

Introducción a la Ciberseguridad

Módulo 3

User Account Control

UAC (*User Account Control*)

UAC es un componente de seguridad incluido en el Sistema Operativo a partir de Windows Vista. El objetivo de **UAC (*User Account Control*)** es minimizar el uso de *privilegios de administración* por parte de los *usuarios estándar* en los equipos. De esta manera, evitamos cambios del sistema operativo que puedan dar lugar a un comportamiento no esperado.

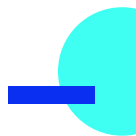
Las ventajas de trabajar con los privilegios de *usuario estándar* por defecto son reducir el número de llamadas al *help desk*, y minimizar el impacto de virus o *malware*, por ejemplo.



Funcionamiento

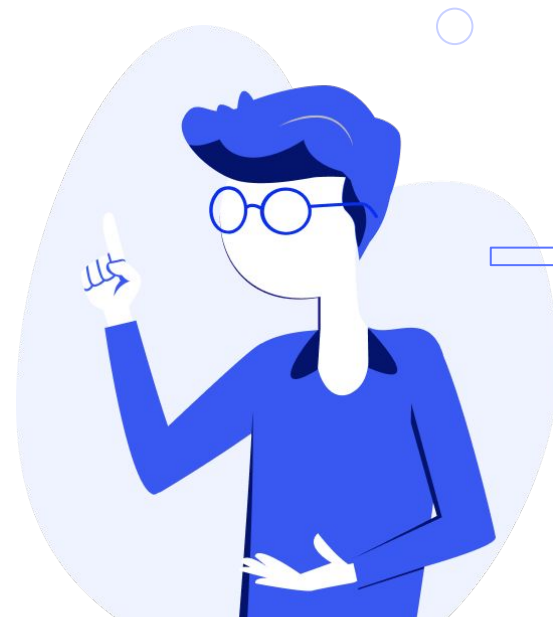
Durante el proceso de *logon* se genera el *token* de acceso del usuario. En la generación de dicho token se evalúan los *SIDs* y privilegios, de forma que si alguno se considera como *elevado*, se produce el ***split (o división) del token***. Por una parte, se genera un token para el *usuario estándar* con los *SIDs* y privilegios, y otro token *elevado* con todos los *SIDs* y privilegios del usuario. Esta funcionalidad se llama ***Protected Admin (PA)***.

Con el *Split* del token incluso los usuarios con privilegios de administración se comportan por defecto como *usuarios estándar*; si se requiere del uso de los privilegios elevados en algún momento, se presentará al usuario el aviso para usar las credenciales administrativas (es decir, el llamado ***token elevado***).



El *Split* del token se producirá siempre que:

- El **usuario** pertenece a alguno de los **grupos administrativos**: *Domain Admins, Domain Controllers, Power Users, Print Operators, etc.*
- Que el **usuario** tenga alguno de los **privilegios elevados**: *Create a token object, Act as part of the operating system, Debug Programs, Impersonate a client after authentication, etc.*



En las siguientes figuras se muestra el comportamiento de **Protected Admin**:

Administrator in Admin
Approval Mode logon



Standard user
access token



Explorer.exe

Full administrator
access token



Standard user logon



Standard user
access token

Explorer.exe

Si el usuario que ha iniciado sesión en el equipo es un **usuario estándar** y la aplicación que se está ejecutando necesita privilegios de administrador, el comportamiento por defecto es solicitar al usuario **las credenciales** para poder hacer dicha operación. Este mensaje se recibe al instalar o desinstalar una programa, abrir o cambiar la configuración del firewall, modificar la configuración de las directivas de seguridad, configurar el acceso al escritorio remoto, etc.





En el caso de los **usuarios estándar no se produce el split del token**, ya que dicha cuenta no contiene ninguno de los SIDs o privilegios mencionados antes. En el caso de los **administradores built-in** (son el administrador

del equipo y el administrador del dominio) **tampoco se produce el split del token**, debido a que estos usuarios no están protegidos por UAC.

Cuatro tipos de notificaciones de UAC

Cuando es necesario un permiso o una contraseña para completar una tarea, **UAC nos advierte** con uno de los **cuatro tipos de cuadro de diálogo** que se describen en la tabla de la siguiente slide. Se detallan los distintos tipos de cuadro de diálogo que aparecen como notificación y las instrucciones para responder a las notificaciones.

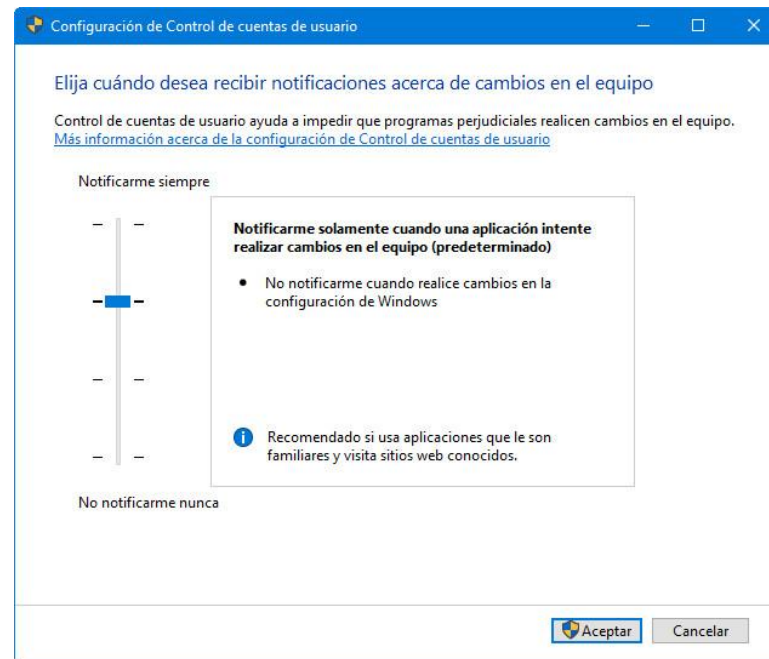


Icono	Tipo	Descripción
	Una opción o característica que forma parte de Windows.	Este elemento tiene una firma digital válida que permite comprobar que su editor es Microsoft. Si aparece este tipo de cuadro de diálogo, normalmente resulta seguro continuar.
	Un programa que no forma parte de Windows.	Este programa tiene una firma digital válida, que ayuda a garantizar que es genuino y permite comprobar la identidad del editor del programa.
	Un programa con un editor que resulta desconocido.	Este programa no tiene una firma digital válida de su editor. Esto no significa necesariamente que haya un peligro, dado que muchos programas legítimos más antiguos no tienen firmas digitales.
	El administrador del sistema ha bloqueado este programa para que no pueda ejecutarlo.	Este programa ha sido bloqueado porque se sabe que no es de confianza.

Configuración

Para abrir **Configuración del Control de cuentas de usuario**, hacemos clic en el botón **Inicio** y, a continuación, hacemos clic en **Panel de control**. En el cuadro de búsqueda, escribimos **uac** y, luego, hacemos clic en **Cambiar configuración de Control de cuentas de usuario**.

A continuación se ofrece una descripción de la configuración de **UAC** y el posible impacto de cada configuración en la seguridad del equipo.



Notificarme siempre

Esta es **la configuración más segura**. Se nos notificará antes de que los programas realicen cambios al equipo o a la configuración de Windows, que requieran los permisos de un administrador.

Cuando se nos notifique, el escritorio aparecerá atenuado y deberá **aprobar o denegar la solicitud en el cuadro de diálogo de UAC** antes de poder realizar cualquier acción en el equipo.



La atenuación del escritorio se denomina **escritorio seguro**, porque no se pueden ejecutar otros programas si está atenuado.



Por cambios en el equipo

- Se nos notificará antes de que los programas hagan cambios al equipo que requieren permisos de administrador.
- No recibirás notificaciones si intentas hacer cambios en la configuración de Windows que requieren permisos de administrador.
- Se nos notificará si un programa fuera de Windows intenta realizar cambios en la configuración de Windows.

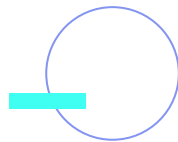
Por lo general es seguro permitir que se realicen cambios en la configuración Windows sin que se nos notifique. Sin embargo, determinados programas incluidos con Windows pueden recibir comandos o datos. El software malintencionado se aprovecha de esta situación y usa estos programas para instalar archivos o cambiar la configuración del equipo. **Deberemos tener siempre cuidado a la hora de permitir los programas que se pueden ejecutar en el equipo.**



Por cambios en el equipo (no atenuar escritorio)

- Se nos notificará antes de que los programas realicen cambios en el equipo que requieran permisos de administrador.
- No se nos notificará si intenta realizar cambios en la configuración de Windows que requieran permisos de administrador.
- Se nos notificará si un programa que se encuentra fuera de Windows intenta realizar cambios en una configuración de Windows.

Debido a que el **cuadro de diálogo de UAC no se encuentra en el escritorio seguro** con esta configuración, es posible que otros programas puedan interferir con el aspecto visual del diálogo. Esto supone un **pequeño riesgo para la seguridad** si ya tiene un programa malintencionado ejecutándose en el equipo.



Nunca

- No se nos notificará antes de que se realicen cambios en el equipo. Si has iniciado sesión como administrador, los programas pueden hacer cambios en el equipo sin que lo sepas.
- Si hemos iniciado sesión como *usuario estándar*, se denegará automáticamente los cambios que requieran permisos de administrador.
- En esta opción, **UAC queda desactivado y no protege el equipo, lo que puede suponer un riesgo importante para la seguridad.**



**¡Sigamos
trabajando!**