El control de cuenta de usuario

Windows Vista introdujo un nuevo concepto de seguridad llamado UAP o *User Account Protection* (en español, control de cuenta de usuario). También se utilizan otros términos: Least-PrivilegeUser Accounts o Limited User Accounts (LUA). Este concepto se ha conservado y mejorado en Windows 7 y en Windows 8 para que sea menos restrictivo para el usuario.

Los usuarios creados por Windows 7 tienen el status de administrador protegido, es decir, la funcionalidad UAC se activa para estas cuentas. No pasa lo mismo con la cuenta Administrador que designa de la cuenta integrada del sistema operativo pero que, por defecto, está desactivada.

Cuando un usuario tiene permisos para interactuar sin restricciones con el sistema, puede instalar un programa, escribir en la rama del registro HKEY_LOCAL_MACHINE, instalar dispositivos, iniciar servicios, etc.

En modo protegido, todos los procesos iniciados por un administrador se ejecutan con un mínimo de privilegios. Si, por ejemplo, abre un programa desde el menú **Iniciar**, el programa se ejecutará en un contexto restringido con el mismo número de permisos que los que ya tiene asignados.

Si el programa requiere de privilegios de administrador para poder ejecutarse adecuadamente, será necesario que la cuenta de administrador pueda iniciar el proceso de una manera no restrictiva. Así pues, el proceso hereda las nuevas ventajas asignadas por esta elevación de privilegios (”Over The Shoulder (OTS) elevation”). Cuando un programa se ejecuta en modo elevación de privilegios, un cuadro de diálogo le avisará de ello. No es posible elevar los privilegios asignados a una aplicación sin el consentimiento expreso del usuario. A continuación, veremos que en Windows 7 es posible desactivar la petición de confirmación del proceso de elevación de privilegios.

En Windows 7 es posible desactivar el control de cuenta de usuario, lo veremos a lo largo de este capítulo. En Windows 8, la principal modificación del control de cuenta de usuario es que el servicio queda activo incluso cuando selecciona la configuración menos segura para esta función.

1. Las cuentas de usuario

Cada vez que abre una sesión de usuario, se le asigna un token de acceso (Token). Este token contiene la lista de privilegios de que usted dispone y enumera los recursos a los que usted accede o intenta acceder. Cada recurso disponible en el sistema posee una lista de control de acceso (DACL) que contiene la lista de usuarios y servicios que pueden acceder a ella, así como el nivel de privilegios que estos poseen:

Por defecto, los administradores reciben dos tokens:

- Un token de acceso como administrador.
- Un token de acceso como usuario estándar, que es el asignado de manera predeterminada.

Durante la elevación de un proceso, un usuario recibe los mismos privilegios que los del administrador; dicho de otro modo, obtiene el mismo token de acceso. El mecanismo que le permite pasar de una identidad a otra se llama *Admin Approval Mode* (AAM).

2. Los niveles de integridad

El Control de integridad (MIC o *Mandatory Integrity Control*) es otro mecanismo creado para Windows Vista. Se le controla mediante una lista de control de acceso ACE en la lista de control de acceso del sistema (SACL) de todo objeto "asegurable" (clave de Registro, archivos, procesos, etc.).

Cada proceso tiene un nivel de integridad pero también el proceso secundario que hereda del nivel de integridad del proceso que lo ha "engendrado". Estos niveles de integridad se llaman *Integrity access levels* o IL.

Señalemos que el nivel de integridad está asociado a la SACL y no a la DACL.

Un proceso no puede interactuar con un nivel de integridad que posea privilegios más elevados. Las interfaces de programación de aplicaciones o API (*Application Programming Interface*) no tendrán éxito desde un proceso que tiene un nivel de integridad cuando se enfrente a un proceso de integridad más elevado. Esto es así para evitar los riesgos de ataques o intrusiones malintencionadas.

Las entradas del Registro pueden escribirse sólo desde un proceso con un nivel alto de integridad. Por esto mismo, Internet Explorer (un proceso de integridad bajo) sólo le permite escribir en áreas mínimas del Explorador o del Registro de Windows.

Los niveles de integridad son los siguientes:

- **High (alto)**: corresponde a los privilegios de sistema de administrador. Este nivel de privilegios le da permiso para escribir en el directorio \Archivos de programa y en la rama de Registro HKEY_LOCAL_MACHINE.
- **Medium (medio)**: corresponde al nivel de Usuario. Este nivel de privilegios le permite escribir en el directorio de usuario y en la rama de Registro HKEY_CURRENT_USER.
- **Low (bajo)**: este nivel sólo le permite escribir en las zonas sin nivel de privilegios como la clave HKEY_CURRENT_USER\Software\LowRegistry o los directorios llamados LOW, que están presentes en el Explorador de Windows. Por otra parte, una función llamada "aislamiento de privilegios en interfaz de usuario" (*User Interface Privilege Isolation* o UIPI) se utiliza para reforzar este dispositivo con el fin de prevenir ataques de tipo "shatter".

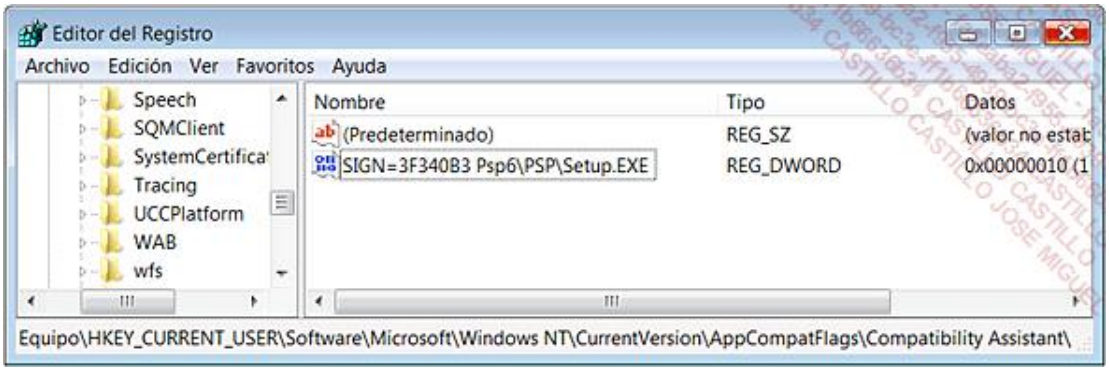
Windows 8 añade a los niveles de integridad anteriores el nivel de aislamiento **AppContainer**. Este nivel de aislamiento se utiliza por defecto para la ejecución de las aplicaciones Windows Store.

3. La elevación de privilegios

Algunas operaciones no están adaptadas para utilizar listas de control de acceso. Imaginemos que un usuario tiene la necesidad de realizar una copia de seguridad de un grupo de archivos. Es mucho más fácil darle el permiso para realizar copias de seguridad independientemente de los permisos NTFS asociados a los archivos, que modificar una a una la máscara de permisos de cada uno de los recursos a los que puede acceder. Se le puede dar una elevación de privilegios a un proceso en las siguientes circunstancias:

- Si el programa está en una plataforma de instalación como Windows Installer o Install Shield.
- Si el programa posee una entrada en la capa de compatibilidad de aplicaciones o en la base de datos de compatibilidad de aplicaciones.

En el primer caso, una entrada aparecerá en este árbol de Registro: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Persisted.



En el segundo caso, el ejecutable CompatAdmin.exe creará un archivo con la extensión *.sdb*.

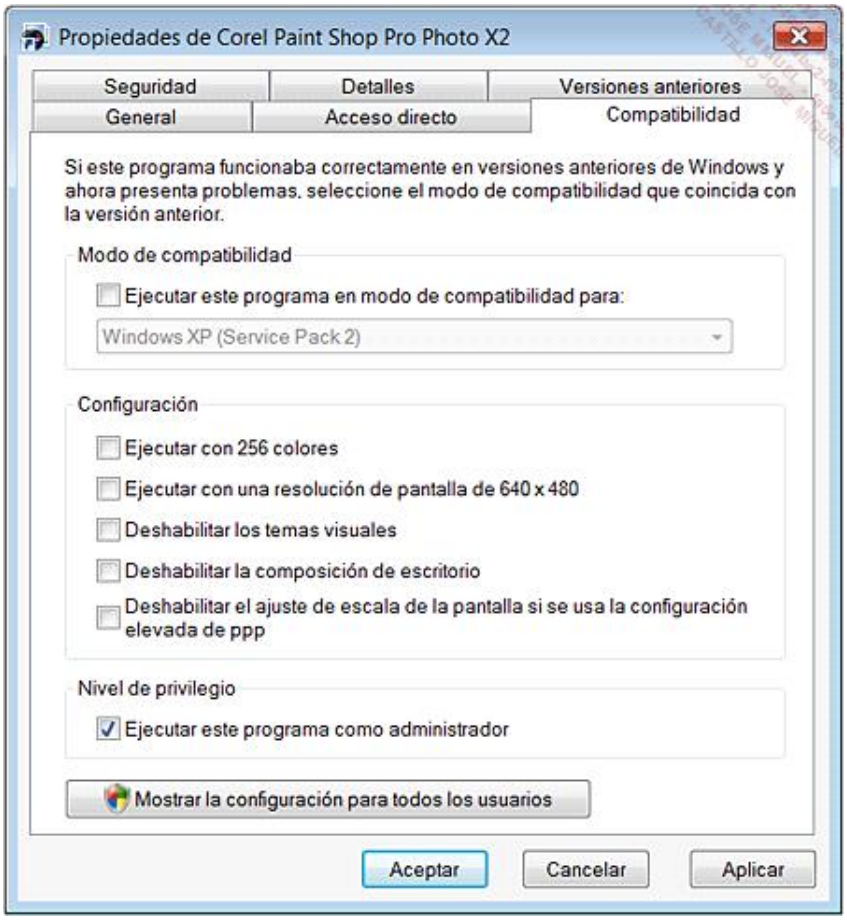
- Si el archivo manifiesto de la aplicación contiene una solicitud de nivel de ejecución que indica que la aplicación requiere un nivel de privilegios elevados.

También puede elevar los privilegios seleccionando la casilla **Ejecutar como administrador** en el menú contextual de la aplicación o acceso directo. Veamos cómo hacerlo:

- Con el botón secundario del ratón haga clic en uno de los programas existentes en el menú **Iniciar**.
- Seleccione la opción **Ejecutar como administrador**.

Para automatizar este proceso, siga el siguiente procedimiento:

- Haga clic con el botón secundario del ratón en el programa que aparece en la lista del menú **Iniciar** y, a continuación, haga clic en el submenú **Propiedades**.
- Haga clic en la pestaña **Compatibilidad** y active la casilla **Ejecutar este programa como administrador**.



Si se realiza en un acceso directo el procedimiento es un poco diferente:

- Haga clic con el botón secundario del ratón en el acceso directo y seleccione la opción **Propiedades** del menú contextual.
- Haga clic en la pestaña **Acceso directo** y en el botón **Opciones avanzadas...**.
- Active la casilla **Ejecutar como administrador**.

He aquí otra posibilidad:

- En el cuadro de texto **Iniciar búsqueda**, situado encima del menú **Iniciar**, introduzca: `cmd`.
- Haga clic con el botón secundario del ratón en la opción **cmd.exe** y en la opción **Ejecutar como administrador**.

En Windows 8, siga este procedimiento:

- Para lanzar una aplicación desde la pantalla de inicio con elevación de permisos, haga clic con el botón derecho del ratón en el icono de este programa.
- A continuación haga clic en el botón **Ejecutar como administrador** en la barra de comandos de la aplicación.

Desde ese momento todos los comandos que ejecute en el Símbolo del sistema se abrirán con permisos de administrador.

Existen otras dos situaciones que permiten una elevación de privilegios:

- Cuando un programa se ejecuta desde un proceso que ya ha recibido esta elevación de privilegios. Un buen ejemplo es el hecho de que muchas herramientas se deben lanzar desde una ventana de Símbolo de sistema en modo administrador.
- Cuando un programa se lanza desde el Administrador de tareas:

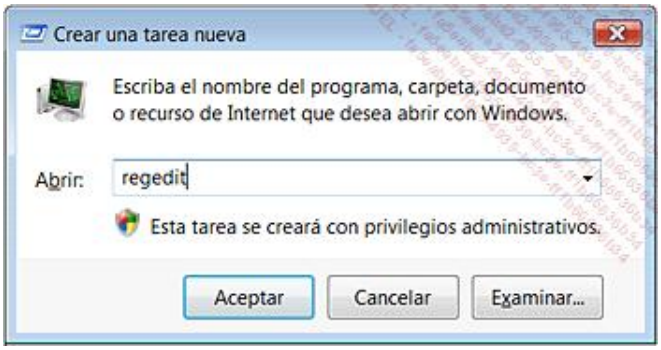
Haga clic en **Inicio - Ejecutar** e introduzca: **`taskmgr`**.

Seleccione el botón **Mostrar procesos de todos los usuarios**.

Haga clic en **Archivo - Nueva tarea (Ejecutar...)**.

Sepa que también puede hacer clic con el botón secundario del ratón en la barra de tareas y después en la opción correspondiente.

Un mensaje le señala que esta tarea se realiza con permisos de administrador.



En este caso, el Administrador de tareas inicia los procesos mediante la API CreateProcess y no CreateRestrictedProcess.

4. El proceso de virtualización

Un proceso iniciado por una cuenta de usuario estándar no puede escribir en la rama del Registro HKEY_LOCAL_MACHINE. Evidentemente, esta particularidad va a provocar problemas ya que, en muchas ocasiones, la aplicación no podrá funcionar con normalidad. Para salvar esta dificultad, Windows Vista ha creado un mecanismo llamado Virtualización. Cuando un proceso con privilegios bajos debe escribir en una zona protegida del Registro o del Explorador, los datos se transfieren de manera instantánea a una zona exclusiva del usuario. Estas zonas de "Usuario" toman la prioridad frente a las zonas de "Equipo".

Cuando un proceso no puede escribir en la rama HKEY_LOCAL_MACHINE\Software las escrituras que faltan se escriben en HKEY_CURRENT_USER\Software\Classes\VirtualStore\MACHINE\Software.

El proceso de virtualización de los archivos realiza, él mismo, este tipo de sustitución: %perfil de usuario% \AppData\Local\VirtualStore\Program Files para %Archivos de programa%, %Perfil de usuario% \AppData\Local\Virtual Store\Windows para %Windir%, etc.

Los procesos son virtuales, excepto en los casos siguientes:

- Los que son lanzados con privilegios de administrador.
- El archivo ejecutable que contiene un manifiesto llamado requestedExecutionLevel.
- Los que conciernen a las operaciones que no se inician desde una sesión interactiva.

5. El funcionamiento del control de cuentas de usuario

Cuando una aplicación no le pregunta automáticamente si desea lanzarla como administrador, es posible:

- Acceder al menú contextual del acceso directo o archivo ejecutable y hacer clic en la opción **Ejecutar como administrador**.
- Ejecutar la aplicación desde otra que haya sido ejecutada como administrador.

Cuando desde una cuenta de administrador usted abre una aplicación que necesita una elevación de privilegios, verá este tipo de cuadro de diálogo: "Windows necesita su permiso para continuar".

Desde una cuenta de usuario estándar, se le pedirá la contraseña de una cuenta con privilegios de administrador para poder continuar.

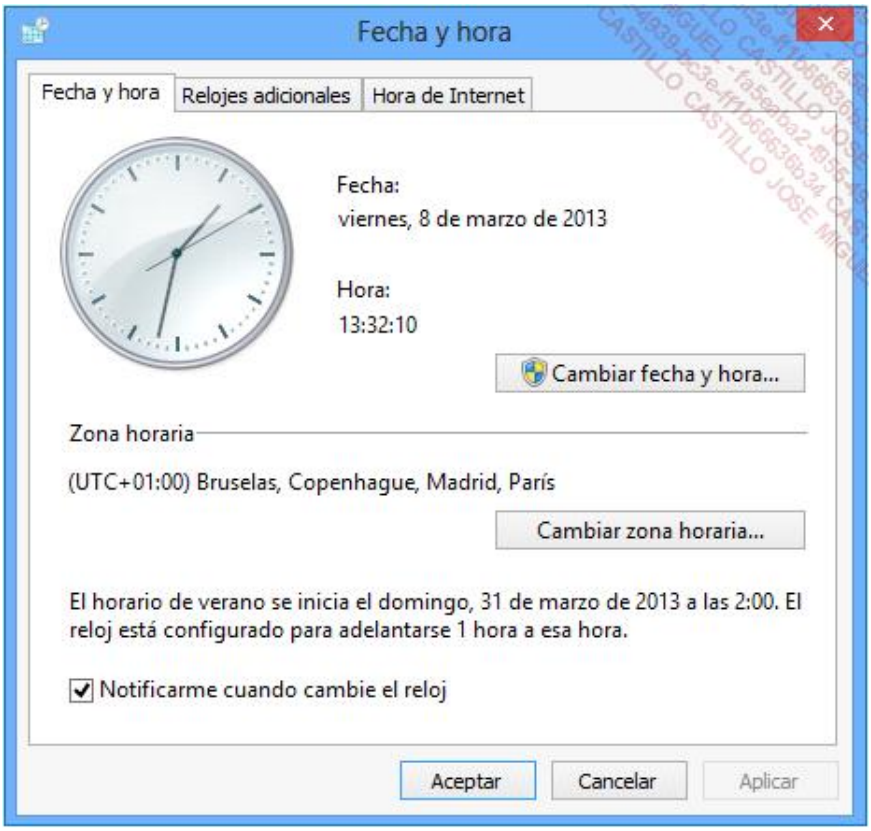
Los pasos son los siguientes:

- El sistema operativo analiza la aplicación.
- Si el editor es Windows Vista, el sistema le indicará que Windows necesita su autorización para continuar (bandera azul).
- Si el editor no es Windows Vista, pero la aplicación está firmada digitalmente, le indicará que Windows necesita su permiso para continuar (bandera gris).
- Si la aplicación no está firmada digitalmente, significa que un programa no identificado quiere acceder a su ordenador (bandera naranja).

Además, en la interfaz gráfica existe una serie de indicadores que señalan que una acción necesita una elevación de privilegios:

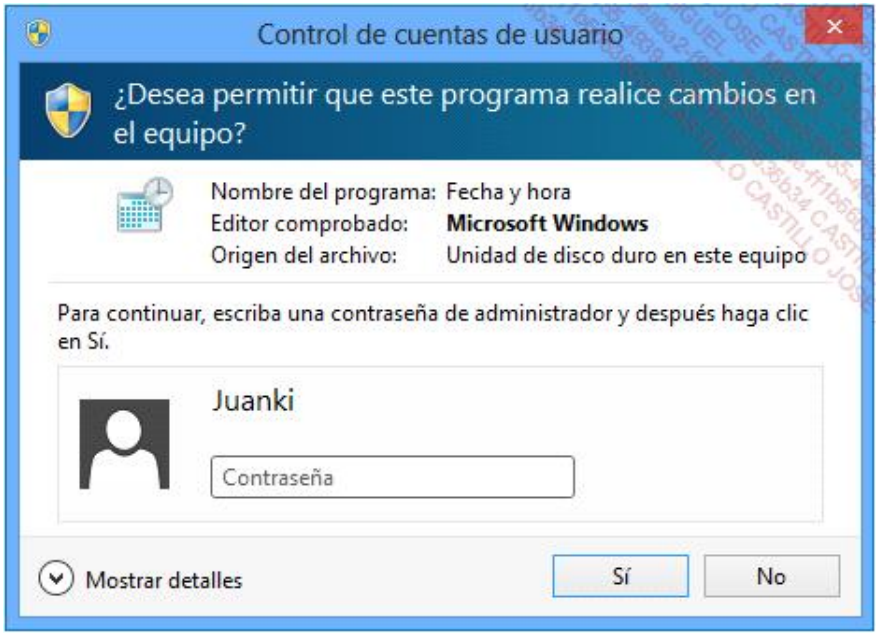
- Haga clic en el reloj situado en el área de notificación.
- Haga clic en el enlace **Cambiar la configuración de fecha y hora**.

El botón **Cambiar la fecha y hora** está acompañado del escudo del Centro de seguridad.



- Haga clic en ese botón.

Puede hacer clic en el botón **Mostrar detalles** para saber cuáles son los archivos de sistema que se ejecutarán.

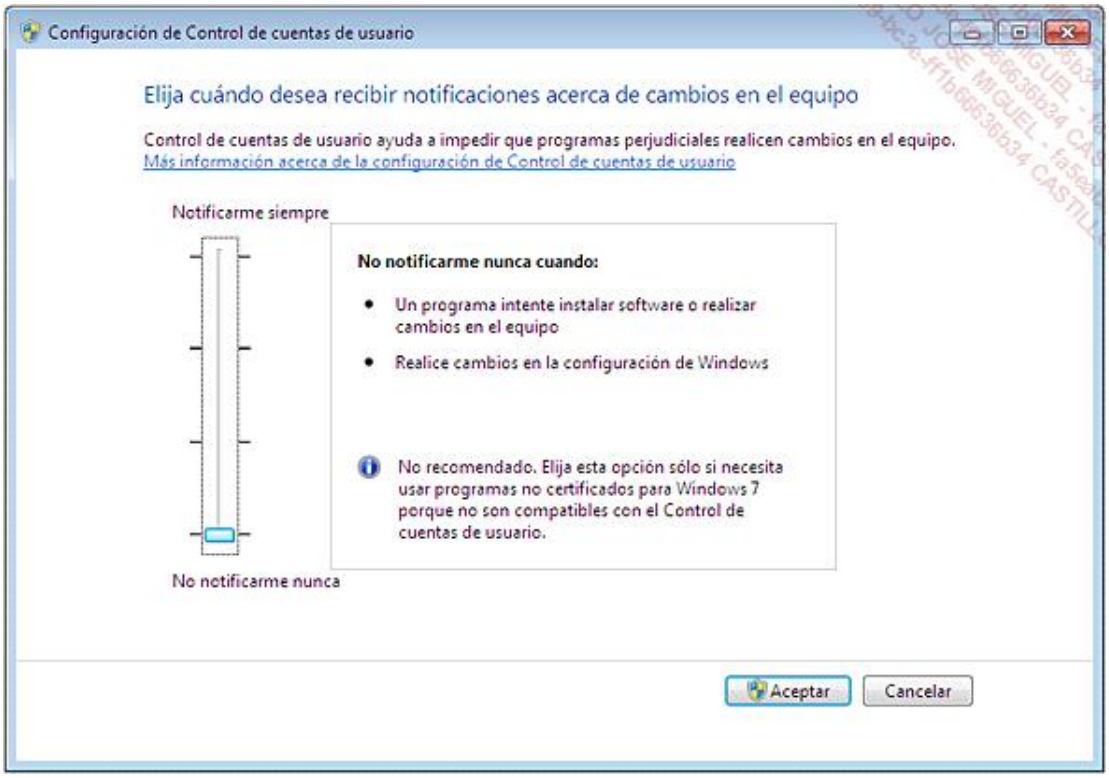


6. Desactivación del Control de cuentas de usuario

- En Windows 7, a partir del **Panel de Control**, en la sección **Cuentas de usuario y protección infantil - Cuentas de usuario**, seleccione la opción **Cambiar configuración de Control de cuentas de usuario**.

  En Windows 8, el acceso al panel de control está disponible desde el Escritorio.

- Configure la funcionalidad desplazando el cursor a la opción **No notificarme nunca**. Haga clic en el botón **Aceptar** para validar el nuevo parámetro.



Puede utilizar también la utilidad de configuración del sistema:

- En el cuadro de texto **Iniciar búsqueda** situado encima del menú **Iniciar**, introduzca: **`msconfig`**.
- Haga clic en la pestaña **Herramientas**.
- Seleccione **Desactivar el control de cuentas de usuario** y haga clic en el botón **Iniciar**.

Atención, en Windows 8, el control de cuentas de usuario no está totalmente desactivado, incluso si selecciona la opción **No notificarme nunca**. No obstante, si desea desactivarlo totalmente, debe configurar el valor EnableLUA a 0 en la clave del registro: HKEY_LOCAL_MACHINE\SOFTWARE\Windows\CurrentVersion\Policies\System.

Tenga cuidado, sin embargo, la desactivación completa del control de cuentas de usuario en Windows 8 tiene un impacto en el funcionamiento de aplicaciones de Windows Store, ya que en esos casos no se podrá lanzar ninguna aplicación.

7. Configuración del control de cuentas de usuario

A continuación, examinaremos los diferentes parámetros que tiene a su disposición mediante el Editor de objetos de directiva de grupo, para lo que deberá abrir el siguiente árbol: *Configuración del equipo/Configuración de Windows/Configuración de seguridad/Directivas locales/Opciones de seguridad*. Hemos señalado cada uno de los cambios correspondientes en el Registro, ya que el Editor de objetos de directiva de grupo no está instalado en muchas versiones de Windows.

Ejecutar todos los administradores en modo de aprobación de administrador

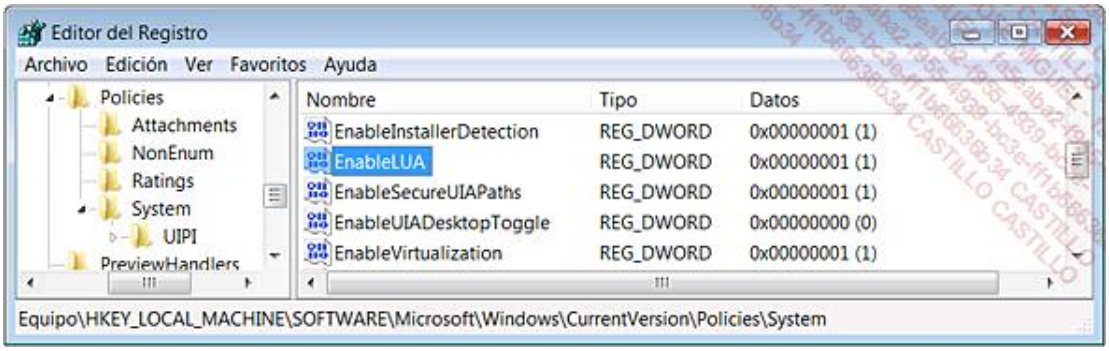
Si esta directiva está deshabilitada, el tipo de usuario del modo de aprobación de administrador y todas las demás

directivas UAC relacionadas también estarán deshabilitadas. En otras palabras, supone eliminar el Control de cuentas de usuario. Una vez desactivada la directiva, reinicie el ordenador.

- Si pulsa el botón **Aplicar**, un mensaje le indicará que la tarea se creará con permisos de administrador.
- Si abre el Centro de seguridad de Windows, un mensaje le avisará de que el control de cuentas de usuario se ha deshabilitado.

Esto corresponde a la siguiente manipulación del Registro de Windows:

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valor DWORD: EnableLUA
- Información del valor: 0.



Comportamiento del indicador de elevación para los administradores en modo de aprobación de administrador

Esta directiva le permite configurar el comportamiento del cuadro de diálogo cuando se lanza una solicitud de elevación de privilegios desde una cuenta con privilegios de administrador. En Windows 7 y 8 hay seis opciones:

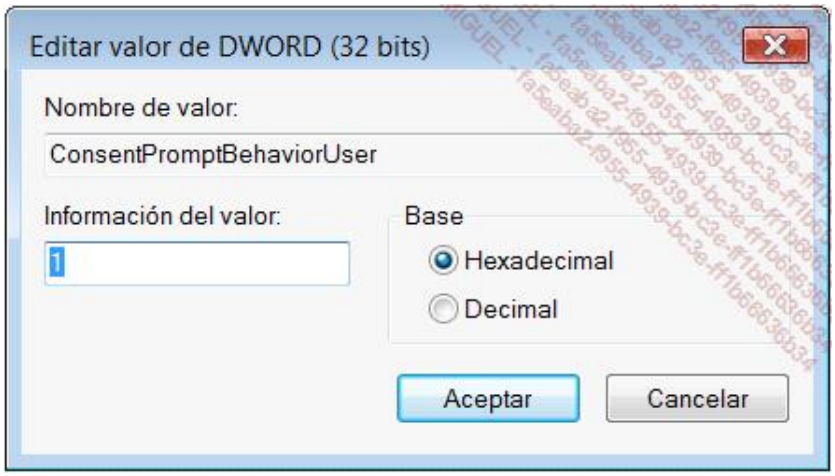
- **Petición de credenciales en el escritorio seguro**: se le pedirá al administrador en el escritorio seguro (entorno de escritorio atenuado) que introduzca su nombre de usuario y su contraseña.
- **Petición de confirmación en el escritorio seguro**: se le pedirá al administrador en el escritorio seguro (entorno de escritorio atenuado) que seleccione Autorizar o Rechazar.
- **Petición de credenciales**: se le pedirá al administrador que introduzca un nombre de usuario y una contraseña directamente en el escritorio activo.
- **Petición de confirmación**: se le pedirá al administrador que seleccione Autorizar o Rechazar en el escritorio activo.
- **Petición de confirmación para los ejecutables no Windows**: para las aplicaciones externas, se le pedirá al administrador en el escritorio seguro (entorno de escritorio atenuado) que seleccione Autorizar o Rechazar.
- **Elevar sin preguntar**: no se pedirá ninguna solicitud de confirmación al administrador. En este último caso, el Control de cuentas de usuario estará activo, pero no aparecerá ningún cuadro de diálogo que interrumpa las tareas de mantenimiento.

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valor DWORD: ConsentPromptBehaviorAdmin

Los valores posibles son:

- 0: Elevar sin preguntar
- 1: Petición de credenciales en el escritorio seguro

- 2: Petición de confirmación en el escritorio seguro
- 3: Petición de credenciales
- 4: Petición de confirmación
- 5: Petición de confirmación para los ejecutables no windows



Cambio a Escritorio seguro cuando se pida confirmación de elevación

Esta directiva determina si la solicitud de elevación se efectuará en el Escritorio de usuarios interactivos o en el Escritorio seguro. Este parámetro evita el efecto retardado cuando se realiza una petición de privilegios.

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valor DWORD: PromptOnSecureDesktop

Modo de aprobación de administrador para la cuenta de administrador integrado

Esta directiva determina el comportamiento del modo de aprobación de administrador para la cuenta de Administrador integrado. El Administrador integrado abrirá una sesión en modo de aprobación de administrador y deberá dar su consentimiento para todas las acciones que requieran una elevación de privilegios. Si esta directiva se encuentra deshabilitada, el Administrador integrado abrirá una sesión en modo Compatible con XP y podrá ejecutar todos los programas con los privilegios de administrador completos. Si utiliza a menudo la cuenta de Administrador, le resultará interesante utilizar esta directiva.

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valor DWORD: FilterAdministratorToken