Windows 11 Hardening

El fortalecimiento de Windows 11 es fundamental para mejorar la seguridad y protegerse contra amenazas cibernéticas. Esto implica configurar ajustes, implementar medidas de autenticación sólidas, realizar actualizaciones periódicas, emplear reglas de firewall, restringir servicios innecesarios y usar software de seguridad. Estas prácticas protegen tu sistema y tus datos de posibles vulnerabilidades y ataques.

El fortalecimiento de Windows 11 implica varios pasos para mejorar tu seguridad. A continuación, se incluye una guía paso a paso:

Instalar Windows 11 de forma segura:

- Utilizar una fuente de instalación segura.
- Elegir contraseñas seguras durante la configuración.
- Actualización de Windows:
  - Habilitar actualizaciones automáticas.
  - Buscar e instalar actualizaciones periódicamente.

Cuentas de usuario:

- Utilizar una contraseña o PIN seguro para tu cuenta de usuario.

Crear una cuenta separada, que no sea de administrador, para el uso diario.

Configuración del firewall:

- Habilitar el Firewall de Windows.
- Configurar reglas para permitir solo el tráfico de red necesario.

Control de cuentas de usuario (UAC):

- Mantener UAC habilitado para solicitar acceso de administrador.

Evitar deshabilitarlo a menos que sea necesario.

Cifrado de disco:

- Utilizar BitLocker o una herramienta similar para cifrar tu disco.

Proteger contra el robo de datos en caso de acceso físico.

Antivirus/Anti-Malware:

- Instalar un software antivirus confiable.
- Mantenerlo actualizado y realizar análisis periódicos.

Seguridad del navegador:

- Utilizar un navegador seguro.
- Habilitar los bloqueadores de ventanas emergentes y la configuración de privacidad.

Arranque seguro:

- Asegurarse de que el Arranque seguro esté habilitado en la configuración del BIOS/UEFI.
- Evitar cambios no autorizados en el sistema operativo o en el cargador de arranque.

Cifrado del dispositivo:

- Cifrar dispositivos extraíbles como unidades USB.

Políticas de restricción de software/AppLocker:

- Limitar la ejecución de aplicaciones desconocidas o no confiables.

Gestión de credenciales:

- Utilizar un administrador de contraseñas.
- Evitar almacenar credenciales confidenciales en los navegadores.

Seguridad de la red:

- Utilizar una contraseña de Wi-Fi segura.
- Desactivar servicios de red innecesarios.

Pantalla inteligente de Windows Defender:

- Habilitar SmartScreen para bloquear descargas maliciosas.

Deshabilitar servicios innecesarios:

- Deshabilitar los servicios de Windows no utilizados.

Auditoría y seguimiento:

- Habilitar la auditoría de seguridad de Windows.
- Supervisar registros de eventos de seguridad.

Política de grupo:

- Utilizar la política de grupo para aplicar la configuración
- de seguridad.

Configurar políticas como bloqueo de cuentas y políticas de contraseñas.

Acceso seguro al escritorio remoto:

- Habilitar 'Escritorio remoto' de forma segura.
- Utilizar métodos de autenticación fuertes.

Copia de seguridad y restauración:

- Realizar copias de seguridad del sistema periódicamente.
- Probar el proceso de restauración.

Educación del usuario:

- Educar a los usuarios sobre el phishing y la ingeniería
- social.

Promover buenas prácticas de seguridad.

Auditorías de seguridad periódicas:

- Realizar evaluaciones de seguridad periódicas.
- Abordar las vulnerabilidades rápidamente.

Lista blanca de aplicaciones:

- Utilizar AppLocker o herramientas similares para permitir que solo se ejecuten aplicaciones confiables.

Recuerda que la seguridad es un proceso continuo. Revisa y actualiza periódicamente tus medidas de seguridad para adaptarse a nuevas amenazas y vulnerabilidades.

Procedimientos detallados

Fuentes de instalación limpias y oficiales de Windows 11

Para realizar una instalación limpia y oficial de Windows 11, debes seguir las pautas más actuales de Microsoft. A continuación, se indican los pasos generales:

1. **Verificar los requisitos del sistema:**
   - Asegúrate de que tu computadora cumpla con los requisitos mínimos del sistema para Windows 11. Estos requisitos pueden incluir un procesador compatible, suficiente memoria RAM y compatibilidad con TPM 2.0.
2. **Realizar una copia de seguridad de tus datos:**
   - Hacer una copia de seguridad de todos los datos importantes en una unidad externa o en un almacenamiento en la nube para evitar la pérdida de datos durante la instalación.
3. **Visitar el sitio web oficial de Microsoft:**
   - Ir al sitio web oficial de Microsoft para acceder a los recursos de instalación y enlaces de descarga de Windows 11.
4. **Descargar el medio de instalación de Windows 11:**
   - En el sitio web oficial de Microsoft, buscar una herramienta de descarga de Windows 11 o un enlace de descarga.
   - Descargar la herramienta de creación de medios de instalación de Windows 11 o el archivo ISO.

5. **Crear medios de instalación:**
   - Ejecutar la herramienta de creación de medios de instalación de Windows 11.

   Seguir las instrucciones que aparecen en pantalla para crear un medio de instalación. Puedes elegir entre crear una unidad USB de arranque o descargar un archivo ISO.
6. **Preparar la unidad USB de arranque (si corresponde):**
   - Si decides crear una unidad USB de arranque, inserta una unidad USB vacía (de al menos 8 GB) en tu computadora.
   - Sigue las instrucciones de la herramienta para crear la unidad USB de arranque.
7. **Insertar el medio de instalación:**
   - Insertar la unidad USB de arranque o montar el archivo ISO de Windows 11 (si no estás usando una unidad USB) en la computadora donde deseas instalar Windows 11.
8. **Arrancar desde el medio de instalación:**
   - Reiniciar la computadora de destino.
   - Acceder a la configuración del BIOS/UEFI durante el inicio (generalmente presionando una tecla como F2, F12 o Supr).
   - Cambiar el orden de arranque para priorizar la unidad USB o el dispositivo que contiene el archivo ISO.

9. **Instalar Windows 11:**
   - Guardar los cambios del BIOS/UEFI y reinizar la computadora.
   - La computadora arrancará desde el medio de instalación.
   - Seguir las instrucciones en pantalla para instalar Windows 11.

   Durante la instalación, deberás elegir tu idioma, región, distribución del teclado e ingresar tu clave de producto si se solicita.

10. **Particionar y formatear unidades (si es necesario):**
    - Puedes crear particiones y formatear la unidad durante el proceso de instalación si es necesario.

11. **Configurar ajustes:**
    - Seguir el asistente de configuración para configurar ajustes como cuentas de usuario, red y preferencias de privacidad.
12. **Activar Windows 11:**
    - Después de la instalación, activar Windows 11 con una clave de producto válida si no se activa automáticamente. Ingresar la clave cuando se solicite.
13. **Instalar controladores y actualizaciones:**
    - Después de la instalación, instalar los controladores de dispositivo necesarios y buscar actualizaciones de Windows para asegurarse de que el sistema esté actualizado y funciona correctamente.
14. **Instalar aplicaciones y restaurar datos:**
    - Instalar tus aplicaciones preferidas y restaurar tus datos desde la copia de seguridad.
15. **Finalizar la configuración de seguridad:**
    - Configurar ajustes de seguridad como Windows Defender, Firewall de Windows y seguridad de la cuenta de usuario.
16. **Actualizar Windows periódicamente:**
    - Habilitar las actualizaciones automáticas de Windows para mantener tu sistema seguro con los últimos parches y mejoras.

Para obtener la información más precisa y actualizada sobre la instalación de Windows 11, consultar el sitio web oficial de Microsoft o consultar la documentación y las pautas oficiales de Microsoft.

Instalar la línea base de seguridad de Windows 11

Para instalar la línea base de seguridad de Windows 11, seguir estos pasos:

1. Visitar el sitio web oficial del Kit de herramientas de cumplimiento de seguridad (SCT) de Microsoft.

2. Descargar la “Línea base de seguridad de Windows 11” desde el enlace proporcionado.
3. Extraer los archivos descargados y revisar la documentación para obtener orientación sobre cómo implementar las recomendaciones de seguridad.
4. Utilizar la política de grupo, scripts de PowerShell u otras herramientas relevantes para aplicar la configuración de seguridad descrita en la línea base a tus dispositivos Windows 11.
5. Probar las configuraciones de seguridad aplicadas para asegurarse de que no interrumpan las operaciones esenciales.
6. Supervisar y actualizar continuamente la configuración de seguridad según sea necesario para adaptarse a las amenazas cambiantes y los requisitos de cumplimiento.

Si sigues estos pasos, podrás mejorar la seguridad de tu entorno de Windows 11 utilizando las configuraciones de base recomendadas proporcionadas por Microsoft.

Bloquear cuenta con contraseña segura

Para bloquear una cuenta de usuario con una contraseña compleja, normalmente se siguen estos pasos:

1. **Iniciar sesión como administrador**: asegúrate de tener privilegios administrativos en el sistema.
2. **Abrir el Símbolo del sistema o PowerShell**: hacer clic derecho en el botón Inicio y elije “Símbolo del sistema (Administrador)” o “Windows PowerShell (Administrador)”.
3. **Elegir una cuenta de usuario:** use el siguiente comando para bloquear una cuenta de

   ```
   net user username /lock
   ```

   usuario específica (reemplácela `username` con el nombre de usuario real):
4. **Establecer una contraseña compleja:** también puede imponer una contraseña compleja para el usuario. Utilizar este comando para cambiar o establecer una nueva contraseña (reemplácela

`NewPassword` con la contraseña compleja que desee): net user Username NewPassword

5. **Desbloquear la cuenta:** si es necesario, puedes desbloquear la cuenta usando el siguiente comando:

```
net user username /unlock
```

Recuerda reemplazar `username` con el nombre de usuario real de la cuenta que desea bloquear o desbloquear, y `NewPassword` con la contraseña compleja deseada.

Tenga cuidado al realizar estas acciones, especialmente en las cuentas de usuario, ya que el uso indebido puede bloquear a los usuarios de tus cuentas, lo que podría causar problemas de acceso.

Utilizar un administrador de contraseñas

El uso de un gestor de contraseñas es un paso fundamental para mejorar nuestra seguridad en línea. A continuación, indicamos cómo hacerlo:

1. **Elegir un administrador de contraseñas:** seleccione un administrador de contraseñas de buena reputación, como LastPass, 1Password, Bitwarden o Dashlane.
2. **Instalar y configurar:** Descargue e instalarla aplicación de administración de contraseñas o la extensión del navegador en tus dispositivos.
3. **Crear una contraseña maestra:** esta es la única contraseña que debes recordar. Hazla compleja, única y fácil de recordar.
4. **Almacenar y generar contraseñas:** permita que el administrador de contraseñas genere y almacene contraseñas complejas y únicas para cada una de tus cuentas en línea.
5. **Completar credenciales automáticamente:** el administrador de contraseñas completará automáticamente tus credenciales de inicio de sesión cuando visite un sitio web o una aplicación, lo que le ahorrará tiempo.

6. **Notas seguras:** utilice el administrador de contraseñas para almacenar de forma segura información confidencial, como detalles de tarjetas de crédito o PIN.
7. **Sincronización entre dispositivos:** asegúrese de que tu administrador de contraseñas sincronice las contraseñas en todos tus dispositivos para mayor comodidad y coherencia.
8. **Habilitar la autenticación de dos factores (2FA):** muchos administradores de contraseñas admiten la autenticación de dos factores para mayor seguridad. Habilítela siempre que sea posible.
9. **Actualizar y revisar periódicamente:** revise periódicamente tus contraseñas almacenadas y actualice aquellas que sean débiles o comprometidas.
10. **Hacer una copia de seguridad de tu administrador de contraseñas:** hacer una copia de seguridad de los datos de tu administrador de contraseñas para evitar la pérdida de datos.

El uso de un administrador de contraseñas mejora significativamente tu seguridad en línea al crear y administrar contraseñas complejas y únicas para cada una de tus cuentas, lo que reduce el riesgo de acceso no autorizado y violaciones de datos.

Deshabilitar inicio de sesión automático

Deshabilitar el inicio de sesión automático en tu computadora agrega una capa adicional de seguridad, lo que garantiza que tenga que ingresar tu contraseña u otra forma de autenticación cada vez que inicie tu computadora. A continuación, se muestra cómo deshabilitar el inicio de sesión automático en Windows 11:

1. **Presionar Win + I**: Esto abre la Configuración de Windows.
2. **Hacer clic en “Cuentas”**: En la ventana Configuración, seleccione “Cuentas”.
3. **Seleccionar “Opciones de inicio de sesión”**: en Cuentas, hacer clic en “Opciones de inicio de sesión” en el panel izquierdo.

4. **Desplázarse hacia abajo hasta “Requerir inicio de sesión”**: en el panel derecho, desplácese hacia abajo hasta la sección “Requerir inicio de sesión”.
5. **Elegir una opción**: Hay varias opciones para elegir:
    - “Nunca” deshabilitar por completo el inicio de sesión automático y solicitará una contraseña cada vez que inicie tu computadora.
    - “Cuando la PC se activa desde el modo de suspensión” requerirá una contraseña después de que tu computadora se active desde el modo de suspensión.
    - “Cada vez” requerirá una contraseña cada vez que tu computadora se bloquee o se active desde el modo de suspensión.
6. **Hacer una selección**: elegir la opción que mejor se adapte a tus preferencias de seguridad.
7. **Cerrar configuración**: una vez que haya realizado tu selección, puede cerrar la ventana Configuración.

Ahora, tu computadora ya no iniciará sesión automáticamente y deberá ingresar tu contraseña o usar otra forma de autenticación cada vez que inicie o active tu sistema. Esto ayuda a proteger tu computadora contra el acceso no autorizado.

Habilitar el Firewall de Windows

Habilitar el Firewall de Windows ayuda a proteger tu computadora contra accesos no autorizados a la red y posibles amenazas de seguridad. A continuación, le indicamos cómo habilitarlo en Windows 11:

1. **Presione Win + I**: Esto abre la Configuración de Windows.
2. **Haga clic en “Privacidad y seguridad”**: En la ventana Configuración, seleccione “Privacidad y seguridad”.
3. **Seleccione “Seguridad de Windows”**: en Privacidad y seguridad, hacer clic en “Seguridad de Windows” en el panel izquierdo.
4. **Haga clic en “Firewall y protección de red”**: En la ventana de Seguridad de Windows, hacer clic en “Firewall y protección de red”.

5. **Activar el Firewall de Windows Defender**:
   - En “Firewall y protección de red”, verá la opción
   - “Firewall de Windows Defender”.
   - Haga clic en él y verá configuraciones separadas para redes privadas y públicas.

   Mueva el interruptor para activar el firewall tanto para “Red privada” como para “Red pública”.
6. **Confirme tu elección** : puede aparecer un cuadro de diálogo de confirmación. Confirme que desea habilitar el firewall.
7. **Cerrar configuración**: una vez que haya habilitado el Firewall de Windows Defender, puede cerrar la ventana de Seguridad de Windows.

Ahora, el Firewall de Windows está activo y ayudará a proteger tu computadora al monitorear y controlar el tráfico de red entrante y saliente. Agrega una importante capa de seguridad a tu sistema Windows 11.

Eliminar controladores innecesarios

Eliminar controladores innecesarios de tu computadora con Windows 11 puede ayudar a mejorar la estabilidad del sistema, liberar espacio en el disco y evitar posibles conflictos de controladores. A continuación, le indicamos cómo eliminar controladores innecesarios: **Nota:** tenga cuidado al eliminar controladores, ya que desinstalar controladores esenciales puede causar problemas de hardware. Elimine únicamente los controladores que sean realmente innecesarios o que causen problemas.

1. **Identificar controladores innecesarios**: a. Presione Win + X y seleccione
   “Administrador de dispositivos” para abrir el Administrador de dispositivos. b. En el Administrador de dispositivos, expanda las categorías para ver los controladores instalados. Busque los controladores con triángulos amarillos o aquellos relacionados con dispositivos que ya no usa o que ha desinstalado.

2. **Desinstalar controladores innecesarios**:
   a. Haga clic derecho en el controlador que desea eliminar y seleccione “Desinstalardispositivo”.
   b. Confirme la desinstalación haciendo clic en “Desinstalar”.
3. **Reinicie tu computadora**:
   a. Después de quitar los controladores, es una buena práctica reiniciar tu computadorapara completar el proceso.
4. **Utilizar las herramientas de desinstalación de controladores (opcional)**:
   a. Para una limpieza más avanzada de los controladores, puede utilizar herramientas dedesinstalación de controladores de terceros, como Display Driver Uninstaller (DDU) para los controladores de gráficos. Estas herramientas pueden ayudarle a eliminar por completo los restos de los controladores.
5. **Copia de seguridad de los controladores (opcional)**:
   a. Si no está seguro de qué controladores eliminar, considere usar una herramienta decopia de seguridad de controladores para guardar los controladores actuales antes de desinstalarlos. De esta manera, puede restaurarlos si es necesario.
6. **Windows Update (opcional)**:
   a. Windows Update puede instalar automáticamente los controladores para tu hardware.Si prefiere administrar los controladores manualmente, puede deshabilitar las actualizaciones automáticas de controladores:
   i. Vaya a “Configuración” > “Privacidad y seguridad” > “Windows Update”.
   ii. Haga clic en “Opciones avanzadas” y luego en “Ver historial de actualizaciones”.iii. Haga clic en “Actualizaciones de controladores” y seleccione el controlador que desea evitar que se reinstale. Haga clic derecho y elija “Desinstalar”.

Tenga siempre cuidado al eliminar controladores y asegúrese de que no sean necesarios antes de desinstalarlos. Eliminar controladores esenciales puede provocar problemas de hardware y requerir que los vuelva a instalar más adelante.

Deshabilitar el escritorio remoto

Para deshabilitar el Escritorio remoto en una computadora con Windows 11, siga estos pasos:

1. **Presione Win + I**: Esto abre la Configuración de Windows.
2. **Haga clic en "Sistema"**: En la ventana Configuración, seleccione "Sistema".
3. **Seleccionar "Escritorio remoto"**: en el panel izquierdo, hacer clic en "Escritorio remoto".
4. **Desactivar "Escritorio remoto"**: en la configuración de Escritorio remoto, verá un interruptor. Deslícelo a la posición "Desactivado" para desactivar el Escritorio remoto.
5. **Confirme tu elección**: puede aparecer un cuadro de diálogo de confirmación. Confirme que desea deshabilitar el Escritorio remoto.
6. **Cerrar configuración**: una vez que hayas deshabilitado el Escritorio remoto, puedes cerrar la ventana Configuración de Windows.

Esta acción desactivará la función de Escritorio remoto en tu computadora con Windows 11, lo que evitará las conexiones remotas. Es una buena práctica de seguridad si ya no necesita acceso remoto a tu computadora o desea reducir los posibles riesgos de seguridad.

Desinstalar software innecesario

Limpiar el equipo desinstalando software innecesario puede mejorar el rendimiento del sistema y liberar valioso espacio de almacenamiento. A continuación, se explica cómo desinstalar software en Windows 11:

Abrir configuración:+

- Presione Win + I para abrir la Configuración de Windows.

Haga clic en “Aplicaciones”:

- En la ventana Configuración, seleccione “Aplicaciones” de la lista.

Ver aplicaciones instaladas:

- En la sección “Aplicaciones y funciones”, verás una lista de todas las aplicaciones instaladas en tu computadora. Esta lista puede tardar un momento en completarse.

Ordenar y filtrar (opcional):

- Puede ordenar la lista por nombre, fecha de instalación o tamaño haciendo clic en los encabezados de columna respectivos.
- Utilizar la barra de búsqueda para encontrar una aplicación específica si tiene muchas instaladas.

Seleccione el software que desea desinstalar

- Haz clic en la aplicación que deseas desinstalar. Se abrirá un menú con más opciones.

Haga clic en “Desinstalar”:

- Haga clic en el botón “Desinstalar” que aparece cuando selecciona la aplicación.

Confirmar desinstalación:

- Aparecerá un cuadro de diálogo de confirmación. Haga clic en “Desinstalar” nuevamente para confirmar la eliminación del software.

Siga el asistente de desinstalación:

- El proceso de desinstalación variará según el software. Siga las instrucciones que aparecen en pantalla para completar la desinstalación.

Repetir para otro software:

- Regrese a la lista de aplicaciones instaladas y repita los pasos 5 a 8 para cualquier otro software que desee desinstalar.

Reinicie tu computadora:

- Es posible que algunas aplicaciones requieran reiniciar el equipo para completar el proceso de desinstalación. Si se le solicita, reinicie el equipo

Es importante revisar con atención la lista de aplicaciones instaladas y desinstalar únicamente el software que esté seguro de que ya no necesita. Tenga cuidado al eliminar software esencial o crítico para el sistema, ya que podría afectar la funcionalidad de tu computadora.

Mantenga Windows actualizado

Mantener Windows actualizado es fundamental para mantener la seguridad y el rendimiento de tu equipo. A continuación, le indicamos cómo asegurarse de que Windows se mantenga actualizado en Windows 11:

1. **Presione Win + I**: Esto abre la Configuración de Windows.
2. **Haga clic en "Windows Update"**: En la ventana Configuración, seleccione "Windows Update".
3. **Buscar actualizaciones**: hacer clic en el botón "Buscar actualizaciones". Windows buscará las actualizaciones disponibles.
4. **Instalar actualizaciones**: si se encuentran actualizaciones, hacer clic en "Instalar" para iniciar el proceso de actualización. Es posible que deba reiniciar tu computadora para completar la instalación.
5. **Actualizaciones automáticas**: para garantizar actualizaciones constantes, puede configurar actualizaciones automáticas:
   - En "Windows Update", hacer clic en "Opciones avanzadas".
   - En "Pausar actualizaciones", asegúrese de que esté
   - configurado en "Desactivado".

En “Opciones de actualización automática”, asegúrese de que la opción “Descargar actualizaciones automáticamente, incluso a través de conexiones de datos medidas” esté activada.

Reiniciar según sea necesario: algunas actualizaciones pueden requerir un reinicio.
Windows le solicitará que reinicie tu computadora cuando sea necesario.

La actualización periódica de Windows proporciona parches de seguridad críticos, correcciones de errores y mejoras de rendimiento, lo que ayuda a proteger tu sistema contra vulnerabilidades y garantiza que funcione sin problemas.

Habilitar cifrado

Activar el cifrado en tu equipo con Windows 11 es un paso fundamental para proteger tus datos del acceso no autorizado en caso de pérdida o robo de tu dispositivo. Windows 11 incluye BitLocker para este fin. A continuación, le indicamos cómo activarlo:

1. **Presione Win + I**: Esto abre la Configuración de Windows.
2. **Haga clic en “Privacidad y seguridad”**: En la ventana Configuración, seleccione “Privacidad y seguridad”.
3. **Seleccione “Seguridad del dispositivo”**: en el panel izquierdo, hacer clic en “Seguridad del dispositivo”.
4. **En “Cifrado del dispositivo”, hacer clic en “Más información”**: esto abrirá la aplicación de Seguridad de Windows.
5. **Comprobar el estado del cifrado**: en la aplicación Seguridad de Windows, en “Cifrado del dispositivo”, comprueba el estado. Si ya está habilitado, ya está todo listo. Si no, haz clic en “Activar” o “Configurar” para comenzar el proceso de cifrado.
6. **Siga las instrucciones en pantalla**: Es posible que se le solicite crear o confirmar un PIN o contraseña, ya que esto será necesario para desbloquear tu dispositivo después del cifrado.

7. **Espere a que se complete el cifrado**: el proceso de cifrado puede tardar algún tiempo, dependiendo del tamaño de tu disco duro y la velocidad de tu computadora.
8. **Reinicie tu computadora**: una vez completado el proceso de cifrado, reinicie tu computadora para asegurarse de que arranque de forma segura.

Una vez que se habilita el cifrado, BitLocker protege tus datos y solo se puede acceder a ellos con la clave de cifrado correcta (protegida por tu PIN o contraseña). Esto agrega una importante capa de seguridad a tu sistema Windows 11.

Administrar permisos de aplicaciones

La administración de permisos de aplicaciones en Windows 11 le permite controlar a qué recursos e información pueden acceder las aplicaciones instaladas. A continuación, le indicamos cómo hacerlo:

1. **Presione Win + I**: Esto abre la Configuración de Windows.
2. **Haga clic en "Privacidad y seguridad"**: En la ventana Configuración, seleccione "Privacidad y seguridad".
3. **Seleccionar "Permisos de la aplicación"**: en el panel izquierdo, hacer clic en "Permisos de la aplicación".
4. **Elija una categoría de permiso**: en "Permisos de la aplicación", verá varias categorías como Cámara, Micrófono, Ubicación, etc. Haga clic en la categoría del permiso que desea administrar.
5. **Administrar permisos de aplicaciones individuales**:
   - Verá una lista de aplicaciones que han solicitado acceso
   - al recurso seleccionado.

   Para otorgar o revocar permisos para una aplicación específica, mueva el interruptor junto al nombre de la aplicación.
   - Algunos permisos pueden tener configuraciones avanzadas u opciones adicionales que puedes configurar.

Configurar permisos avanzados:

- Para algunos permisos, puede hacer clic en “Permisos avanzados de aplicaciones” para acceder a configuraciones más detalladas.
- Aquí puedes controlar qué aplicaciones pueden acceder a recursos específicos, incluso en segundo plano.

Revisar y ajustar otros permisos: repita el proceso para otras categorías de permisos según sea necesario.

Cerrar configuración: una vez que haya configurado los permisos de la aplicación a tu satisfacción, puede cerrar la ventana Configuración de Windows.

Al administrar los permisos de las aplicaciones, puede mejorar tu privacidad y seguridad al garantizar que solo las aplicaciones confiables tengan acceso a tus recursos confidenciales, como tu cámara, micrófono o datos de ubicación en tu dispositivo Windows 11.

Aumentar la configuración del Control de cuentas de usuario (UAC)

Para aumentar la configuración del Control de cuentas de usuario (UAC) en Windows 11, puedes seguir los siguientes pasos:

1. **Presionar Win + I**: Esto abre la Configuración de Windows.
2. **Hacer clic en “Privacidad y seguridad”**: En la ventana Configuración, seleccione “Privacidad y seguridad”.
3. **Seleccionar “Seguridad de Windows”**: en el panel izquierdo, hacer clic en “Seguridad de Windows”.
4. **Hacer clic en “Protección contra virus y amenazas”**: en Seguridad de Windows, hacer clic en “Protección contra virus y amenazas”.
5. **Administrar configuración**: en Configuración de protección contra virus y amenazas, hacer clic en “Administrar configuración” en la sección “Configuración de protección contra virus y amenazas”.

6. **Activar “Acceso controlado a carpetas”**: desplázate hacia abajo y busca “Acceso controlado a carpetas”. Activa esta función si aún no está habilitada.
7. **Configurar el acceso controlado a carpetas**: hacer clic en “Administrar acceso controlado a carpetas” para configurar qué carpetas están protegidas. Puede agregar o eliminar carpetas según sea necesario.
8. **Regresar a Seguridad de Windows**: cierre la ventana de configuración de Acceso a carpeta controlada y regrese a la página principal de Seguridad de Windows.
9. **Hacer clic en “Control de aplicaciones y navegadores”**: en la página de Seguridad de Windows, hacer clic en “Control de aplicaciones y navegadores”.
10. **Configurar los ajustes de SmartScreen**: en “Comprobar aplicaciones y archivos”, puede elegir entre “Advertir” y “Bloquear” para los archivos descargados. Seleccione el nivel de protección que desee.
11. Regresar a Seguridad de Windows: cierre la ventana de configuración de Control de aplicaciones y navegadores y regrese a la página principal de Seguridad de Windows.
12. Haga clic en “Seguridad del dispositivo”: en la página de Seguridad de Windows, hacer clic en “Seguridad del dispositivo”.
13. Detalles del procesador de seguridad: hacer clic en “Detalles del procesador de seguridad” para acceder a la configuración de seguridad del hardware.
14. Configurar la seguridad basada en hardware: según el hardware que tenga, puede tener opciones para configurar funciones de seguridad basadas en hardware. Siga las instrucciones en pantalla para configurarlas.
15. Cerrar configuración: una vez que haya configurado los ajustes de UAC deseados y otras características de seguridad, puede cerrar la ventana de configuración de Seguridad de Windows.

Al aumentar la configuración de UAC y configurar funciones de seguridad adicionales, mejora la protección de tu sistema

Windows 11 contra malware, acceso no autorizado y amenazas potenciales.

Habilitar la integridad de la memoria

Habilitar la integridad de la memoria en Windows 11 proporciona una capa adicional de seguridad al proteger la integridad de la memoria de tu computadora contra varios tipos de ataques. Para habilitar la integridad de la memoria, siga estos pasos:

1. Presione Win + I: Esto abre la Configuración de Windows.
2. Haga clic en “Privacidad y seguridad”: En la ventana Configuración, seleccione “Privacidad y seguridad”.
3. Seleccione “Seguridad del dispositivo”: en el panel izquierdo, hacer clic en “Seguridad del dispositivo”.
4. En “Aislamiento del núcleo”, hacer clic en “Detalles del aislamiento del núcleo”: esto le permitirá habilitar la integridad de la memoria.
5. Habilitar integridad de la memoria: active el interruptor junto a “Integridad de la memoria” para activarlo.
6. Confirme tu elección: puede aparecer un cuadro de diálogo de confirmación. Confirme que desea habilitar la integridad de la memoria.
7. Reinicie tu computadora: después de habilitar la integridad de la memoria, deberá reiniciar tu computadora para aplicar los cambios.

Una vez que se activa la integridad de la memoria, el sistema estará mejor protegido contra ataques que tengan como objetivo vulnerabilidades en el núcleo y la memoria de Windows. Esta función utiliza mecanismos de seguridad basados en hardware para garantizar la integridad de la memoria de tu computadora.

Puertos de escucha cerrados

Para cerrar los puertos de escucha en una computadora con Windows 11, deberá usar el Firewall de Windows para bloquear o restringir el acceso a puertos específicos. A continuación, le indicamos cómo hacerlo:

1. Presione Win + Sy busque “Seguridad de Windows”. Abra la aplicación Seguridad de Windows.
2. En la aplicación de Seguridad de Windows, hacer clic en “Firewall y protección de red”.
3. En “Firewall y protección de red”, verá dos perfiles de red: “Red privada” y “Red pública”. Estos perfiles corresponden a diferentes tipos de red (por ejemplo, tu red doméstica y Wi-Fi pública).
4. Haga clic en el perfil de red para el cual desea cerrar los puertos de escucha (por ejemplo, “Red privada” para tu red doméstica).
5. En “Firewall de Windows Defender”, hacer clic en “Configuración avanzada”. Esto abrirá el Firewall de Windows con seguridad avanzada.
6. En la ventana Firewall de Windows con seguridad avanzada, verás “Reglas de entrada” en el panel izquierdo. Estas reglas controlan el tráfico entrante.
7. Para bloquear un puerto específico, hacer clic derecho en “Reglas de entrada” y seleccione “Nueva regla”.
8. En el “Asistente para nueva regla de entrada”, seleccione “Puerto” y hacer clic en “Siguiente”.
9. Especifique el número de puerto o el rango que desea bloquear, elija si desea bloquear la conexión o permitirla (es probable que desee bloquearla) y hacer clic en “Siguiente”.
10. Seleccione el tipo de red al que se aplica esta regla (por ejemplo, “Dominio”, “Privado” o “Público”). Por lo general, seleccionaría “Dominio” y “Privado” para una red doméstica, pero elija según la configuración de tu red. Haga clic en “Siguiente”.
11. Proporcione un nombre y una descripción opcional para la regla. Haga clic en “Finalizar” para crear la regla.

Repita estos pasos para cualquier otro puerto que desee cerrar. Asegurarse de seguir el mismo proceso para los perfiles de red “Privado” y “Público” si es necesario.

Tenen cuenta que el cierre de puertos debe realizarse con precaución, ya que puede afectar a la funcionalidad de las aplicaciones o servicios que dependen de estos puertos. Asegúrate de comprender las implicaciones antes de bloquear cualquier puerto.

Seguridad del navegador

Garantizar la seguridad del navegador en Windows 11 es fundamental para proteger tu privacidad en línea y evitar infecciones de malware. A continuación, se indican los pasos para mejorar la seguridad del navegador en Windows 11, independientemente del navegador web que elija:

- **Mantener navegadores actualizados**:
  - Actualice periódicamente tu navegador web a la última versión para recibir parches de seguridad y correcciones de errores.
- **Utilizar un navegador seguro y de buena reputación**:
  - Elegir un navegador conocido por sus funciones de seguridad y actualizaciones frecuentes, como Google Chrome, Mozilla Firefox, Microsoft Edge o Safari.
- **Habilitar actualizaciones automáticas**:
  - Asegurarse de que tu navegador esté configurado para actualizarse automáticamente a la última versión para mantenerse protegido contra vulnerabilidades conocidas.
- **Instalar extensiones del navegador**:
  - Agregue extensiones de navegador centradas en la seguridad:

Bloqueadores de anuncios: bloquean anuncios y posibles fuentes de malware

Extensiones de privacidad: mejore la privacidad bloqueando las cookies de seguimiento.

- Gestores de contraseñas: almacene y genere de forma segura contraseñas complejas.
- HTTPS Everywhere: obliga a los sitios web a utilizar conexiones HTTPS seguras.

- **Utilizar una contraseña segura y única para tu navegador**:
  - Proteger tu navegador con una contraseña segura para evitar el acceso no autorizado a tus contraseñas y configuraciones guardadas.
- **Habilitar la autenticación de dos factores (2FA)**:
  - Si tu navegador lo admite, habilitar 2FA para obtener una capa adicional de seguridad.
- **Tener cuidado con las extensiones**:
  - Instalarúnicamente extensiones de navegador de fuentes confiables y revise los permisos que solicitan.
- **Revisar y actualice periódicamente las extensiones**:
  - Mantenga las extensiones actualizadas para garantizar que reciban actualizaciones de seguridad.
- **Configurar ajustes de privacidad**:
  - Personalice la configuración de privacidad de tu navegador para limitar el seguimiento y la recopilación de datos.
  - Utilizar el modo de navegación privado o de incógnito para tareas confidenciales.
- **Deshabilitar o eliminar extensiones no utilizadas**:
  - Desinstalaro deshabilitar las extensiones que ya no utilice para reducir la superficie de ataque
- **Establecer políticas sólidas de contenido y seguridad**:
  - Algunos navegadores permiten configurar políticas de contenido y seguridad.
    Ajústelas según tus preferencias.
- **Borrar cookies y caché**:
  - Borre periódicamente las cookies y el caché de tu navegador para eliminar los datos de seguimiento.
- **Utilizar un motor de búsqueda seguro**:
  - Elija un motor de búsqueda centrado en la privacidad como DuckDuckGo o Startpage para evitar el seguimiento.
- **Tener cuidado con los intentos de phishing**:
  - Evite hacer clic en enlaces sospechosos o descargar archivos de fuentes no confiables.

- **Informarse sobre hábitos de navegación seguros**:
  - Mantenerse informado sobre las amenazas en línea comunes y las tácticas de phishing para reconocerlas y evitarlas.
- **Realizar copias de seguridad periódicas de tus marcadores y**
  - **configuraciones**: Realizar periódicamente copias de seguridad de los marcadores, la configuración y las contraseñas de tu navegador para evitar la pérdida de datos en caso de problemas o malware.
- **Monitorizar complementos y plug-ins del navegador**:
- Mantenga actualizados los complementos y plug-ins del navegador de terceros o elimine los innecesarios.

Al implementar estas prácticas de seguridad del navegador, puede mejorar significativamente tu seguridad en línea y proteger tu sistema Windows 11 de posibles amenazas mientras navega por la web.

Seguridad de la red

La seguridad de la red es fundamental para proteger el sistema y los datos de Windows 11 de amenazas y accesos no autorizados. A continuación, se indican los pasos para mejorar la seguridad de la red:

- **Seguridad del enrutador**:
  - Cambie las credenciales de inicio de sesión predeterminadas para tu enrutador.
  - Habilitar el cifrado WPA3 para Wi-Fi.
  - Cambie el SSID (nombre de red) predeterminado a algo único.
  - Deshabilitar la administración remota a menos que sea necesario.
  - Actualice periódicamente el firmware de tu enrutador.

Cortafuegos:

Habilitar el Firewall de Windows integrado o utilice un firewall de terceros para controlar el tráfico entrante y saliente.

Configurar las reglas del firewall para permitir solo el tráfico necesario.

- **Antivirus y antimalware**:
- Instalar software antivirus y antimalware confiable.
- Mantenga el software de seguridad y las definiciones de virus actualizados.
- **Actualizaciones periódicas**:
- Asegurarse de que Windows 11 esté actualizado con los últimos parches de seguridad.
- Mantenga el software de terceros, especialmente navegadores y complementos, actualizados.
- **Segmentación de red**:
- Separe tu red en diferentes segmentos, como redes internas y de invitados, utilizando VLAN o políticas de red.
- **Fuerte seguridad Wi-Fi**:
- Utilizar una contraseña de Wi-Fi segura y única con encriptación WPA3.
- Deshabilitar WPS (Configuración protegida Wi-Fi) si no es necesario.

Monitoreo de red:

Utilizar sistemas de detección y prevención de intrusiones (IDS/IPS) para supervisar el tráfico de la red en busca de anomalías.

- **Seguridad de contraseña**:
- Utilizar contraseñas seguras y únicas para tu enrutador, Wi-Fi y otros dispositivos de red.
- Habilitar la autenticación multifactor (MFA) siempre que sea posible.<
- **Red de invitados**:
- Configurar una red de invitados separada para los visitantes para mantenerlos aislados de tu red principal.
- **VPN (Red Privada Virtual)**:
- Utilizar un servicio VPN, especialmente cuando acceda a redes Wi-Fi públicas o cuando trabaje de forma remota.
- **Control de acceso a la red (NAC)**:
- Implemente soluciones NAC para controlar y administrar el acceso a tu red, especialmente en entornos empresariales.

- **Copias de seguridad periódicas**:
  - Realizar copias de seguridad periódicas de los datos importantes en una ubicación segura, incluidos dispositivos de almacenamiento conectados a red (NAS) o almacenamiento en la nube.
- **Políticas de seguridad**:
  - Defina y aplique políticas de seguridad de red para tu organización o red doméstica.
- **Educación del usuario**:
  - Educar a los usuarios sobre los ataques de phishing, la ingeniería social y el comportamiento seguro en línea.
- **Seguridad del dispositivo**:
  - Asegurarse de que todos los dispositivos conectados a la red tengan software de seguridad actualizado y estén configurados de forma segura.
- **Seguridad de acceso remoto**:
  - Si necesita acceso remoto a tu red, utilice métodos seguros como VPN y protocolos de escritorio remoto seguros.
- **Monitoreo y registro**:
  - Configurar herramientas de monitoreo de red y registre la actividad de la red para análisis y detección de amenazas.
- **Plan de respuesta a incidentes**:
  - Desarrollar y actualizar periódicamente un plan de respuesta a incidentes para abordar violaciones de seguridad e incidentes de red.
- **Reseñas de proveedores y servicios**:
  - Revisar y evaluar periódicamente la seguridad de los servicios y dispositivos de terceros conectados a tu red.
- **Auditorías de seguridad periódicas**:
  - Realizar auditorías de seguridad periódicas y evaluaciones de vulnerabilidad para identificar y mitigar las debilidades de la red.

Al implementar estas medidas de seguridad de red, puede reducir significativamente el riesgo de violaciones de seguridad y proteger tu sistema y tus datos de Windows 11 de amenazas.