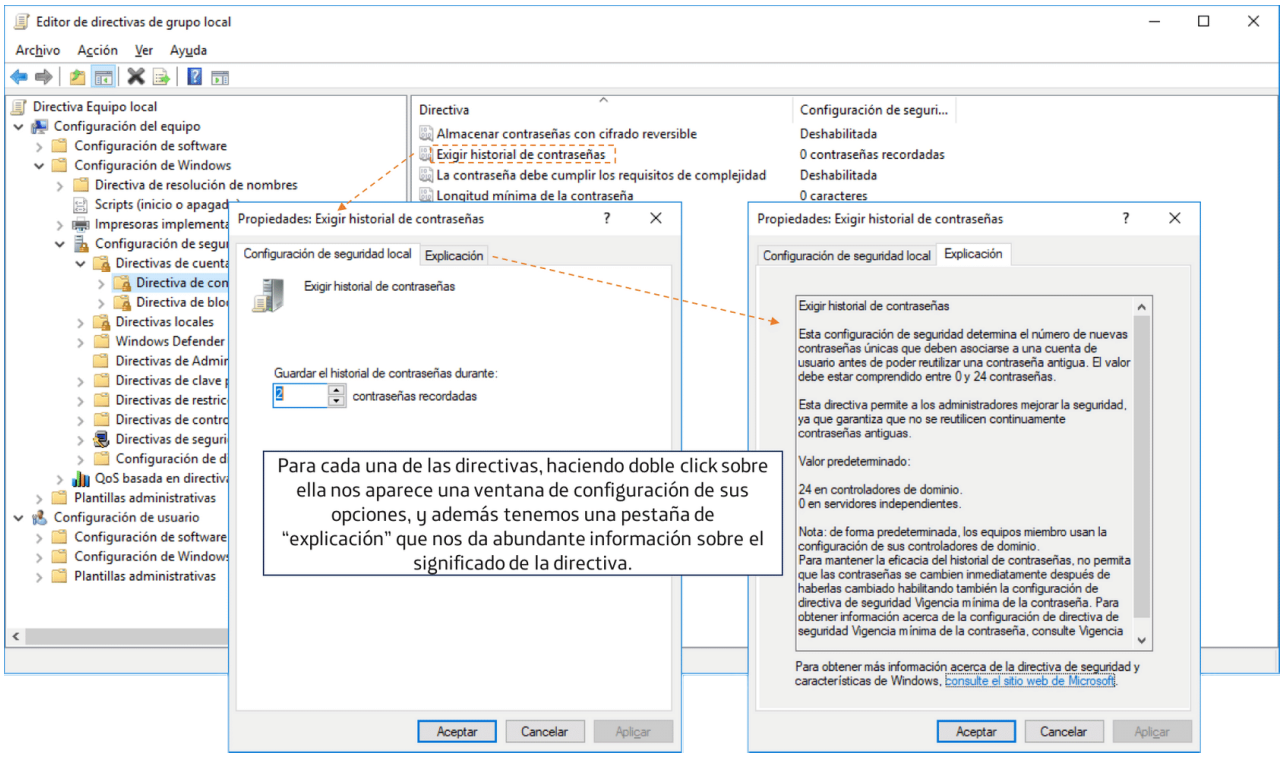
Para abrir el editor de directivas de grupo a nivel local, desde el cuadro de diálogo de ejecutar (tecla Windows+R) introducimos "gpedit.msc" y nos aparecerá la ventana que ves en la figura inferior.

Windows tiene una gran potencia y complejidad en la confección de directivas, por lo cual simplemente te mostraremos un ejemplo sencillo para comprender el concepto. En un caso real debemos estudiar bien cual es al directiva que necesitamos antes de ponernos a hacer pruebas.

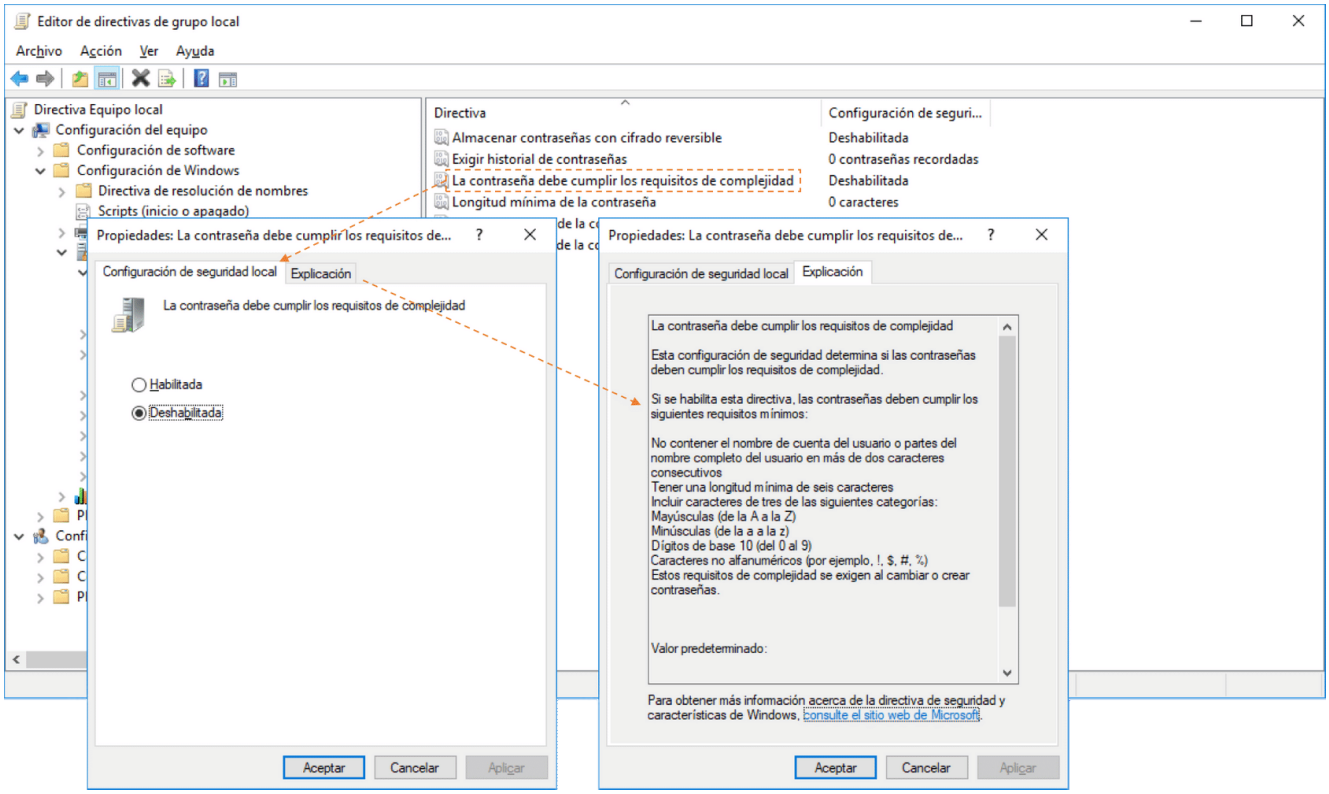


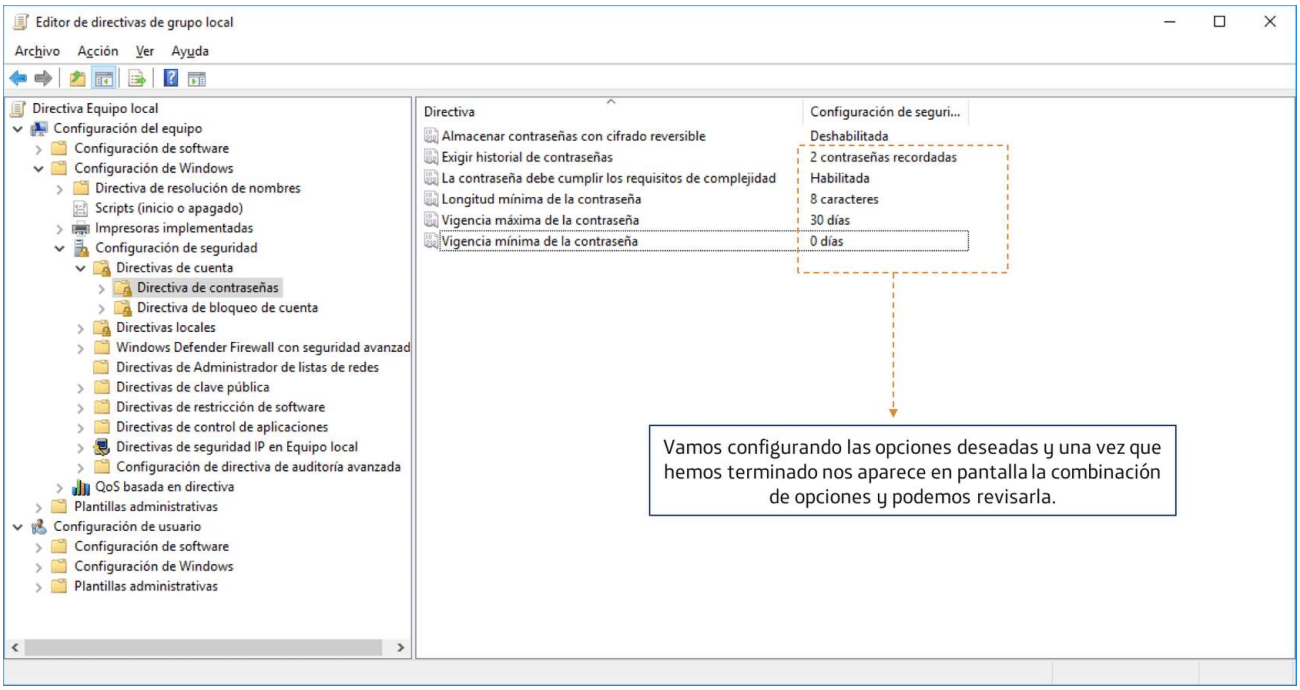


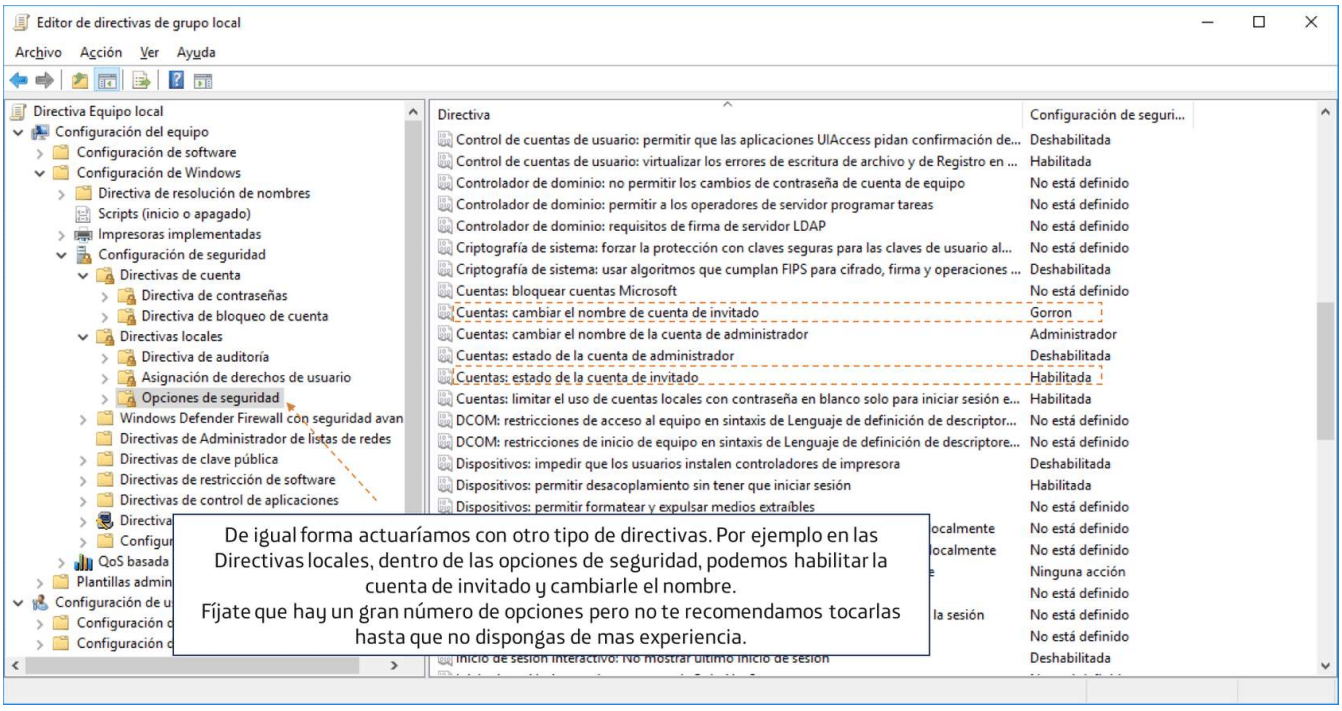
En la ventana del editor de directivas de grupo vamos extendiendo las opciones sobre el menú de la izquierda, hasta que nos sale una lista de directivas en el cuerpo de la ventana.

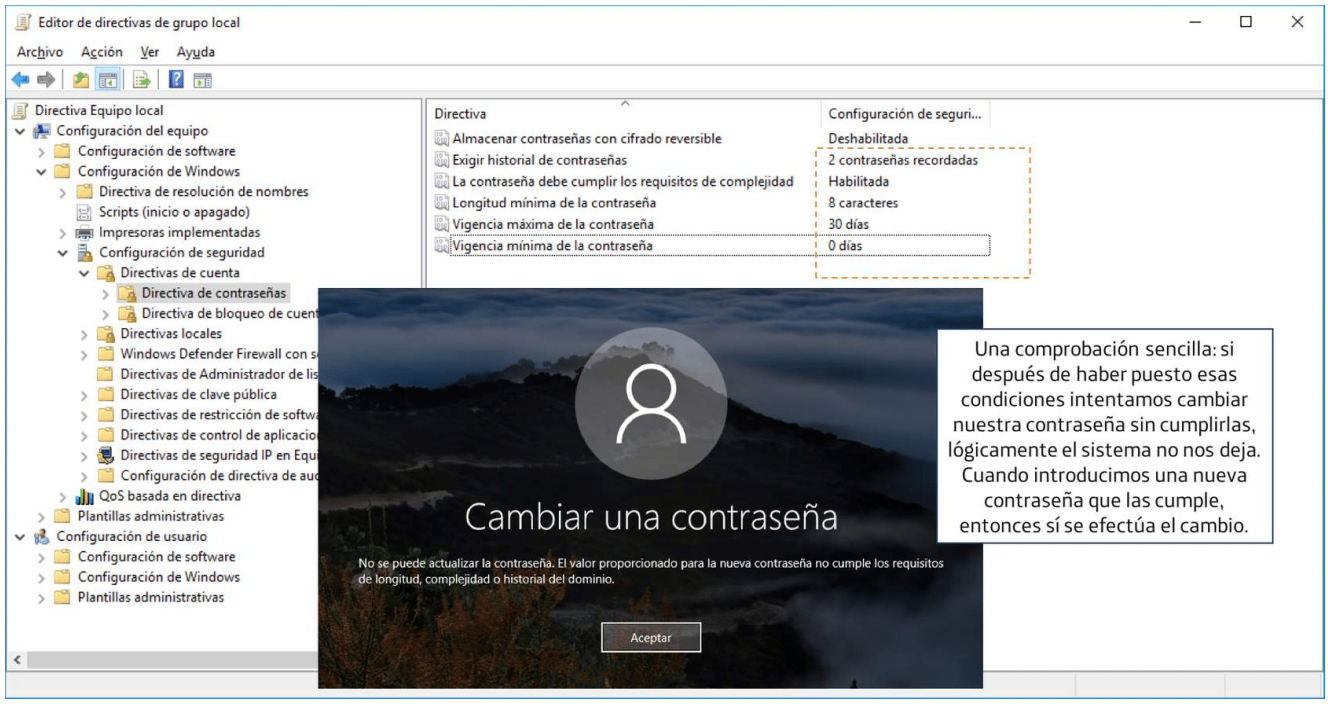


Para cada una de las directivas, haciendo doble click sobre ella nos aparece una ventana de configuración de sus opciones, y además tenemos una pestaña de "explicación" que nos da abundante información sobre el significado de la directiva.




Editor de directivas de grupo local
Archivo Acción Ver Ayuda
Directiva Equipo local
Configuración del equipo
Configuración de software
Configuración de Windows
Directiva de resolución de nombres
Scripts (inicio o apagado)
Impresoras implementadas
Configuración de seguridad
Directivas de cuenta
Directiva de contraseñas
Directiva de bloqueo de cuenta
Directivas locales
Windows Defender Firewall con seguridad avanzad
Directivas de Administrador de listas de redes
Directivas de clave pública
Directivas de restricción de software
Directivas de control de aplicaciones
Directivas de seguridad IP en Equipo local
Configuración de directiva de auditoría avanzada
QoS basada en directiva
Plantillas administrativas
Configuración de usuario
Configuración de software
Configuración de Windows
Plantillas administrativas
Directiva
Configuración de seguri...
Almacenar contraseñas con cifrado reversible
Deshabilitada
Exigir historial de contraseñas
2 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad
Habilitada
Longitud mínima de la contraseña
8 caracteres
Vigencia máxima de la contraseña
30 días
Vigencia mínima de la contraseña
0 días
Vamos configurando las opciones deseadas y una vez que hemos terminado nos aparece en pantalla la combinación de opciones y podemos revisarla.


Editor de directivas de grupo local
Archivo Acción Ver Ayuda
Directiva Equipo local
Configuración del equipo
Configuración de software
Configuración de Windows
Directiva de resolución de nombres
Scripts (inicio o apagado)
Impresoras implementadas
Configuración de seguridad
Directivas de cuenta
Directiva de contraseñas
Directiva de bloqueo de cuenta
Directivas locales
Directiva de auditoría
Asignación de derechos de usuario
Opciones de seguridad
Windows Defender Firewall con seguridad avan
Directivas de Administrador de listas de redes
Directivas de clave pública
Directivas de restricción de software
Directivas de control de aplicaciones
Directiva
Configuración de seguri...
Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de...
Deshabilitada
Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de Registro en ...
Habilitada
Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo
No está definido
Controlador de dominio: permitir a los operadores de servidor programar tareas
No está definido
Controlador de dominio: requisitos de firma de servidor LDAP
No está definido
Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario al...
No está definido
Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones ...
Deshabilitada
Cuentas: bloquear cuentas Microsoft
No está definido
Cuentas: cambiar el nombre de cuenta de invitado
Gorron
Cuentas: cambiar el nombre de la cuenta de administrador
Administrador
Cuentas: estado de la cuenta de administrador
Deshabilitada
Cuentas: estado de la cuenta de invitado
Habilitada
Cuentas: limitar el uso de cuentas locales con contraseña en blanco solo para iniciar sesión e...
Habilitada
DCOM: restricciones de acceso al equipo en sintaxis de Lenguaje de definición de descriptor...
No está definido
DCOM: restricciones de inicio de equipo en sintaxis de Lenguaje de definición de descriptore...
No está definido
Dispositivos: impedir que los usuarios instalen controladores de impresora
Deshabilitada
Dispositivos: permitir desacoplamiento sin tener que iniciar sesión
Habilitada
Dispositivos: permitir formatear y expulsar medios extraíbles
No está definido
De igual forma actuaríamos con otro tipo de directivas. Por ejemplo en las Directivas locales, dentro de las opciones de seguridad, podemos habilitar la cuenta de invitado y cambiarle el nombre.
Fíjate que hay un gran número de opciones pero no te recomendamos tocarlas hasta que no dispongas de mas experiencia.


Editor de directivas de grupo local
Archivo Acción Ver Ayuda
Directiva Equipo local
Configuración del equipo
Configuración de software
Configuración de Windows
Directiva de resolución de nombres
Scripts (inicio o apagado)
Impresoras implementadas
Configuración de seguridad
Directivas de cuenta
Directiva de contraseñas
Directiva de bloqueo de cuent
Directivas locales
Windows Defender Firewall con s
Directivas de Administrador de lis
Directivas de clave pública
Directivas de restricción de softwa
Directivas de control de aplicacio
Directivas de seguridad IP en Equi
Configuración de directiva de auc
QoS basada en directiva
Plantillas administrativas
Configuración de usuario
Configuración de software
Configuración de Windows
Plantillas administrativas
Directiva
Configuración de seguri...
Almacenar contraseñas con cifrado reversible
Deshabilitada
Exigir historial de contraseñas
2 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad
Habilitada
Longitud mínima de la contraseña
8 caracteres
Vigencia máxima de la contraseña
30 días
Vigencia mínima de la contraseña
0 días
Cambiar una contraseña
No se puede actualizar la contraseña. El valor proporcionado para la nueva contraseña no cumple los requisitos de longitud, complejidad o historial del dominio.
Aceptar
Una comprobación sencilla: si después de haber puesto esas condiciones intentamos cambiar nuestra contraseña sin cumplirlas, lógicamente el sistema no nos deja. Cuando introducimos una nueva contraseña que las cumple, entonces sí se efectúa el cambio.

Requisitos y mecanismos de seguridad

Cualquier sistema operativo, ya sea local o en red, ha de cumplir con una serie de requisitos relacionados con la seguridad del propio sistema y los datos que contiene.

Algunos de los **requisitos de seguridad** que en general deben cumplir los sistemas pueden ser:

- **Identificación y autentificación de los usuarios** del sistema estableciendo un control de acceso.
- **Controlar el acceso** a la información y los recursos del sistema en base al principio del mínimo privilegio.
- **Monitorizar, registrar y auditar la actividad** de los usuarios del sistema.
- Establecer medidas para verificar y **mantener la integridad de la información** almacenada.
- **Auditar los eventos** que representen un posible riesgo para el sistema.
- **Asegurar la disponibilidad de la información** para los usuarios y las aplicaciones que la necesiten (en un alto porcentaje de probabilidad, ya que la garantía total no existe).

- **Controlar** el acceso y la información intercambiada a través de las **conexiones de red** y los enlaces exteriores del sistema.

- Establecer medidas especiales para asegurar la **confidencialidad y encriptado** de la información sensible.

- Tomar medidas para **prevenir, detectar y corregir posibles ataques** o eventos externos que puedan afectar a la confidencialidad, integridad o disponibilidad de la información y los servicios del sistema.

- Verificar y garantizar el funcionamiento de los propios mecanismos de seguridad del sistema.

- Establecer y documentar la política y procedimientos de seguridad del sistema.

Mecanismos de seguridad

Para cumplir con los requisitos de seguridad, el administrador del sistema podrá establecer diferentes mecanismos, implementados a través de las opciones de comandos o de las interfaces gráficas que nos ofrece cada sistema. Aunque el mecanismo y su objetivo sea similar, la forma de "construirlo" será diferente de un sistema a otro. Por ejemplo:

Mecanismos de prevención

- Mecanismos de autentificación e identificación.
- Mecanismos de control de acceso.
- Barreras y mecanismos de separación (físicos, temporales, lógicos, fragmentación, ACL, permisos).
- Mecanismos de cifrado y criptografía.

Mecanismos de detección

- Detección de intrusos ("*Intruder Detection System*" – IDS).
- Auditorías sobre el tráfico.
- Auditorías de enrutamientos.
- Auditorías sobre históricos ("*logs*").

Mecanismos de recuperación

- Copias de seguridad (*backup*).
- Técnicas informáticas forenses: herramientas de análisis y recuperación de la información.

Seguridad a nivel de usuarios

Para establecer las políticas y directrices de seguridad (que especifican qué hay que proteger, qué usuarios pueden acceder a que datos, etc.) existen una serie de mecanismos disponibles en el sistema operativo que pueden ser a nivel de usuario, de equipo o de red.

A nivel de usuario los mecanismos de seguridad a poner en práctica pueden variar mucho y, por ejemplo, diseñarse para ser aplicados a nivel de cuenta de usuario, a la configuración de todo el equipo o al conjunto de equipos de la red.

Hay que tener en cuenta que las políticas de seguridad pueden cambiar en una organización. Esto puede hacer que se cambien o utilicen de otra forma los mecanismos implementados (por ejemplo, puede tener que cambiar las directivas de seguridad).

Consecuencias de no tener buenas medidas de seguridad

Las **consecuencias de la "no seguridad"** afecta tanto a usuarios como a equipos:

Para los usuarios

- Pérdida de datos o del acceso a ellos.
- Pérdida de tiempo (sistemas más lentos).
- Pérdida económica (datos bancarios o coste del esfuerzo adicional).
- Coste adicional de la reparación (si hay que contratarla externamente).
- Pérdida de funcionalidad en sus procesos/aplicaciones (parcial o total).
- Otros tipos de costes asociados a la vulnerabilidad (costes de oportunidad u organizacionales, imagen de la compañía, credibilidad, imagen personal, etc.).

Para equipos y sistemas

- Denegación del servicio.
- Pérdida / eliminación de evidencias.
- Ejecuciones de acciones indebidas (no permitidas).
- Acceso a datos por parte de agentes no autorizados.
- Alteración o pérdida de los datos.
- Pérdida de control sobre el sistema.
- Daño a otros sistemas de la red desde el equipo infectado.
- Disminución del rendimiento / recursos disponibles.
- Pérdida de funcionalidad (parcial o total).

Seguridad de usuarios en sistemas Windows y Linux

Cada sistema ofrecerá diferentes formas de implementar los mecanismos de seguridad, tanto a nivel de cuenta de usuario como a nivel de equipo o conjunto de equipos en una red.

En general, **a nivel de usuario** cualquier sistema impondrá algún **mecanismo de control de acceso**, y una vez dentro se le aplicarán una serie de **permisos/restricciones** en su capacidad de operación sobre los recursos del propio equipo y los compartidos en la red.

A nivel de equipo suele haber también un control de acceso definiendo qué usuarios pueden acceder a él, ya sea localmente o de forma remota a través de la red, y luego los recursos y servicios del equipo podrán estar disponibles para unos grupos de usuarios u otros.

El principio general es el de la prudencia y el de **limitar las acciones sobre el sistema a aquello necesario para el trabajo**, impidiendo cualquier otra cosa que no sea necesaria. De una definición adecuada de "lo que es necesario", "cuántos grupos de usuarios necesitamos" y "qué privilegios debe tener cada uno", depende en gran parte la fiabilidad de las medidas de seguridad adoptadas.

Seguridad de usuarios en Windows

En **Windows** los usuarios se pueden definir a nivel local o a nivel de dominio en la red (en el caso de sistemas como Windows Server).

La **cuenta de usuario** de un dominio contendrá toda la información para su utilización en ese dominio, es decir: nombre de usuario y clave de acceso, grupos a los que pertenece ese usuario, derechos y permisos del usuario, etc. y esta información estará replicada en los controladores de dominio de la red.

La seguridad a nivel de usuarios está basada, como sabemos, en el sistema de **autentificación mediante nombre de usuario y contraseña**, de forma que cuando se inicia una sesión el sistema asigna un "**SID**" ("*Security Identifier*") único para ese usuario (y cada grupo tendrá también un identificador único).

Además, al proceso inicial que crea el usuario al iniciar sesión se le asigna un "*token* de seguridad" ("*Access Token*"), que es un parámetro que heredan los siguientes procesos que lance ese usuario y lleva aparejado el contexto de datos de seguridad (identificadores, tiempo máximo de expiración y privilegios).

> Recuerda que un "**dominio**" en este contexto no es más que una forma de organizar los equipos y recursos en una red con sistemas Windows. Algo parecido es un "**grupo de trabajo**", pero en el grupo de trabajo todos los equipos se configuran localmente y como independientes (en ellos se definen cuentas, directivas de seguridad, etc.), mientras que en el dominio unos equipos actuarán de servidores (son los "**controladores de dominio**") y guardarán la configuración de seguridad a aplicar a los demás, por ejemplo.

Seguridad de usuarios en Linux

En los sistemas **Unix/Linux** cada usuario tiene asignado un identificador de usuario (UID) y cuando accede al sistema hace el "*login*" asociado a ese UID (el usuario invitado que se permite en algunos sistemas es un usuario más).

En Linux cada cuenta es una entidad independiente, con un nombre de usuario, una contraseña y unos permisos y derechos particulares para ella. Además el sistema mantiene aislados los directorios de los usuarios y permite establecer reglas para autorizar o no el acceso de un usuario a las conexiones de red.

Por otra parte, el sistema globalmente está compuesto y es administrado como un conjunto de "**grupos de usuarios**". Cada grupo también tendrá su identificador (**GID**), de forma que **cada pareja de (UID + GID) forma un "dominio" en Linux**, sobre el que se definen los recursos y dispositivos que se pueden usar y con que nivel de permisos. En Linux un usuario puede pertenecer a varios grupos y, por lo tanto, podrá pertenecer a varios dominios y se le aplicarán los permisos efectivos del conjunto de ellos.

> En Unix/Linux, el usuario "*root*" es el administrador del sistema (usuario especial con UID=0) y con privilegios totales sobre todos los recursos, es decir:**"Si alguien obtiene la *password* del *root* puede hacer lo que quiera sobre el sistema (perfiles de usuarios y equipos)."**

Recuerda que en Unix/Linux **cada fichero y dispositivo pertenecerá a un usuario y un grupo**, y sobre él se pueden especificar los permisos que tiene cada usuario sobre ese archivo (referidas al propietario, el grupo y el resto de usuarios, el sistema UGO que ya conoces).

Por otra parte, **cada proceso se ejecutará con los privilegios del usuario que lo lanza**, aunque también sabemos que pueden existir excepciones si se usan los bits "*setuid*" (se lanza con la identidad del propietario del ejecutable) y "*setgid*" (se lanza con la identidad del grupo al que pertenece el propietario del ejecutable).

Seguridad a nivel de equipos y sistema

La seguridad en los ordenadores y el resto de equipos de la red depende de las medidas específicas tomadas para protegerlos.

Existen vulnerabilidades que pueden estar generadas por una política inadecuada o unas **prácticas poco seguras**, como por ejemplo:

- Realizar "instalaciones estándar" (por defecto) sin estar diseñadas para establecer mecanismos adecuados de seguridad.
- **Automatización excesiva** de procesos u operaciones (por comodidad para el usuario) que no deberían estarlo.
- Permitir **riesgos relacionados con la conexión a la red**: puertos abiertos, aplicaciones corriendo sin control, ejecución automática de *scripts* o código externo en algunos tipos de documentos, etc.
- Permitir la ejecución de servicios innecesarios.
- Dar demasiados privilegios al usuario.
- Permitir la **instalación de SW externo** por parte de los usuarios cuando no es estrictamente necesario.
- Falta de **actualización y mantenimiento del SW** (sistema operativo y aplicaciones).
- En sistemas complejos pueden surgir interacciones y casos no previstos.
- En sistemas distribuidos el hecho de estarlo es un factor de complejidad.
- Falta de mecanismos de separación y prevención de ataques (*firewalls*, DMZ, etc.).
- Falta de formación en conceptos de seguridad por parte de los administradores del sistema.

En general, no hay una única pauta y las **medidas a tomar para asegurar los equipos del sistema** son, en gran parte, fruto del "sentido común" de los administradores y de su trabajo y esfuerzo dedicado a planificar cómo llevarlas a cabo e implementarlas con calidad.

Para cualquier equipo instalado en nuestra red se aconseja, por ejemplo:

- Definir **contraseñas de administración y mantenimiento específicas** (y por supuesto las de cada usuario) y limitar estas cuentas.
- Si se trata de equipos (p. ej. *routers*) que admitan cifrado, este no suele activarse por defecto; entonces debemos asegurarnos de que lo emplean.
- **Desactivar el control remoto** (p. ej. *telnet*) siempre que no sea necesario.
- **Filtrar y bloquear el acceso a los puertos** del equipo.
- Activar todas las opciones relacionadas con la seguridad y el tiempo de espera de claves, sesiones, verificación de datos, etc.
- Establecer **contraseñas para al BIOS y la consola**.
- Cuando es posible, establecer controles de acceso biométrico adicionales.
- Ocuparse de la seguridad física de los equipos (mecanismos antirrobo, ubicación en armarios ignífugos, etc.).
- Identificar e inventariar todos los equipos de la red y disponer de un documento descriptivo de su ubicación y funcionalidad.

Resumen

Has finalizado esta unidad. Repasemos los puntos más importantes que hemos tratado.

En esta unidad hemos visto algunos conceptos nuevos relacionados también con la seguridad del sistema, como por ejemplo las "directivas de seguridad" y su uso.

Es importante que recuerdes que si tienes que administrar un conjunto de equipos conectados en una red (ya sea interna a una organización oa través de Internet), resulta importante pensar tanto en los mecanismos de seguridad que debemos establecer un nivel de cuentas de usuario, como a nivel de equipos o de todo el conjunto del sistema.

PROEDUCA