

Protección de los puestos de trabajo con Windows 10

Con la llegada de las interconexiones entre redes privadas y públicas, cada vez más empresas abren sus sistemas de información a sus socios comerciales.

Se hace entonces primordial conocer los recursos críticos y proteger los puestos de trabajo fijos y móviles de los colaboradores de la empresa.

Cuando el administrador desea desplegar una arquitectura segura debe, en primer lugar, conocer las fuerzas en juego, evaluando sus propias competencias, redactar un documento detallado del **Sistema de Información** (SI) y controlar el soporte organizacional. La segunda etapa consiste en olvidar los estereotipos para ponerse en el lugar del atacante, intentando conocer sus motivaciones: un empleado descontento, espionaje para obtener beneficios financieros, la respuesta a un reto, etc.

El administrador de seguridad debe defender todos los puntos de su SI manteniéndose siempre alerta, ya que el atacante puede seleccionar el punto menos fiable y atacar cuando lo desee. Las diferentes redes deben estar controladas y ser seguras: la red local, la red de área extensa y los socios profesionales de tipo extranet, con el fin de protegerse de espionajes de red, de suplantaciones de identidad o modificaciones.

El sistema Windows 10 posee las mismas bases de seguridad que Windows 7, como el control de acceso de usuarios o el **Centro de actividades**, pero aporta mejoras en las características **AppLocker** y **BitLocker**.

Dos novedades vinculadas a la seguridad de los datos hacen su aparición: Credential Guard y Device Guard.

Además, la funcionalidad de EDP (*Enterprise Data Protection*), junto con RMS (*Rights Management Services*), permite proteger los datos locales de la empresa, incluso cuando se convierten en itinerantes.

El administrador puede crear una directiva de grupo de protección con cuatro niveles para la funcionalidad EDP:

- Bloquear: si un recurso compartido no autorizado es detectado, el empleado verá rechazada su acción.
- Remplazar: se informa al empleado de un recurso compartido no apropiado pero puede seleccionar el reemplazo de la directiva aplicada.
- Audit: EDP registra los recursos compartidos no apropiados sin prohibirlos.
- Desactivada: la funcionalidad EDP no se activa y no protege los datos empresariales.

En todo momento, un empleado puede cambiar el estado de un documento EDP a un documento personal. Esta acción será siempre auditada y registrada para que el administrador pueda validarla.

Observe que EDP requiere un puesto de trabajo con Windows 10 Enterprise e Intune para la gestión del parque informático.

La autenticación por huella digital, iris o reconocimiento facial del usuario se encuentra integrada (consultar el capítulo Instalación del cliente Windows 10 - Autenticación) en el sistema operativo, y permite proveerse de controladores o aplicaciones suministradas por los fabricantes. Además, la compra de apps en la Tienda de Windows se gestiona, al igual que la apertura de sesión por este mecanismo, en un dominio Active Directory.

1. Control de cuentas de usuario

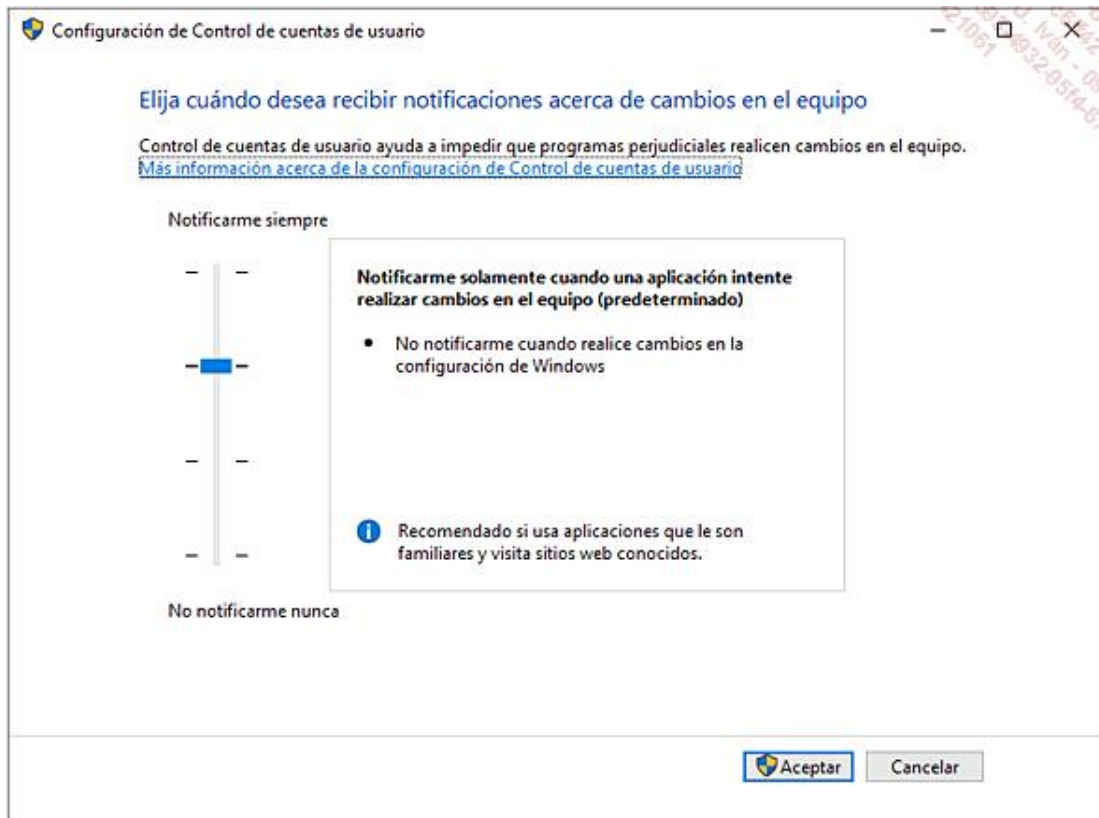
El **UAC** (*User Account Control*) es una característica de seguridad cuya finalidad es enmarcar las operaciones sensibles presentando a un usuario estándar la posibilidad de elevar su situación, hasta ser administrador durante la ejecución de una tarea específica. Disponible desde Windows Vista, el UAC fue muy criticado por la ralentización que inducía en el cumplimiento de tareas corrientes. Con Windows 7 y Windows 8.1, muchas solicitudes de control

fueron suprimidas y los parámetros de configuración se han extendido a cuatro niveles modulares.

Cuando aparece un escudo amarillo y azul al lado de un parámetro, significa que el sistema Windows 10 requiere que el usuario actual tenga privilegios de administrador para poder acceder a él, por lo que deberá aumentar temporalmente su nivel de acceso. Sin embargo, un usuario puede emprender un gran número de acciones sin necesidad de aumentar sus privilegios, como por ejemplo la instalación de actualizaciones de seguridad, la configuración de parámetros de red, la personalización del ordenador (fondo de pantalla, tema, etc.) o la restauración de archivos guardados. A veces, el usuario podrá visualizar parámetros, como las reglas creadas en el firewall, pero su modificación necesitará aumentar los privilegios.

Para configurar el UAC, es necesario autenticarse empleando una cuenta de administrador local en el sistema Windows 10:

→ Introduzca **control** en la zona de búsqueda situada en la barra de tareas, y seleccione **Cambiar configuración de Control de cuentas de usuario**.

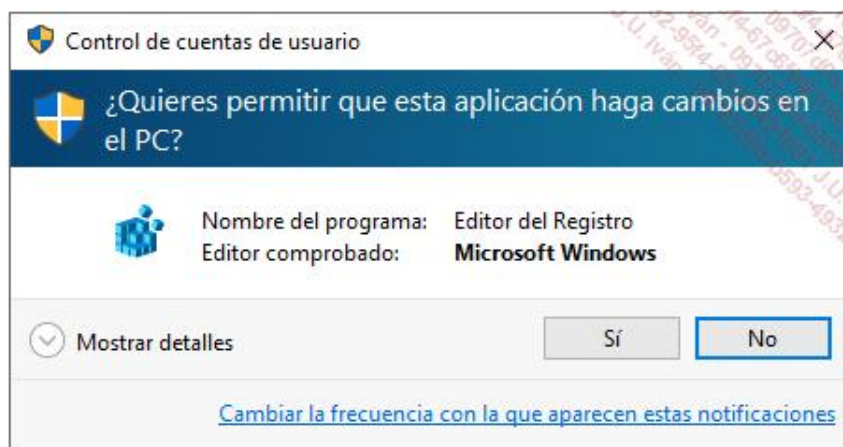


Puede configurar el UAC desplazando el cursor de acuerdo con cuatro niveles:

- **Notificarme siempre:** es el nivel de advertencia más sensible, el usuario recibirá un mensaje si los programas o él mismo intentan modificar parámetros sensibles de Windows.
- **Notificarme solamente cuando una aplicación intente realizar cambios en el equipo (predeterminado):** nivel predeterminado, que no muestra mensajes cuando es el usuario quien modifica los parámetros.
- **Notificarme solamente cuando una aplicación intente realizar cambios en el equipo (no atenuar el escritorio):** mismo parámetro que el anterior, con la excepción de que el cuadro de diálogo no atenuará el escritorio. El usuario podrá de esta forma ignorar fácilmente los mensajes.
- **No notificarme nunca:** es el nivel más bajo y el menos seguro, no se mostrará ningún mensaje si una aplicación procede a realizar modificaciones. Si el usuario actual utiliza una cuenta sin nivel de administrador, todo cambio que necesite privilegios de administrador será prohibido.

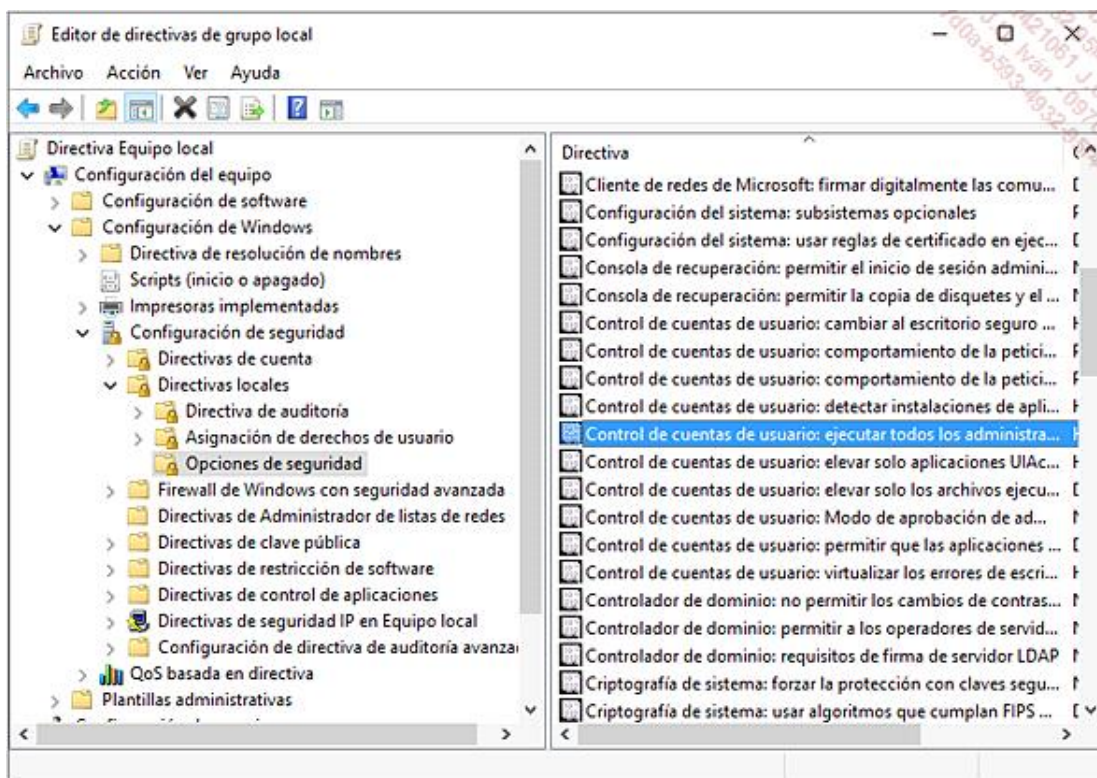
Haciendo clic en el botón **Aceptar**, el usuario debe aumentar sus privilegios para convertirse en administrador local

del puesto con Windows 10, mediante la ventana de validación **Control de cuentas de usuario**:



En un dominio Active Directory, el administrador puede configurar el comportamiento del UAC en los puestos cliente empleando un objeto de directiva de grupo. Es, así, posible configurar el comportamiento del sistema durante la instalación de aplicaciones, como con el parámetro **Detectar instalaciones de aplicaciones y pedir confirmación de elevación**, o el parámetro **eleva solo los archivos ejecutables firmados y validados**.

Para configurar el UAC en un dominio, basta con editar el objeto de directiva de grupo **Directivas de dominio predeterminado** y, a continuación, desplegar el nodo **Configuración del equipo - Directivas - Configuración de Windows - Configuración de seguridad - Directivas locales y Opciones de seguridad**. Localice los parámetros que comienzan con **Control de cuentas de usuario**.




- Estos parámetros pueden configurarse localmente en el sistema Windows 10 mediante el Editor de directivas de grupo local (gpedit.msc), como muestra la imagen anterior.

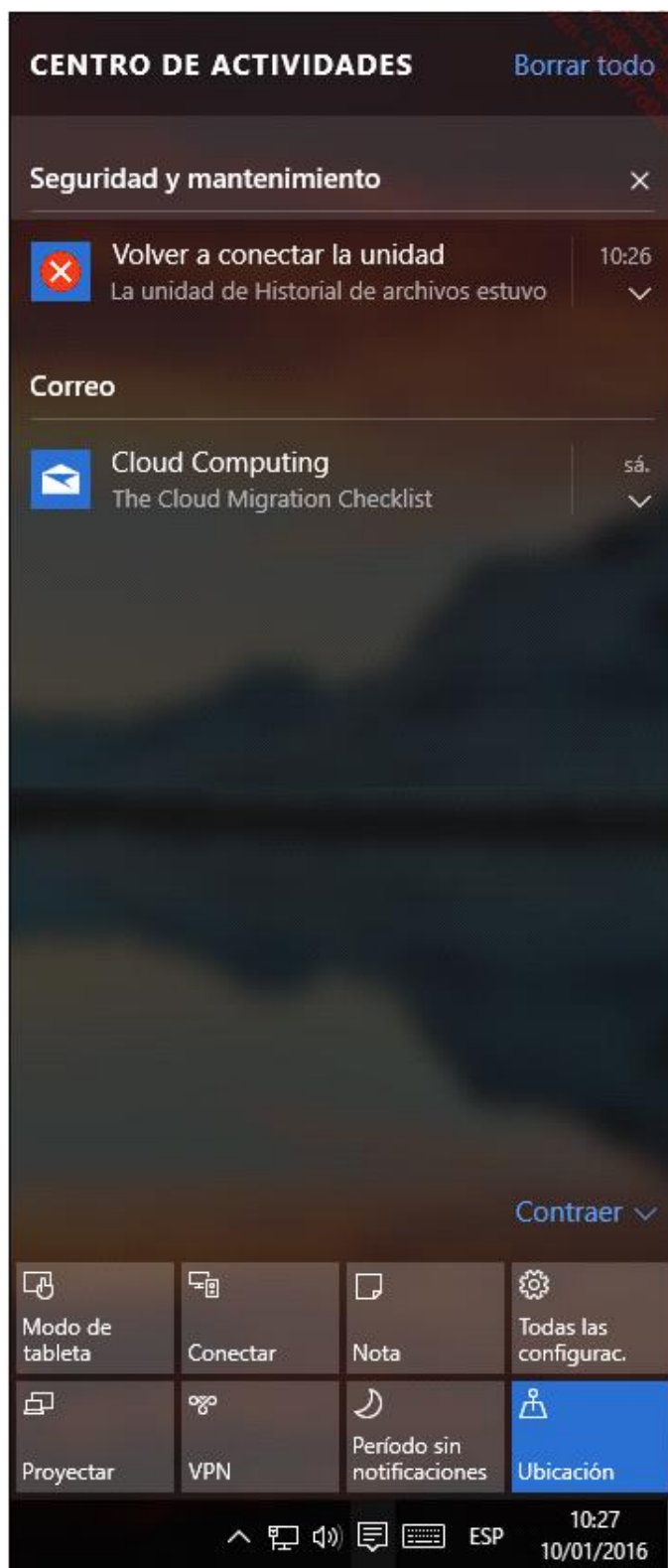
El UAC contribuye a impedir que programas malintencionados del tipo virus y troyanos se instalen en el puesto con

Windows 10 restringiendo el uso de privilegios aumentados y controlando los archivos de instalación (ActiveX, Windows Installer, etc.), el registro y muchos otros parámetros críticos del sistema.

2. Centro de actividades

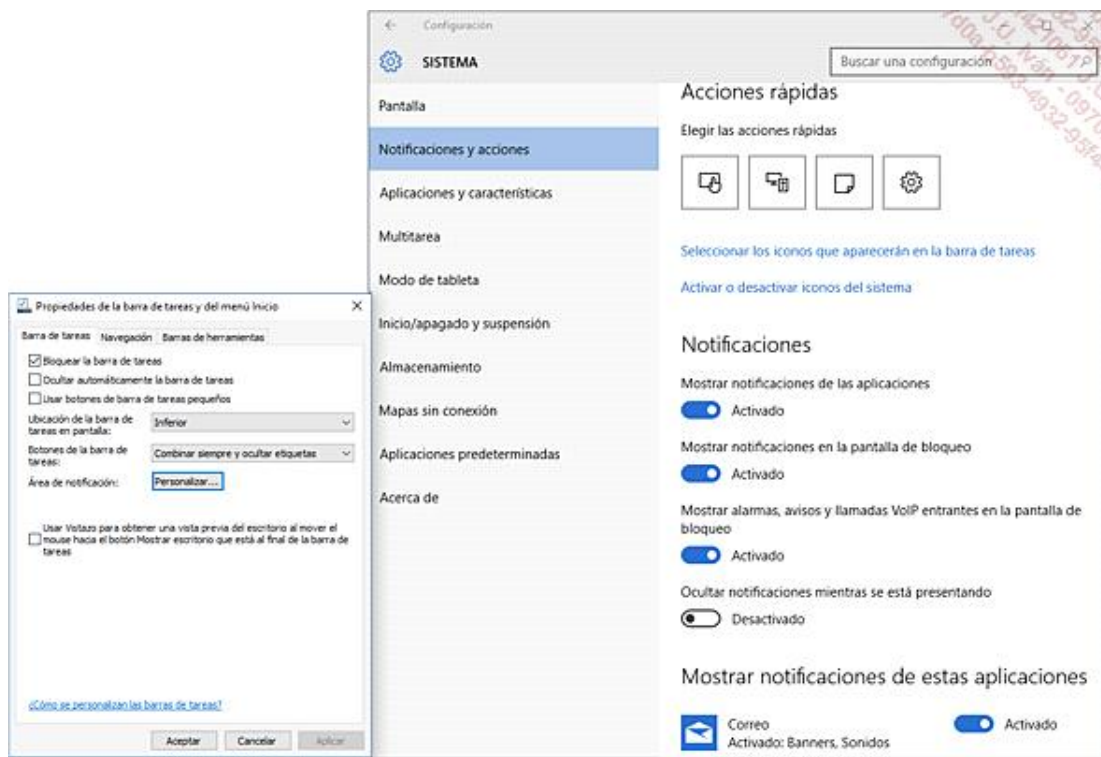
El Centro de actividades muestra en una vista centralizada las alertas recientes relativas a la seguridad del cliente Windows 10, así como parámetros importantes (red, ubicación, VPN, etc.) vinculados al sistema.

Se supervisan los parámetros de seguridad, como el estado del firewall, la aplicación de actualizaciones de seguridad, las definiciones de virus o el mantenimiento del equipo. Los mensajes de aviso se muestran en la zona de notificación situada abajo a la derecha de la pantalla del escritorio, en la barra de tareas, encima del icono , tal y como muestra la siguiente imagen:



El estado de alerta cambia en función de la criticidad del evento (una notificación importante se señala, por ejemplo, mediante una cruz blanca con un fondo rojo, como en la imagen anterior).

El centro de actividades es personalizable haciendo clic con el botón derecho en la barra de tareas, **Propiedades**. En la pestaña **Barra de tareas**, haga clic en el botón **Personalizar...**:

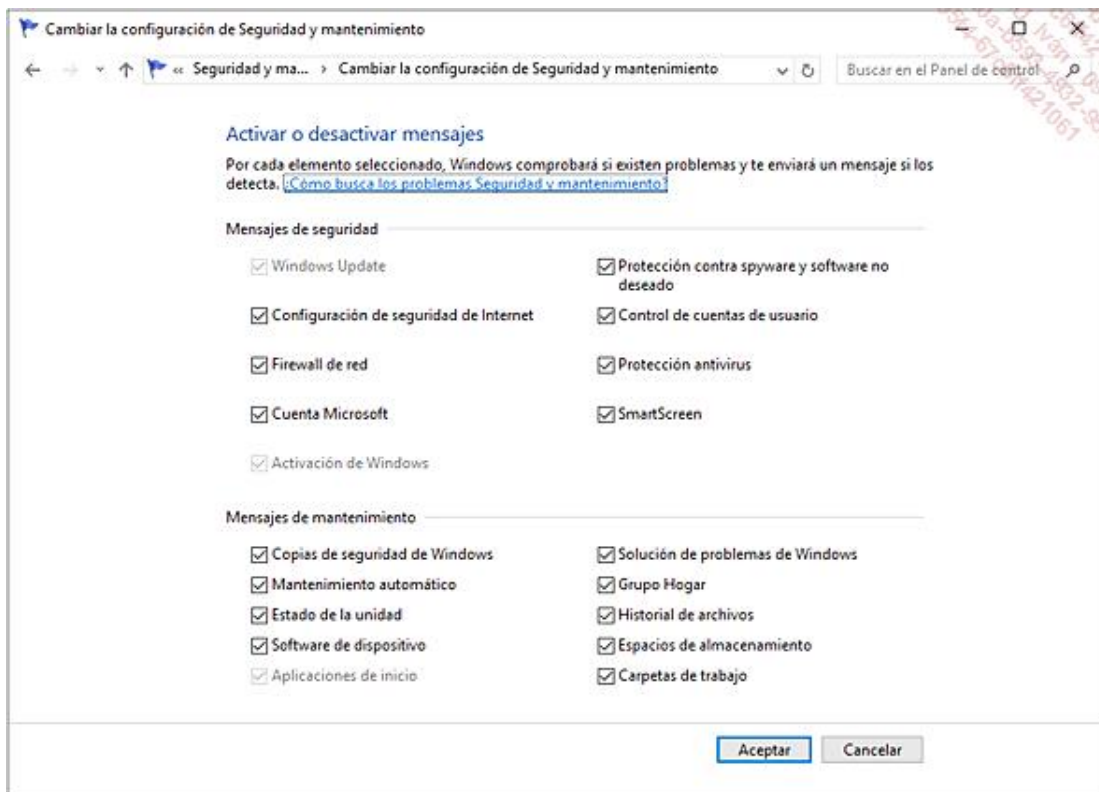


El usuario puede, por ejemplo, desactivar las notificaciones provenientes de aplicaciones específicas.

Podemos configurar otros parámetros, como la toma de notas (empleando de OneNote) o la activación del modo de tableta al utilizar una pantalla táctil.

El Centro de actividades es, pues, una herramienta que muestra el conjunto de parámetros de seguridad propios de Windows 10 en una vista única.

Si queremos que no se muestren otras categorías de mensajes, bastará con que el administrador haga clic en **Seguridad y mantenimiento** desde el **Panel de control** y seleccione los mensajes de mantenimiento o seguridad gestionados por Windows 10.



3. Cifrado de archivos

La criptografía es una ciencia que permite convertir información comprensible en información codificada con el fin de ocultar el contenido para protegerlo. El cifrado es el procedimiento utilizado para hacer incomprensible la información mientras no se conozca la clave de descifrado.

Existen dos tipos principales de cifrado:

- Simétrico: una clave única permite cifrar y descifrar un mensaje.
- Asimétrico: emplea dos claves, la clave privada, que se mantiene en secreto, descifra la información, mientras que la clave pública, proporcionada por ejemplo a un corresponsal, sirve para el cifrado de la información por su parte.

Windows 10 utiliza estos dos tipos de cifrado para proteger los datos personales del usuario.

a. Sistema EFS

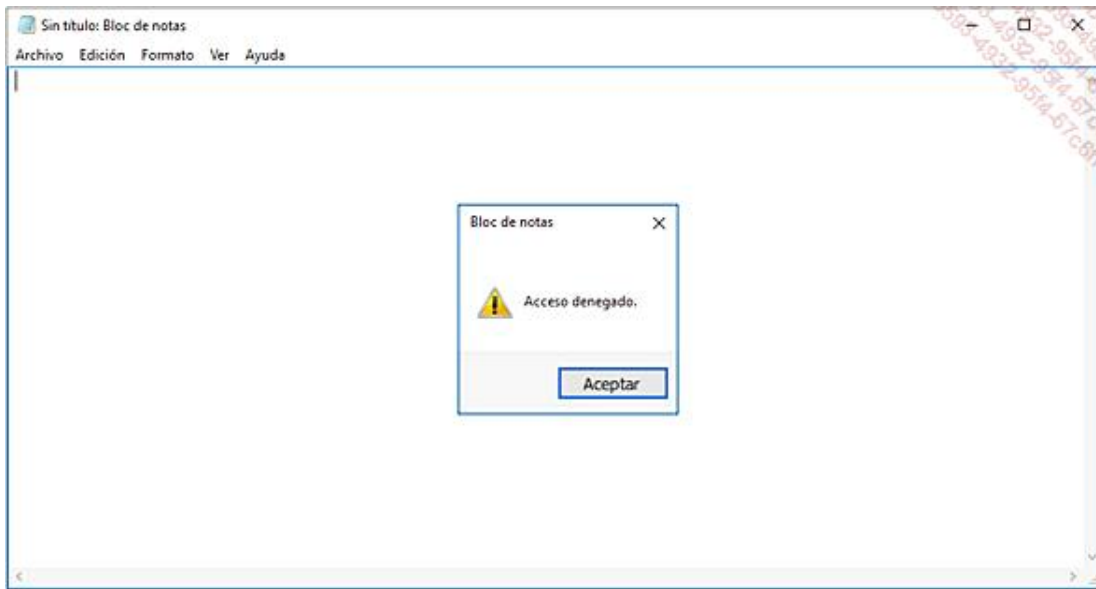
EFS (*Encrypting File System*) cifra los archivos seleccionados de forma transparente en una partición NTFS. Disponible desde Windows 2000, este sistema permite compartir un archivo cifrado añadiendo los certificados EFS de los usuarios que necesiten acceder a él.

Basado en un cifrado de clave pública, EFS puede cifrar una carpeta y todos los archivos que contiene sin solicitar una contraseña al usuario: la clave de cifrado está basada en la cuenta y la contraseña asociada a ella. En caso de copiar o mover un archivo cifrado a una partición FAT, este perderá su condición de cifrado.

EFS utiliza una clave simétrica que está, también, cifrada utilizando la clave pública del usuario. Un certificado, basado en las claves pública y privada de aquel (cifrado asimétrico), se almacena en su perfil.

Si un usuario no cuenta con la clave de descifrado durante la apertura de un archivo cifrado, aparecerá el mensaje

"Acceso denegado".



El par de claves pública y privada, válidas durante 100 años, está protegido por la contraseña del usuario. Esta puede generarse por una autoridad de certificación o por el puesto con Windows 10.

Un ataque por fuerza bruta sobre la contraseña de la cuenta podría comprometer el acceso a los archivos cifrados. Por tanto, cuanto más compleja sea la contraseña de inicio de sesión, mejor será la protección de los archivos cifrados.



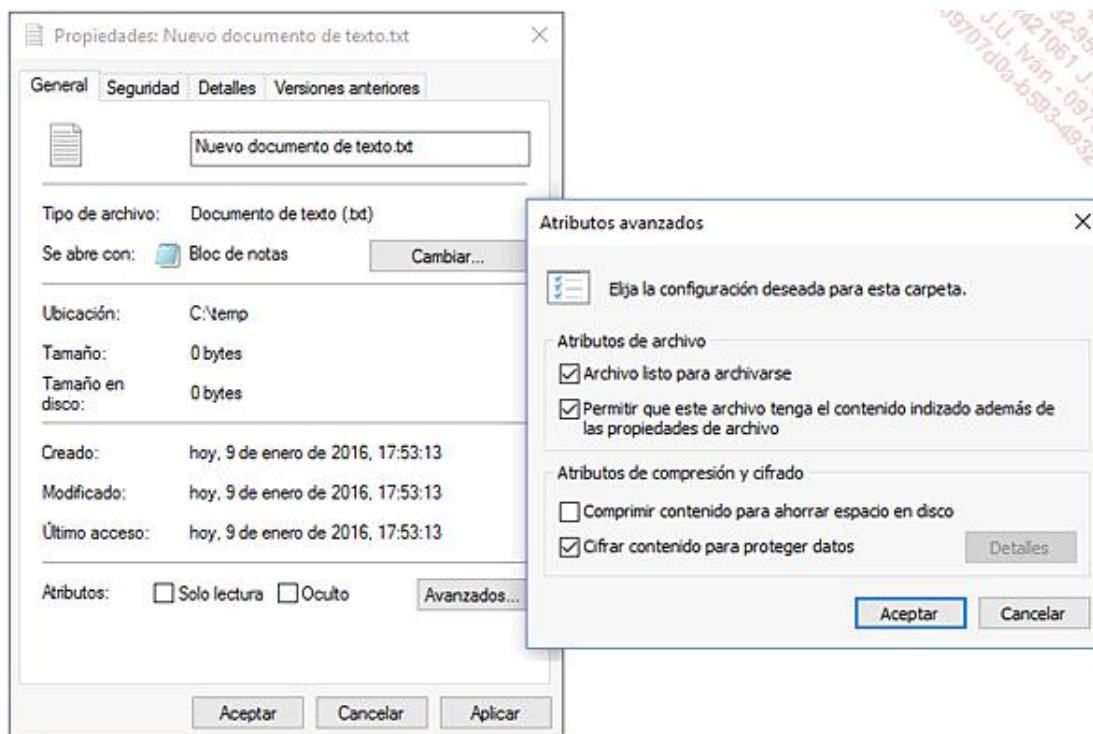
Durante el acceso a un archivo cifrado almacenado en una carpeta compartida, este será descifrado durante la transferencia de los datos. Las claves de cifrado están disponibles en el servidor de archivos.

Por defecto, la funcionalidad EFS utiliza el algoritmo de cifrado AES (*Advanced Encryption Standard*) de 256 bits.

Windows 10 soporta el almacenamiento de claves privadas en tarjetas inteligentes, el cifrado del archivo de paginación y los archivos sin conexión, e incluye un asistente de gestión de certificados por EFS.

Para cifrar un archivo almacenado en una partición NTFS:

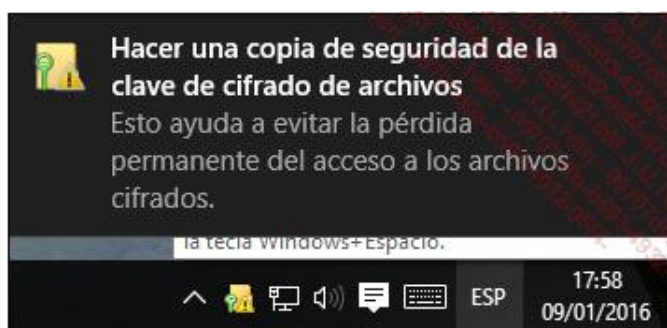
- Haga clic con el botón derecho en el archivo que desee cifrar y, a continuación, seleccione **Propiedades**. Haga clic en el botón **Avanzados** y marque la opción **Cifrar contenido para proteger datos**.



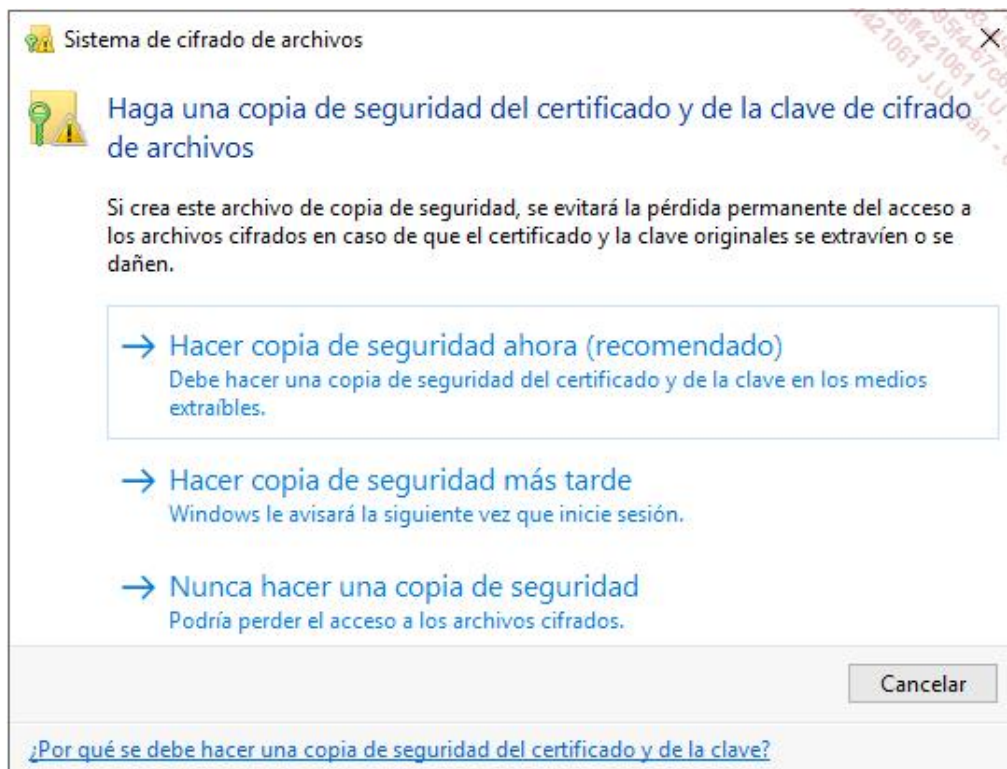
- Observe que no puede cifrar y comprimir un archivo al mismo tiempo, aunque el tipo de casilla de selección parezca sugerir lo contrario.

Una vez cifrado el archivo, el botón **Detalles** no aparecerá en gris; el usuario podrá, así, agregar los certificados de usuarios (no de grupos) locales o miembros de un dominio para los que desea autorizar el acceso al documento.

La primera vez que se cifra un archivo, Windows 10 propone guardar la clave y el certificado de cifrado y muestra un mensaje en la barra de tareas del escritorio, abajo a la derecha.



Haciendo clic en el mensaje se ejecuta la ventana del asistente **Sistema de cifrado de archivos**. El usuario puede optar por **Hacer copia de seguridad ahora** en formato PKCS#12 (*Public Key Cryptographic Standards*) (.PFX), **Hacer copia de seguridad más tarde** o **Nunca hacer una copia de seguridad** de la clave y el certificado.



- ➔ Es aconsejable almacenar la clave y el certificado en un medio extraíble o una carpeta compartida segura porque, en caso de pérdida, los datos cifrados no podrán descifrarse.

El administrador también puede exportar sus certificados críticos desde el complemento **Certificados (almacén Personal)**.

El asistente Sistema de cifrado de archivos EFS llamado **rekeywiz** permite gestionar los certificados de cifrado de archivo para los usuarios de un puesto de trabajo con Windows 10: crear un nuevo certificado, realizar una copia de seguridad de este para evitar la pérdida de acceso definitiva a los archivos cifrados o también configurar EFS con una tarjeta inteligente.

Para ejecutar el asistente:

- ➔ Pulse las teclas **Win** y **R**. Introduzca **rekeywiz** en la ventana **Ejecutar** y confirme con la tecla [Intro].
- ➔ En la ventana **Sistema de cifrado de archivos**, haga clic en el botón **Siguiente**.
- ➔ Marque la opción correspondiente a sus necesidades: **Usar este certificado** o **Crear un nuevo certificado** y, a continuación, haga clic en el botón **Siguiente**. En nuestro ejemplo vamos a utilizar un certificado existente. Seleccione **Hacer copia de seguridad del certificado y la clave ahora** en un archivo con la extensión .pfx (PKCS#12) y defina una **Contraseña**.


- Pase a la siguiente etapa haciendo clic en **Siguiente**.
- Puede aplicar la nueva clave generada actualizando los archivos cifrados. Confirme haciendo clic en el botón **Siguiente**. Termine el asistente haciendo clic en el botón **Cerrar**.

El comando **cipher** muestra y modifica el cifrado de los archivos almacenados en una partición NTFS. El parámetro **REKEY** actualiza todos los archivos cifrados para los que se utiliza la clave EFS configurada.

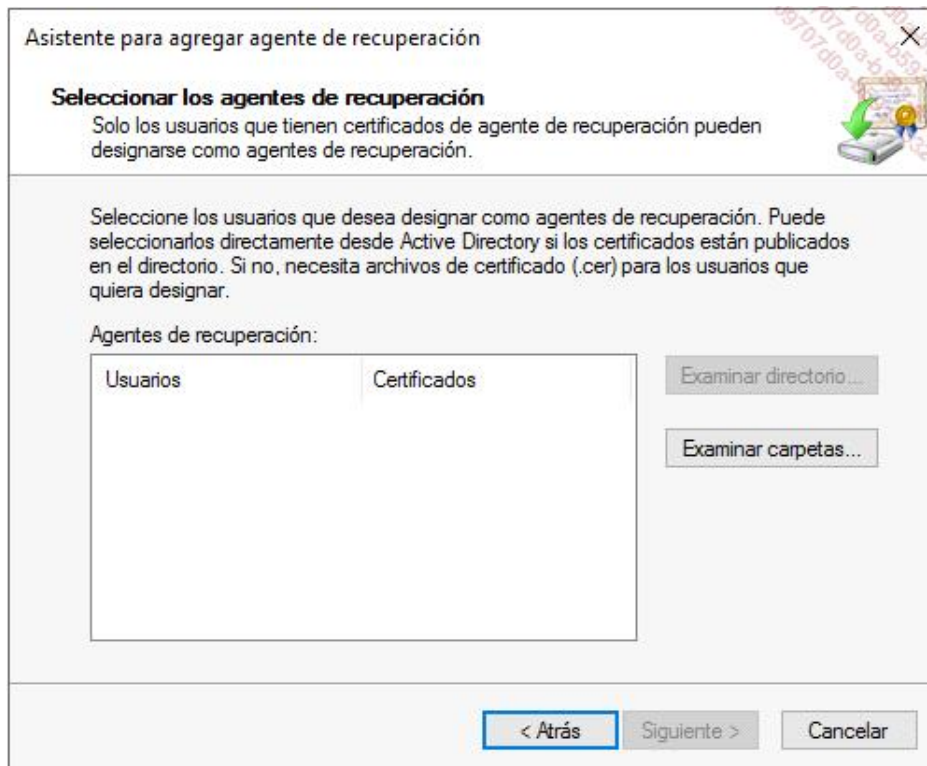
b. Agente de recuperación

Cuando un usuario cifra un archivo, la clave de descifrado se crea en función de su cuenta Windows y de su SID (*Security Identifier*) único asociado. El SID permite al sistema Windows 10 identificar los objetos realizando acciones. En caso de que algún empleado se dé de baja, si se elimina su cuenta, su SID será también eliminado. De este modo, no será posible abrir los archivos cifrados por este usuario, incluso si vuelve a crear la misma cuenta de usuario, ipues su SID será forzosamente diferente! Para paliar esta problemática, Microsoft permite crear un agente de recuperación, que es en definitiva una cuenta de usuario que puede descifrar cualquier archivo cifrado.

Para crear un agente de recuperación local en un puesto con Windows 10:

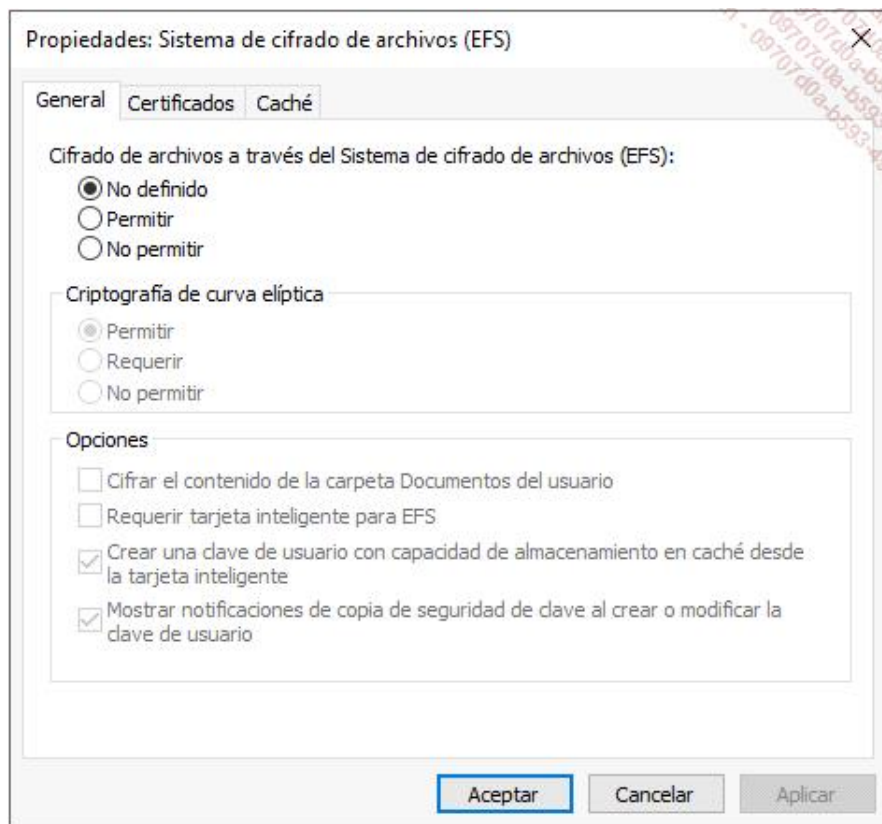
- Pulse las teclas  y **R**. Introduzca **gpedit.msc** en la ventana **Ejecutar** y confirme con la tecla [Intro].
- En la ventana **Editor de directiva de grupo local**, despliegue los nodos **Configuración del equipo - Configuración de Windows - Configuración de seguridad - Directivas de clave pública**.

- Haga clic con el botón derecho en **Sistema de cifrado de archivos (EFS)** y seleccione **Agregar Agente de recuperación de datos**.
- En el **Asistente para agregar agente de recuperación**, haga clic en **Siguiente**.
- A continuación, seleccione el certificado (.cer) o el usuario miembro de un dominio al que desee asignar el rol de agente de recuperación y haga clic en **Siguiente**. Siga las etapas del asistente.



La configuración general de EFS se realiza mediante las propiedades del nodo **Sistema de cifrado de archivos (EFS)**:

- Haga clic con el botón derecho en el nodo **Sistema de cifrado de archivos (EFS)** y seleccione **Propiedades**.
- En la pestaña **General**, autorice el cifrado empleando EFS y defina las opciones apropiadas (**Cifrar el contenido de la carpeta Documentos del usuario, Requerir tarjeta inteligente para EFS**, etc.).



- La pestaña **Certificados** permite seleccionar el modelo del certificado, así como el comportamiento de EFS cuando no hay disponible ninguna autoridad de certificación utilizando certificados autofirmados.
- La última pestaña, **Caché**, define los casos en que debe ocultarse la caché de clave de cifrado.

Aunque la tecnología EFS proporcione una seguridad importante, la protección física de un equipo sigue siendo primordial.

Protección de datos fuera de línea

La vigilancia es fundamental para la prevención del robo de discos duros o de medios extraíbles, como llaves USB.

Para paliar esta problemática, Microsoft presenta la tecnología de cifrado de unidades BitLocker, que apareció con el sistema Windows Vista.

1. BitLocker

Incluido en las versiones Enterprise, Education y Profesional de Windows 10, BitLocker protege todos los datos almacenados en las particiones en modo sin conexión. En efecto, durante el proceso de arranque, el disco duro se descifra mediante BitLocker, que impide el acceso no autorizado a los datos mientras Windows 10 funciona. Dé prioridad en este caso a EFS para cifrar sus documentos aunque el equipo esté arrancado.

BitLocker es también útil en caso de baja definitiva de un disco duro. Cifrándolo completamente, la solución se hace enseguida rentable si la comparamos con el coste de una empresa especializada en la destrucción de discos físicos.

Otra funcionalidad interesante aportada por BitLocker es el control de integridad, que autentica a través de una tarjeta **TPM** (*Trusted Platform Module*) el hardware del equipo y los archivos críticos (NTFS boot sector, boot manager, etc.) de Windows 10. De esta forma, en caso de robo de un disco duro cifrado mediante este método, los datos que contiene no serán accesibles en otro ordenador. Un virus tampoco podrá instalarse durante la fase de arranque del sistema operativo.

He aquí una tabla comparativa de las dos tecnologías, BitLocker y EFS:

	BitLocker	EFS
Cifrado completo de las particiones	X	
Autenticación fuerte (contraseña y memoria flash USB)	X	
Método de recuperación (contraseña o Agente)	X	X
Cifrado completo de un dispositivo extraíble	X	
Verificación de la integridad del sistema y del hardware	X	
Protección de datos una vez arrancado el equipo		X
Cifrado de archivos	X	X
Utilización de un certificado de usuario		X
Garantiza DLP (<i>Data Loss Prevention</i>)	X	X
Soporte de particiones no NTFS para los dispositivos extraíbles	X	

Hay que tener en cuenta la disminución de rendimiento al elegir un método de cifrado de dispositivo sin conexión. Al activar BitLocker en un disco duro, su rendimiento de acceso se ve reducido entre un 3 y un 5% según Microsoft.

BitLocker necesita los siguientes requisitos previos:

- Una BIOS que soporte el arranque desde dispositivos USB o la presencia de una tarjeta TPM en la placa base.
- Una partición del sistema creada por defecto de manera automática, con un tamaño aproximado de 100 MB, no cifrada, sin letra de unidad y definida como activa.
- Opcionalmente, una partición que contenga datos puede estar formateada en FAT16, FAT32, exFAT y por supuesto NTFS, pero debe poseer al menos 64 MB de espacio libre en disco.

Windows 10 aporta las siguientes funcionalidades con BitLocker:

- Cifrado solo del espacio en disco utilizado, acelerando así el tiempo de cifrado del dispositivo. Esta funcionalidad puede asignarse desde la directiva de grupo local usando los nodos **Configuración del equipo - Plantillas administrativas - Componentes de Windows - Cifrado de unidad BitLocker - Unidades del sistema operativo (Unidades de datos fijas o Unidades de datos extraíbles)** y el parámetro **Aplicar el tipo de cifrado de unidad en unidades del sistema operativo**.

- Nuevos parámetros en las directivas de grupo, como la posibilidad de especificar una carpeta predeterminada para almacenar las claves de recuperación o de asignar criterios de complejidad en las contraseñas para los lectores. En lo sucesivo, es posible realizar la copia de seguridad en un dominio Active Directory de la información del propietario de la tarjeta TPM.
- Cifrado de la partición durante la fase de instalación, mediante Windows PE. Antes del cifrado definitivo, la unidad aparece junto a un signo de exclamación amarillo con el mensaje "Esperando activación". BitLocker emplea un cifrado con una potencia de cifrado AES de 128 bits.
- Una gestión de modo de espera conectado para poder cifrar los periféricos en los ordenadores con una arquitectura x86 o x64 con una tarjeta TPM.
- Soporte de Full Volume Encryption (FVE), que cifra los discos a nivel de hardware. El parámetro **Configurar el uso de cifrado en hardware para las unidades del sistema operativo** activa esta característica, desde los nodos **Configuración del equipo - Plantillas administrativas - Componentes de Windows - Cifrado de unidad BitLocker - Unidades del sistema operativo (o Unidades de datos fijas)** de la directiva de grupo local.
- Posibilidad de cambio del código PIN o de la contraseña por parte de un usuario con privilegios estándar. Después de cinco intentos fallidos al introducir la contraseña actual para poder cambiarla, el sistema debe reiniciarse para que la


cuenta vuelva a ponerse a cero. Un administrador puede, por supuesto, cambiar el código PIN o la contraseña. Se puede desactivar esta funcionalidad desde el parámetro **No permitir que usuarios estándar cambien el PIN o la contraseña** desde los nodos **Configuración del equipo - Plantillas administrativas - Componentes de Windows - Cifrado de unidad BitLocker - Unidades del sistema operativo**.

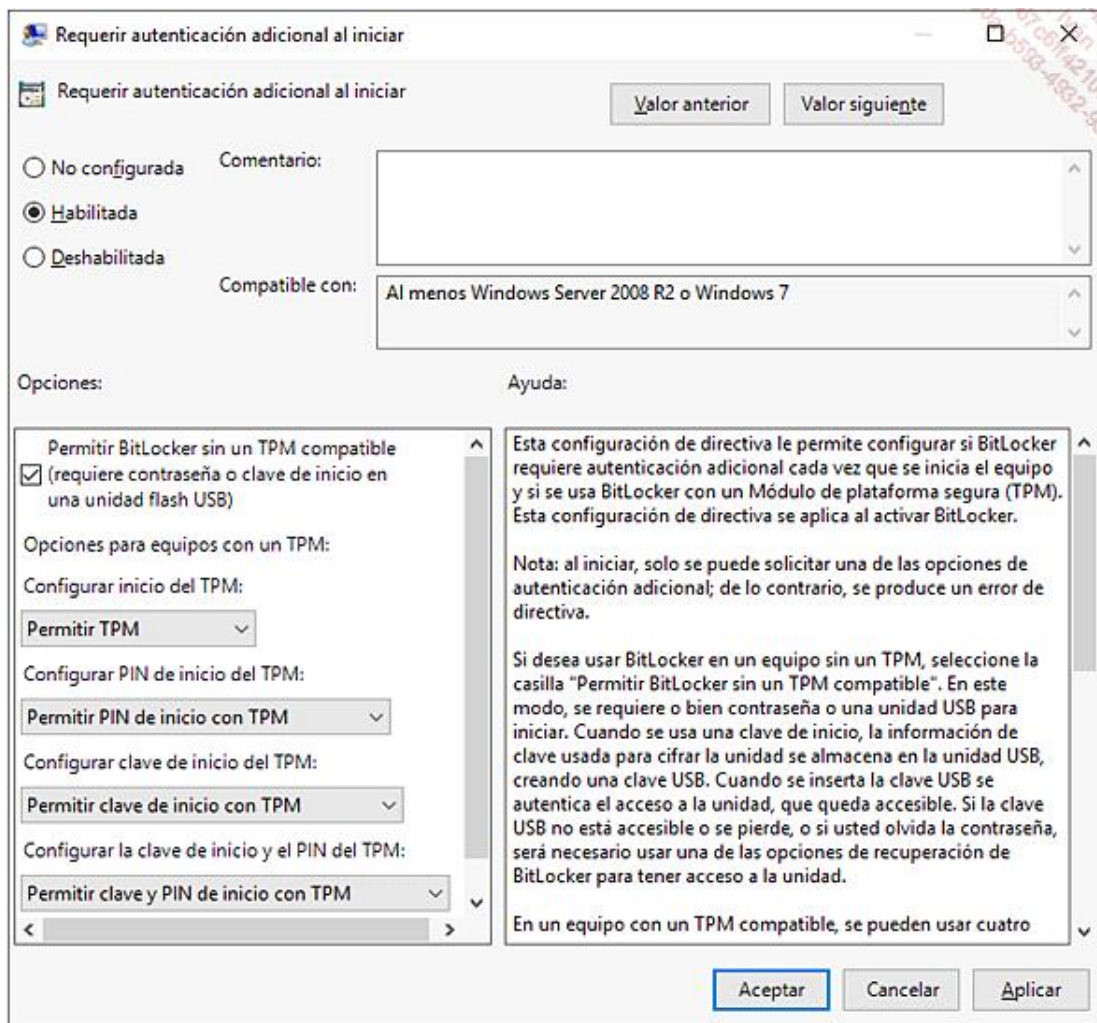
Por defecto, cifrar la partición que contiene el sistema operativo Windows 10 requiere de un ordenador con una tarjeta TPM. En su ausencia, aparece un mensaje de error:



Para verificar que un equipo dispone de una tarjeta TPM, consulte la documentación del fabricante o haga clic en **Administración de TPM** en la ventana **Cifrado de unidad BitLocker**, accesible desde el **Panel de control**.

Si no se cuenta con una tarjeta TPM, existe un método que permite evitar este comportamiento, desactivando el requerimiento de la presencia de este componente. Esta acción se efectúa desde la directiva de grupo local:

- Utilice la combinación de teclas  y **R**, introduzca **gpedit.msc** y confirme con [Intro].
- En la pantalla **Editor de directiva de grupo local**, despliegue los nodos **Configuración del equipo - Plantillas administrativas - Componentes de Windows - Cifrado de unidad BitLocker y Unidades del sistema operativo**.
- Haga doble clic en el parámetro **Requerir autenticación adicional al iniciar**. Marque la opción **Habilitada** y verifique que la opción **Permitir BitLocker sin un TPM compatible (requiere contraseña o clave de inicio en una unidad flash USB)** esté marcada.



En adelante, el arranque de Windows necesitará la inserción de una llave USB específica o bien que se introduzca la contraseña adecuada.

Es posible realizar una configuración homogénea de BitLocker en los equipos con Windows 10 de un dominio Active Directory empleando un objeto de directiva de grupo.



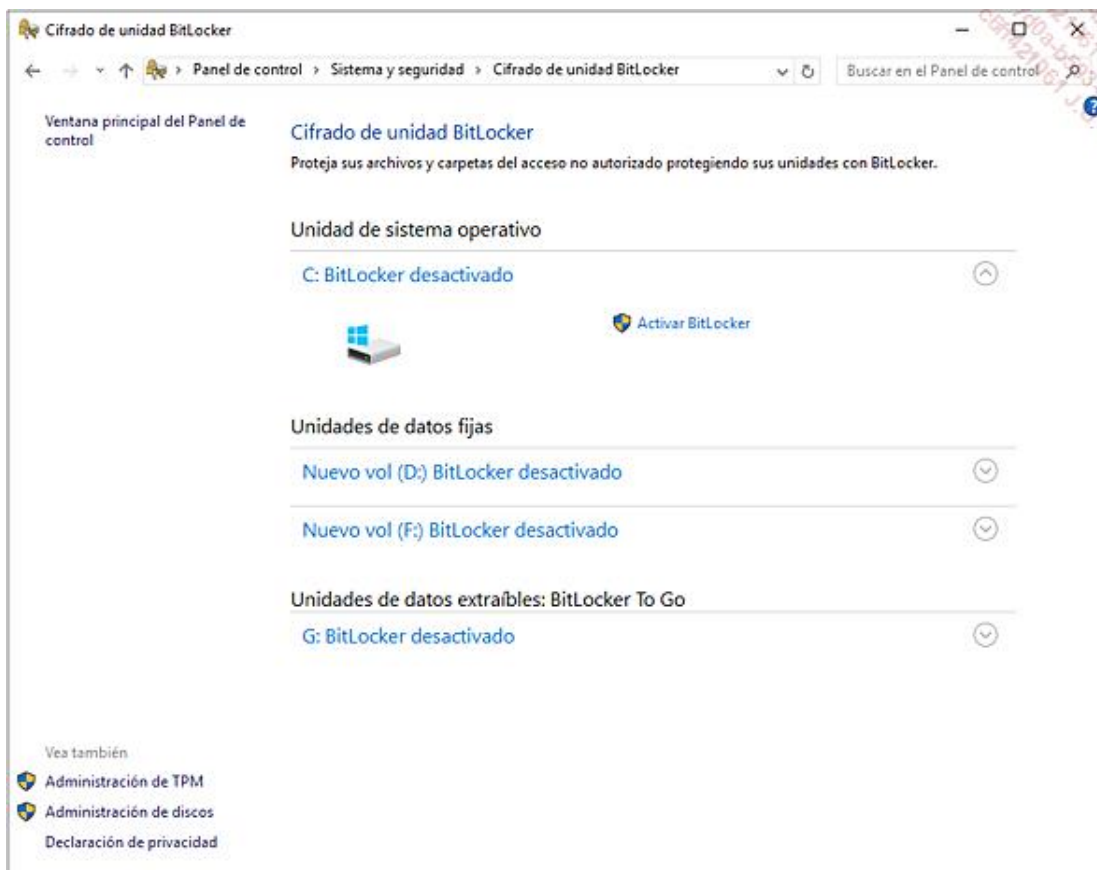
Observe que Windows Server 2008 o superior soporta esta tecnología de forma nativa, y es posible instalarla con el siguiente comando PowerShell: **Install-WindowsFeature BitLocker -IncludeAllSubFeature**

Cuando la partición del sistema operativo está protegida por BitLocker, el usuario no puede arrancarlo sin emplear una clave de descifrado, según tres métodos:

- Módulo TPM versión 1.2 o posterior: disponible en los ordenadores portátiles recientes, esta tarjeta es un componente de hardware instalado en la placa base. Asegura un control de integridad, además del cifrado de las unidades de disco. Puede combinar otros factores de autenticación agregando un PIN o la inserción de un dispositivo USB que contenga la clave de inicio. En caso de que la tarjeta TPM quedara inaccesible, o de que un usuario intentara arrancar el equipo desde un CD o un DVD, Windows 10 pasaría al modo de recuperación y necesitaría una contraseña de recuperación.
- Dispositivo extraíble USB, como una llave USB: la BIOS del equipo debe soportar el arranque desde dispositivos USB. La llave USB contendrá la clave de inicio y deberá estar obligatoriamente conectada mientras el equipo esté encendido. Este método no proporciona verificación de integridad de los componentes de hardware durante el prearranque del equipo, pero asegura un cifrado de los volúmenes.
- Contraseña compleja introducida durante la primera etapa del asistente.

En este estado, no queda más que activar el cifrado de unidad BitLocker en la partición del sistema Windows 10 llamada C:, utilizando privilegios de administrador:

- Introduzca **BitLocker** en la zona de búsqueda del menú **Inicio** y seleccione **Administrar BitLocker**.
- En la pantalla **Cifrado de unidad BitLocker**, haga clic en **Activar BitLocker** junto a la unidad que se ha de cifrar, en nuestro ejemplo **C:**.

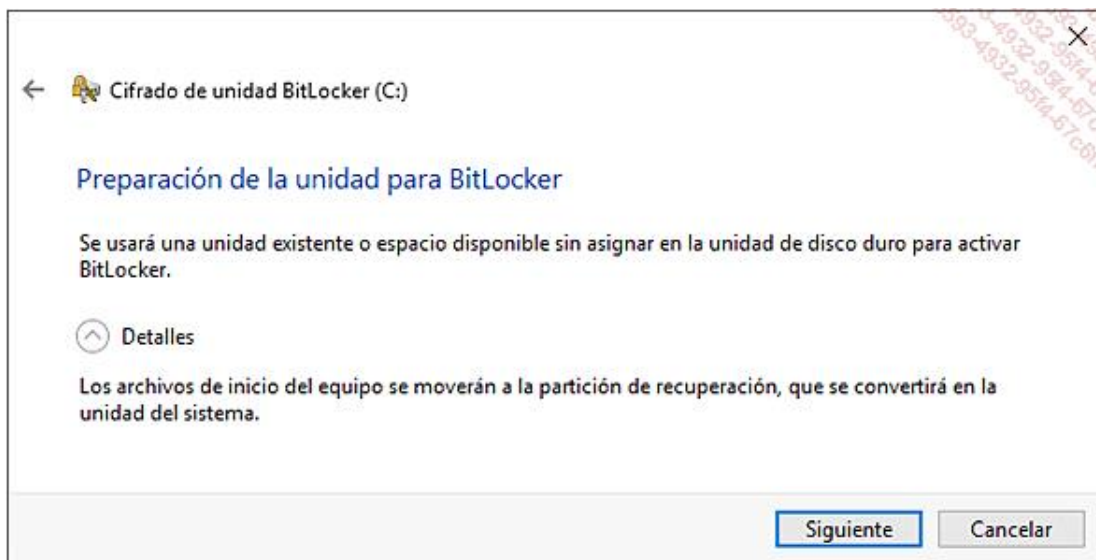


Observe que es posible cifrar unidades extraíbles USB con **BitLocker To Go**.

- ➔ Puede también cifrar un disco duro desde el **Explorador de Windows** seleccionando la letra de unidad con el botón derecho y, a continuación, seleccionando la opción **Activar BitLocker**, o bien desde un símbolo del sistema, mediante el archivo ejecutable **manage-bde.exe**. La ventaja de este script es la posibilidad de configurar BitLocker en equipos remotos.

En ausencia de partición del sistema, el asistente de cifrado analiza la configuración necesaria para activar BitLocker en la unidad C:.

- Haga clic en el botón **Siguiente**. El equipo se va a reiniciar y creará la partición del sistema oculta.



La siguiente etapa ofrece dos métodos para desbloquear la partición C: durante el inicio del equipo:

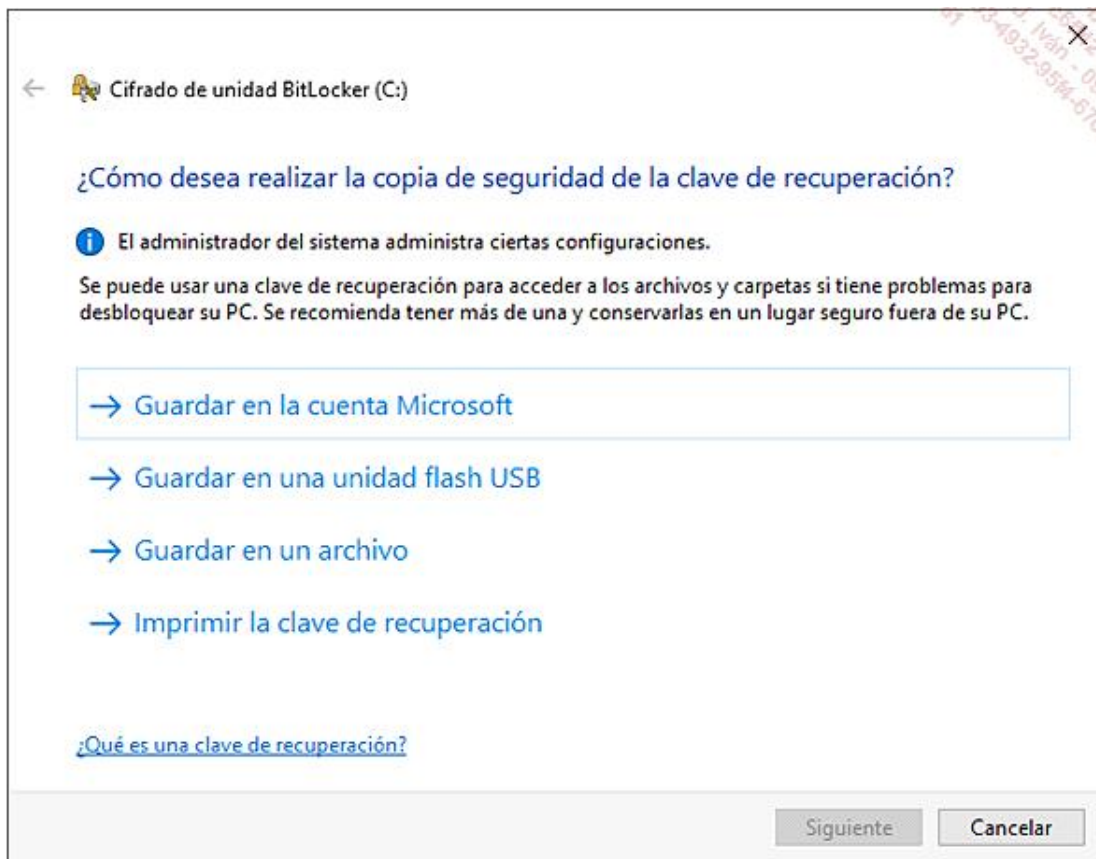
- Inserción de una memoria flash USB.
- Introducir una contraseña.



Si la activación de BitLocker está definida en una partición diferente a la del sistema operativo, un asistente verifica la configuración y presenta dos métodos de cifrado: por contraseña o por tarjeta inteligente.

A continuación, se invita al usuario a elegir un método de almacenamiento de la clave de recuperación:

- En su cuenta Microsoft (consulte el capítulo Instalación del cliente Windows 10 - Autenticación), accesible desde otros equipos.
- En un dispositivo flash USB. El archivo tendrá automáticamente el atributo **Solo lectura**.
- En un archivo almacenado en una partición de red o en un disco del equipo local. Este método es poco recomendable debido a los riesgos de eliminación vinculados, por ejemplo, a un ataque de virus.
- En una hoja de papel, que habrá que guardar meticulosamente en un lugar seguro (caja fuerte o armario cerrado con llave).



La clave de recuperación se compone de 48 cifras divididas en ocho grupos y es propia de cada unidad cifrada. Se utiliza en varios casos: pérdida de la contraseña principal o de la memoria flash USB, cambio de la configuración de hardware.

➤ En un entorno Active Directory, los puestos de trabajo cifrados unidos al dominio pueden almacenar la clave de recuperación en el directorio. En este caso, el administrador de dominio deberá obtener del usuario bloqueado o bien la etiqueta de la unidad cifrada, o el Password ID (32 caracteres) disponible en las propiedades del sistema del ordenador con Windows 10 afectado, con el fin de proporcionar una clave de recuperación.

El administrador también puede crear un Agente de recuperación de datos, habilitado para descifrar cualquier unidad del ordenador elegido.

En la penúltima etapa, el asistente propone por defecto verificar que su unidad podrá leer correctamente las claves de recuperación y de cifrado.

Su equipo se reiniciará.

BitLocker presenta por último la opción de cifrar solamente el espacio de disco usado (método rápido) o la unidad completa (método más lento). Observe, no obstante, que, si se escoge la primera opción, cualquier dato nuevo que se copie en el disco se cifrará automáticamente.

➔ Haga clic en el botón **Continuar**.

El botón **Iniciar cifrado** ejecuta el cifrado de la partición.

Como hemos visto antes, el comando **manage-bde.exe** permite realizar las operaciones complementarias de la funcionalidad BitLocker.

Por ejemplo, el comando **manage-bde -on D:** cifrará el volumen D: sin método de autenticación. Para cifrar el disco que contiene el sistema operativo Windows 10 C: sin una tarjeta TPM pero almacenando la clave de recuperación en un dispositivo extraíble E:, introduzca los siguientes comandos: **manage-bde -protectors -add C: -startupkey E:** y **manage-bde -on C:**. El parámetro **-status** muestra el cifrado de un volumen. El comando ofrece también la posibilidad de eliminar los datos fragmentados que existan en el espacio en disco libre de un volumen cifrado (parámetro **-w**).

Repair-bde permite acceder a los datos almacenados en un volumen cifrado, incluso si está dañado. Observe que el comando no puede reparar un disco que se ha corrompido durante la fase de cifrado o descifrado.

Existen comandos PowerShell que permiten administrar BitLocker, como por ejemplo **Enable-BitLocker** para cifrar un volumen específico, o **Get-BitLockerVolume** para obtener información de un disco cifrado.

2. BitLocker To Go

BitLocker To Go es una funcionalidad que aparece con Windows 7: permite realizar un cifrado completo de los dispositivos de almacenamiento portátiles, como las llaves USB y los discos duros externos.

Haciendo clic con el botón derecho en la letra del dispositivo extraíble y seleccionando **Activar BitLocker**, se solicita al usuario que introduzca una contraseña de recuperación o inserte una tarjeta inteligente con un código PIN (*Personal Identification Number*) y, a continuación, salvguarde la clave de recuperación según tres métodos:

- Guardar en la cuenta Microsoft.
- Guardar en un archivo (atributo **Solo lectura** aplicado automáticamente).
- Imprimir en una página almacenada en lugar seguro.

BitLocker permite entonces cifrar solamente el espacio de disco usado (método rápido) o bien la unidad completa (método más lento).

Una vez cifrada la llave USB, es posible definir opciones suplementarias, como su desbloqueo automático en el equipo de destino o la modificación/eliminación de la contraseña:

→ Introduzca **bitLocker** en la zona de búsqueda situada en la barra de tareas y seleccione **Administrar BitLocker**.

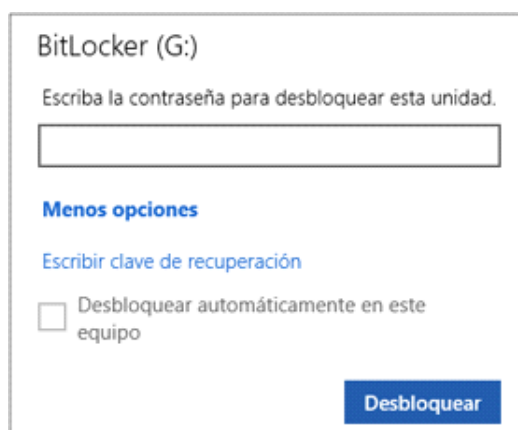
→ En la pantalla **Cifrado de unidad BitLocker**, haga clic en la opción seleccionada junto al dispositivo extraíble cifrado:

- **Copia de seguridad de la clave de recuperación**, para crear una nueva copia de seguridad de la clave de recuperación.
- **Cambiar o Quitar la contraseña** actual.
- **Agregar tarjeta inteligente**, para utilizar un método de desbloqueo por tarjeta inteligente.
- **Activar desbloqueo automático**, para desbloquear automáticamente una unidad extraíble durante su conexión al equipo actual sin requerir un método de autenticación.
- **Desactivar BitLocker** para eliminar el cifrado de una unidad sin borrar los datos que contiene.




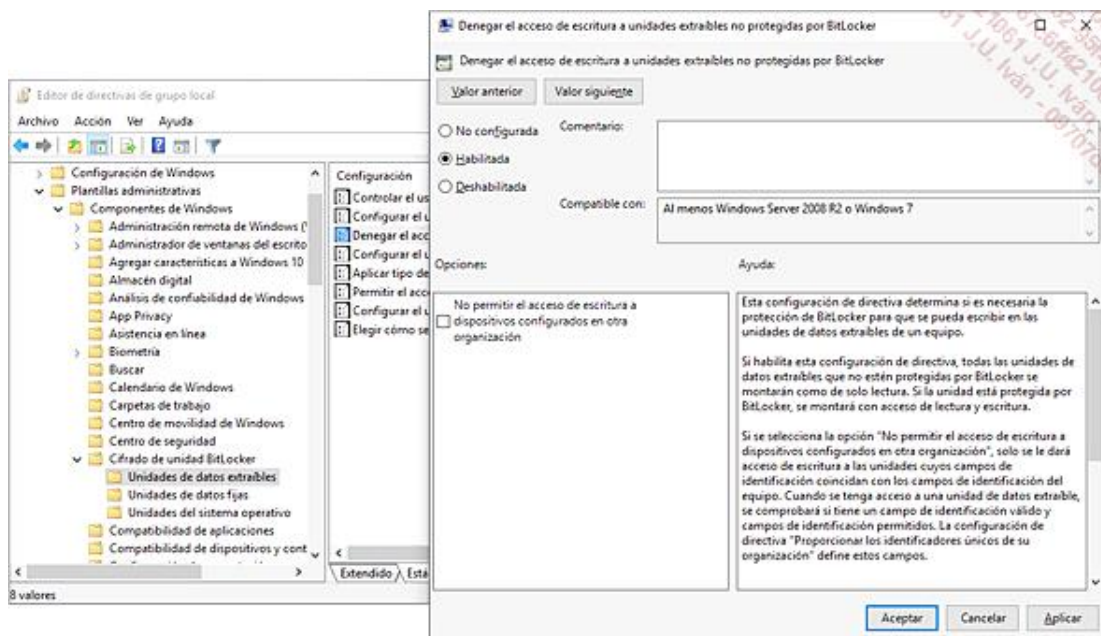
Cuando la llave USB cifrada se inserte en otro equipo con un sistema operativo Microsoft Windows XP SP2 o posterior, el usuario deberá introducir la contraseña de descifrado. Tendrá también la posibilidad de configurar BitLocker To Go para que se desbloquee automáticamente al insertar esta llave en el ordenador.

Al insertar el dispositivo extraíble cifrado en un puesto de trabajo con Windows 10, el usuario puede introducir la clave de recuperación haciendo clic en **Más opciones** y **Escribir clave de recuperación**.



Dado el cada vez mayor número de pérdidas y de robos de memorias flash USB, el responsable de los sistemas de información de una empresa debe poder garantizar que el personal no podrá copiar datos en este tipo de soporte sin que esté previamente protegido. Una opción interesante es la prohibición de acceder en modo escritura a una unidad extraíble no protegida por BitLocker To Go. Esta acción se realiza mediante un objeto de directiva de grupo, local o de dominio:

- Desde la pantalla de inicio, pulse las teclas  + R e introduzca **gpedit.msc** en la ventana **Ejecutar** y confirme con la tecla [Intro].
- Desde el árbol de consola **Editor de directiva de grupo local**, despliegue los nodos **Configuración del equipo** - **Plantillas administrativas** - **Componentes de Windows** - **Cifrado de unidad BitLocker** y **Unidades de datos extraíbles**.
- Haga doble clic en el parámetro **Denegar el acceso de escritura a las unidades extraíbles no protegidas por BitLocker** y marque la opción **Habilitada**. Observe que el administrador puede **No permitir el acceso de escritura a dispositivos configurados en otra organización** marcando la opción correspondiente. Será preciso, en este caso, proporcionar la lista de dispositivos autorizados con el parámetro **Proporcionar los identificadores únicos de su organización**.



En adelante, cuando un dispositivo flash USB se conecte al equipo, aparecerá un mensaje solicitando al usuario el cifrado de la unidad para poder escribir datos en ella:



Si el puesto de trabajo con Windows 10 es miembro de un dominio, puede ser interesante hacer copia de seguridad de la información de recuperación BitLocker (contraseña de recuperación y datos de identificación) con el fin de prevenir cualquier pérdida de datos en caso de no contar con las claves. El parámetro **Almacenar información de recuperación BitLocker en los servicios de dominio de Active Directory** debe de estar activo en el nodo **Configuración del equipo - Plantillas administrativas - Componentes de Windows - Cifrado de unidad BitLocker**.

Sepa que, al cifrar una llave USB cuyo sistema de archivos es FAT, un cliente Windows XP o Windows Vista podrá leer el contenido, pero no modificarlo.

Si el sistema de archivos de la llave USB se convierte a NTFS (comando **convert LETRAUNIDAD /fs:ntfs**), esta será ilegible en Windows XP y Windows Vista; estos sistemas propondrán entonces formatear la llave para poder acceder a ella.

Microsoft Passport

Microsoft Passport combina una autenticación fuerte basada en un dispositivo gestionado y Windows Hello con identificación biométrica (o un código PIN). Los usuarios pueden autenticarse con una cuenta Microsoft (Hotmail, Windows Live, etc.), una cuenta de un dominio Active Directory, una cuenta presente en el modelo PaaS (*Platform as a Service*) de Active Directory Azure o un servicio que soporte el modelo FIDO (*Fast IDentity Online*).

Una vez que el usuario ha introducido sus datos de identificación estándar basada en nombre de usuario y contraseña, es redirigido de forma automática a la página de configuración de su cuenta Microsoft Passport unida a Windows Hello. A partir de entonces, no le será requerida ninguna contraseña; solo serán necesarios un código PIN y su cara/iris/huella digital.

Este método de autenticación requiere de forma predeterminada una tarjeta TPM versión 1.2 o 2.0.

La primera etapa consiste en crear una directiva Passport en la que el empleo de Passport se establecerá como obligatorio, detallando la complejidad del código PIN confidencial (longitud mínima, máxima, caracteres especiales, etc.).

Dos escenarios posibles:

- Autenticación basada en clave: se requiere una suscripción a Azure Active Directory. Además, los servicios ADFS deberán estar instalados en los controladores de dominio del sitio, al igual que Microsoft System Center 2012 R2 Configuration Manager SP2.
- Autenticación basada en certificados: se requiere una suscripción Azure Active Directory, Intune (gestión de aplicaciones y dispositivos móviles, así como de ordenadores desde la *cloud*) y una infraestructura PKI. Los servicios ADFS deberán estar instalados en los controladores de dominio del sitio, al igual que Microsoft System Center 2012 R2 Configuration Manager SP2.

Intune gestiona la directiva Passport y el despliegue de los certificados protegidos Passport.

El modelo PaaS Azure AD inscribe los dispositivos a nivel empresarial.

Active Directory permite autorizar los usuarios y dispositivos que emplearán las claves protegidas por Passport si los controladores de dominio ejecutan la última versión de Windows Server.

Para obtener información adicional sobre la implementación de Microsoft Passport, siga el vínculo: [https://technet.microsoft.com/es-es/library/mt219734\(v=vs.85\).aspx](https://technet.microsoft.com/es-es/library/mt219734(v=vs.85).aspx)

Mediante Microsoft Passport, el usuario portará consigo la información de autenticación (cara/iris/huella digital y el código PIN). El concepto mismo de una contraseña se ha quedado obsoleto.

Gestión de las actualizaciones de seguridad

Microsoft publica el segundo martes (patch Tuesday) de cada mes las actualizaciones de seguridad destinadas a empresas y particulares. De esta forma, los administradores pueden prepararse para la aplicación de los parches, a principios de semana, y así anticipar y corregir los posibles problemas. Sin embargo, si se descubriera y explotara un fallo altamente crítico, la publicación del boletín de seguridad correspondiente podría efectuarse excepcionalmente fuera del ciclo.

Mantener Windows 10 actualizado permite asegurar la estabilidad y la protección del sistema. El servicio Windows Update gestiona la descarga e instalación de las actualizaciones de los productos de Microsoft cuando el usuario está conectado a la red Internet. En caso de desconexión durante una descarga, se reintentará cuando se restablezca la conexión.

Cuando un usuario está conectado a una red inalámbrica cuyos datos utilizados se facturan, como una red 3G o 4G, Windows 10 difiere la descarga de actualizaciones de seguridad en segundo plano hasta conectarse a una red inalámbrica Wi-Fi, menos costosa.

Sin embargo, si una actualización de seguridad clasificada como crítica está disponible para su descarga, el servicio Windows Update la descargará, sea cual sea el tipo de red. El usuario puede obviar estas dos reglas, iniciando manualmente una búsqueda y descarga de actualizaciones.

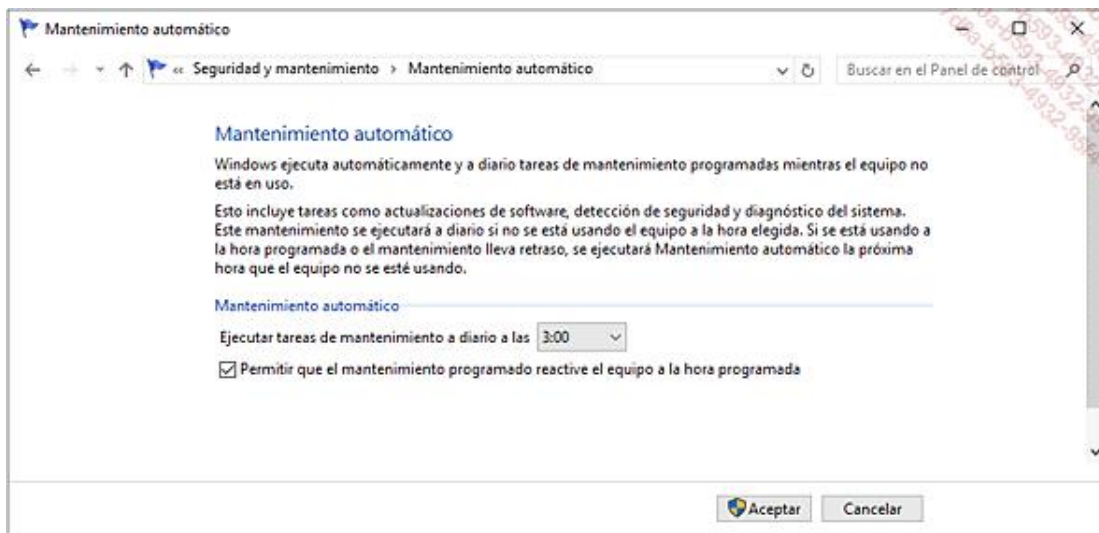
Es recomendable utilizar los parámetros predeterminados durante la configuración del servicio de administración de actualizaciones: cada día a las 2:00 A.M., Windows 10 ejecuta un mantenimiento automático si el ordenador no está en uso. En caso contrario, o si a esa hora el puesto de trabajo está apagado, el mantenimiento se ejecutará la vez siguiente. Si la tarjeta de red integrada soporta la funcionalidad **WOL** (*Wake On LAN*), el ordenador apagado puede iniciarse de manera remota para instalar las actualizaciones.

La mayoría de las tarjetas más recientes implementan el componente necesario para este inicio, pero a veces necesitan la activación de dicha función en la BIOS.

1. Configuración de parámetros de mantenimiento y actualización

Para configurar los parámetros del mantenimiento automático, siga este procedimiento:

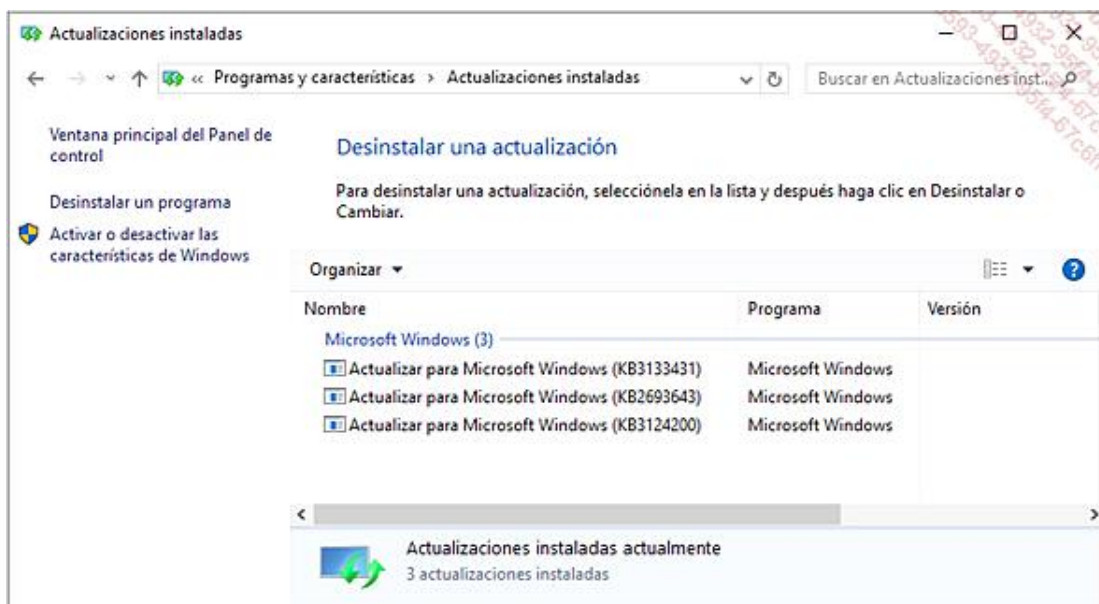
- Desde el campo de búsqueda del menú **Inicio**, introduzca **mantenimiento** y seleccione **Cambiar la configuración de mantenimiento automático**.
- En la ventana **Mantenimiento automático**, configure la hora de inicio del mantenimiento, así como la funcionalidad Wake On LAN.



Cuando una aplicación de Microsoft está en curso de ejecución y se aplica una actualización de seguridad que le afecta, Windows 10 realiza una copia de seguridad de sus datos, la actualiza y, a continuación, la reinicia.

Los parámetros de Windows Update se configuran desde el panel:

- Haga clic en el menú **Inicio**, luego en **Configuración y Actualización y seguridad**. En la sección **Windows Update**, el usuario puede forzar la búsqueda de actualizaciones.
- Haciendo clic en **Opciones avanzadas**, seleccione el modo de gestión de las actualizaciones entre las opciones:
 - **Automático** (recomendado) o **Notificar para programar reinicio**. Windows 10 se reiniciará de forma automática si esta opción no es utilizada. Podemos perder trabajos en curso en este caso.
 - **Aplazar actualizaciones**.
 - **Ver el historial de actualizaciones**: opción particularmente útil cuando deseamos desinstalar actualizaciones o la última versión de evaluación.



- **Elige el modo en que quieres que se entreguen las actualizaciones**: nueva funcionalidad que permite descargar las actualizaciones en otros PC de la misma red, en lugar de usar el ancho de banda de Internet de la

empresa para conectarse al servicio de actualización de Microsoft.



Haciendo clic en el botón **Empezar**, situado en la sección **Obtener compilaciones de Insider Preview**, el usuario, utilizando una cuenta Microsoft y definiendo de forma opcional un código PIN, puede recibir las últimas características y versiones de evaluación de la versión del puesto de trabajo de Microsoft Windows.

Configurar un PIN

El uso de un PIN es más rápido y más seguro que una contraseña. Esperamos que te guste la experiencia.

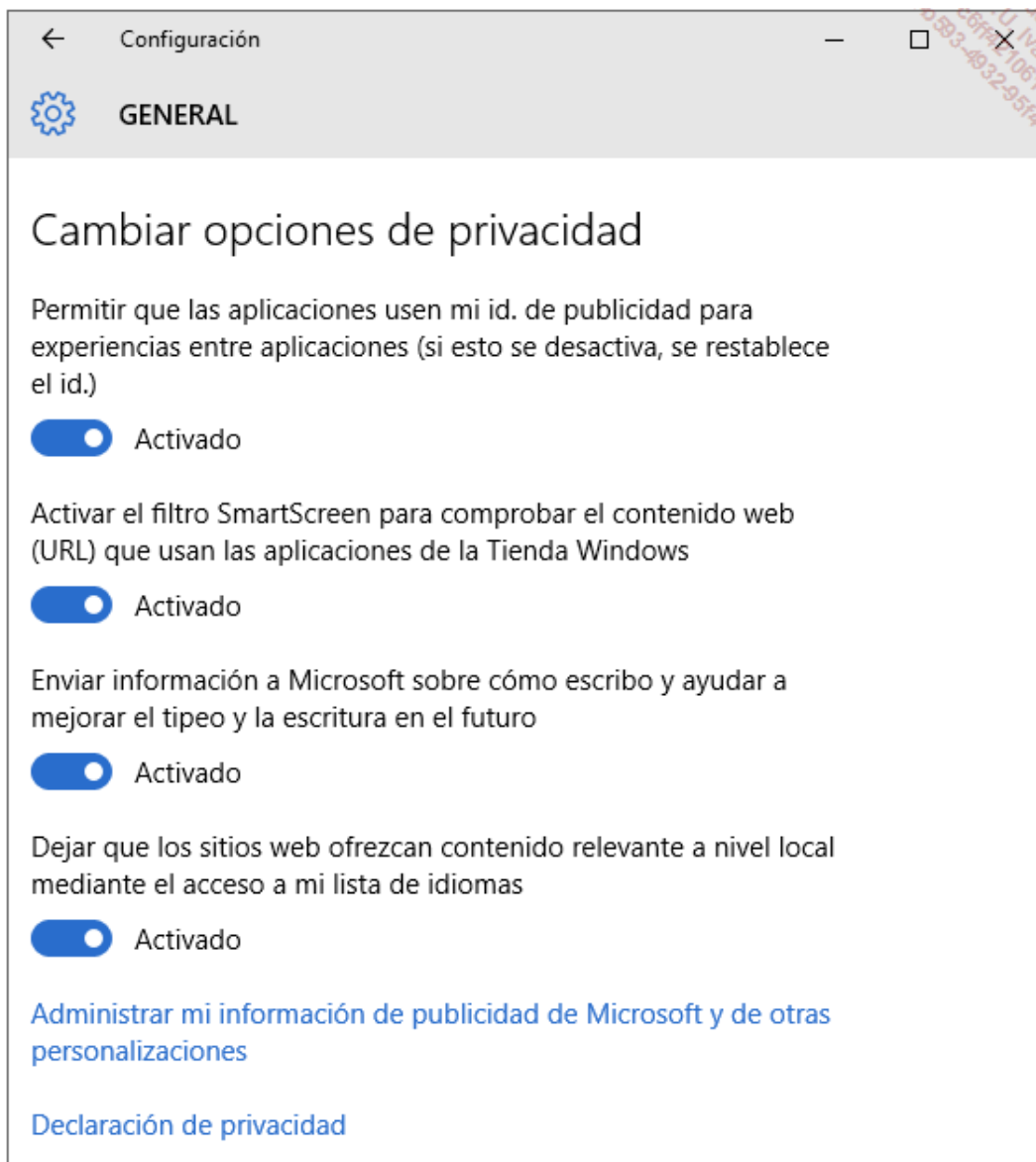
¿Cómo puede ser un PIN más seguro que una contraseña larga?



[Omitir este paso](#)

[Establecer un PIN](#)

Por último, en la ventana **Opciones avanzadas**, las opciones de privacidad ofrecen al usuario opciones en cuanto a la protección de sus datos personales, tales como no dejar a las aplicaciones la libertad de utilizar su identificador de publicidad o impedir a los sitios web acceder a la lista de idiomas para proporcionar contenido local:



La empresa puede también utilizar un servidor WSUS (*Windows Server Update Services*), ubicado en la red local, para gestionar los parches de seguridad. Este servicio descarga las actualizaciones desde Microsoft Update y se encarga de implementarlas en los clientes Windows de la empresa. De ella se deriva un uso sustancialmente mejor del ancho de banda de Internet porque el servidor WSUS utiliza la red local, que emplea generalmente una arquitectura de 10/100 Mbits/s o gigabyte. El rol WSUS necesita una versión servidor de Microsoft Windows, como Windows Server 2012.

Mediante un objeto de directiva de grupo, el administrador de un dominio puede definir los parámetros estándar de gestión de parches y aplicarlos de forma integral al parque informático del que es responsable.

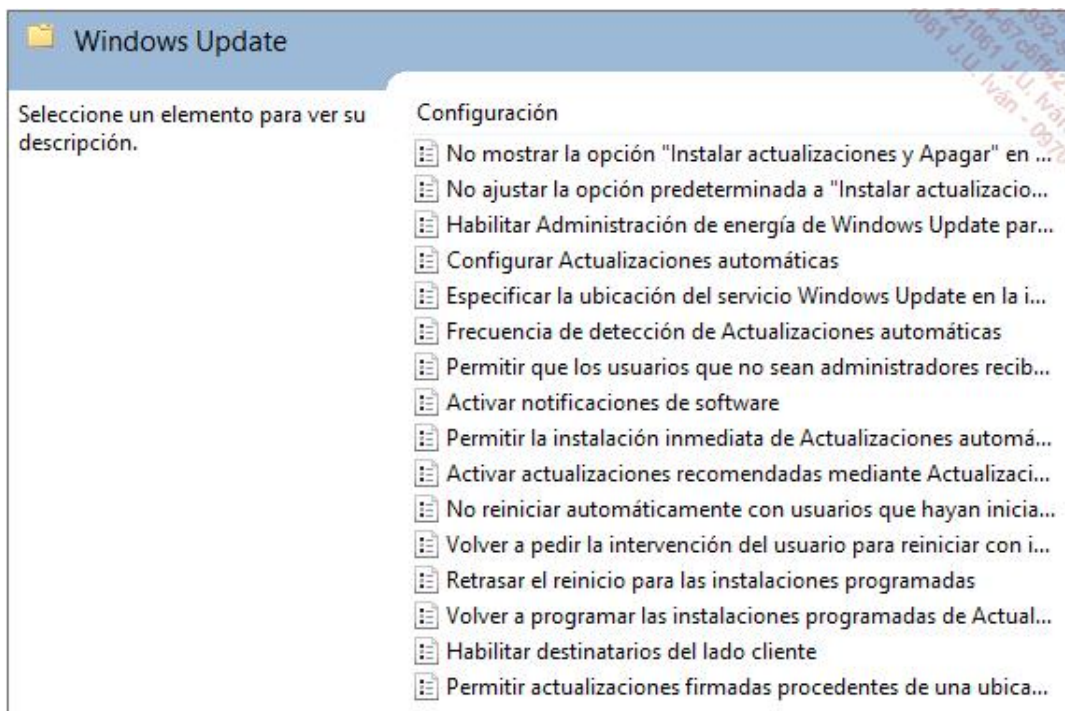
Para que un cliente WSUS pueda recibir las actualizaciones, es necesario que posea el componente **Actualizaciones automáticas** integrado en los sistemas operativos Windows 2000 Profesional SP4 y superiores. Para configurar este componente, utilice el nodo de directiva de grupo **Configuración del equipo - Directivas - Plantillas administrativas - Componentes de Windows - Windows Update**.

He aquí algunos de los parámetros configurables:

- Dirección del servidor WSUS en el cual el cliente debe registrarse.
- Visualización o no de las notificaciones de actualización.

- Frecuencia de búsqueda de las actualizaciones: por defecto configurada diariamente a las 22:00 horas.
- Aplazamiento de actualización: para las versiones Pro y Enterprise de Windows 10, el usuario puede diferir la actualización hasta el próximo periodo de actualización.
- Comportamiento del reinicio automático, al igual que su posible retardo.
- Pertenencia al grupo de usuarios WSUS; se trata de los destinatarios del lado cliente.
- Salida del modo de hibernación de los equipos si la instalación de actualizaciones está planificada.

La siguiente imagen resume los parámetros disponibles en un objeto de directiva de grupo:



Del lado del usuario, es posible restringir el acceso a las características de Windows Update. Se trata del parámetro **Quitar el acceso a todas las características de Windows Update** al que se puede acceder desplegando el nodo **Configuración de usuario - Plantillas administrativas - Componentes de Windows - Windows Update**.

2. Windows Update for Business

Se encuentra disponible una versión profesional de Windows Update para las empresas. El administrador puede definir ahora los equipos prioritarios para su actualización o los periodos del año más propicios para la aplicación de actualizaciones de seguridad. Un sistema *peer-to-peer* permite a un equipo ubicado en la LAN (*Local Area Network*) actuar como pasarela para otros equipos con las actualizaciones que ha recibido.

Las actualizaciones y las funcionalidades se desplegarán sin tener que esperar al "patch Tuesday". A nivel de la gestión del ancho de banda de las empresas que emplean conexiones WAN (*Wide Area Network*), Windows Update for Business federa los envíos mediante Microsoft System Center Configuration Manager o WSUS.

De esta forma, es posible limitar las actualizaciones de los parches de seguridad sin aplicar evoluciones funcionales.

Por último, Windows Update for Business gestiona también la evolución de los equipos con Windows 10 desde versiones de servidor de los sistemas operativos de Microsoft.

Control de aplicaciones con AppLocker

El control de aplicaciones instaladas y licenciadas en los puestos de una empresa es una cuestión muy importante para todo administrador de sistemas. Frente a este desafío, Microsoft presenta la funcionalidad **AppLocker**, que restringe la ejecución e instalación de software definido desde un servidor Windows Server 2008 R2 (o Windows Server 2012, Windows Server 2012 R2) en clientes Windows 7, Windows 8 y Windows 10 (Enterprise y Education). Esto se traduce en una reducción de gastos generales y un mayor control administrativo de los tipos de archivos ejecutables, evitando así la propagación de malware, como los troyanos.

AppLocker combina el inventario y la estandarización de aplicaciones, la protección contra software no autorizado y la conformidad de las licencias.

AppLocker sustituye la funcionalidad de directivas de restricción de software de versiones anteriores de Windows. Por ejemplo, durante la actualización a Windows 10 de un ordenador con Windows 7 y con una directiva de restricción de software aplicada. Será preciso crear una nueva regla AppLocker para dar soporte al bloqueo de un software.

Existen reglas de restricción disponibles para la ejecución de software, de scripts y para la instalación de programas.


Las siguientes extensiones pueden estar sujetas a restricción con un servidor Windows Server 2012 y clientes Windows 10 (Professional o Enterprise) con la funcionalidad AppLocker activada:

- Archivos ejecutables: .exe, .com.
- Scripts: .ps1, .bat, .cmd, .vbs, .js.
- Archivos de instalación: .msi, .msp, .mst.
- Aplicaciones empaquetadas: .appx.
- Archivos DLL (*Dynamic Link Library*): .dll, .ocx.

AppLocker presenta reglas basadas en el fabricante y en la firma digital de sus aplicaciones: por ejemplo, una organización crea una regla que autoriza la ejecución de cualquier versión de la aplicación Skype posterior a la versión 2.0 si está firmada por su fabricante, Microsoft. De esta forma, no será necesario crear una nueva regla si el producto recibe una actualización.

AppLocker integra ahora la gestión de aplicaciones e instalaciones empaquetadas, que son las apps de estilo Windows 10 disponibles en la Tienda (Windows Store). Este tipo de aplicación no necesita privilegios elevados para instalarse y comparte los mismos atributos: nombre de fabricante y de paquete, así como versión. La creación de una regla AppLocker única se aplica *de facto* a todos los archivos contenidos en el paquete.

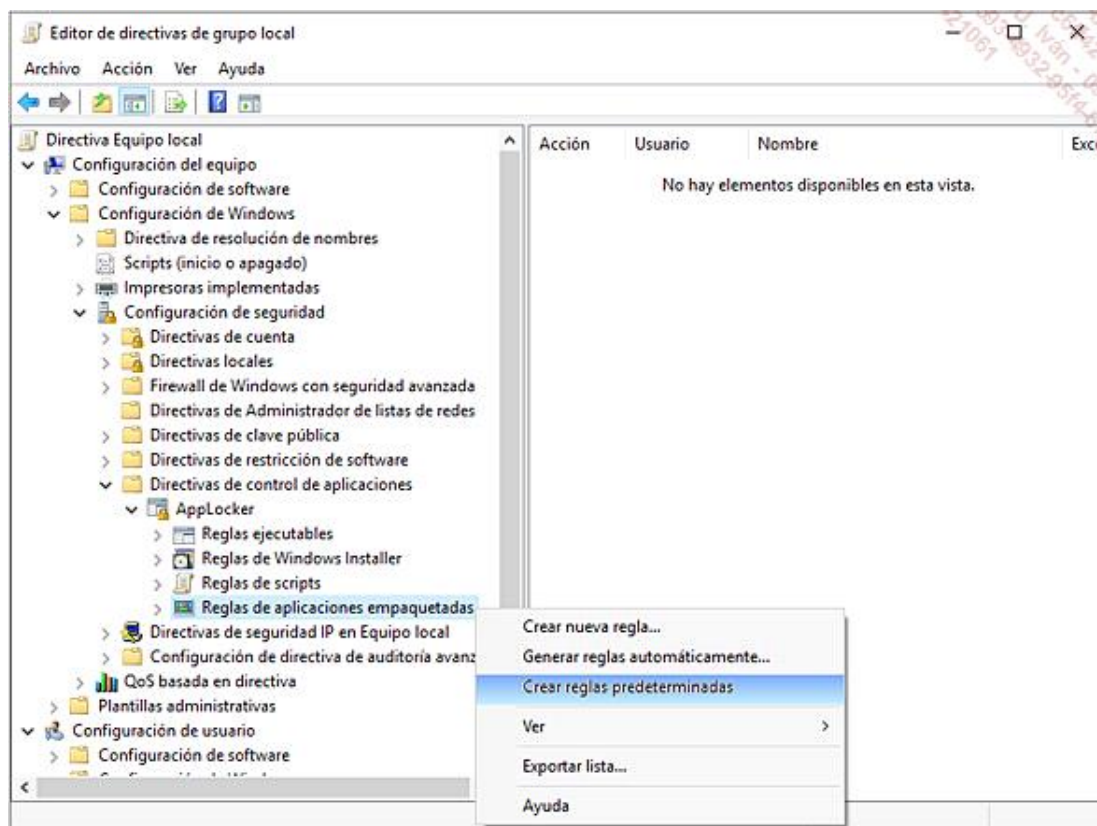
Aplicación incluida en los clientes Windows 10 miembros de un dominio Active Directory, AppLocker también está accesible de manera local, desde la consola **Editor de directiva de grupo local**:

→ Utilice la combinación de teclas  y **R** y, a continuación, introduzca **gpedit.msc** y seleccione **gpedit**.

Despliegue el nodo **Configuración del equipo - Configuración de Windows - Configuración de seguridad - Directivas de control de aplicaciones** y haga clic en **AppLocker**.

Antes de crear manualmente las reglas o de generarlas de forma automática, es importante crear el conjunto de reglas predeterminadas de AppLocker.

La creación de reglas predeterminadas se efectúa haciendo clic con el botón derecho en el tipo de reglas y seleccionando la acción **Crear reglas predeterminadas**.

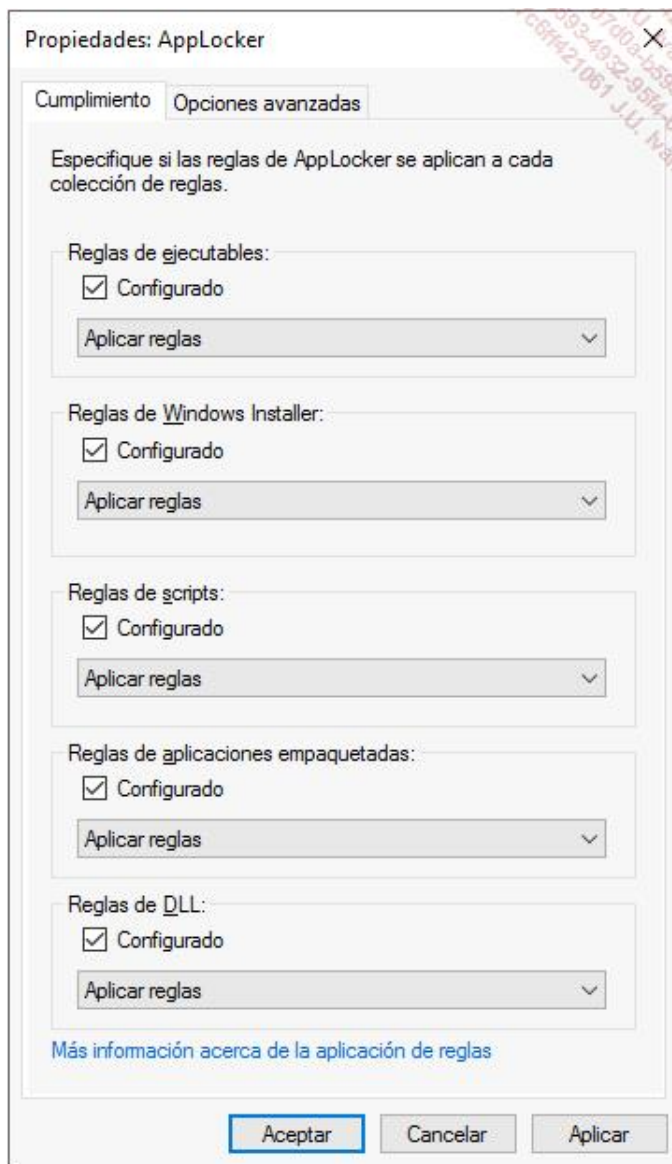


Las reglas predeterminadas permiten realizar las siguientes operaciones:

- **Reglas ejecutables:** todos los usuarios pueden ejecutar los programas contenidos en la carpeta **Programas** y en la carpeta **Windows**; los administradores pueden ejecutar todos los archivos, estén donde estén.
- **Reglas de Windows Installer:** todos los archivos firmados digitalmente pueden ser instalados, así como aquellos que se encuentren en la carpeta %systemdrive%\Windows\Installer. Los administradores pueden instalar todos los programas, estén o no firmados.
- **Reglas de scripts:** todos los scripts almacenados en las carpetas **Programas** y **Windows** pueden ser ejecutados; los administradores pueden ejecutar todos los scripts.
- **Reglas de aplicaciones empaquetadas:** todos los usuarios pueden instalar aplicaciones empaquetadas y firmadas digitalmente.
- **Reglas DLL:** por defecto, la creación de este tipo de reglas no está habilitada: marque la opción **Habilitar la colección de reglas DLL** en la pestaña **Opciones avanzadas** de las **Propiedades** del nodo **AppLocker**.

➤ Observe que los usuarios que no sean administradores no podrán ejecutar los programas instalados en su perfil (C:\Usuarios).

Haciendo clic con el botón derecho en el nodo **AppLocker** y seleccionando **Propiedades**, es posible auditar solamente las reglas, de forma que no se apliquen pero que se añada una entrada al registro de eventos de AppLocker. De este modo, el administrador puede evaluar la directiva de restricción de software que quiera implementar.




Para cada categoría, puede **Aplicar reglas**.

La pestaña **Opciones avanzadas** permite activar las reglas DLL y la posibilidad de crear restricciones en los archivos con extensiones .dll y .ocx.

Una vez creadas y aplicadas las reglas predeterminadas, es posible crear reglas de aplicación, empleando el asistente **Generar reglas automáticamente**, y esto para archivos firmados y no firmados. La definición de una regla puede ir acompañada de la creación de una excepción.

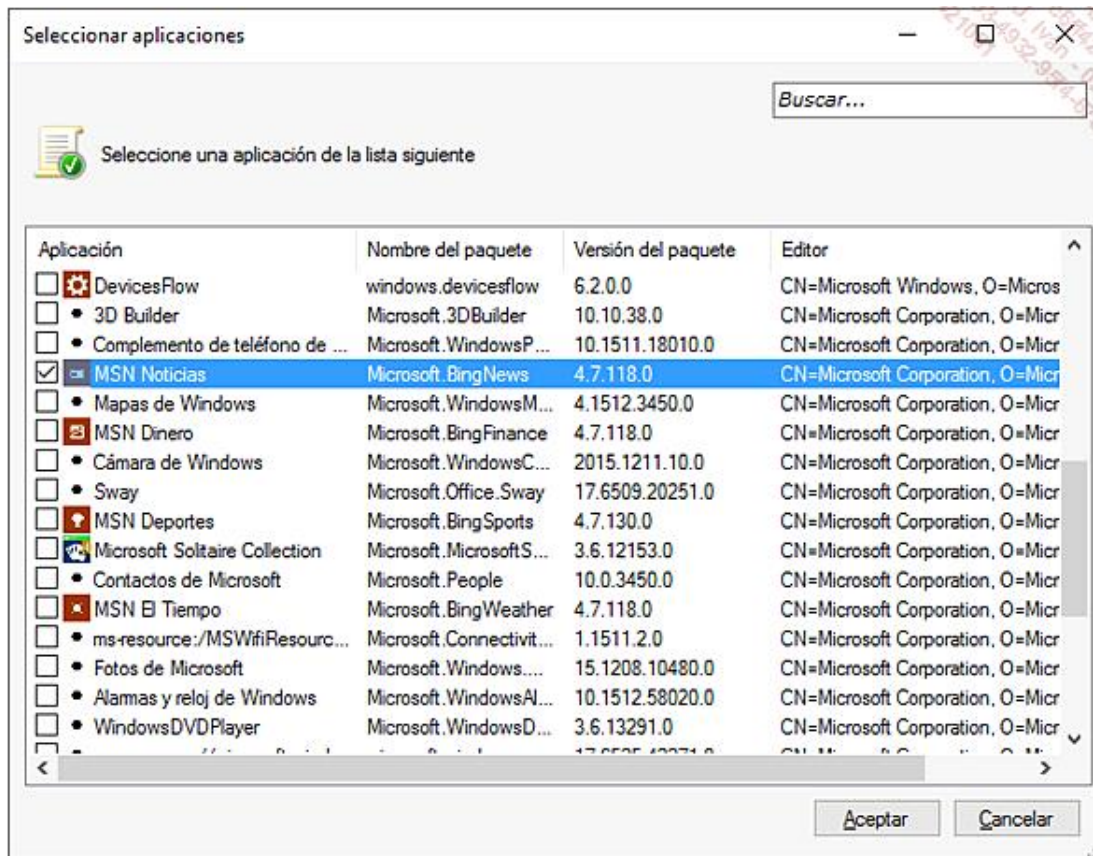
Cuando se crea manualmente una regla, es necesario especificar si esta debe ser autorizada o denegada.

Para crear una regla que impida la ejecución de la app **Noticias** de la Tienda de Windows en un equipo con Windows 10, proceda de la siguiente forma:

- Utilice la combinación de teclas  y **R** e introduzca **gpedit.msc** y seleccione **gpedit**. Despliegue el nodo **Configuración del equipo - Configuración de Windows - Configuración de seguridad - Directivas de control de aplicaciones** y haga clic en **AppLocker**.
- Haga clic con el botón derecho en **Reglas de aplicaciones empaquetadas** y crear reglas por defecto. Luego haga clic otra vez con el botón derecho en **Reglas de Aplicaciones empaquetadas** a continuación, haga clic

en **Crear nueva regla** y en **Siguiente**. Seleccione la opción **Denegar** y escoja el grupo predeterminado (**Todos**). Haga clic en **Siguiente**.


- Marque la opción **Usar una aplicación empaquetada instalada como referencia** y, a continuación, haga clic en el botón **Seleccionar**. Marque la opción **MSN Noticias**, correspondiente a la aplicación de Windows 10 Noticias.



- Confirme haciendo clic en el botón **Aceptar** y **Crear**.

➤ Evite crear reglas en las carpetas de los perfiles de los usuarios; la seguridad puede verse disminuida. En efecto, un virus podría propagarse fácilmente en el perfil en curso.

Para aplicar las reglas en el cliente Windows 10, el servicio AppLocker **Identidad de aplicación**, deshabilitado por defecto, debe activarse:

- Desde la pantalla de inicio, pulse las teclas  + **R**, introduzca **services.msc** en la ventana **Ejecutar** y confirme con la tecla [Intro].
- Haga clic con el botón derecho en el servicio **Identidad de aplicación** y, a continuación, en **Iniciar**.

➤ Verifique también que la casilla **Configurado** esté marcada en el campo **Reglas de aplicaciones empaquetadas** de las propiedades de **AppLocker** y que **Aplicar las reglas** esté seleccionado en el menú desplegable correspondiente.

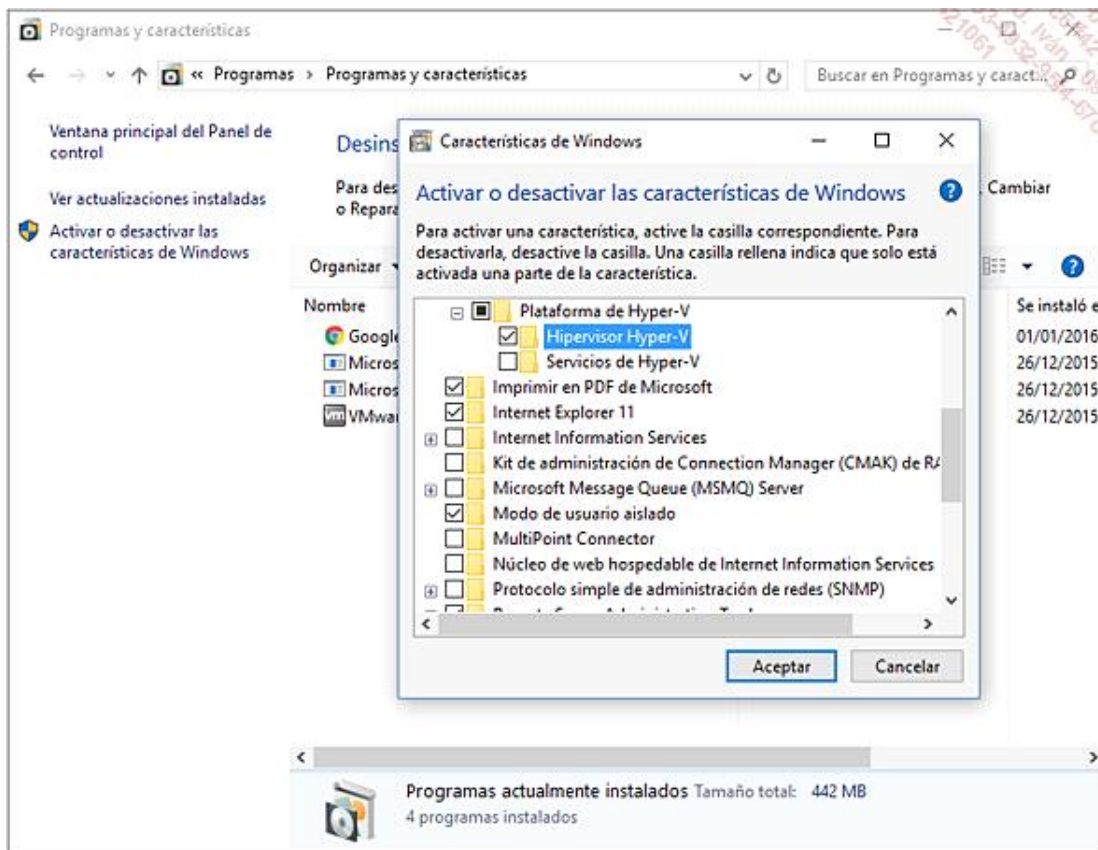
Device Guard

Device Guard representa un conjunto de funcionalidades vinculadas a la seguridad de hardware y software que, al ser definidas de forma simultánea, obligan al usuario a utilizar solo las aplicaciones preaprobadas por el administrador.

La funcionalidad utiliza una seguridad basada en la virtualización de Windows 10 Enterprise para aislar el servicio de integridad del código del núcleo. El equipo del empleado solo puede utilizarse para ejecutar código firmado aprobado por la empresa.

Device Guard requiere de microcódigo UEFI 2.3.1 o posterior, que soporte el arranque seguro, para impedir la carga en memoria de aplicaciones malintencionadas durante el proceso de arranque del sistema operativo. Además, se requiere un contenedor protegido por Hyper-V que aísle los procesos críticos de Windows 10.

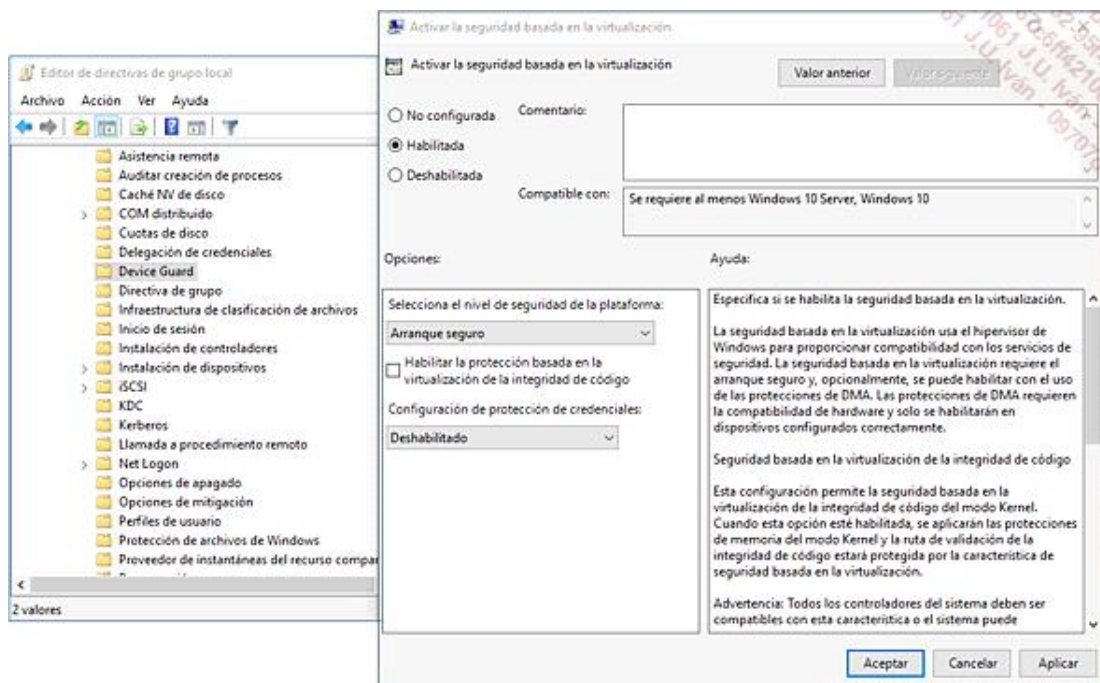
Este debe ser activado desde el **Panel de control** y **Programas y características** seleccionando **Hipervisor Hyper-V** y **Modo de usuario aislado**.



La aprobación por Device Guard de sus aplicaciones se crea cuando estas se firman empleando una firma emitida por la Tienda de Windows, de su PKI o de una autoridad de certificación de confianza.

La gestión de equipos protegidos por Device Guard se garantiza empleando directivas de grupo, Windows PowerShell, Intune o por último Microsoft System Center Configuration Manager.

La directiva de grupo local (**gpedit.msc**) emplea el nodo **Activar la seguridad basada en la virtualización** para activar el soporte del modo **Secure-Boot** desde la ruta siguiente: **Configuración del equipo - Plantillas administrativas - Sistema - Device Guard**.



Credential Guard

Credential Guard aporta una capa de seguridad adicional, de forma conjunta con Device Guard; los usuarios de un dominio Active Directory tendrán su contraseña almacenada en un contenedor virtual, y no en la LSA (*Local Security Authority*).

Se requiere de una arquitectura de 64 bits con Windows 10 Enterprise instalado en un equipo físico, al igual que un microcódigo UEFI 2.3.1 o superior y una infraestructura Hyper-V con las extensiones Intel VT-x/AMD-V y SLAT (*Second Level Address Translation*).

La directiva de grupo local (**gpedit.msc**) debe activar el parámetro **Habilitar Protección de credenciales** desde el nodo **Activar la seguridad basada en la virtualización: Configuración del equipo - Plantillas administrativas - Sistema - Device Guard**.

Configuración del Firewall de Windows con seguridad avanzada

Un firewall es el equivalente de una cerradura colocada en una puerta: complica la tarea de una persona malintencionada, pero no protege completamente el conjunto de la casa. Debe utilizarse junto con otras medidas, como la utilización de un antivirus o la gestión de las actualizaciones de seguridad.

Su función es proteger el puesto de trabajo con Windows 10 contra accesos no autorizados de equipos presentes en una red (Internet, local, etc.).

El firewall proporcionado con Windows XP estaba considerado como poco seguro, porque no filtraba más que las comunicaciones entrantes. El Firewall de Windows con seguridad avanzada, incluido en Windows 10, verifica que los paquetes que circulan son seguros mediante una conexión iniciada (firewall con estado) y procura un filtrado en los dos sentidos del tráfico.

Windows 10 gestiona los perfiles de red en función del lugar donde se encuentra el usuario. Cada vez que se establece una primera conexión, se invita al usuario a definir su ubicación actual: privado (Domicilio), dominio (empresa) y público (cibercafé). Por ejemplo, el administrador puede autorizar el acceso al **Escritorio remoto** (puerto predeterminado **3389** en TCP) siempre que el usuario se encuentre en el dominio de la empresa, y prohibir su uso cuando esté conectado desde una red menos segura, como la de un cibercafé. Para cada ubicación, el firewall posee un conjunto de reglas aplicadas por defecto.

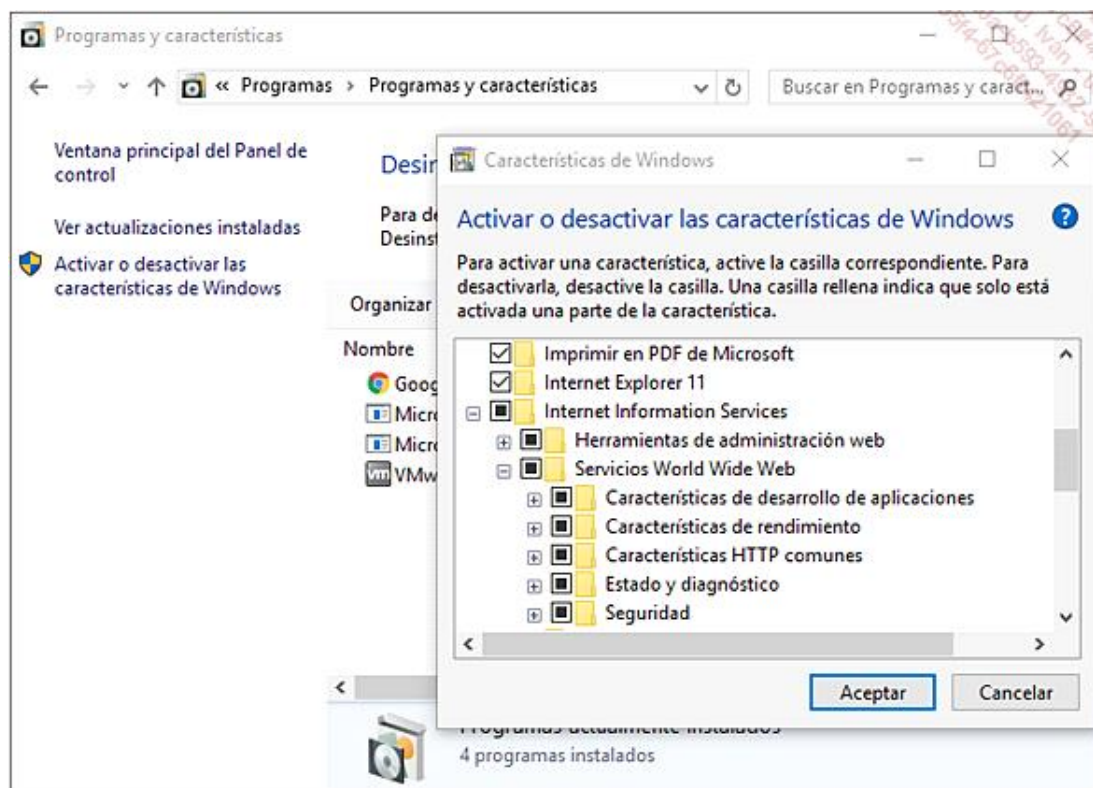
Windows 10 se suministra con dos firewalls: uno ofrece acciones simples, como autorizar o no un programa, el **Firewall de Windows**; el otro ofrece una gestión más precisa de los parámetros, se trata del **Firewall de Windows con seguridad avanzada**.


Es posible acceder al firewall de Windows desde el **Panel de control**, mientras que el firewall con seguridad avanzada está disponible en **Herramientas administrativas** o desde **Configuración avanzada** de la interfaz Firewall de Windows.

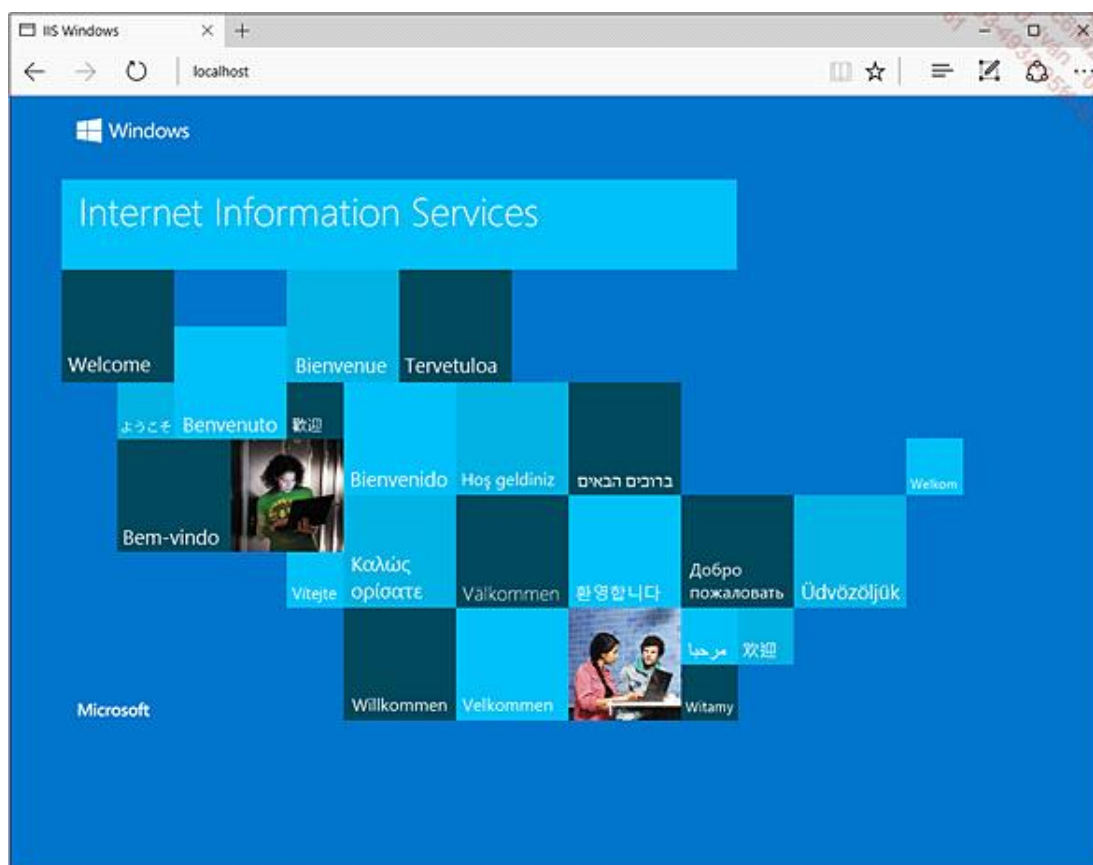
El firewall de Windows 10 permite crear excepciones manualmente, lo que permite que los programas o puertos se comuniquen con el exterior. En caso de ocurrir problemas de seguridad vinculados al uso del firewall, las notificaciones se muestran en el **Centro de actividades**.

Por ejemplo, para crear una regla de tráfico entrante denegando el acceso a su servidor web Windows 10 en el firewall con características avanzadas, es necesario, en primer lugar, instalar la característica IIS, que es el servidor web de Microsoft:


- ➔ Haga clic con el botón derecho del ratón en el menú **Inicio** y luego en el **Panel de control**. Haga doble clic en **Programas y características** y seleccione **Programas y características**. Haga clic en **Activar o desactivar las características de Windows**.
- ➔ En la ventana **Características de Windows**, marque la opción **Internet Information Services**.



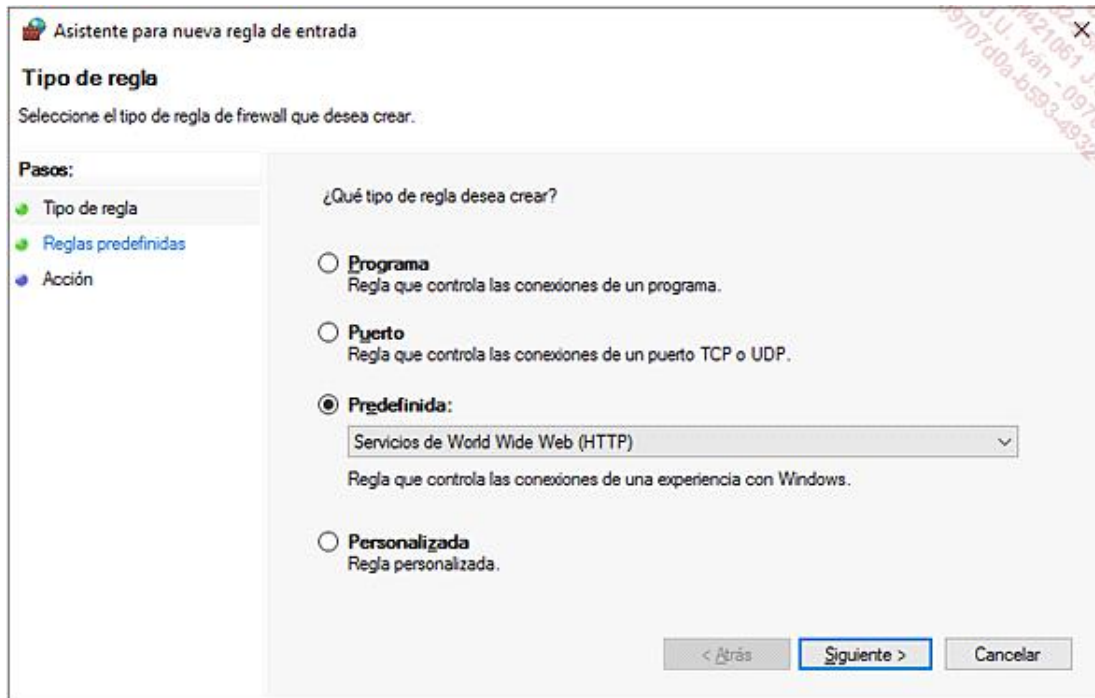
- Confirme con **Aceptar**.
- Una vez terminada la instalación, haga clic en el botón **Cerrar**. Ejecute el navegador **Microsoft Edge** desde el icono  situado en la barra de tareas e introduzca la URL **http://localhost/** en la barra de direcciones. Aparece el logotipo IIS:



Falta ahora configurar el firewall para impedir el acceso al sitio IIS:

- Desde la pantalla de inicio, pulse las teclas  y **R**, introduzca **wf.msc** en la ventana **Ejecutar** y confirme con la tecla [Intro].
- En el panel izquierdo de la ventana **Firewall de Windows con seguridad avanzada**, haga clic con el botón derecho en **Reglas de entrada** y, a continuación, seleccione **Nueva regla**. Seleccione el tipo de regla que desea crear: **Programa**, **Puerto** (UDP o TCP), **Predefinida** (vinculada a las funcionalidades de Windows 10) y **Personalizada** (combina programa, protocolo y puertos).

Para este ejemplo, elija **Predefinida** y seleccione **Servicios de World Wide Web (HTTP)** en la lista desplegable.



- Haga clic en el botón **Siguiente**, marque la opción **Servicios World Wide Web (HTTP)** y de nuevo en **Siguiente**.
- Marque la opción **Bloquear la conexión**. Observe que podría **Permitir la conexión si es segura** (protocolo IPsec). Confirme haciendo clic en el botón **Finalizar**.

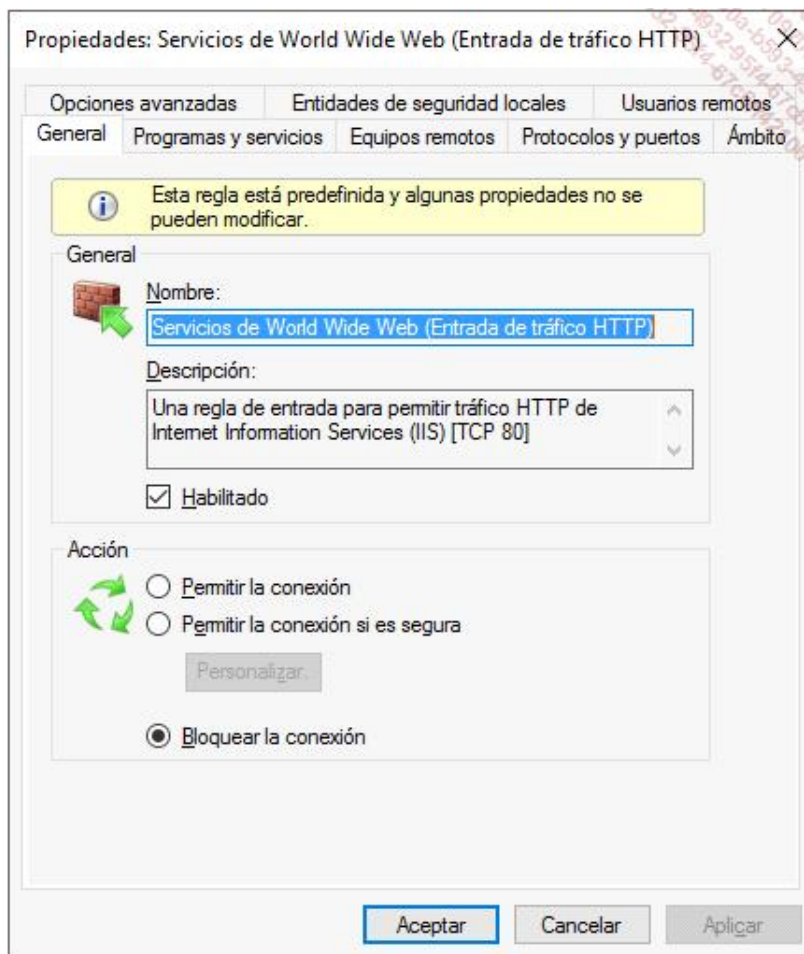
En PowerShell, el comando **New-NetFirewallRule** permite crear reglas de entrada o de salida en un conjunto de puestos: **New-NetFirewallRule -DisplayName "Bloqueo ISS" -DirectionInbound -LocalPort 80 -Protocol TCP -Action Block** bloquea el puerto TCP 80 de entrada en el puesto de trabajo con Windows 10.

Para modificar una regla existente, emplee el comando PowerShell **Set-NetFirewallRule**. La eliminación de una regla del firewall se realiza mediante el comando **Remove-NetFirewallRule**.

A continuación, pruebe la conexión al sitio interno IIS:

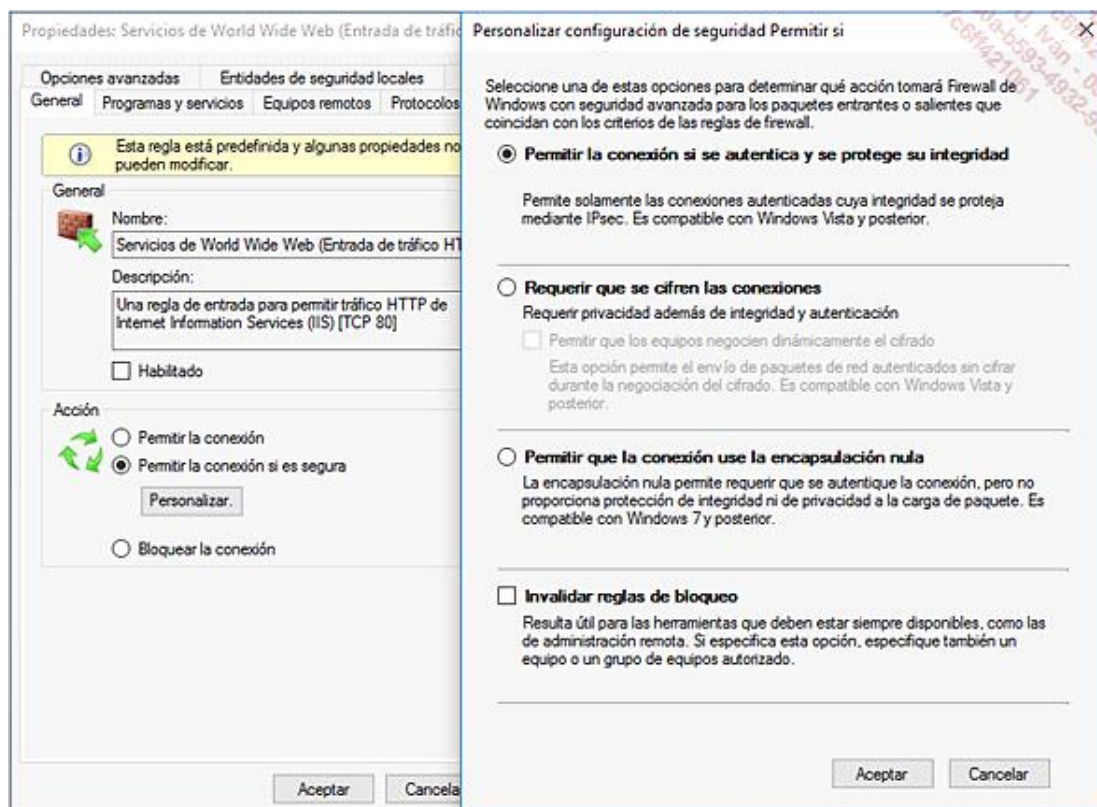
- Introduzca otra vez la URL <http://localhost> en el navegador Microsoft Edge. El sitio IIS no aparece más.

Una vez creada la regla, es posible definir para ella parámetros avanzados seleccionándola con el botón derecho y editando sus **Propiedades**. Por ejemplo, la pestaña **Ámbito** especifica las direcciones IP locales y remotas a las que la regla se debe aplicar. El administrador puede también definir una regla de conexión segura entre dos recursos en la

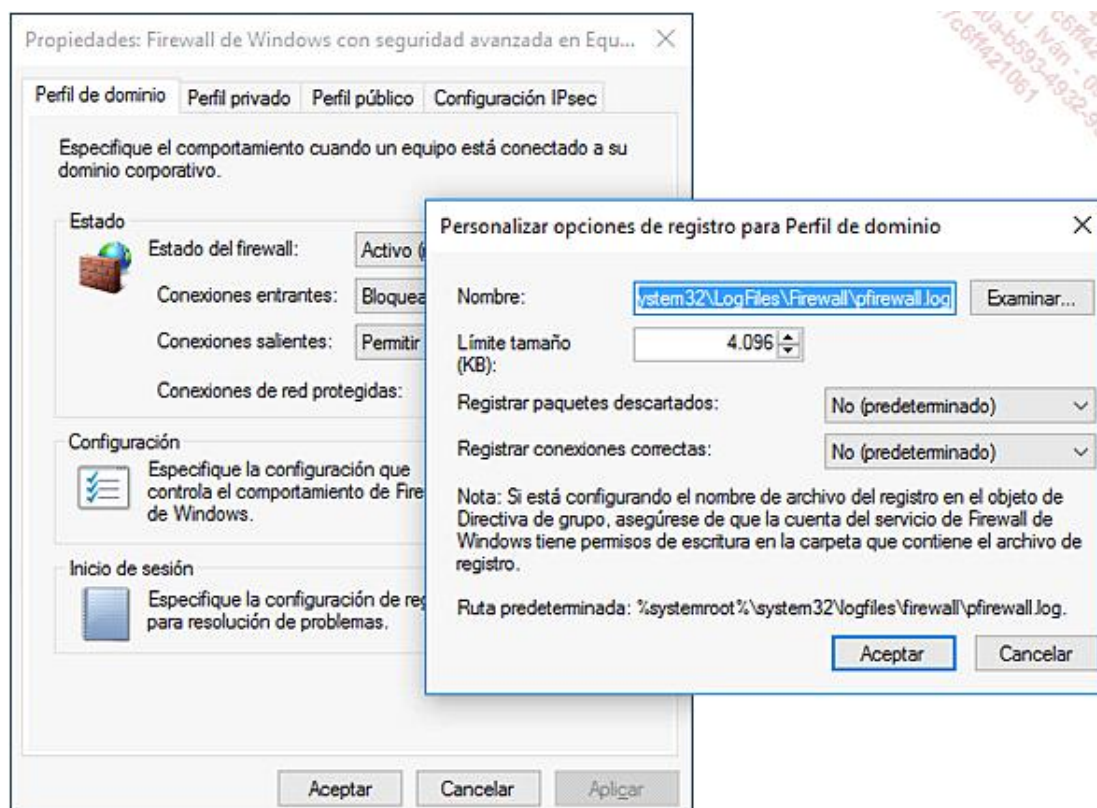


De esta forma, es posible garantizar que un servidor de archivos no responderá a las peticiones de clientes si la conexión iniciada no es segura. Los comandos, accesibles mediante el botón **Personalizar...**, son los siguientes:

- **Permitir la conexión si se autentica y se protege su integridad:** esta opción requiere un sistema Windows Vista o superior.
- **Requerir que se cifren las conexiones:** el administrador puede autorizar a los equipos a negociar el cifrado de forma dinámica. Esta regla solo es aplicable al tráfico entrante.
- **Permitir que la conexión use la encapsulación nula:** esta opción está disponible solamente para un cliente Windows 7 o superior. Exige que el cliente se autentifique, pero no asegura el control de integridad o de cifrado de la conexión entre las partes.
- **Invalidar reglas de bloqueo:** en las reglas predeterminadas del firewall de Windows, las reglas que bloquean explícitamente son siempre prioritarias sobre aquellas que permiten el acceso. Seleccionando esta opción, la conexión se autorizará aunque otra regla la bloquee. Necesita que se especifiquen los equipos remotos autorizados en la pestaña **Equipos remotos** de las propiedades de la regla.



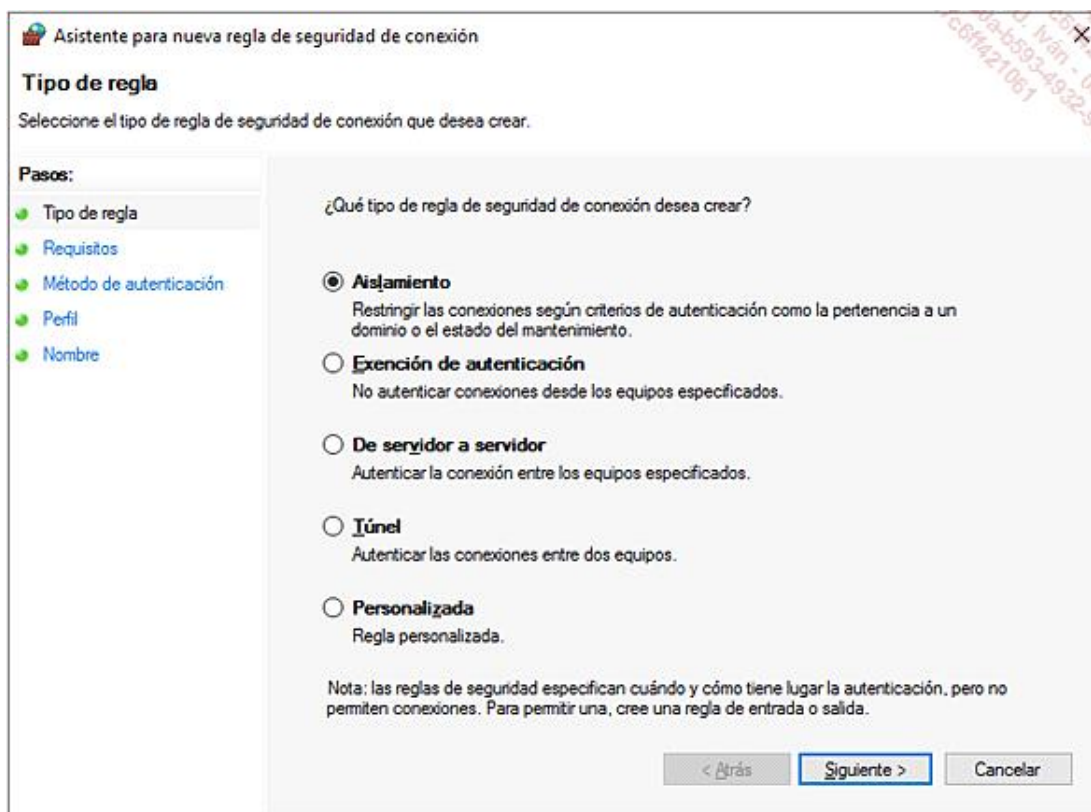
Haciendo clic con el botón derecho en el nodo **Firewall de Windows con seguridad avanzada en Equipo local** y seleccionando **Propiedades**, el usuario puede configurar los parámetros de registro relativos a cada perfil: nombre del registro, tamaño máximo en KB y los tipos de eventos que se han de registrar (**paquetes descartados**, **conexiones correctas**). Por defecto, los registros se almacenan en la carpeta **%systemroot%\system32\LogFiles\Firewall\pfirewall.log**. Esta configuración se efectúa haciendo clic en el botón **Personalizar** de la sección **Inicio de sesión**.



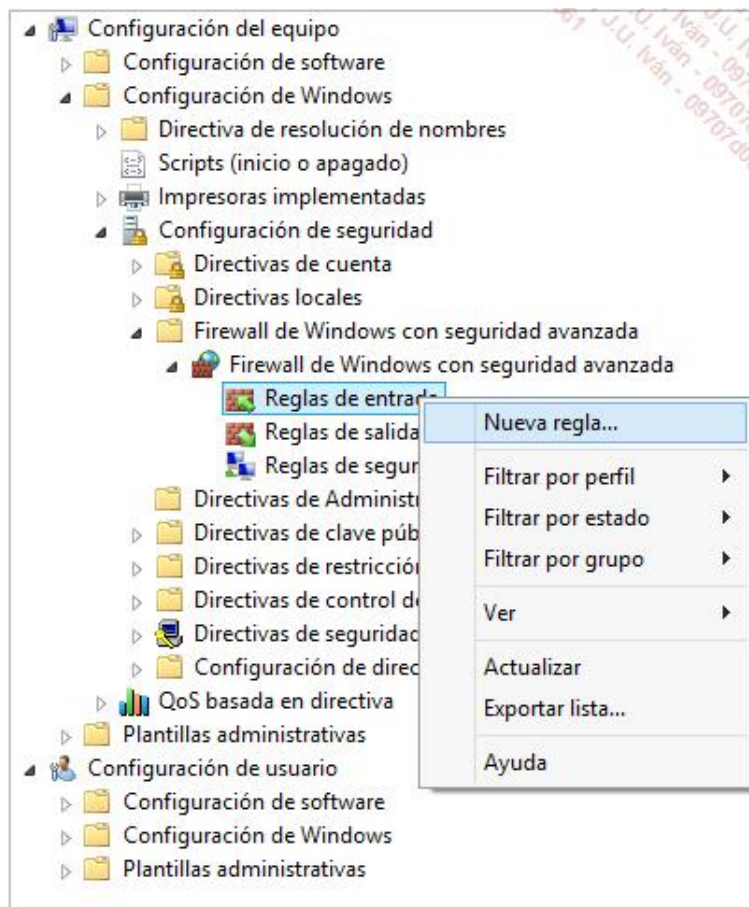
Para verificar que el puerto 80 está efectivamente abierto en el firewall de Windows 10, ejecute el comando **netstat -an | find "80"** en un símbolo del sistema y verifique la línea **LISTENING**.

En la consola de administración del firewall con seguridad avanzada, el nodo **Reglas de seguridad de conexión** ofrece un conjunto de reglas predefinidas para mejorar la seguridad de una conexión. Se presentan cuatro tipos de reglas:

- **Aislamiento:** el equipo aceptará solo las conexiones de equipos o usuarios miembros de su dominio. Cualquier otra conexión será rechazada.
- **Exención de autenticación:** los equipos especificados no tendrán necesidad de autenticarse durante la conexión.
- **De servidor a servidor:** funciona de forma análoga al aislamiento, pero solo se aplica a un conjunto definido de direcciones IP cuyos hosts sean miembros de un dominio.
- **Túnel:** protege las comunicaciones sin utilizar el modo de transporte IPsec, sino el modo túnel.



Creando un objeto de directiva de grupo, el administrador del dominio tiene la posibilidad de forzar la activación del firewall y crear reglas personalizadas homogéneas en su red: estos parámetros prevalecerán aunque el usuario final sea el administrador local de su puesto con Windows 10. Esta acción se efectúa editando un objeto de directiva de grupo y seleccionando el nodo **Configuración del equipo - Directivas - Configuración de Windows - Configuración de seguridad - Firewall de Windows con seguridad avanzada y Firewall de Windows con seguridad avanzada**.

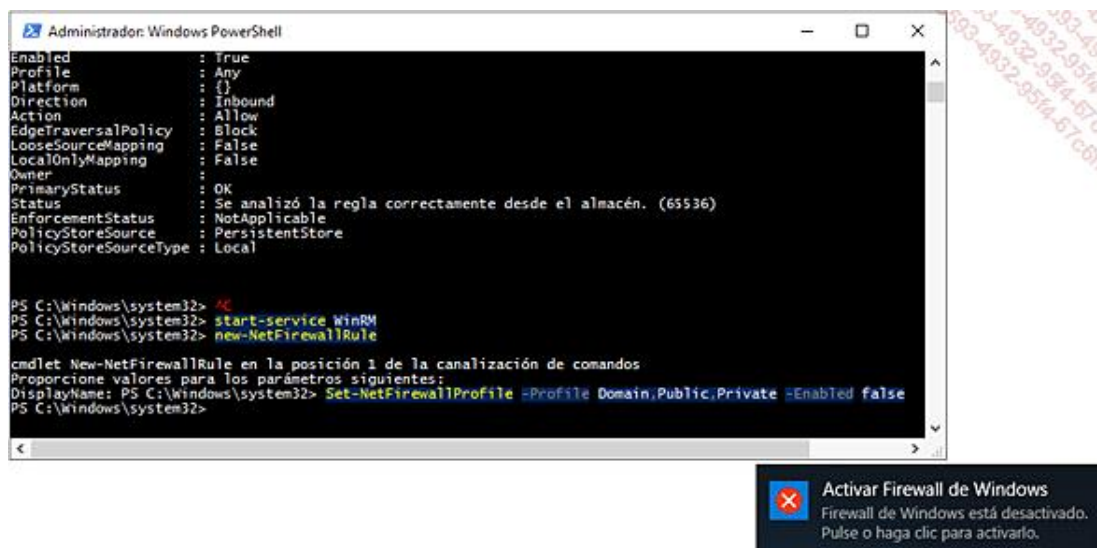


Para dejar inactivo un perfil del firewall:

- En la consola MMC **Firewall de Windows con seguridad avanzada (wf.msc)**, haga clic con el botón derecho en **Firewall de Windows con seguridad avanzada del equipo local** y seleccione **Propiedades**.
- Haga clic en la pestaña del perfil que se debe desactivar y seleccione **Inactivo** en el campo **Estado del firewall**.

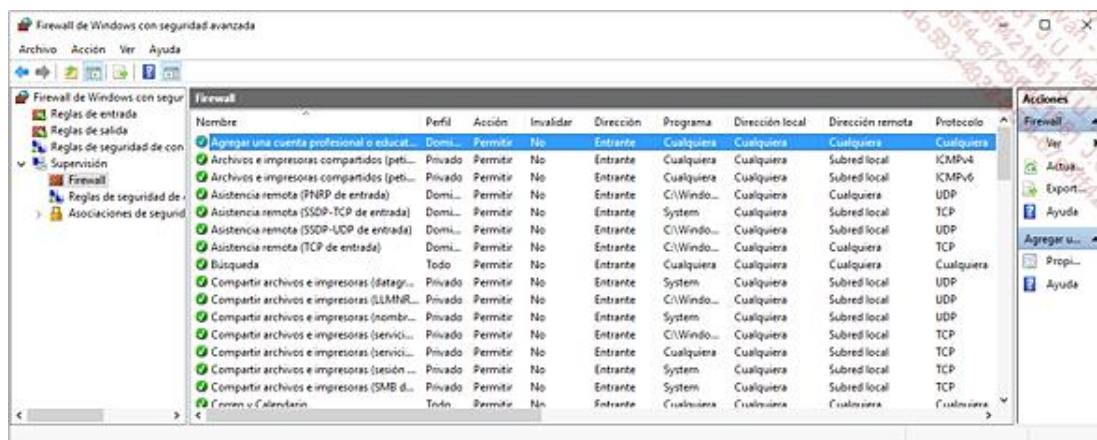
Para desactivar todos los perfiles, ejecute un símbolo del sistema como administrador local, introduzca **netsh advfirewall set allprofiles state off** y confirme con [Intro].

Es posible deshabilitar el firewall en todos los perfiles de un conjunto de puestos con Windows 10 mediante el comando PowerShell **Set-NetFirewall-Profile: Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled false**



En la consola de administración del firewall con seguridad avanzada, el nodo **Supervisión** muestra las reglas de firewall y de seguridad en vigor, los perfiles activos, así como sus parámetros y las asociaciones de seguridad.

Su uso tiene todo el sentido cuando el administrador tiene la necesidad de una visión global de los puertos abiertos. Las columnas **Dirección local** y **Dirección remota** muestran la información en función de la regla del firewall. El menú **Ver** y **Agregar o quitar columnas...** permite al administrador personalizar la interfaz.



➤ Solo las reglas aplicadas a los perfiles actualmente activos se muestran en el nodo **Supervisión**.

El nodo **Asociaciones de seguridad** muestra la información utilizada para proteger las comunicaciones entre dos equipos, incluyendo los puntos finales.

Administrador de credenciales

El inicio de sesión único, o SSO (*Single Sign On*), permite a un usuario de un sistema Windows 10 realizar una única autenticación para acceder a varios recursos (servidores, sitios de Internet, etc.). Con frecuencia, un usuario utiliza la misma contraseña para acceder a sitios de Internet diferentes (Facebook, LinkedIn, correo electrónico como Windows Live) reduciendo de esta manera el nivel de seguridad de estos servicios: si la contraseña compartida se sustrajera, todos los recursos que protege se verían comprometidos.

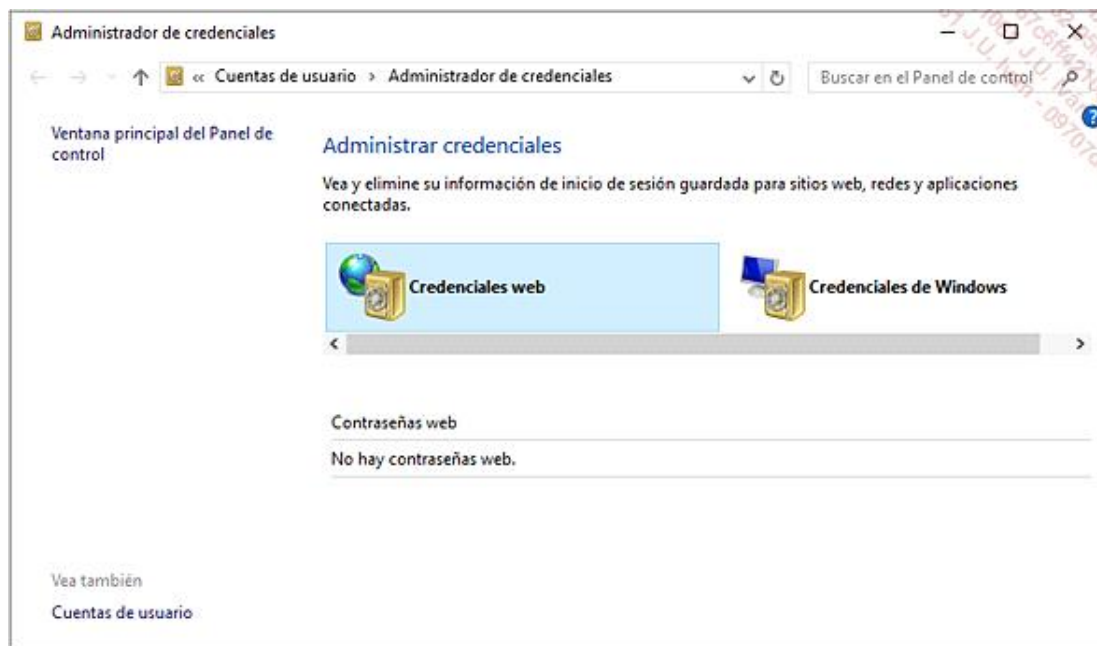
Frente a esta problemática, Microsoft presenta el **Administrador de credenciales**, que es una caja fuerte electrónica cuya principal función es el almacenamiento seguro de los identificadores y contraseñas utilizados regularmente por una cuenta de usuario. Windows 10 se encarga, en lo sucesivo, de introducirlos automáticamente durante el acceso a un recurso específico.

Las contraseñas pueden volverse más complejas porque el trabajo de memorizarlas ya no es necesario: aquello que ignoramos no puede ser revelado.

Utilizando una cuenta de Microsoft para autenticarse, el usuario puede abrir sesiones en otros puestos con Windows 10 y así acceder a sus aplicaciones protegidas por contraseñas almacenadas en la caja fuerte. Esta característica está activada de forma predeterminada cuando el equipo es miembro de un grupo de trabajo, pero se desactiva automáticamente al unirse a un dominio Active Directory para evitar la fuga de datos confidenciales.

El **Administrador de credenciales** está asociado a la protección de los usuarios:

- Desde el campo de búsqueda situado en la barra de tareas, introduzca **administrador de credenciales** y seleccione **Administrador de credenciales**. También puede acceder desde el **Panel de control**.



Se ofrecen dos categorías:

- **Credenciales web**: cuando el usuario desea acceder a una página de Internet que solicite una autenticación de tipo nombre de usuario y contraseña, Microsoft Edge muestra una cinta en la parte inferior de la ventana que permite almacenar las credenciales.



Así, en el próximo acceso al sitio de Internet, las credenciales se introducirán automáticamente. Microsoft Edge gestiona

la creación de la copia de seguridad de las credenciales. El Administrador de credenciales gestiona la lectura y la eliminación de esa información.


- **Credenciales de Windows:** Windows 10 permite guardar el identificador y la contraseña que se utilizan al conectarse a un servidor remoto. Cuando se realiza la autenticación empleando una tarjeta inteligente, es posible almacenar las **Credenciales basadas en certificados**. La sección **Credenciales genéricas** almacena las identidades vinculadas a aplicaciones como el servicio Windows Live. A diferencia de la categoría Credenciales Web, la categoría Credenciales de Windows ofrece al usuario la posibilidad de agregar o modificar manualmente las credenciales.

Para proteger el acceso a un servidor Windows, siga el siguiente procedimiento:

- En la ventana **Administrador de credenciales**, haga clic en **Credenciales de Windows** y, a continuación, en **Agregar una credencial de Windows**.
- Introduzca la dirección IP del servidor remoto, en este ejemplo 192.168.0.5, y, a continuación, introduzca un nombre de usuario y una contraseña para poder acceder.

- Confirme haciendo clic en el botón **Aceptar**.
- Posteriormente podrá **Editar** o **Quitar** las credenciales introducidas previamente desde la sección llamada 192.168.0.5 del **Administrador de credenciales**.

Para desactivar el almacenamiento de credenciales vinculadas a una autenticación de red, es preciso editar la directiva de seguridad:

- Desde la pantalla de inicio, pulse las teclas  y **R**, introduzca **secpol.msc** en la ventana **Ejecutar** y acepte con la tecla [Intro].
- Desde el árbol de la consola **Directiva de seguridad local**, despliegue los nodos **Directivas locales** y **Opciones de seguridad**. Haga doble clic en el parámetro **Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de red** y marque la opción **Habilitada**.

Auditoría

La auditoría en un dominio Active Directory o un grupo de trabajo permite seguir las acciones realizadas por los usuarios y sus equipos. En función de la información registrada, el administrador podrá visualizar y corregir un problema, pero también detectar una intrusión y, de este modo, anticipar un nuevo tipo de ataque.

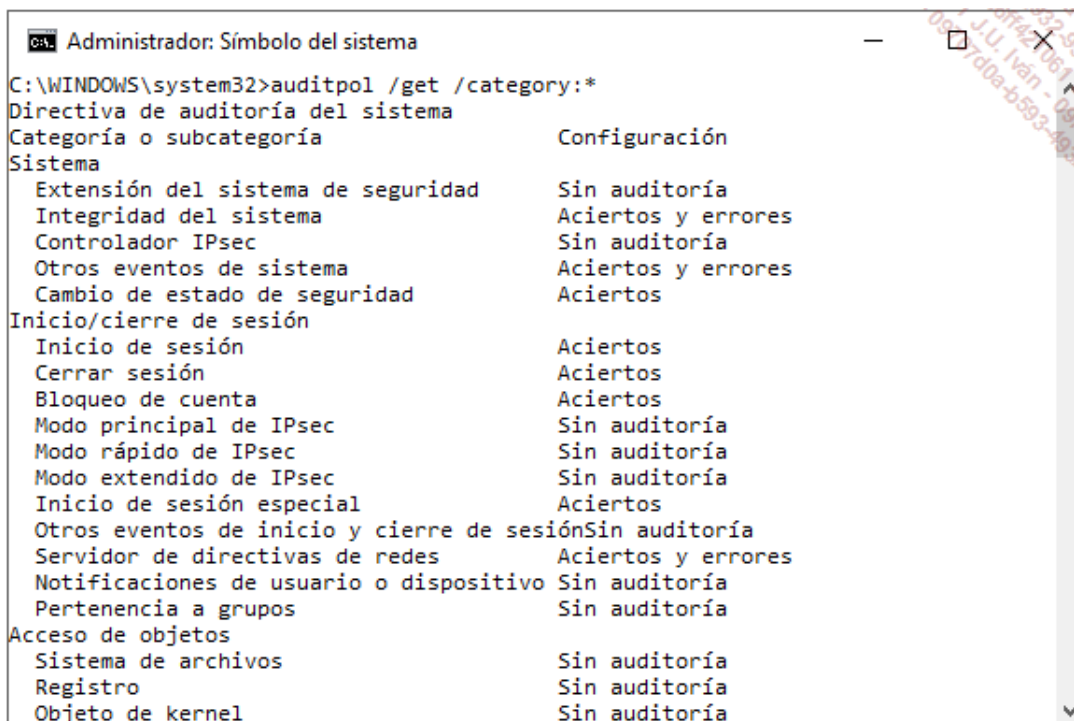
Generalmente, los eventos de error son más instructivos que aquellos vinculados al éxito. No todo debe ser auditado, ya que el uso de esta funcionalidad conlleva un carga adicional (CPU, RAM, espacio en disco) en los puestos de trabajo, servidores y controladores de dominio.

Un atacante con privilegios de administrador podrá eliminar sus huellas y, por tanto, los registros en los que se inscriben sus acciones malintencionadas: puede ser interesante separar los roles, otorgando a una cuenta de servicio, por ejemplo, el derecho de generar los eventos en un servidor remoto dedicado al almacenamiento, pero no concediendo a esa cuenta los permisos para eliminarlos o modificarlos. Una cuenta de auditoría tendrá acceso de lectura al registro con el fin de evaluarlo. Estas acciones pueden realizarse mediante los eventos reenviados (consulte el capítulo Protección y recuperación del sistema - Reparación del sistema).

La directiva de auditoría se ha ampliado con Windows Server 2012 y Windows 10. Recibe el nombre de **Configuración de directiva de auditoría avanzada**. Ya no son 9 categorías de eventos que pueden ser objeto de una auditoría, sino 53 (contando las subcategorías), clasificadas en las categorías siguientes:

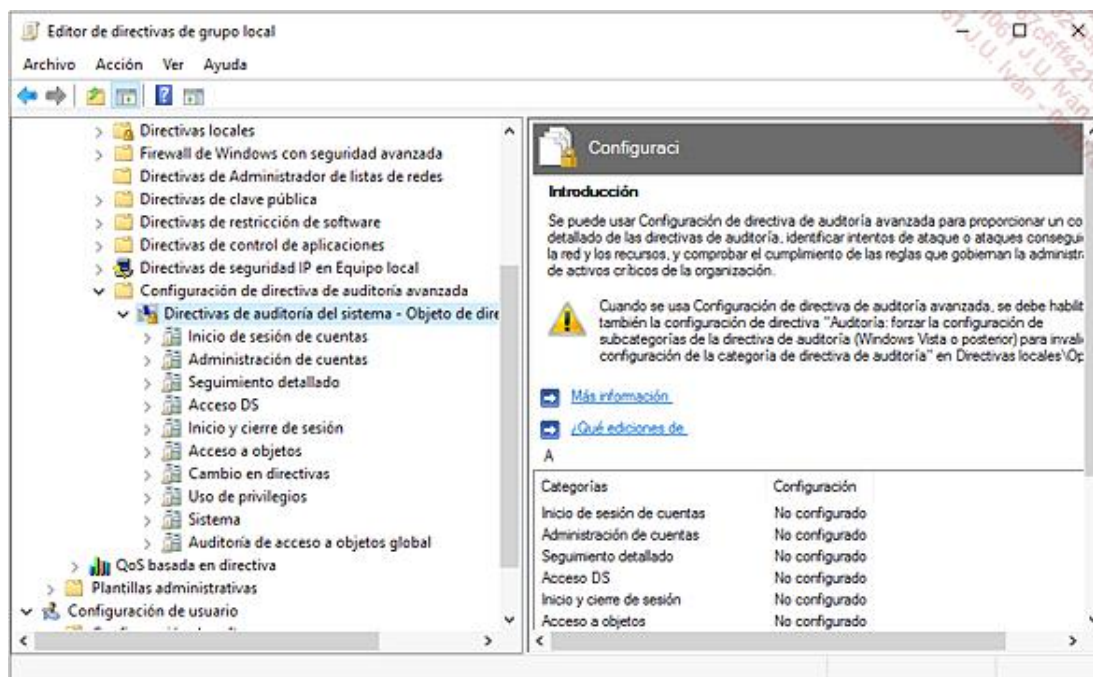
- Conexión de cuenta
- Administración de cuentas
- Seguimiento detallado
- Acceso DS
- Inicio/cierre de sesión
- Acceso de objetos
- Cambio de plan
- Uso de privilegios
- Sistema
- Auditoría de acceso a objetos global

Para mostrar la lista de categorías y subcategorías disponibles, introduzca el comando **auditpol /get /category:*** en un símbolo del sistema ejecutado como administrador:



Por ejemplo, si desea auditar las modificaciones realizadas con éxito en los grupos de seguridad en un cliente Windows 10 miembro de un grupo de trabajo, realice las siguientes operaciones:

- Pulse las teclas **Windows** + **R**. Introduzca **gpedit.msc** en la ventana **Ejecutar** y confirme con la tecla [Intro].
- En la ventana **Editor de directivas de grupo local**, despliegue los nodos **Configuración del equipo** - **Configuración de Windows** - **Configuración de seguridad** - **Configuración de directiva de auditoría avanzada** y **Directivas de auditoría del sistema** - **Objeto de directiva de grupo local**.



- Haga clic en la categoría **Administración de cuentas** y doble clic en **Auditar administración de grupos de seguridad**. En la ventana **Propiedades**, marque las opciones **Configurar los siguientes eventos de auditoría** y **Correcto**.

- La configuración avanzada de la directiva de auditoría puede modificarse mediante un objeto de directiva de grupo y aplicarse a miembros específicos de un dominio.

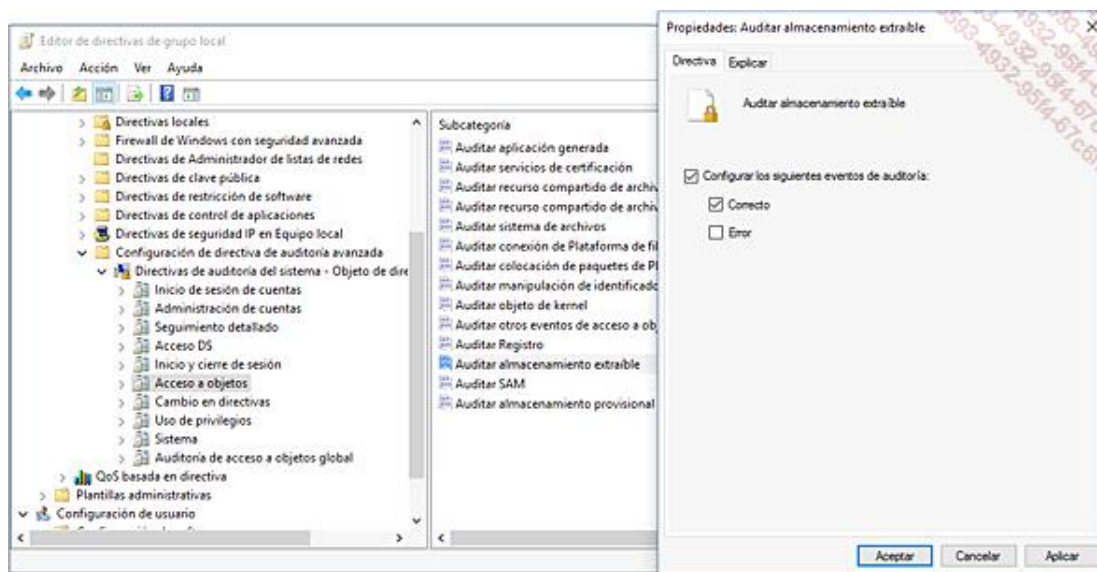
Un registro de eventos interesante es el concerniente a la **Razón de acceso**: cuando un evento se produce, se registra la razón por la cual la operación ha sido autorizada o rechazada.

El parámetro **Auditar acceso a archivos** contiene ahora información detallada sobre los atributos del archivo al que un usuario accede (eventos número 4656 y 4663).

Si un administrador desea conocer el uso de los dispositivos de almacenamiento extraíbles en la red empresarial, puede hacerlo empleando la opción **Auditoría de dispositivos de almacenamiento extraíble**. Se crea un evento de auditoría cada vez que un usuario accede a una memoria flash USB:

- Escritura o lectura exitosa (evento número 4663).
- Errores de acceso (evento número 4656).

Esta directiva de auditoría se configura desde el nodo **Configuración del equipo - Configuración de Windows - Configuración de seguridad - Configuración de directiva de auditoría avanzada - Directivas de auditoría del sistema - Objeto de directiva de grupo local y Acceso a objetos**. El parámetro se llama **Auditar almacenamiento extraíble**.



Las anteriores directivas de auditoría están todavía disponibles, pero pueden entrar en conflicto con la auditoría avanzada. En ese caso, active el parámetro **Auditoría: forzar la configuración de subcategorías de la auditoría de directiva (Windows Vista o posterior)** para invalidar la configuración de la categoría de directiva de auditoría en el nodo **Configuración del equipo - Configuración de Windows - Configuración de seguridad - Directivas locales - Opciones de seguridad**. De esta forma, la auditoría de seguridad básica será sistemáticamente ignorada en beneficio de la auditoría avanzada.

Otra mejora importante es el registro de las modificaciones del servicio de directorio. Con las anteriores versiones de servidor de Windows, la auditoría de los servicios de Active Directory registraba el nombre del atributo modificado, pero no su antiguo ni su nuevo valor. Con Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2, la subcategoría **Auditar cambios de servicio de directorio** resuelve esta carencia.

La gestión de los registros de eventos (archivo, eliminación, etc.) es importante en un entorno empresarial, al igual que la comprensión de los eventos generados. El comando **wevtutil.exe** gestiona los eventos y los mensajes

asociados.

De esta forma, **wevtutil el** muestra todos los registros de Windows. Para obtener una lista de proveedores de eventos, el comando **wevtutil gp "Microsoft-Windows-Application Server-Applications" /ge:true /gm:true** presenta un listado con todos los eventos vinculados a las aplicaciones de servidor de Microsoft.

Seguridad en Microsoft Edge

Microsoft Edge es el navegador de Internet incluido con Windows 10. Ya no incluye soporte para barras de herramientas, scripts Visual Basic ni ActiveX, elementos que eran frecuentemente explotados por los hackers. Las extensiones usarán solamente HTML5 y JavaScript.

Además, Microsoft Edge alberga cada pestaña en un "sandbox", contenedor totalmente independiente que hospeda la página web visitada.

Otra funcionalidad interesante es la posibilidad de autenticarse en un sitio de Internet empleando su cuenta Passport (código PIN e identificación biométrica).

Aporta mejoras en términos de seguridad, tales como **Exploración de InPrivate**, que permite visitar sitios de Internet sin dejar huella. **SmartScreen** comprueba el sitio visitado es una lista de sitios reportados como maliciosos. La protección de rastreo (funcionalidad **Do Not Track**) tiene como objetivo impedir que un sitio obtenga sus hábitos de navegación para proponerle anuncios publicitarios.



El navegador de Microsoft se ha creado utilizando el ciclo de vida de desarrollo de la seguridad (SDL): Microsoft Edge impide, por ejemplo, que código malintencionado se ejecute en una memoria definida como no ejecutable. En adelante, el bloqueo de ventanas emergentes se encuentra activado, limitando de esta forma la aparición intempestiva de publicidad.

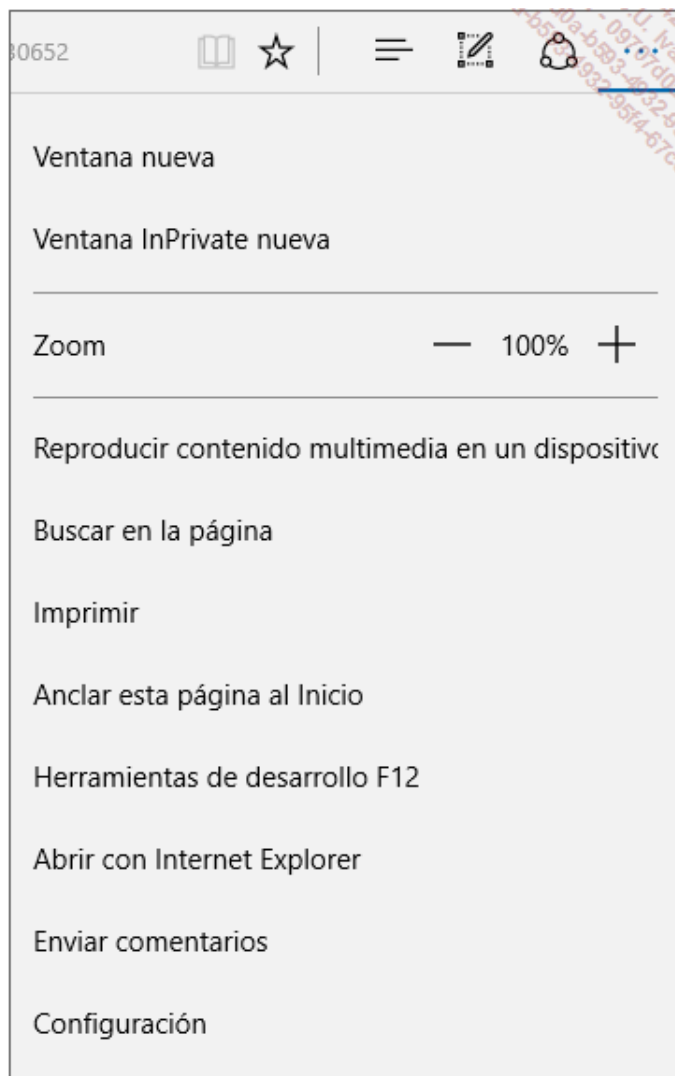
1. Protección Do Not Track

Cuando un usuario visita un sitio de Internet, es posible que exista contenido publicitario, diseñado en función de sus hábitos y comportamiento, que se muestre en el navegador para, de este modo, explotarse con fines comerciales.

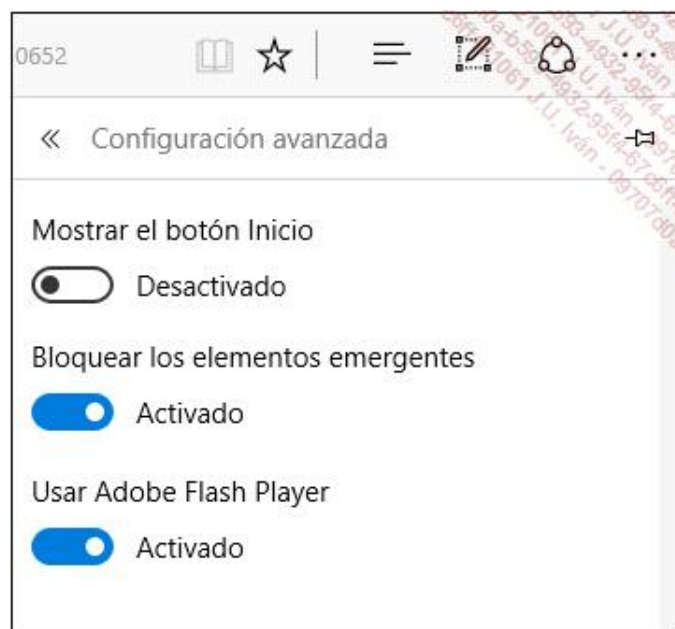
Microsoft parte del principio de que es el usuario quien debe decidir qué información quiere comunicar para su explotación a sitios de terceros, y no a la inversa.

La funcionalidad Do Not Track no se encuentra activada por defecto; este es el procedimiento que hay que seguir para remediarlo:

→ Desde el escritorio, ejecute el navegador **Microsoft Edge** haciendo clic en el icono  situado en la barra de tareas. A continuación, seleccione el menú  y luego **Configuración**.



→ Haga clic en el botón **Ver configuración avanzada**. En **Configuración avanzada**, active el parámetro **Bloquear los elementos emergentes**.



La protección contra el rastreo permanece activa para cualquier sitio visitado.

Microsoft Edge refuerza la confidencialidad de los hábitos de los usuarios enviando cabeceras DNT (*Do Not Track*) a los sitios para que no realicen seguimiento. Sin embargo, un sitio puede solicitar una excepción requiriendo la autorización de seguimiento a los usuarios que naveguen por él. Si el usuario aprueba la solicitud, Microsoft Edge registra una excepción y envía las cabeceras DNT al sitio de Internet autorizado al seguimiento.


2. Filtro SmartScreen

El filtro **SmartScreen** verifica los sitios de Internet visitados comparándolos con una lista de sitios de phishing (suplantación de identidad) que se mantiene al día.

La suplantación de identidad se utiliza para recuperar información confidencial (número de tarjeta de crédito, nombre de usuario y contraseña) de los usuarios haciendo creer a la víctima que se dirige a un sitio de confianza. La mayoría de los sitios falsificados hacen referencia a bancos o a medios de pago asociados, como Paypal.

Si se detecta un sitio de Internet falsificado, Microsoft Edge bloquea la totalidad del sitio. El filtro SmartScreen se combina con el módulo de descargas para controlar el software descargado.

Microsoft mantiene una lista de sitios conocidos como potencialmente peligrosos.


El filtro SmartScreen está activado por defecto. Para desactivarlo, bastará con hacer clic en el menú  y, a continuación, seleccionar **Configuración** y **Ver configuración avanzada**. En **Configuración avanzada**, desactive el parámetro **Proteger mi PC contra las descargas y los sitios malintencionados con el filtro SmartScreen**.

3. Navegación InPrivate


La navegación **InPrivate** responde a una creciente necesidad de protección de la vida privada de los internautas; esta funcionalidad borra las huellas dejadas en un puesto de trabajo con Windows 10 cuando se visitan sitios de Internet.


Las cookies, los archivos temporales de Internet, el historial de páginas web visitadas, los datos de formularios, el autocompletar para la búsqueda son eliminados cuando el usuario cierra la ventana de navegación InPrivate. De este modo, las huellas del usuario se borran del sistema.

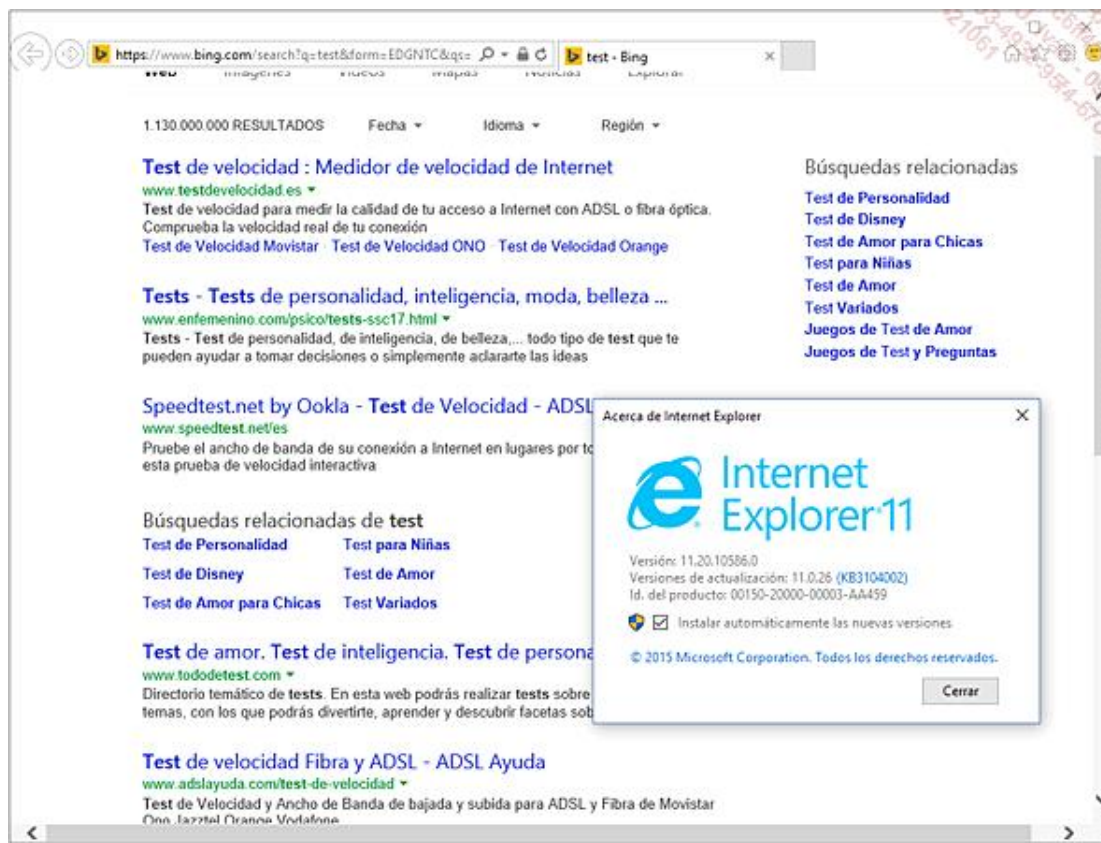
Para activar la navegación InPrivate:

- Desde el navegador **Microsoft Edge**, haga clic en el menú  y, a continuación, en **Ventana InPrivate nueva**.



-  La navegación InPrivate solo está disponible mientras la pestaña esté abierta.

Por último, sepa que el antiguo navegador de Microsoft se encuentra disponible con Windows 10 desde la zona de búsqueda situada en la barra de tareas (introduzca **Internet explorer**) o bien desde Microsoft Edge haciendo clic en el menú  y en **Abrir con Internet Explorer**.



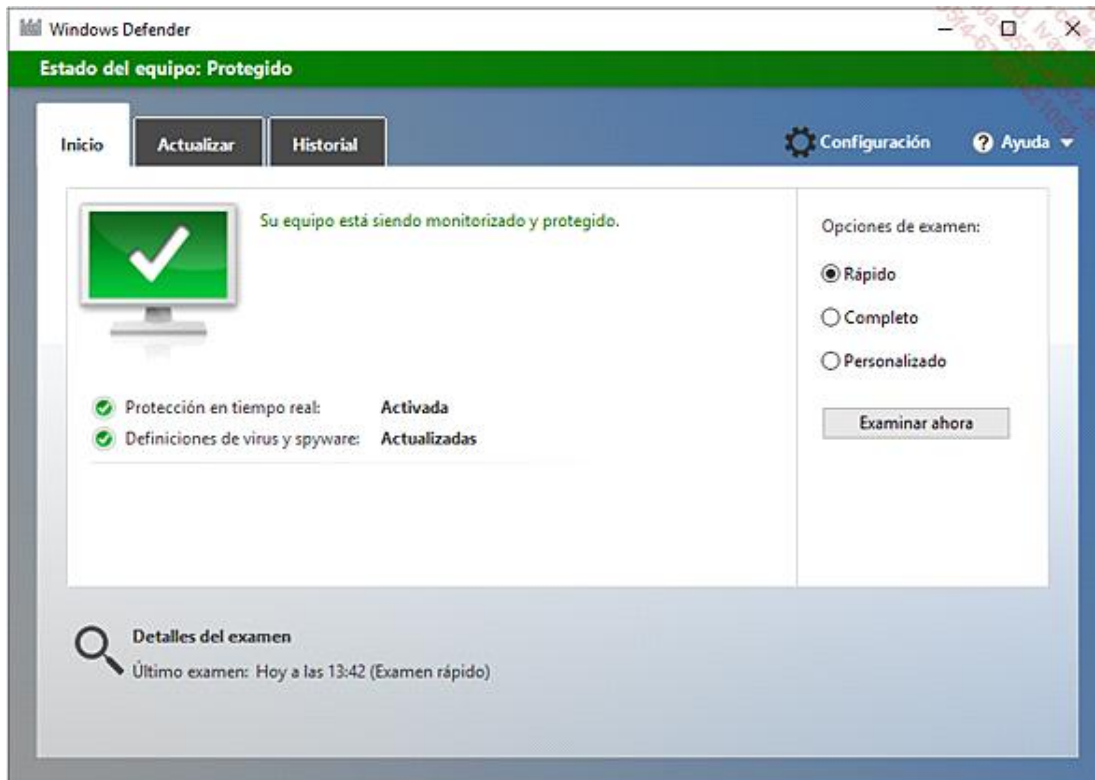
Windows Defender

Para ayudar al administrador a proteger Windows 10 contra un software espía o malintencionado, Microsoft proporciona **Windows Defender** de forma gratuita. Esta aplicación permite verificar los puestos de trabajo físicos o virtuales y ofrece las funciones comunes a los programas de la competencia:

- Actualizaciones automáticas de las definiciones de virus empleando el servicio Windows Update.
- Análisis rápido, completo, manual o planificado: posibilidad de excluir archivos, carpetas, particiones y procesos.
- Alertas que se muestran en el Centro de actividades durante la instalación o ejecución de programas no deseados: según su nivel, se proponen cuatro acciones: ignorar, poner en cuarentena, eliminar o autorizar siempre.
- Protección en tiempo real de los componentes críticos del sistema: un agente controla los programas iniciados automáticamente, los parámetros de Windows 10, los componentes adicionales y descargas de Microsoft Edge, los servicios y controladores, la inscripción y ejecución de aplicaciones.

Es posible acceder a Windows Defender desde el Panel de control:

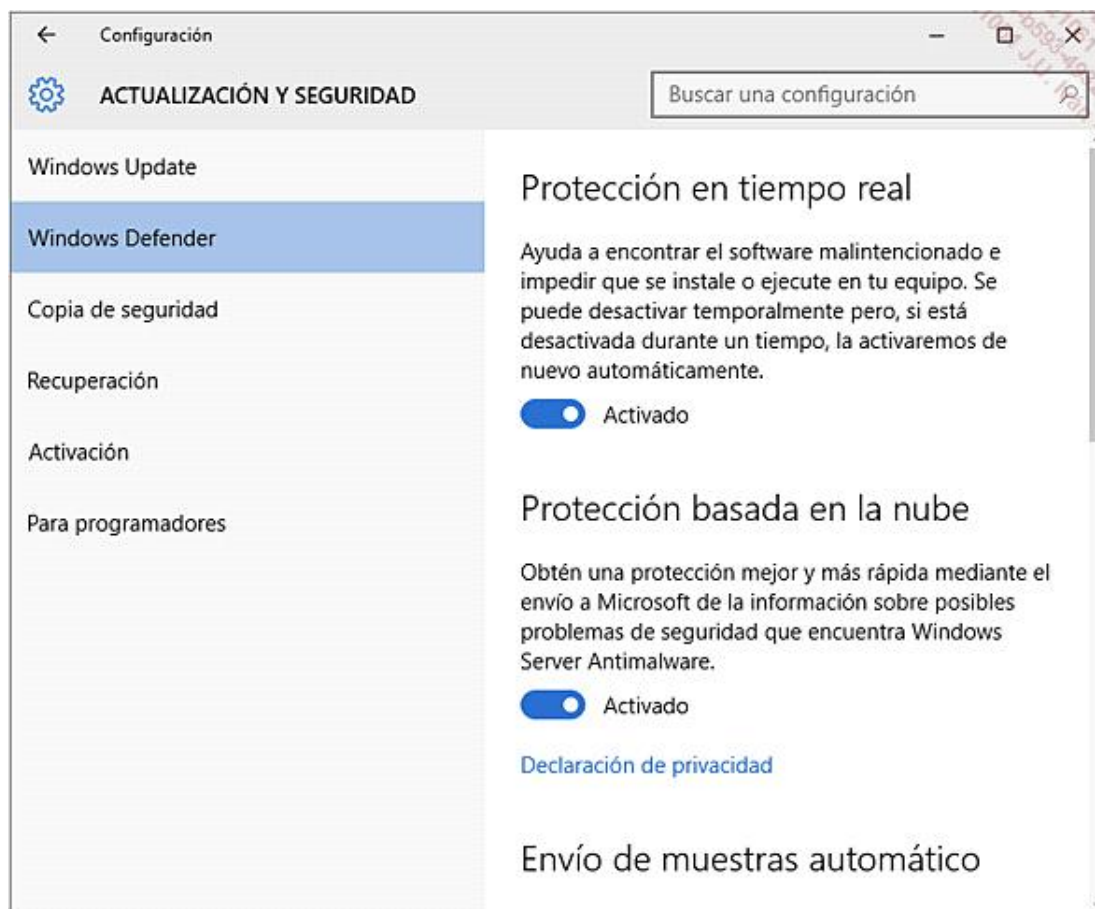
→ Haga clic con el botón derecho en el menú **Inicio** y luego en **Panel de control**. Luego haga clic en **Windows Defender**.



El software adopta la misma interfaz que el antivirus MSE (*Microsoft Security Essentials*):

- La pestaña **Inicio**: muestra el estado de protección del antivirus. Permite iniciar un examen rápido, completo o personalizado del ordenador.
- La pestaña **Actualizar**: permite, empleando el botón **Actualizar**, forzar una actualización de la base de datos de definiciones de virus. Se muestra la fecha de las definiciones de virus y de software espía.
- La pestaña **Historial**: muestra los virus detectados y puestos en cuarentena. Como administrador, es posible eliminarlos de manera selectiva, eliminarlos todos o restaurarlos.
- El botón **Configuración**: permite configurar Windows Defender de forma precisa, activando la protección en tiempo

real, especificando los archivos que se han de excluir y sus extensiones, etc.



La herramienta **MpCmdRun.exe**, ubicada en la carpeta **C:\Program Files\Windows Defender**, permite descargar actualizaciones de definiciones de virus o ejecutar exámenes. Se crean entradas en el **Planificador de tareas** para llevar a cabo acciones periódicamente, como la actualización de las definiciones de virus.