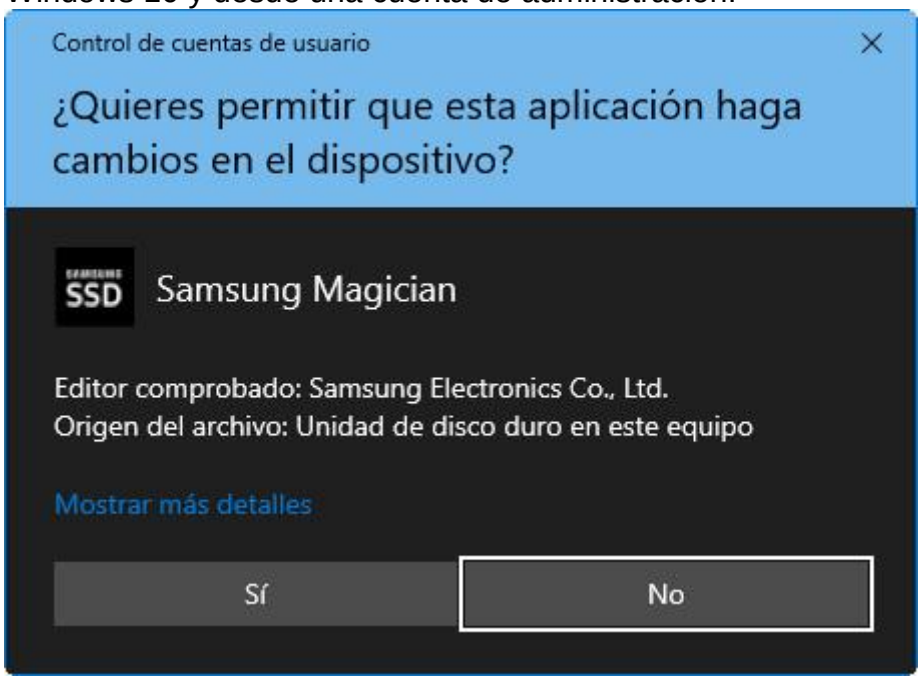
Sistemas Operativos

Control de cuentas de usuario en Windows

El Control de cuentas de usuario en Windows es una función de seguridad que ayuda a evitar cambios no autorizados en el sistema operativo. Una parte de usuarios lo deshabilita y es un error como vamos a ver en esta guía donde te mostraremos su objetivo, funcionamiento, gestión y los beneficios de mantenerlo activo.
Cuando se implementó en Windows Vista, el Control de cuentas de usuario (también conocido como UAC) fue una de las características más criticadas, seguramente al no ser bien explicada/entendida y ante la gran cantidad de avisos que los usuarios percibieron más como una molestia que ralentizaba su trabajo que como una mejora de su seguridad. Microsoft lo ha ido mejorando en cada versión posterior de sus sistemas y recomendamos mantenerlo activado aunque sea en su opción mínima.

Qué es y cómo se activa UAC

Como decíamos, UAC es una capa de seguridad añadida en Windows que previene de cambios no autorizados en el sistema operativo que puedan afectar a la seguridad o a la configuración de otras personas que usen un mismo equipo.
Estos cambios pueden ser realizados por usuarios sin permisos suficientes, aplicaciones, controladores y, lo peor, por cualquiera forma de malware que se haya introducido o pretenda introducirse en el equipo. El Control de cuentas de usuario se asegura de que ciertos cambios se realicen solo con la aprobación del administrador. Si los cambios no son aprobados por él no se ejecutan y el sistema permanece sin cambios.
Su funcionamiento del lado del usuario es simple. Cuando ejecutas un archivo, una aplicación o algún elemento de la configuración que esté a punto de realizar cambios importantes en el sistema, la función mostrará una notificación similar a la siguiente. Para el ejemplo, el software de gestión de las SSD de Samsung en Windows 10 y desde una cuenta de administración:

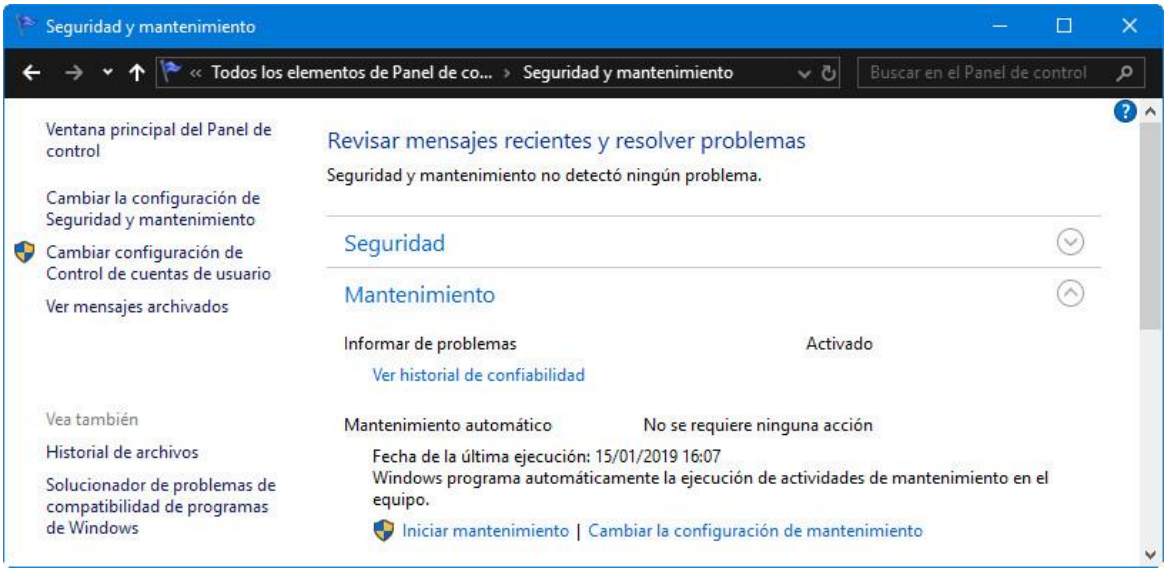


La solicitud de la UAC muestra el nombre del programa que está a punto de realizar un cambio de sistema que requiere la aprobación de un administrador. También muestra el editor del programa y el origen del archivo ejecutable. Un enlace a «más detalles» informa del certificado del editor y el acceso a la gestión de estas notificaciones que veremos después. Si la aplicación es de confianza y se ejecuta desde una cuenta de administración solo es necesario autorizar la petición.

Si el acceso se ha realizado desde una cuenta sin privilegios de administración la notificación será diferente y, siguiendo el ejemplo de Windows 10, la solicitud del UAC solicita el PIN del administrador (si está establecido) o la contraseña. En otros sistemas como Windows 7 y Windows 8.1, el indicador de UAC siempre solicita la contraseña del administrador.

Conocer los programas que activarán el control de cuentas es muy sencillo porque tienen un símbolo de UAC en la esquina inferior derecha del icono en el escritorio y también en el mismo ejecutable que puedes ver en el explorador de archivos.

Puedes encontrar este mismo tipo de símbolos en algunos elementos de configuración del sistema o en las herramientas del panel de control. Así sabrás de antemano que esos elementos necesitarán la aprobación del administrador cuando los ejecutes.



Cómo funciona UAC

En Windows, al contrario de como sucede de forma general en otros sistemas como Linux, las aplicaciones se ejecutan de forma predeterminada sin ningún permiso administrativo. Tienen los mismos permisos de una cuenta de usuario estándar, no pueden realizar ningún cambio en el sistema operativo, sus archivos de sistema o la configuración del registro. Además, no pueden cambiar nada que sea propiedad de otras cuentas de usuario. Las aplicaciones solo pueden cambiar archivos propios y en el registro los exc, los relativos al usuario y la configuración del registro o los archivos del usuario y la configuración del registro.
Cuando una aplicación requiere cambios que afecten a otras cuentas de usuario, modificaciones a los archivos y carpetas del sistema de Windows o instalación de nuevo software, se muestra un indicador de UAC, que solicita el permiso. Si el usuario niega la autorización el cambio no se llevará a cabo. Si el usuario lo autoriza (e ingresa la contraseña del administrador cuando se requiera), la aplicación recibe permisos administrativos y puede hacer los cambios del sistema que desee.

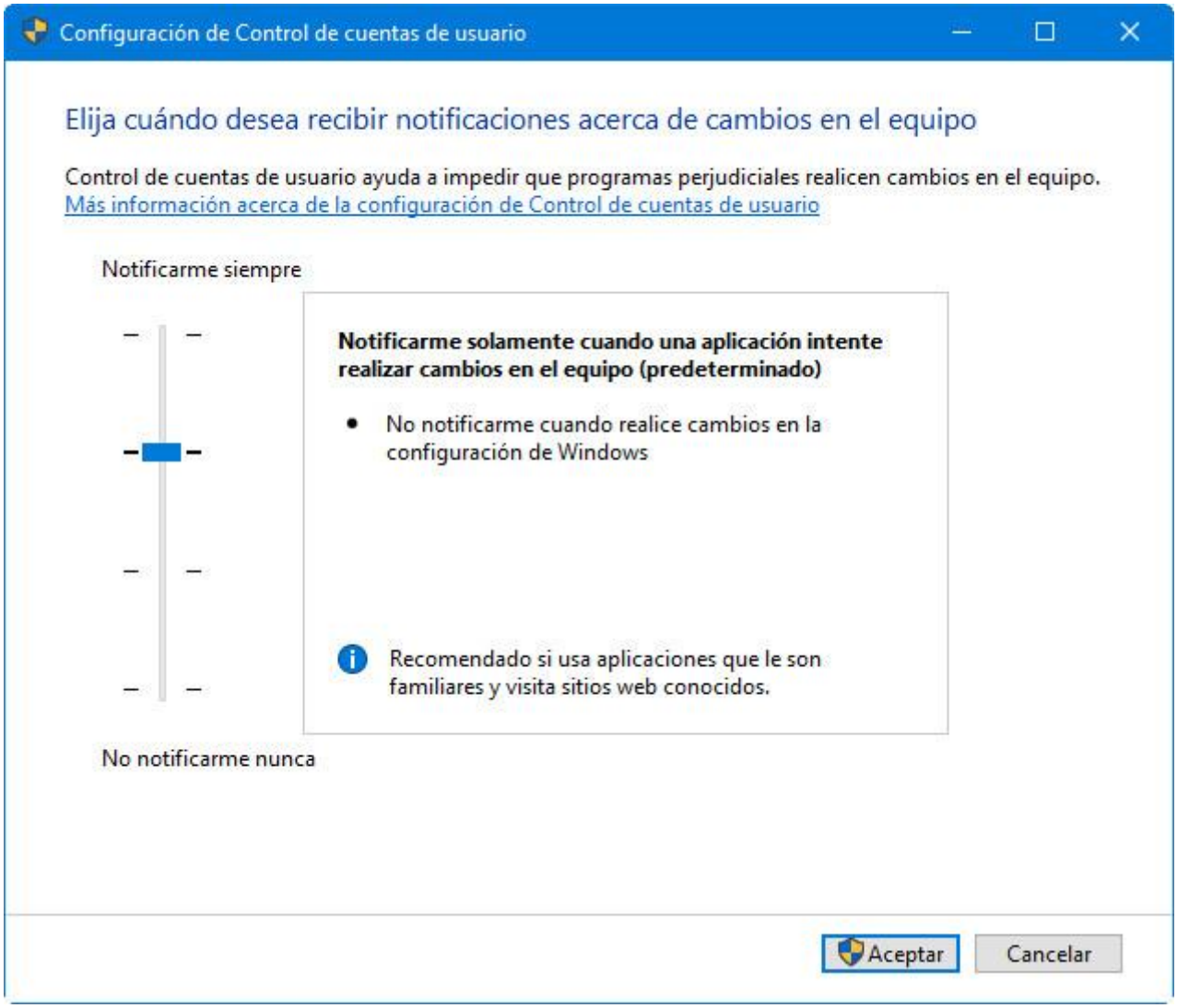
Estos permisos se otorgan solo hasta que la aplicación deja de ejecutarse o el usuario la cierra. Lo mismo ocurre con los archivos que activan una solicitud de UAC. Hay muchos cambios que requieren privilegios administrativos en Windows, dependiendo de cómo esté configurado el UAC en tu computadora puede activarse en muchas acciones:

- Ejecutando una aplicación como administrador.
- Cambios en la configuración del sistema, archivos en las carpetas de Windows o Archivos de programa.
- Instalar y desinstalar controladores y aplicaciones.
- Ver o cambiar las carpetas y archivos de otro usuario.
- Agregar o eliminar cuentas de usuario.
- Configurando la actualización de Windows.
- Cambiar la configuración del Firewall de Windows.
- Cambiar la configuración de la misma UAC.
- Cambiar el tipo de cuenta de un usuario.
- Ejecutando el Programador de Tareas.

- Restaurando archivos de sistema respaldados.
- Cambiando la fecha y hora del sistema.
- Configuración de controles parentales o seguridad.
- Instalación de controles ActiveX (en Internet Explorer).
- Etc.

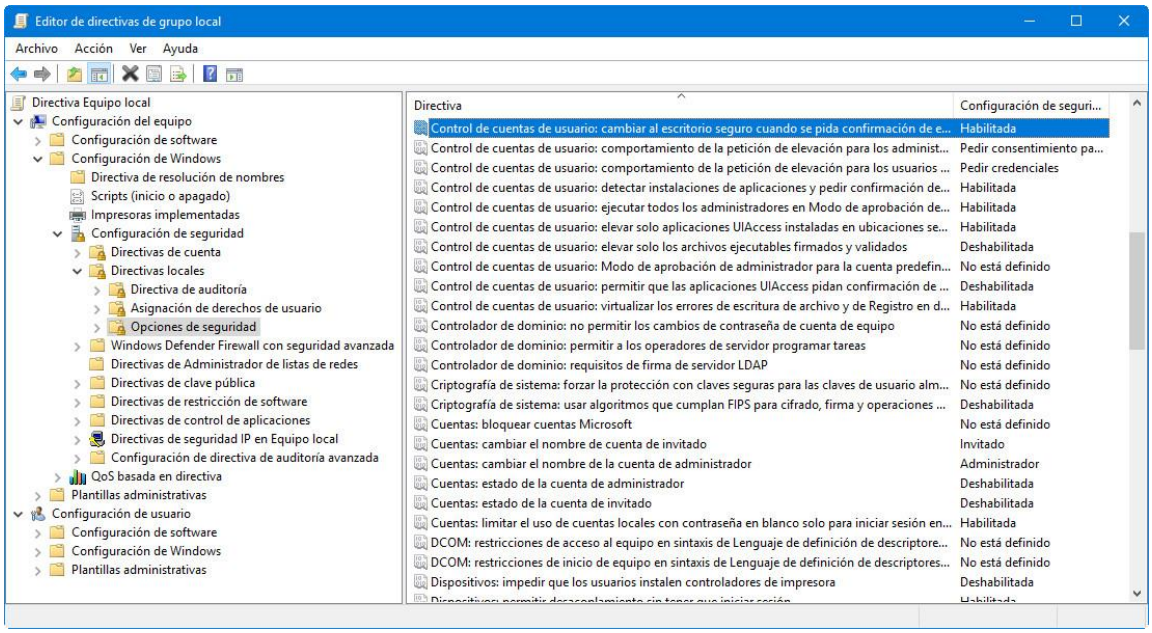
Cómo se gestiona el Control de cuentas de usuario en Windows

Hay dos maneras básicas de configurar esta función, una básica desde la configuración de usuario y otra más avanzada mediante políticas de grupo.
La gestión más sencilla se realiza accediendo al UAC desde el «Panel de control > Seguridad y mantenimiento > Cambiar configuración de Control de cuentas de usuarios». También se accede desde «ejecutar > msconfig > herramientas». Más directo es utilizar la búsqueda de Windows. En todos los casos nos encontraremos con la herramienta que ves en la imagen:



Frente al original de Windows Vista que solo ofrecía dos niveles, las versiones más recientes de Windows ofrecen cuatro niveles para elegir según el tipo de usuario y el uso del equipo. Cada nivel se explica por sí solo y va desde el deshabilitado (no recomendado) a la máxima protección donde la UAC pedirá autorización ante cualquier cambio, cuando las aplicaciones intenten instalar software o hacer cambios en el equipo y/o en la configuración de Windows.

Para usuarios avanzados y administradores la gestión más completa se realiza con el editor de políticas de grupo, accesibles desde el «Menú de Inicio > ejecutar > gpedit.msc». Una vez en el editor navega a «Configuración del Equipo > Configuración de Windows > Configuración de seguridad > Opciones de seguridad». Busca las directivas de Control de cuentas de usuario para adecuar su uso a tus necesidades. Hay una decena que puedes gestionar.



Resumiendo. El Control de cuentas de usuario en Windows (UAC) es una capa de seguridad añadida en Windows que mejora la protección del equipo ayudando a evitar cambios no autorizados en el sistema operativo. Aunque a veces sus múltiples notificaciones puedan resultar pesadas recomendamos mantenerlo activado al menos en sus niveles básicos.

Actividad:

- Básicamente, ¿En qué consiste el UAC?
- ¿De qué manera se activa el UAC?
- ¿Los archivos ejecutables pueden ser peligrosos para un Sistema Operativo?
- ¿Es útil un sistema que controle la ejecución de Software en un Sistema Operativo?
- ¿Android controla de alguna manera los cambios que se pueden realizar en el Sistema? ¿Cómo?