Directivas de seguridad

Las directivas de seguridad abordan múltiples aspectos críticos para mantener la integridad y la protección de los datos. En el contexto **local**, estas directivas se enfocan en la configuración de políticas individuales del equipo, tales como las restricciones de acceso y los permisos de usuarios locales, garantizando así un entorno seguro desde el propio dispositivo.

Cuando se trata del **controlador de dominio**, las directivas se centran en la administración centralizada de usuarios y dispositivos dentro de una red, utilizando herramientas y configuraciones específicas para supervisar y aplicar normas de seguridad uniformes.

Por otro lado, en el ámbito del **dominio**, las directivas de seguridad se amplían para armonizar políticas y reglamentos que afecten a toda la estructura organizacional, asegurando que todos los sistemas conectados al dominio cumplan con los requisitos de seguridad preestablecidos, lo cual es importante para la defensa contra amenazas internas y externas.

1.1 Directivas locales

Las directivas locales en los sistemas operativos son un conjunto de configuraciones que permiten definir y gestionar el comportamiento y la seguridad del sistema en un **entorno local**, es decir, sin depender de políticas centralizadas como las que se aplican en dominios administrados por *Active Directory*.

En un sistema operativo como **Windows**, las directivas locales se configuran a través del **Editor de directivas de grupo local** (*Local Group Policy Editor*). Estas directivas abarcan una amplia gama de configuraciones, desde aspectos relacionados con la seguridad, como el control de contraseñas y la gestión de accesos, hasta ajustes en el comportamiento del sistema, como restricciones de software y configuraciones de red.

Cada configuración definida a través de estas directivas impacta directamente en cómo los usuarios interactúan con el sistema y cómo este responde a ciertas acciones o situaciones.

Una de las características más importantes de las directivas locales es su capacidad para **personalizar** el entorno del sistema según las necesidades específicas del usuario o administrador. Por ejemplo, es posible usar directivas locales para imponer restricciones de acceso a ciertas aplicaciones, configurar reglas para el bloqueo automático de la pantalla tras un período de inactividad o definir los permisos de acceso a dispositivos externos como unidades USB. Estas configuraciones permiten aumentar la **seguridad** y el control sobre el equipo sin necesidad de herramientas externas.

En **Windows**, las directivas locales son configuraciones específicas que controlan el comportamiento y la seguridad de un equipo individual. Estas directivas abarcan una amplia gama de ajustes que afectan tanto al sistema como a los usuarios, y permiten personalizar y proteger el entorno sin depender de un dominio. Se clasifican en varias categorías, cada una diseñada para gestionar diferentes aspectos del sistema operati vo. Además, Windows proporciona herramientas específicas para gestionarlas.

1.1. **Directivas de seguridad local**: relacionadas con la protección del sistema y los usuarios. Incluyen ajustes para la política de contraseñas, el bloqueo de cuentas tras varios intentos fallidos, permisos de acceso a recursos locales, auditoría de eventos de seguridad y restricciones en el uso de dispositivos externos. Por ejemplo, se puede configurar el requisito de contraseñas complejas o determinar quién puede iniciar sesión localmente.

1.2. **Directivas de usuario:** afectan la experiencia de los usuarios al interactuar con el sistema. Incluyen opciones como restricciones en el uso de aplicaciones, la personalización del escritorio, el control del acceso a ciertas configuraciones del sistema y la limitación de privilegios específicos. Por ejemplo, es posible impedir que los usuarios accedan al Panel de Control o modificar la configuración del sistema.

1.3. **Directivas de equipo**: están orientadas a la configuración global del sistema operativo y su hardware. Incluyen ajustes para la instalación de controladores, la configuración de red, las políticas de actualización automática y los permisos para ejecutar scripts en el sistema.

1.4. **Directivas de auditoría**: permiten definir qué eventos del sistema o de seguridad deben ser registrados. Por ejemplo, se puede auditar el acceso a archivos, cambios en configuraciones críticas o intentos de inicio de sesión fallidos. Estos registros son esenciales para el diagnóstico de problemas y la supervisión de la seguridad.

1.5. **Directivas de restricciones de software y AppLocker**: permiten controlar qué programas pueden ejecutarse en el sistema, estableciendo listas blancas o negras de aplicaciones según su ruta, firma digital o reglas específicas. Son especialmente útiles para prevenir la ejecución de software malicioso.

1. **Editor de directivas de grupo local (gpedit.msc)**: es la herramienta principal para configurar las directivas locales en sistemas Windows Pro, Enterprise y Education. Ofrece una interfaz gráfica organizada en dos categorías principales: configuración de equipo y configuración de usuario. Dentro de estas categorías, las directivas están organizadas por nodos jerárquicos que facilitan la navegación y la modificación de ajustes.

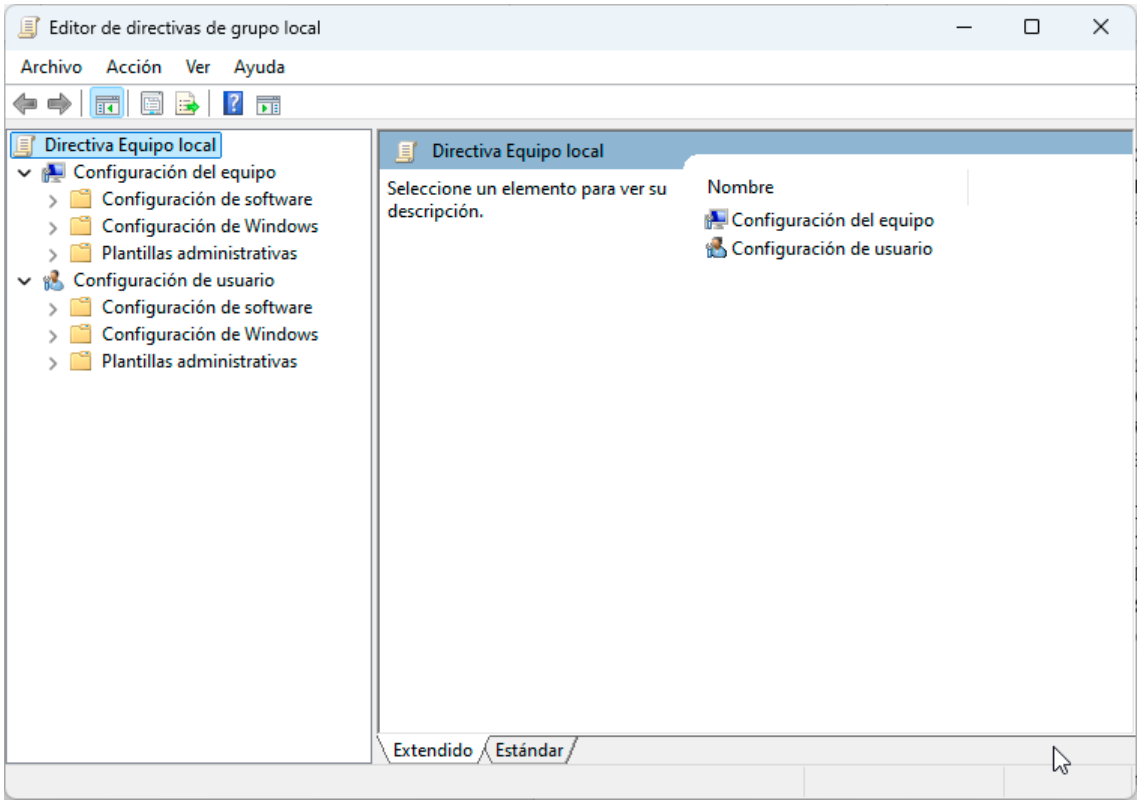

Ilustración 1. Editor de directivas de grupo local.

2. **Directiva de seguridad local (secpol.msc)**: es una herramienta específica para gestionar las políticas de seguridad local, como los requisitos de contraseñas, las reglas de auditoría y los permisos de acceso. Es particularmente útil para personalizar los aspectos de seguridad de un equipo.

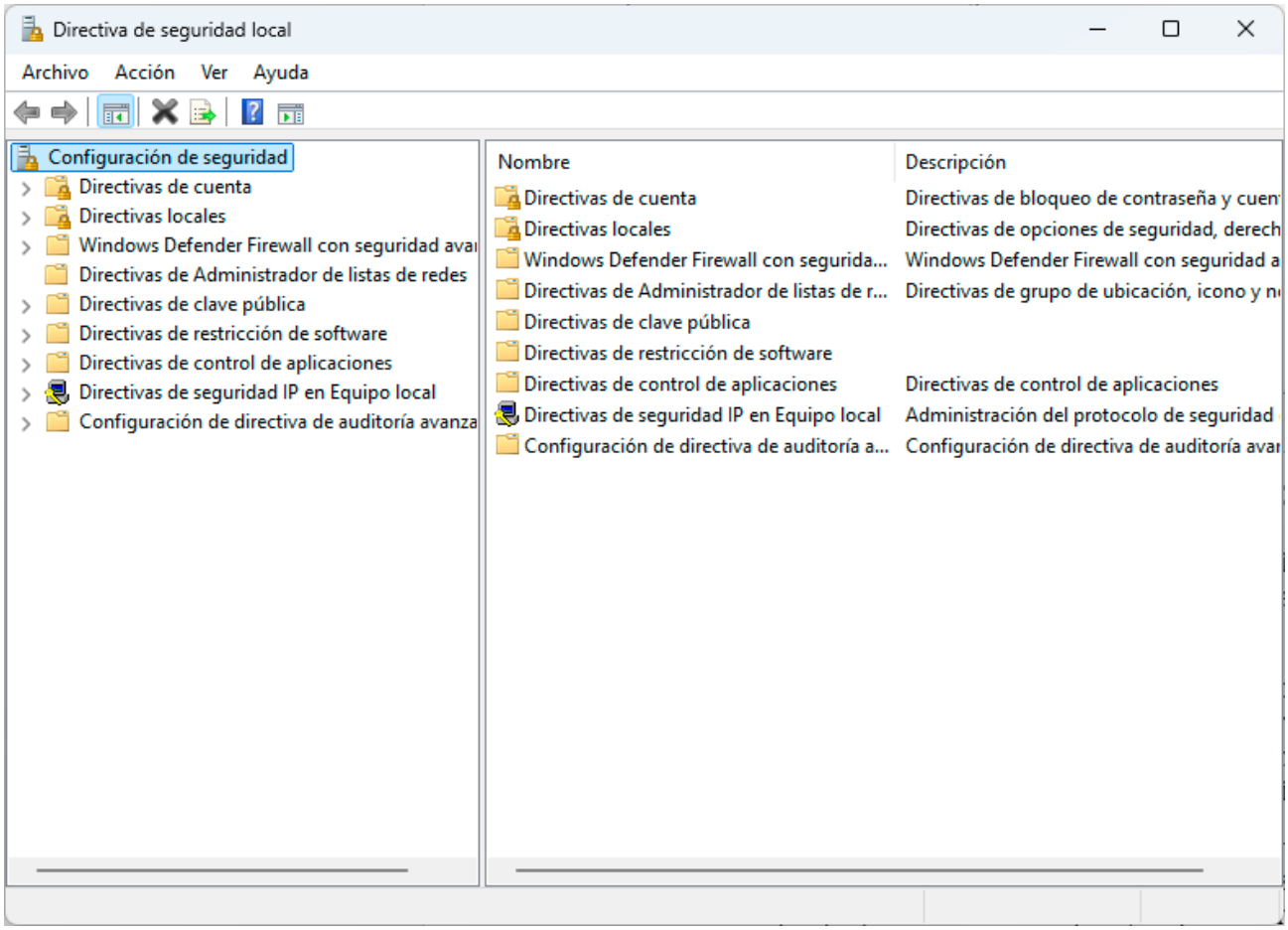

Ilustración 2. Directiva de seguridad local.

3. **Registro de Windows (regedit.exe)**: aunque no está diseñado específicamente para gestionar directivas, muchas configuraciones de políticas locales se reflejan en el Registro. Los administradores avanzados pueden realizar ajustes directa- mente aquí, aunque es menos intuitivo y puede ser arriesgado si no se sabe exactamente qué modificar.

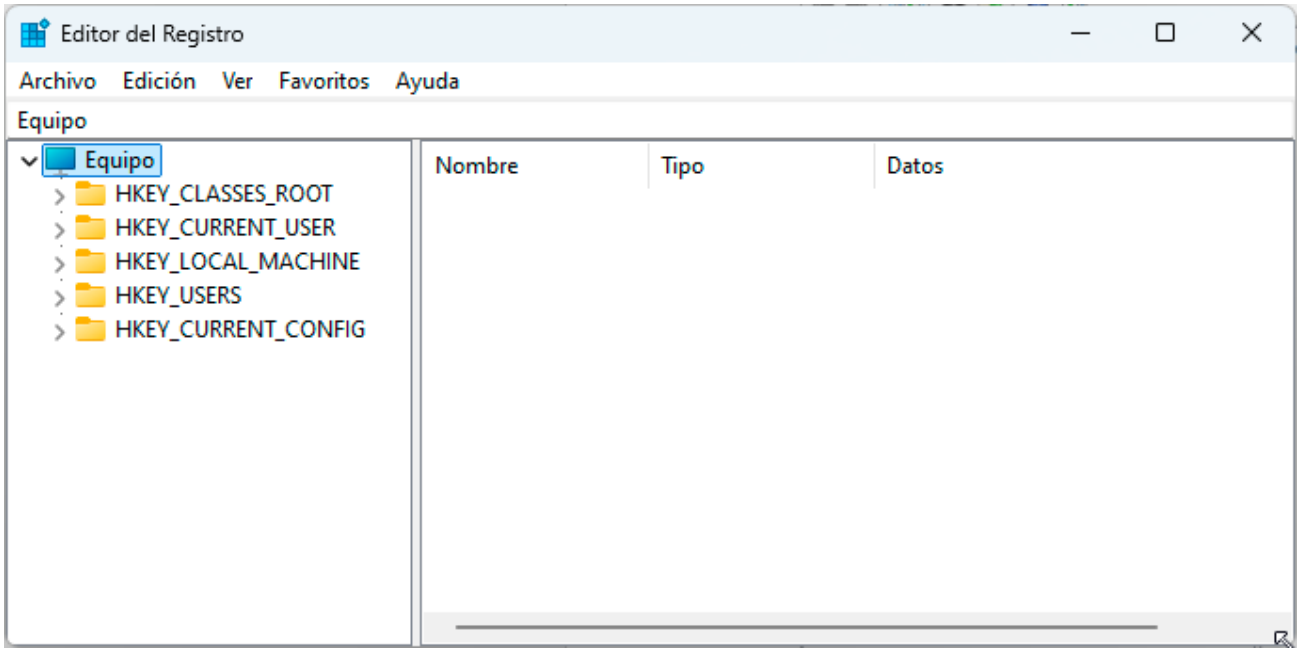

Ilustración 3. Editor de registro.

4. **Comandos de línea (PowerShell y cmd)**: Windows ofrece cmdlets y comandos específicos para gestionar directivas locales a través de PowerShell. Por ejemplo, con Set-ItemProperty se pueden modificar valores en el Registro que controlan ciertas políticas, y Auditpol permite configurar políticas de auditoría.

5. **Plantillas administrativas (*Administrative Templates*)**: son archivos que definen configuraciones de políticas en el Editor de directivas de grupo local. Se pueden importar plantillas adicionales (archivos .admx y .adml) para gestionar nuevas configuraciones introducidas por actualizaciones de Windows o aplicaciones de terceros.

6. **Panel de control y Configuración**: algunas configuraciones relacionadas con directivas locales, como las de energía o red, pueden gestionarse desde interfaces más accesibles como el Panel de Control o la aplicación de Configuración de Windows.

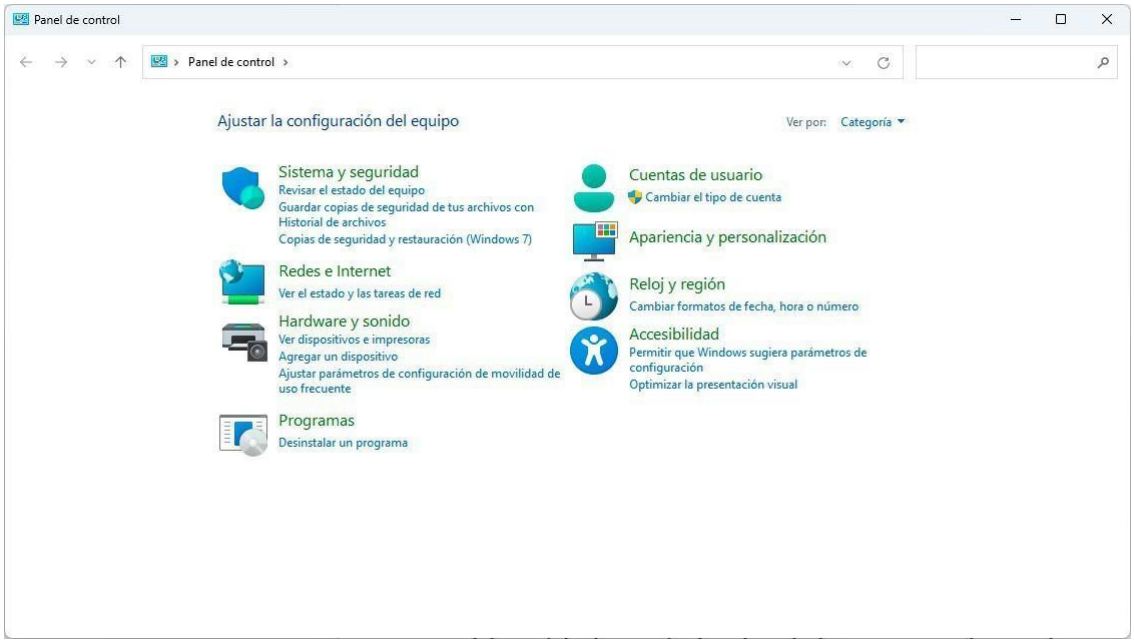

Ilustración 4. Panel de control en Windows.

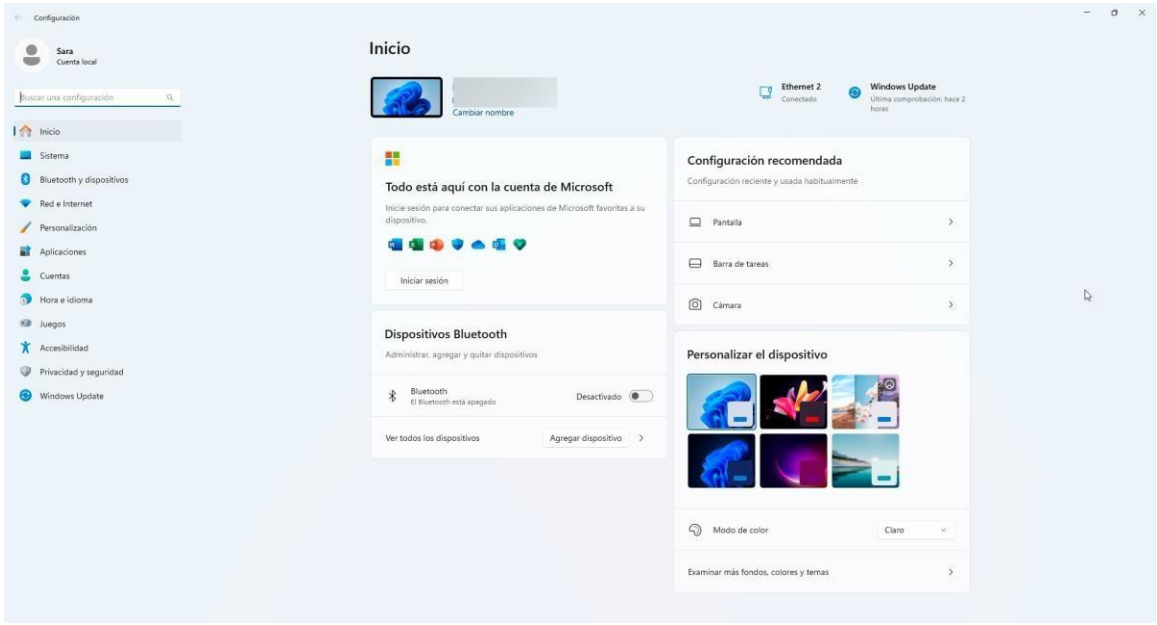

Ilustración 5. Aplicación Configuración de Windows.

En sistemas operativos como **Linux**, aunque el concepto de directivas locales no está estructurado del mismo modo que en Windows, se pueden aplicar configuraciones equivalentes a través de archivos de configuración local o scripts, como los ajustes en
/etc/security para políticas de contraseñas o los permisos definidos en /etc/sudoers. Estas configuraciones permiten personalizar y proteger el entorno local sin requerir herramientas centralizadas de gestión.

Esto significa que las directivas no se propagan a otros dispositivos de la red, lo que las diferencia de las políticas de dominio que se gestionan en entornos corporativos mediante *Active Directory*. Sin embargo, en redes pequeñas, las directivas locales son una herramienta poderosa para estandarizar configuraciones en cada máquina de manera independiente.

La administración de estas directivas es especialmente relevante en situaciones donde los equipos no están conectados a un dominio, como en estaciones de trabajo inde- pendientes o en dispositivos utilizados por usuarios individuales. Además, en entornos más grandes, las directivas locales pueden complementarse con políticas centraliza- das, proporcionando un control adicional sobre configuraciones específicas que deben aplicarse de manera local en cada equipo.