

Actividad 18. Configuración de seguridad Windows

Windows 11 es uno de los sistemas con mayores herramientas de seguridad en la actualidad, que se consideran realmente efectivas para proteger la privacidad de sus usuarios.

Hay una serie de funciones que ayudan a mantener la seguridad de la información de tu equipo:

Actualizar Windows 11

Una de las formas de evitar que tus datos se expongan es mantener actualizado Windows 11 a la última versión siempre que se requiera. Para ello, lo único que tienes que hacer es dirigirte al menú de Inicio y escribir la palabra Configuración en la barra de búsqueda. También puedes acceder haciendo clic en el icono de menú de Inicio con el botón derecho.

A continuación, pinga en la pestaña donde dice **Windows Update** y haz clic en **Buscar actualizaciones**. Si hay alguna disponible, simplemente descárgala e instálala y reinicia el PC cuando te lo pida. Hacer este proceso con regularidad garantizará que tu información esté resguardada, además de mejorar el sistema en su conjunto.

Este consejo lo aplicamos en Windows 11, pero la realidad es que nos sirve para cualquier programa o para cualquier dispositivo. Las actualizaciones no solo sirven para añadir nuevas características, también para cerrar agujeros de seguridad.

Windows Update



¡Todo está actualizado!

Última comprobación: hoy, 6:52

Buscar actualizaciones

Más opciones



Obtén las últimas actualizaciones en cuanto estén disponibles

Sé de los primeros en obtener las últimas actualizaciones, correcciones y mejoras que no sean de seguridad a medida que se implementen.

Más información

Activado



Pausar actualizaciones

Pausar durante 1 semana



Historial de actualizaciones



Opciones avanzadas

Optimización de la entrega, actualizaciones opcionales, horas activas, otros ajustes de actualización



Programa Windows Insider

Obtenga versiones preliminares de Windows para compartir comentarios sobre las nuevas características y actualizaciones





Introduce contraseñas


Otra manera de proteger tus datos más sensibles es estableciendo una contraseña de inicio de sesión que tú solo conozcas. Para ello, vuelve al menú de Inicio e ingresa en Configuración. Ve a **Cuentas** y luego a **Opciones de inicio de sesión**. En la siguiente página, en **Formas de inicio de sesión**, selecciona la que consideres, como huella dactilar en algunos casos, reconocimiento facial en otros o con un PIN, o expande la opción Contraseña y haz clic en Agregar para introducir una contraseña.


Cuentas > **Opciones de inicio de sesión**


Formas de iniciar sesión


 Reconocimiento facial (Windows Hello)
Esta opción no está disponible actualmente

 Reconocimiento de huellas digitales (Windows Hello)
Esta opción no está disponible actualmente

 PIN (Windows Hello)
Iniciar sesión con un PIN (recomendado)

 Llave de seguridad
Iniciar sesión con una clave de seguridad física

 Contraseña
Iniciar sesión con la contraseña de la cuenta

 Contraseña de imagen
Desliza el dedo y pulsa en tu foto favorita para desbloquear el dispositivo

Observa que Windows Defender esté activo

A pesar de no ser el antivirus más efectivo, Windows Defender está instalado de forma predeterminada y adaptado perfectamente al sistema operativo, por lo que, si no dispones de otro defensor de malware, nunca está de más tener habilitado constantemente el oficial de Microsoft.

De esta forma, para cerciorarte de ello deberás entrar en Configuración, **Privacidad y Seguridad y Seguridad de Windows**. Las áreas de protección tendrán que estar con un tick verde. De no ser así, pulsa en Abrir seguridad de Windows y activa todas las casillas.



Utiliza la cuenta Estándar

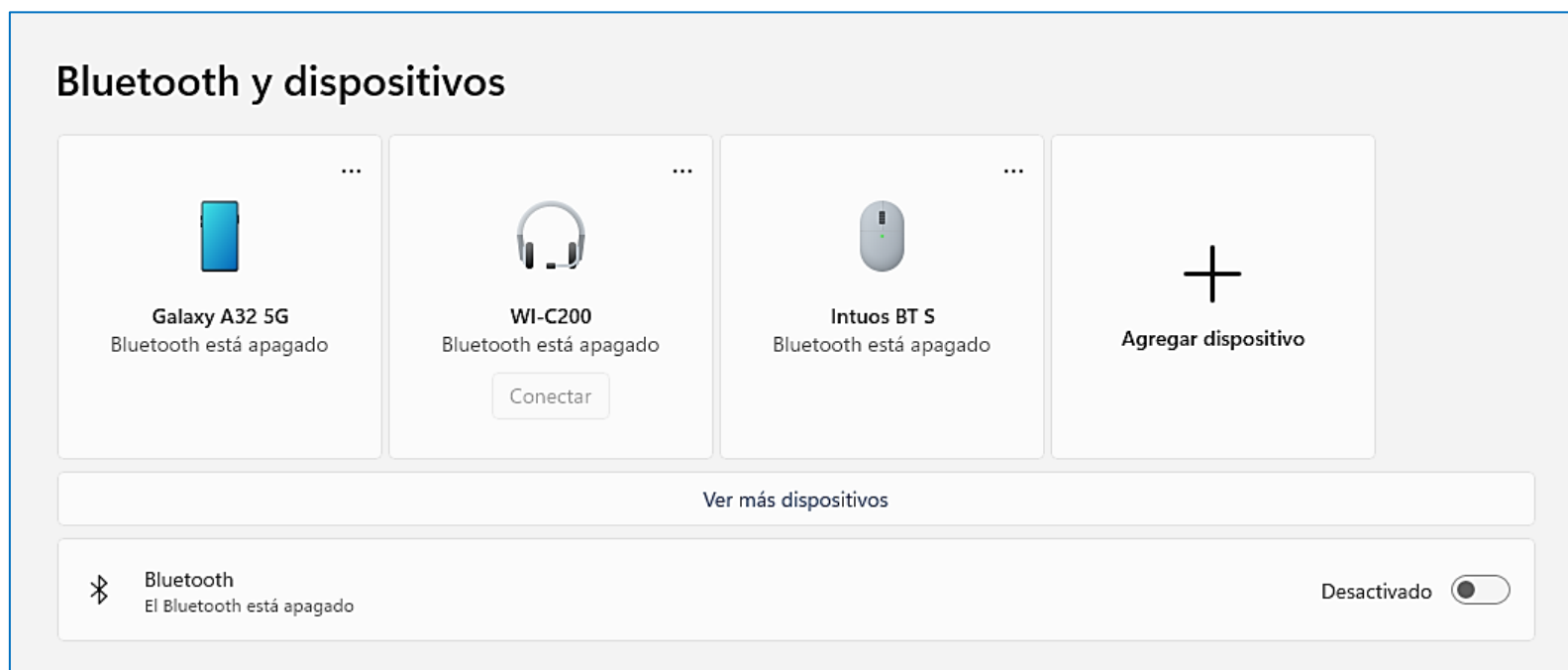
En el caso de que un familiar y o un amigo quiera usar tu PC y quieras a toda costa evitar que salgan a la luz tus datos, lo mejor que puedes hacer es **agregar una cuenta de usuario Estándar** y cada vez que se tenga que realizar un cambio en el sistema se solicitará la contraseña del Administrador, con el fin de limitar el acceso.

Para realizar esta acción, ve a Configuración, **Cuentas, y selecciona Otros usuarios**. Después pincha en **Agregar cuenta** y en el texto azul donde dice No tengo información sobre esta persona. Agrega un usuario sin cuenta de Microsoft e ingresa el nombre y contraseña de la nueva cuenta.

Bloquea dispositivos Bluetooth

En el momento que **añadas un dispositivo Bluetooth** y dejes de usarlo, hay una manera para bloquearlo. En este contexto, accede a Configuración, Cuentas y ve a Opciones de inicio de sesión. Finalmente, deslízate hasta **Bloqueo dinámico** y habilita la casilla para permitir que Windows bloquee el dispositivo automáticamente cuando estés ausente.

Como has podido ver, estas son solo unas cuentas medidas de seguridad para conseguir que Windows 11 se convierta en un medio mucho más escudado. A pesar de ello, muchas funciones de seguridad están habilitadas de forma predeterminada, así que la protección está más que asegurada.



Descargar solo de sitios fiables

En este caso se trata de un problema muy habitual que puede provocar la **entrada de malware** de todo tipo. Siempre que descargues algún programa, sea cual sea, debes asegurarte de que lo haces desde una fuente fiable. Por ejemplo debes usar tiendas oficiales como Microsoft Store o ir directamente a la página web de esa aplicación.

Pero esto también lo debes aplicar a la hora de bajar cualquier documento de Internet. Si por ejemplo recibes un archivo Word o PDF por correo, no lo descargues si no reconoces la fuente o sabes que realmente no se trata de una amenaza de seguridad. De lo contrario podrías estar descargando un virus sin que lo sepas.

Tener una revisión constante

Mantener la máxima seguridad en Windows 11 requiere de una revisión constante. Tienes que ver periódicamente que el equipo esté actualizado, que el antivirus funciona bien, pero también las aplicaciones que tienes instalada y comprobar que no generan ningún tipo de problema.

Una **revisión constante** puede servir para detectar una amenaza lo antes posible. Por ejemplo un fallo de seguridad sin corregir y poder solucionarlo antes de que un pirata informático pueda explotarlo, una aplicación que hayas instalado y esté robando datos sin que lo sepas, etc. Puedes crearte una serie de pautas para realizar periódicamente.

Proteger también otros dispositivos

Para proteger tu ordenador con Windows, no debes centrarte únicamente en este sistema, sino también en **cualquier otro dispositivo** que vayas a conectar o que tengas en la misma red. Por ejemplo, si vas a enchufar un disco duro debes asegurarte de que no tiene virus. Lo mismo si vas a conectar un móvil por cable, es importante que sigas los mismos consejos también en esos aparatos. Muchos ataques de seguridad llegan a través de la red. Por ejemplo, un pirata informático podría explotar nuestra red Wi-Fi vulnerable para poder acceder a otros dispositivos. Por ello es fundamental proteger también el router, la red inalámbrica y cualquier otro aparato que vayamos a conectar.

Se pide:

1. Busca información sobre cómo proteger la seguridad de Windows
2. Elabora un resumen sobre las opciones de configuración de Windows
3. Revisa y muestra las opciones de seguridad de tu equipo Windows