O&O software

O&O SafeErase



Tabla de contenidos

1 Introducción 4

2 Primeros pasos 6

2.1 Descripción general de las funciones 6

2.2 Requisitos del sistema 8

2.3 Instalación y activación 10

2.4 Borrar el primer archivo 12

2.5 Interfaz de usuario 13

3 Conceptos básicos 15

3.1 Cómo funciona el borrado seguro 15

3.2 Métodos de borrado y unidades SSD 17

3.3 Informes y certificados de borrado 19

4 Borrar datos 20

4.1 Borrar archivos y carpetas 20

4.2 Vaciar la Papelera de reciclaje de forma segura 22

4.3 Limpiar el espacio libre 23

4.4 Borrar rastros del navegador y de Windows 25

4.5 Conservar las cookies de determinados sitios web 28

4.6 Borrar unidades y particiones 29

4.7 Borrar desde el Explorador de archivos 31

4.8 Supervisar y cancelar un borrado 32

5 Borrar todo el equipo 34

5.1 Configurar e iniciar el Modo Fortaleza 34

5.2 Borrar todo el equipo 36

5.3 Guardar los registros después de borrar un PC 38

6 Informes y certificados de borrado 40

6.1 Administrar informes 40

6.2 Verificar un certificado de borrado 42

7 Configuración 44

8 Referencia 49

8.1 Línea de comandos 49
8.2 Glosario 60
9 Solución de problemas 63
10 Preguntas frecuentes 66
11 Novedades de la versión 22 68
12 Soporte técnico y otros recursos de O&O 70

Introducción

O&O SafeErase permite borrar de forma irreversible archivos y carpetas, rastros del navegador y de Windows, espacio libre y unidades completas. En el Modo Fortaleza también puede borrar todo el equipo, incluido Windows. Un informe con un certificado de borrado firmado documenta el resultado.

Al eliminar un archivo en Windows o vaciar la Papelera de reciclaje, el contenido permanece en la unidad y a menudo puede recuperarse. Téngalo en cuenta antes de vender, devolver o desechar un equipo o una unidad, y también al manejar documentos confidenciales. Consulte Cómo funciona el borrado seguro.

> **Los datos borrados no se pueden restaurar**
>
> O&O SafeErase sobrescribe los datos de forma irrecuperable. Haga una copia de seguridad de todo lo que todavía necesita en otra unidad antes de iniciar un borrado.

Por dónde empezar

Si desea…	Consulte
Probar O&O SafeErase con un archivo de prueba	Borrar el primer archivo
Borrar archivos o carpetas confidenciales	Borrar archivos y carpetas
Eliminar restos de archivos borrados anteriormente	Limpiar el espacio libre
Eliminar el historial del navegador, las cookies y los archivos temporales	Borrar rastros del navegador y de Windows
Borrar por completo una memoria USB o un segundo disco	Borrar unidades y particiones
Preparar un equipo para venderlo o desecharlo	Borrar todo el equipo
Documentar un borrado	Verificar un certificado de borrado
Borrar datos en scripts	Línea de comandos

Licencia

O&O SafeErase es un programa comercial. Puede utilizarlo durante el período de prueba. Para seguir utilizándolo después, necesita una licencia válida. La versión de prueba no permite borrar unidades o particiones ni acceder al Modo Fortaleza. Consulte Instalación y activación.

Acerca de esta ayuda

Esta ayuda describe O&O SafeErase 22. Los nombres de los botones y las opciones de la interfaz se indican en **negrita**.

Descripción general de las funciones

O&O SafeErase sobrescribe los datos para impedir que los programas de recuperación los restauren. A continuación se resumen las funciones y las diferencias entre ediciones.

Funciones

Función	Qué permite hacer	Detalles
Archivos y carpetas	Borra archivos y carpetas seleccionados.	Borrar archivos y carpetas
Espacio libre	Sobrescribir restos de archivos eliminados, incluido el espacio sobrante en clústeres y las entradas de la MFT. Se conservan los archivos existentes.	Limpiar el espacio libre
Rastros del navegador y de Windows	Borrar el historial, las cookies, la caché, las contraseñas, los archivos temporales, las miniaturas y otros rastros. Puede conservar determinadas cookies.	Borrar rastros del navegador y de Windows
Unidades y particiones	Borrar discos o particiones completos y, si se desea, inicializar y formatear el disco al finalizar.	Borrar unidades y particiones
Equipo completo	Borrar Windows y todos los discos internos en el Modo Fortaleza sin un medio de arranque aparte.	Borrar todo el equipo
Métodos de borrado	Elegir entre seis métodos, desde una pasada con datos aleatorios según NIST 800-88 Clear / BSI CON.6 hasta el método Gutmann. También se ofrece SolidErase para SSD.	Métodos de borrado y unidades SSD
Informes y certificados de borrado	Documentar cada borrado con un certificado firmado, un sello de tiempo opcional y una cadena de certificados.	Informes y certificados de borrado
Recomendaciones	La página de inicio muestra cuándo se borraron los rastros por última vez y recomienda borrarlos nuevamente.	Interfaz de usuario
Explorador de archivos	Borra archivos, espacio libre y la Papelera de reciclaje desde el menú contextual.	Borrar desde el Explorador de archivos
Línea de comandos	Borrar datos mediante scripts y tareas programadas y verificar certificados de borrado.	Línea de comandos

Ediciones

Edición	Destinatarios	Particularidades
Professional Edition	Equipos con Windows 10 y Windows 11	Borra una unidad a la vez. No se puede utilizar en Windows Server.
Server Edition	Servidores y PC	También se ejecuta en Windows Server. Puede borrar varias unidades o limpiar el espacio libre de varias unidades al mismo tiempo.

Ambas ediciones ofrecen las mismas funciones de borrado. Consulte Requisitos del sistema.

Versión de prueba

En la versión de prueba, puede borrar archivos, carpetas y rastros y limpiar el espacio libre. El borrado de unidades y particiones, y el Modo Fortaleza con el borrado de todo el PC, requieren una licencia.

Requisitos del sistema

O&O SafeErase 22 requiere Windows de 64 bits. El instalador incluye los componentes necesarios, entre ellos el entorno de ejecución de .NET.

Sistema operativo

Edición	Versiones de Windows compatibles
Professional Edition	Windows 10 y Windows 11 de 64 bits (x64)
Server Edition	Windows 10 y Windows 11 de 64 bits (x64), además de Windows Server 2016, 2019 y 2022. No se admiten instalaciones Server Core.

Professional Edition no se puede instalar ni ejecutar en Windows Server. No se admiten las versiones de Windows de 32 bits ni Windows en ARM.

Permisos

- La instalación de O&O SafeErase requiere derechos de administrador.
- En el programa, la limpieza del espacio libre, el borrado de unidades y particiones, la configuración del Modo Fortaleza y el cambio de la integración de la Papelera de reciclaje requieren derechos de administrador. El programa ofrece **Reiniciar como administrador** donde sea necesario.

Modo Fortaleza

El Modo Fortaleza, necesario para borrar la unidad del sistema o el equipo completo, se ejecuta en el entorno de recuperación de Windows (Windows RE). Si Windows RE falta o está desactivado, el asistente puede repararlo. Si utiliza BitLocker en la unidad del sistema, tenga a mano la clave de recuperación.

Navegadores

O&O SafeErase admite los siguientes navegadores a partir de la versión indicada.

Navegador	Desde la versión
Google Chrome	115
Microsoft Edge	115
Mozilla Firefox	115
Brave	115
Opera, Opera GX	101
Vivaldi	6

Para Brave, Opera, Opera GX y Vivaldi solo se admiten versiones estables. Internet Explorer y la versión anterior de Microsoft Edge (Edge Legacy) no se pueden limpiar.

Sistemas de archivos

Al limpiar el espacio libre, **Borrar restos de clúster (DeepErase)** solo funciona en unidades NTFS**.Limpiar referencias en la MFT** trata las entradas de la MFT en NTFS y las entradas de directorio en unidades FAT. Las unidades y particiones se pueden borrar con independencia del sistema de archivos.

Instalación y activación

Instale O&O SafeErase y luego actívelo con una clave de licencia o inicie la versión de prueba.

Requisitos previos. El equipo debe cumplir los requisitos del sistema. Inicie sesión con una cuenta con permisos de administrador. Para instalar Server Edition en Windows Server, utilice el instalador de esa edición.

Instalar O&O SafeErase

1. Cierre todos los programas en ejecución.
2. Ejecute el instalador descargado del sitio web de O&O.
3. Acepte la solicitud de permisos de administrador de Windows.
4. Acepte el contrato de licencia y siga las indicaciones del asistente.
5. En la selección de componentes puede marcar o desmarcar los componentes opcionales.

- **Extensiones del shell**. Añaden comandos al menú contextual del Explorador de archivos.
- **Shredder**. Añade al escritorio un icono al que puede arrastrar archivos y carpetas para borrarlos.
- **Línea de comandos:** `OOSafeEraseCmd.exe` para scripts; véase Línea de comandos.

6. Reinicie el equipo si se lo solicita el asistente.

Resultado. Se instalan O&O SafeErase, su servicio y el entorno de ejecución de .NET que necesita el programa.

Activar la licencia o iniciar la prueba

Cuando O&O SafeErase se inicia sin licencia, muestra que aún no está activado.

1. Seleccione **Introducir licencia**.
2. Introduzca la clave de licencia exactamente como en su confirmación de pedido o en su tarjeta de licencia. No confunda el dígito 1 con la letra I, o 0 con O.
3. Confirme la clave o elija iniciar el período de prueba.

Resultado. El programa queda activado o se inicia la prueba. Durante el período de prueba, un aviso indica los días restantes.

La versión de prueba no permite borrar unidades o particiones ni utilizar el Modo Fortaleza. Al vencer el período de prueba, deberá activar una licencia para volver a borrar datos. **Comprar ahora** abre la tienda de O&O.

Una licencia corresponde a un equipo. Para varios equipos o para borrar equipos por encargo de clientes, consulte al departamento comercial de O&O o a su distribuidor.

Buscar actualizaciones

La información del programa en la parte inferior de la navegación muestra la versión instalada y la licencia, y comprueba si hay actualizaciones. De forma predeterminada, O&O SafeErase también busca actualizaciones automáticamente; consulte Configuración > LiveUpdate.

La licencia se mantiene al actualizar dentro de la misma versión principal. Una nueva versión principal requiere otra clave. Si tiene configurado el Modo Fortaleza, vuelva a crearlo después de la actualización.

Desinstalar O&O SafeErase

1. En Windows, abra **Configuración > Aplicaciones > Aplicaciones instaladas**.
2. Seleccione **O&O SafeErase > Desinstalar** y confirme.

Si ha configurado el Modo Fortaleza, quítelo primero desde O&O SafeErase. Consulte Volver a crear o quitar el Modo Fortaleza.

Próximos pasos

- Borrar el primer archivo

Borrar el primer archivo

Seleccione un archivo de prueba para familiarizarse con O&O SafeErase. A continuación podrá revisar la tarea, ejecutar el borrado y consultar el informe.

Requisitos previos. Instale O&O SafeErase y active su licencia o inicie el período de prueba. Cree un archivo cuyo contenido pueda perder, por ejemplo, un archivo de texto en el escritorio.

1. En la página de inicio, seleccione **Archivos y carpetas**.
2. Seleccione **Archivos** y elija el archivo de prueba o arrástrelo a la lista.
3. Seleccione **Vista > Mostrar ruta** y compruebe que en la lista solo esté el archivo de prueba.
4. Continúe con **Revisar la tarea de eliminación**.
5. En **Qué**, compruebe el archivo. En **Cómo**, revise el método. En **Después**, active **Guardar y firmar el informe**.
6. Seleccione **Eliminar de forma segura ahora**.
7. Espere hasta que aparezca la página de finalización y, a continuación, seleccione **Mostrar informe**.

Resultado. El archivo se sobrescribe y se elimina sin pasar por la Papelera de reciclaje. El informe identifica el archivo, el método utilizado y el resultado **OK**.

> **El borrado no se puede deshacer**
>
> Una vez iniciado, un borrado no se puede revertir. Compruebe la lista antes de cada borrado.

Próximos pasos

- Borrar archivos y carpetas con todas las opciones
- Borrar rastros del navegador y de Windows
- Limpiar el espacio libre para eliminar los restos de archivos eliminados anteriormente

Interfaz de usuario

O&O SafeErase se abre en la página de inicio. Desde esta página y el panel de navegación izquierdo puede acceder a todas las tareas.

Navegación

Zona	Finalidad
Inicio	Historial de limpieza, recomendaciones y fichas de tareas.
Eliminar de forma segura > **Archivos y carpetas**	Borrar archivos y carpetas.
Eliminar de forma segura > **Espacio libre**	Limpiar el espacio libre.
Eliminar de forma segura > **Unidades / particiones**	Borrar unidades y particiones.
Privacidad	Borrar rastros del navegador y de Windows.
Borrar todo el equipo	Modo Fortaleza y borrado de todo el equipo.
Informes	Administrar informes.
Herramientas	Ayuda de la línea de comandos, si está instalada.

En la parte inferior del panel encontrará la configuración y la información sobre el programa, la licencia y las actualizaciones. En el Modo Fortaleza también puede seleccionar **Apagar** para apagar el equipo.

Página de inicio

En **Eliminar datos de forma segura** encontrará las tareas **Archivos y carpetas**, **Espacio libre**, **Unidades y particiones**, **Datos del navegador**, **Datos de Windows y de programas** y **Borrar todo el equipo**. Un candado indica que la tarea no está disponible, por ejemplo en la versión de prueba o en el Modo Fortaleza. El aviso explica el motivo.

Encima de las tareas se muestra la fecha del último borrado seguro de los datos del navegador, los datos de Windows, el espacio libre de cada unidad y la Papelera de reciclaje. Es un historial de las limpiezas realizadas. No analiza el equipo en busca de datos recuperables.

Recomendaciones y borrado conjunto de rastros

Si ha pasado más tiempo del recomendado desde la última limpieza, aparecerá una sugerencia para borrar los rastros. El aviso no inicia el borrado.

Borrar rastros de forma segura… permite seleccionar datos del navegador, datos de Windows, la Papelera de reciclaje y el espacio libre. Las categorías pendientes aparecen marcadas. El espacio libre solo se preselecciona si ya se ha sobrescrito en alguna ocasión. Revise la selección y el método antes de confirmar.

En **Cambiar la recomendación…** puede elegir un intervalo de 7, 14, 30, 60 o 90 días, o seleccionar **Nunca**. El valor inicial es de 30 días. También puede cambiarlo en Configuración > Recomendación.

En el Modo Fortaleza se oculta el historial de limpieza y no se pueden borrar los datos del navegador ni de Windows.

Cómo funciona el borrado seguro

El borrado seguro sobrescribe el contenido de un archivo o de una unidad antes de liberar el espacio que ocupa. Así los programas de recuperación no pueden reconstruir los datos. O&O SafeErase aplica este principio a archivos, carpetas, rastros de uso, espacio libre y unidades completas.

Qué queda después de una eliminación convencional

Al eliminar un archivo o vaciar la Papelera de reciclaje, Windows quita la referencia del sistema de archivos y marca el espacio como libre. El contenido permanece en la unidad hasta que lo sobrescriben otros datos. Los programas de recuperación pueden leer esas zonas.

También pueden quedar datos en zonas que no se ven directamente.

Tipo de resto	Dónde se encuentra
Espacio libre	Contenido de archivos eliminados de la forma habitual, por ejemplo, antes de instalar O&O SafeErase.
Espacio sobrante en clústeres	Espacio sin utilizar al final del último clúster de un archivo existente. Puede contener fragmentos de archivos anteriores.
Entradas del sistema de archivos	Nombres, tamaños y fechas de archivos eliminados que permanecen en la tabla maestra de archivos (MFT) de una unidad NTFS. Los archivos muy pequeños se almacenan íntegramente en la MFT.
Rastros de uso	Historial del navegador, cookies, caché, archivos temporales, miniaturas, volcados de memoria y Papelera de reciclaje.

Lo que hace O&O SafeErase

O&O SafeErase sobrescribe los datos con el método de borrado seleccionado y luego los elimina. Dependiendo de la tarea, trata diferentes áreas:

- Archivos y carpetas y rastros de uso. Se sobrescribe el contenido de los elementos seleccionados.
- Espacio libre. Se tratan el espacio libre, el espacio sobrante en clústeres y las entradas de la MFT. Se conservan los archivos existentes.
- Unidades y particiones. Se sobrescribe cada sector del disco o de la partición seleccionados, incluidos todos los archivos.
- Equipo completo. Se borran todos los discos internos, incluido Windows. Para ello se inicia el equipo en el Modo Fortaleza.

Tras el borrado, un informe recoge los elementos tratados, el método utilizado y las advertencias. El certificado de borrado firmado documenta el resultado.

Límites

- El borrado seguro es irreversible. Ni siquiera O&O Software puede recuperar los datos sobrescritos.
- Si existen copias en archivos de respaldo, servicios en la nube, adjuntos de correo u otras unidades, se conservan. Bórrelas por separado.
- Si otro programa mantiene abierto un archivo, no se puede borrar. El informe lo identifica mediante una advertencia.
- En una SSD, el controlador decide dónde se escriben físicamente los datos. El software solo puede sobrescribir las zonas a las que Windows tiene acceso. Consulte Métodos de borrado y unidades SSD.

Métodos de borrado y unidades SSD

El método de borrado determina qué patrón escribe O&O SafeErase al sobrescribir los datos y cuántas pasadas realiza. El método predeterminado es adecuado para las unidades actuales. Hacer más pasadas prolonga considerablemente el proceso sin aumentar la seguridad del borrado.

Seleccione el método predeterminado en Configuración > Método de eliminación. Antes de iniciar un borrado puede revisar el método en **Cómo** y elegir otro para esa ejecución.

Métodos

Método	Pasadas	Patrón
NIST 800-88 Clear / BSI CON.6 (1× datos aleatorios) (predeterminado)	1	Datos aleatorios. Corresponde al procedimiento «Clear» de NIST SP 800-88 Rev. 2 y a la sobrescritura completa con datos aleatorios que exige el módulo CON.6 de BSI IT-Grundschutz.
Sobrescribir con ceros	1	Ceros. Es rápido y proporciona un borrado básico.
US DoD 5220.22-M (Legacy)	3	Datos aleatorios, ceros y datos aleatorios.
Procedimiento BSI anterior (Legacy)	6	00, FF, 00, FF, 00 y datos aleatorios.
US DoD 5220.22-M ECE (Legacy)	7	Secuencia fija de patrones y datos aleatorios.
Método Gutmann (Legacy)	35	Patrones que Peter Gutmann describió en 1996 para los discos duros magnéticos de la época.

Los métodos marcados como **(Legacy)** siguen disponibles para mantener configuraciones existentes y cumplir requisitos anteriores. Según NIST SP 800-88 Rev. 2, las unidades actuales no requieren varias pasadas.

El informe indica el método utilizado en cada destino. El nombre describe el procedimiento y no certifica por sí solo que el borrado se haya completado. Compruebe el resultado en el informe.

El tiempo estimado depende del volumen de datos, de la velocidad de la unidad, del método y de la actividad del equipo.

Unidades SSD y SolidErase

En una SSD, el controlador distribuye las escrituras entre las celdas de memoria flash y reserva zonas a las que Windows no tiene acceso. Las pasadas adicionales aumentan el desgaste de la unidad sin aportar mayor seguridad.

La opción **Eliminar SSD con SolidErase**, en Configuración > SSD, está activada de forma predeterminada. Con esta opción, O&O SafeErase utiliza SolidErase en las SSD que detecta. SolidErase sobrescribe los datos una sola vez con datos aleatorios para evitar ciclos de escritura innecesarios. El informe indica que se ha utilizado SolidErase en lugar del método elegido.

> **Limitaciones en unidades SSD**
>
> El software solo puede sobrescribir las zonas accesibles desde Windows. No puede alcanzar las que el controlador ha reservado o reasignado. SolidErase no ejecuta órdenes de firmware como Secure Erase o Sanitize ni realiza un borrado criptográfico.

Pasos siguientes

- Cambiar el método predeterminado
- Borrar unidades y particiones

Informes y certificados de borrado

Cada borrado puede generar un informe que indica qué elementos se borraron, con qué método y con qué resultado. Desde la versión 22 se guarda también un certificado firmado que permite detectar cambios posteriores en el informe.

Informe

El informe recoge la tarea, la hora de inicio, la duración, los destinos, el método utilizado para cada destino, el resultado general y todas las advertencias o errores. Para discos completos, puede incluir el número de inventario, el destino del soporte y la necesidad de protección de los datos que indique antes del borrado, así como los datos del operador que figuren en la configuración.

Los informes se guardan como archivos XML. Para abrirlos, seleccione **Informes**. Consulte Gestionar informes.

Certificado de borrado

El certificado acompaña al informe en dos formatos, un archivo JSON y un archivo firmado `.oose`. Conserve juntos todos los archivos que correspondan al mismo informe.

- **Firma**. El servicio de O&O SafeErase firma el certificado con una clave propia de esa instalación. En el Modo Fortaleza, o si el servicio no está disponible, se utiliza una clave temporal y esta circunstancia queda reflejada en el certificado. Puede consultar la huella digital del certificado en la configuración o utilizar un certificado de su empresa.
- **Sello de tiempo**. Si activa esta opción, un servicio de sellado de tiempo acredita cuándo se firmó el certificado (RFC 3161). El servicio solo recibe un valor hash. Si el certificado se crea sin conexión, es posible añadir el sello más adelante. En ese caso quedará indicado que se añadió con posterioridad.
- **Cadena de certificados**. Cada certificado nuevo hace referencia al anterior. Si falta uno sin que exista una nota de eliminación firmada, la verificación indica que hay una interrupción en la cadena.

Qué acredita la firma

Una firma válida acredita que el certificado no ha cambiado desde que se firmó. Para saber si se borraron todos los destinos, consulte también el resultado del informe. Compruebe ambos tal como se explica en Verificar un certificado de borrado.

En los informes anonimizados, los nombres de archivos y carpetas se sustituyen por asteriscos. Consulte Configuración.

Borrar archivos y carpetas

Puede borrar archivos individuales o carpetas completas con todo su contenido de forma irreversible.

Requisitos previos. Cierre los archivos que estén abiertos en otros programas y asegúrese de tener una copia de los datos que desee conservar.

1. Seleccione **Archivos y carpetas** en la página de inicio o en el panel de navegación.
2. Seleccione **Archivos** o **Carpeta** y elija los objetos. También puede arrastrarlos desde el Explorador de archivos a la lista.
3. Si añade carpetas grandes, espere a que termine la lectura. Debajo de la lista aparece un resumen con el número de elementos y archivos y el tamaño total.
4. En **Vista**, active **Mostrar ruta** y **Mostrar tipo** para ver más columnas. Para quitar un elemento de la selección, márquelo y pulse **Eliminar**. El archivo permanece en su ubicación.
5. Continúe con **Revisar la tarea de eliminación**.
6. Revise la selección en **Qué** y el método de borrado en **Cómo**. En **Después**, decida si desea **Guardar y firmar el informe** y **Apagar el equipo al terminar**.
7. Seleccione **Eliminar de forma segura ahora**.

Resultado. Los archivos se sobrescriben y se eliminan. La página de resultados indica cuántos elementos se han borrado y recoge las advertencias. Consulte Supervisar o cancelar un borrado.

Carpetas con enlaces

Las carpetas pueden contener puntos de unión y enlaces simbólicos que apuntan a otras ubicaciones. De forma predeterminada, O&O SafeErase solo borra el enlace. Si activa **Seguir enlaces en carpetas** en la configuración, también se borrarán los datos del destino.

> **Datos fuera de la selección**
>
> Al activar **Seguir enlaces en carpetas**, se pueden borrar datos situados fuera de la carpeta seleccionada si un enlace apunta a ellos. Compruebe los enlaces antes de empezar.

Incluso con esta opción activada, O&O SafeErase no sigue enlaces a puntos de montaje de volúmenes, ubicaciones de red, raíces de unidades, carpetas de Windows y de programas ni carpetas de perfiles de usuario.

Próximos pasos

- Para eliminar restos de archivos borrados anteriormente, consulte Limpiar el espacio libre.

- Para borrar desde el menú contextual, consulte Borrar desde el Explorador de archivos.

Vaciar la Papelera de reciclaje de forma segura

Al vaciar de forma segura la Papelera de reciclaje de Windows, se sobrescribe el contenido de los archivos antes de quitarlos de la Papelera.

Requisito previo. Revise la Papelera en Windows y restaure los archivos que aún necesite. Después del vaciado seguro ya no podrá recuperarlos con **Restaurar**.

1. En la página de inicio, seleccione **Borrar rastros de forma segura…**.
2. Seleccione **Papelera de reciclaje** y desmarque las zonas que no desee borrar ahora.
3. Compruebe el método de borrado y confirme.

Resultado: La Papelera de reciclaje está vacía y sus archivos están sobrescritos. La página de inicio muestra la fecha del vaciado seguro.

Otras formas de obtener el mismo resultado:

- En el Explorador de archivos, haga clic con el botón derecho en la Papelera de reciclaje y seleccione **Vaciar la Papelera de reciclaje de forma segura**. El comando está disponible cuando está activado bajo Integración con Windows.
- En **Privacidad**, puede seleccionar **Papelera de reciclaje** junto con otros rastros. Consulte Borrar rastros del navegador y de Windows.

Si ya ha vaciado la Papelera de la forma habitual, pueden quedar restos de esos archivos en la unidad. Limpie el espacio libre de esa unidad.

Próximos pasos

- Borrar rastros del navegador y de Windows
- Limpiar el espacio libre

Limpiar el espacio libre

Puede sobrescribir el espacio libre de una unidad para impedir que se recuperen los archivos eliminados de la forma habitual. Los archivos existentes se mantienen intactos.

Requisitos previos. O&O SafeErase debe ejecutarse con permisos de administrador. Si ve **Reiniciar como administrador**, seleccione esa opción. En la configuración debe estar activada al menos una de las subtareas que se describen a continuación.

1. Seleccione **Espacio libre**.
2. Seleccione las unidades por nombre y capacidad. El resumen muestra cuánto espacio libre se sobrescribirá.
3. Abra **Método de eliminación y opciones** y compruebe las subtareas y el **Método para discos duros**.
4. Seleccione **Borrar el espacio libre ahora**.

Resultado: Las áreas libres de las unidades seleccionadas se sobrescriben. La página de inicio muestra la fecha de la limpieza para cada unidad.

Subtareas

Opción	Efecto
Sobrescribir el espacio libre	Sobrescribe las áreas de la unidad que no ocupa ningún archivo.
Borrar restos de clúster (DeepErase)	Sobrescribe el espacio no utilizado al final de los clústeres ocupados.
Limpiar referencias en la MFT	Elimina del sistema de archivos los nombres y las referencias de archivos eliminados.

Las subtareas se activan y desactivan en Configuración > Espacio libre. Si todas están desactivadas, la página muestra un aviso con el botón **Abrir configuración**.

Las unidades SSD se tratan con SolidErase si esta función está activada en **Configuración > SSD**. Consulte Métodos de borrado y unidades SSD.

La duración depende principalmente de la cantidad de espacio libre y del método. Evite escribir grandes cantidades de datos en la unidad durante la limpieza.

> **La limpieza del espacio libre conserva los archivos existentes**
>
> Para borrar también los archivos existentes, seleccione **Borrar unidades enteras en su lugar**. Se abrirá la página Borrar unidades y particiones.

Próximos pasos

- Consultar el informe de limpieza.
- Para borrar también otros rastros, consulte Borrar rastros de forma segura.

Borrar rastros del navegador y de Windows

Borre los rastros que dejan los navegadores, Windows y los programas, como el historial, las cookies, los archivos temporales y las miniaturas.

Requisitos previos. Guarde los datos de formularios y el trabajo pendiente en el navegador. Los navegadores abiertos se cerrarán antes del borrado. Compruebe qué contraseñas y marcadores necesita conservar.

1. Seleccione **Privacidad**, o en la página de inicio seleccione **Datos del navegador** o **Datos de Windows y de programas**.
2. Seleccione **Comprobar ahora** (o **Volver a comprobar**). La lista muestra cuántos rastros contiene cada categoría.
3. Expanda las áreas y seleccione las categorías. **Seleccionar todo** y **Borrar selección** cambian todas las categorías a la vez. La selección se guarda para la próxima vez.
4. Compruebe la selección una vez más, en particular **Contraseñas y datos de formularios**, **Marcadores** y **Configuración del navegador**.
5. Seleccione **Borrar los rastros seleccionados**.
6. Si hay navegadores abiertos, confirme que permite cerrarlos.

Resultado: Los rastros seleccionados se sobrescriben y eliminan. La página de inicio muestra la fecha de la limpieza para los datos del navegador y los datos de Windows.

Datos del navegador

O&O SafeErase admite Google Chrome, Microsoft Edge, Mozilla Firefox, Brave, Vivaldi, Opera y Opera GX, incluidos todos sus perfiles. Consulte las versiones compatibles en Requisitos del sistema. La página muestra la versión de cada navegador instalado. Si una versión figura como incompatible, se omite.

Categoría	Lo que se elimina
Historial	Sitios web visitados.
Historial de descargas	Lista de descargas. Los archivos descargados permanecen en el equipo.
Cookies	Datos de sesión y datos que guardan los sitios web. Al borrarlos se cierran las sesiones. Para establecer excepciones, consulte Conservar las cookies de determinados sitios web.
Caché	Páginas e imágenes en caché.
Contraseñas y datos de formularios	Contraseñas guardadas y entradas de formulario. Se eliminan de forma permanente.
Marcadores	Favoritos guardados.
Configuración del navegador	Se restablecen la página de inicio, el buscador y otros ajustes.

Brave y Vivaldi no ofrecen la categoría **Configuración del navegador**; Opera y Opera GX no ofrecen ni **Marcadores** ni **Configuración del navegador**.

Datos que se conservan

Brave, Vivaldi, Opera y Opera GX almacenan datos de sus propias características en los mismos archivos que sus ajustes y marcadores. O&O SafeErase nunca borra estos datos, cualquiera que sea la categoría que seleccione:

- **Brave**. Se conservan Brave Wallet y Brave Rewards.
- **Vivaldi**. Se conservan las notas, el correo, las fuentes de noticias, el calendario, los contactos y las sesiones guardadas. Los accesos de Marcación rápida son marcadores y se borran si selecciona **Marcadores**.
- **Opera y Opera GX**. Se conservan los accesos de Speed Dial, la configuración de la VPN y de la barra lateral, los datos de los servicios de mensajería de la barra lateral y de Pinboards, así como los GX Mods. Al borrar las **Cookies** se cierran las sesiones de los servicios de mensajería.

Datos de Windows y de programas

Categoría	Lo que se elimina
Documentos recientes	Accesos directos de «Recientes». Los documentos se conservan.
Archivos temporales de Windows	Contenido de `%TEMP%` y `Windows\Temp`.
Caché de miniaturas	Vista previa de imágenes en el Explorador de archivos.
Papelera de reciclaje	Elementos eliminados en la papelera de reciclaje.
Volcados de memoria	Volcados del núcleo de Windows generados después de un fallo del sistema.
Archivos de CheckDisk	Fragmentos recuperados por CheckDisk (`*.chk`).
Datos de acceso FTP guardados	Credenciales FTP guardadas en el Explorador de archivos.

Los rastros del navegador y de Windows no se pueden borrar en el Modo Fortaleza.

Próximos pasos

- Conservar las cookies de determinados sitios web
- Elija qué navegadores se limpian: Configuración

Conservar las cookies de determinados sitios web

Si conserva las cookies de los sitios que utiliza con frecuencia, podrá mantener la sesión iniciada cuando borre el resto de las cookies.

Requisito previo. Cierre los navegadores antes de empezar. O&O SafeErase no puede leer las cookies de un navegador abierto ni mostrar los dominios correspondientes.

1. Abra **Configuración > Cookies que se conservarán**.
2. Seleccione **Añadir…**.
3. Escriba parte del dominio, por ejemplo `bank.example`. La lista muestra dominios coincidentes para los que sus navegadores han almacenado cookies. También puede ingresar un dominio que no está en la lista.
4. En **Se aplica a**, elija **Solo este dominio** o **Este dominio y todos sus subdominios**. El cuadro de diálogo indica cuántas cookies guardadas se conservarán.
5. Seleccione **Añadir** y, a continuación, confirme la configuración con **Aceptar**.

Resultado: La próxima vez que borre las cookies, las cookies de este dominio se mantendrán en todos los navegadores compatibles.

Si desea que se vuelvan a borrar las cookies de un dominio, quite ese dominio de la lista. Si la lista está vacía, se borrarán todas las cookies de los navegadores seleccionados.

> **Nota**
>
> La excepción solo se aplica a las cookies. Se siguen borrando el historial, la caché y las demás categorías seleccionadas para ese sitio web. Que la sesión permanezca abierta depende también del propio sitio.

Próximos pasos

- Borrar rastros del navegador y de Windows

Borrar unidades y particiones

Antes de vender o desechar una unidad, puede borrar un disco completo o una sola partición con todos sus archivos.

> **Se pierden todos los datos de la unidad**
>
> Al seleccionar un disco completo se borran todas sus particiones, incluidas las que no tienen letra de unidad, como algunas particiones Linux o de recuperación. Haga una copia de los datos que necesite en otra unidad. Identifique el disco por el modelo, el número y la capacidad.

Requisitos previos. O&O SafeErase debe tener una licencia activada y ejecutarse con permisos de administrador. Para borrar la unidad del sistema debe utilizar el Modo Fortaleza.

1. Seleccione **Unidades / particiones**. Si ha conectado o desconectado una unidad, seleccione **Actualizar**.
2. Seleccione un disco completo o las particiones que desee borrar. Para ver además las zonas que no pertenecen a ninguna partición, seleccione **Vista > Mostrar áreas sin particionar**.
3. Abra **Método de eliminación y opciones** y revise el método. Si va a borrar el disco completo y desea volver a utilizarlo inmediatamente en Windows, active **Inicializar y formatear después**.
4. Seleccione **Borrar unidad…**.
5. En la ventana de confirmación, compruebe de nuevo el disco. Aquí aparecen también las particiones que no figuraban en la lista.
6. Si borra todo el disco, puede introducir el número de inventario, el destino del soporte y la necesidad de protección de los datos para el certificado de borrado.
7. Si la unidad contiene un sistema operativo, introduzca el código de seguridad mostrado y, a continuación, seleccione **Borrar de forma irrecuperable ahora**.

Resultado: Todos los sectores de la unidad seleccionada se sobrescriben. Sin formatear, el disco no tiene partición y no aparece en el Explorador de archivos.

Inicializar y formatear después

Si activa **Inicializar y formatear después**, tras borrar el disco completo O&O SafeErase crea una partición que ocupa todo el disco, realiza un formato rápido y le asigna una letra de unidad.

Disco	Estilo de partición y sistema de archivos
Disco interno	GPT, NTFS
Unidad USB o tarjeta de memoria	exFAT, con MBR hasta 2 TB

La opción está desactivada de forma predeterminada y solo se aplica a la ejecución actual. No está disponible en el Modo Fortaleza ni en Borrar todo el equipo. Si falla el formateo, O&O SafeErase muestra una advertencia, pero el borrado ya ha finalizado. Puede inicializar después el disco desde la Administración de discos de Windows.

Si la unidad ha cambiado

Al conectar o desconectar un disco después de seleccionarlo, pueden cambiar los números de disco. O&O SafeErase detiene el borrado e indica que la unidad ha cambiado. Pulse **Actualizar** y vuelva a seleccionarla.

Próximos pasos

- Verificar un certificado de borrado
- Borrar la unidad del sistema y todos los discos internos: Borrar todo el equipo

Borrar desde el Explorador de archivos

Borre archivos y carpetas, el espacio libre de una unidad o la Papelera de reciclaje directamente desde el menú contextual del Explorador de archivos.

Requisito previo. En **Configuración > Integración con Windows**, active **Menú contextual del Explorador** y, para habilitar el comando de la Papelera, **Papelera de reciclaje**. Confirme con **Aceptar**. Windows solicita permisos de administrador. La opción de la Papelera solo se puede cambiar si O&O SafeErase se ejecuta como administrador.

1. En el Explorador de archivos, seleccione los archivos o carpetas.
2. Haga clic con el botón derecho en la selección y seleccione **Eliminar de forma segura**. Para una unidad, seleccione **Borrar espacio libre**; para la Papelera de reciclaje, **Vaciar la Papelera de reciclaje de forma segura**.
3. Revise los elementos y el método en el cuadro de diálogo. **Más opciones…** abre O&O SafeErase con la selección actual.
4. Inicie el borrado.

Resultado. Se borran los elementos con el método indicado. La operación también aparece en la página de inicio de O&O SafeErase.

En Windows 11, los comandos aparecen en el menú contextual compacto. Si faltan, seleccione **Mostrar más opciones** y compruebe los ajustes de **Integración con Windows**.

Para borrar una unidad completa, consulte Borrar unidades y particiones. Esta función no está disponible en el menú contextual.

Próximos pasos

- Cambiar el método de borrado predeterminado

Supervisar y cancelar un borrado

Puede seguir trabajando mientras se realiza el borrado y comprobar el resultado cuando termine.

Durante el borrado, se muestran el progreso, el número de elementos, la pasada actual, el tiempo transcurrido y el tiempo restante estimado. No apague el equipo hasta que finalice.

Seguir trabajando durante el borrado

- **Continuar en segundo plano** oculta la página mientras prosigue el borrado. Un aviso en la parte superior de la ventana muestra el progreso. Pulse **Mostrar** para volver a la página.
- **Apagar al terminar** apaga el equipo una vez finalizado el borrado. Guarde antes los informes o registros que necesite.

Solo un borrado puede ejecutarse a la vez. Espere hasta que haya terminado, o cancele, antes de comenzar otro.

Cancelar el borrado

1. Seleccione **Cancelar ahora**.
2. Espere hasta que la página muestre que se canceló el borrado.

Resultado. El proceso se detiene. Los elementos ya borrados no pueden recuperarse. Los elementos pendientes o tratados solo en parte aún podrían recuperarse.

> **Cancelar un borrado de unidad**
>
> Tras un borrado parcial, la unidad o partición ya no conserva todos los datos originales ni tiene un sistema de archivos utilizable. Vuelva a borrarla por completo. Si cancela el borrado de la unidad del sistema en el Modo Fortaleza, es probable que Windows ya no arranque.

Comprobar el resultado

La página de finalización muestra si el borrado se realizó correctamente, se completó con advertencias, falló para algunos elementos o se canceló.

1. Abra **Registro** y active **Solo advertencias y errores**.
2. Revise cada entrada. Una causa frecuente es que otro programa mantenga abierto un archivo.
3. Seleccione **Mostrar informe** para obtener todos los detalles.
4. Corrija la causa del problema, por ejemplo, cerrando el programa, y vuelva a borrar los elementos pendientes.

Resultado. Puede identificar qué elementos se han borrado. Si hubo advertencias o errores, quedaron elementos sin borrar.

Próximos pasos

- Administrar informes
- Después de borrar todo el PC: Guardar los registros

Configurar e iniciar el Modo Fortaleza

En el Modo Fortaleza, O&O SafeErase se ejecuta en el entorno de recuperación de Windows (Windows RE). En ese entorno, Windows no mantiene archivos bloqueados y es posible borrar las unidades del sistema o incluso todo el equipo. Primero debe configurar el modo y reiniciar el equipo en él.

Requisitos previos

- Debe disponer de una licencia de O&O SafeErase. El Modo Fortaleza no está disponible en la versión de prueba.
- O&O SafeErase se ejecuta con derechos de administrador. De lo contrario, seleccione **Reiniciar como administrador** en la página.
- El equipo debe disponer de Windows RE. Si está desactivado, el asistente puede repararlo.
- No se está ejecutando ningún borrado.

Configurar el Modo Fortaleza

1. Seleccione **Borrar todo el equipo**. La tarjeta **Modo Fortaleza** indica el estado, la versión, la ubicación y el estado de Windows RE.
2. Seleccione **Configurar el Modo Fortaleza**.
3. Espere a que aparezca **Configurado**. La configuración tarda unos minutos y no reinicia el equipo.

Resultado. El Modo Fortaleza queda integrado en el entorno de recuperación de Windows y puede iniciarlo cuando lo necesite.

Iniciar el Modo Fortaleza

1. Guarde todos los documentos abiertos y cierre todos los programas.
2. Seleccione **Iniciar el Modo Fortaleza** y confirme el reinicio.
3. Si la unidad del sistema está protegida con BitLocker, confirme que acepta suspender la protección hasta que Windows vuelva a iniciarse normalmente. Tenga a mano la clave de recuperación de BitLocker.

Resultado. El equipo se reinicia y O&O SafeErase se abre en el Modo Fortaleza. Continúe con Borrar todo el equipo o borre unidades y particiones concretas, incluida la unidad del sistema.

El Modo Fortaleza no permite borrar los rastros del navegador ni de Windows. Si reinicia el equipo sin borrar Windows, este volverá a iniciarse normalmente.

Volver a crear o quitar el Modo Fortaleza

Después de actualizar O&O SafeErase, la tarjeta puede mostrar **Actualización recomendada** o **Desconocido**. Seleccione **Volver a crear** para que el Modo Fortaleza utilice la versión instalada.

La opción **Eliminar** quita la entrada de arranque y la carpeta del Modo Fortaleza. Puede volver a configurarlo cuando lo necesite.

Próximos pasos

- Borrar todo el equipo
- Guardar los registros después de borrar un PC

Borrar todo el equipo

Puede borrar todos los discos internos, incluidos Windows y los programas instalados, antes de vender, devolver o desechar el equipo.

> **Se borrarán Windows y todos los discos internos**
>
> Los datos, los programas y el sistema operativo se sobrescriben de forma irreversible. Los discos internos se borran siempre. Después del borrado, el equipo ya no podrá iniciar Windows.

Requisitos previos

- Guarde en una unidad externa los archivos que necesite y las claves de licencia de los programas instalados.
- Desconecte las unidades externas que desee conservar, salvo la que utilizará para guardar los registros.
- Configure el Modo Fortaleza y reinicie el equipo en ese modo.

Seleccionar los discos

1. En el Modo Fortaleza, seleccione **Borrar todo el equipo**.
2. Compruebe el nombre, la capacidad y el tipo de cada disco. Los discos internos están siempre seleccionados.
3. Seleccione también los discos externos que desee borrar.
4. En **Guardar registros en:**, elija una unidad externa que vaya a conservar o seleccione **Recurso compartido de red…**. Consulte Guardar los registros. Si conecta una memoria USB, pulse **Actualizar** para volver a detectar las unidades.
5. Compruebe el método de borrado. Si SolidErase está activado en la configuración, se utilizará en las unidades SSD.
6. Seleccione **Siguiente**.

Confirmar e iniciar el borrado

1. Revise el resumen y la advertencia final.
2. Si procede, rellene los campos **Número de inventario**, **Destino del soporte** y **Necesidad de protección de los datos** para el certificado de borrado.
3. Introduzca el código de seguridad mostrado.
4. Seleccione **Borrar todo el equipo ahora**.

Resultado: Todos los discos seleccionados se sobrescriben. Al final, O&O SafeErase copia los registros y el informe al destino seleccionado.

Antes de apagar o reiniciar el equipo, compruebe el resultado y los registros guardados. Al reiniciar se pierden los registros que solo estén en memoria. Guárdelos con **Guardar registros…**.

La opción **Inicializar y formatear después** no está disponible para esta tarea. Para reutilizar el disco, inicialícelo desde la nueva instalación, por ejemplo, en la Administración de discos de Windows.

Próximos pasos

- Guardar los registros después de borrar un PC
- Verificar un certificado de borrado

Guardar los registros después de borrar un PC

Para documentar el borrado de todo el equipo, guarde el informe y los registros en una unidad que vaya a conservar.

Durante el borrado, los registros permanecen en memoria. Al finalizar, O&O SafeErase copia el registro de borrado, el informe y los registros del programa y del servicio en el destino seleccionado en **Guardar registros en:**.

Guardar en una unidad externa

1. Conecte una unidad USB que vaya a conservar.
2. En **Guardar registros en:**, seleccione **Actualizar** y luego la unidad.

Asegúrese de que esa unidad no esté seleccionada para el borrado. Si no hay ninguna unidad externa conectada o si se van a borrar todas, no podrá guardar los registros en una unidad externa.

Guardar en un recurso compartido de red

Requisito previo. El equipo debe estar conectado a la red y el entorno de recuperación de Windows debe disponer de un controlador para el adaptador de red.

1. En **Guardar registros en:**, seleccione **Recurso compartido de red…**.
2. En **Recurso compartido:**, escriba la ruta con el formato `\\server\share` o `\\server\share\folder`.
3. En **Nombre de usuario:**, utilice el formato `DOMAIN\user` e introduzca la **Contraseña:**. Si el recurso compartido no requiere nombre de usuario, deje el campo vacío.
4. Confirme la selección. O&O SafeErase comprueba la conexión, las credenciales y el permiso de escritura.

Resultado: Al final del borrado, los registros se guardan en la carpeta `OOSE-Logs\<computer>_<timestamp>` en el recurso compartido. La contraseña no se almacena.

Si la comprobación falla, el mensaje indica la causa. Puede faltar la conexión de red, el servidor podría no estar disponible, las credenciales podrían ser incorrectas o podrían faltar permisos de escritura. Corrija los datos, elija una unidad USB o seleccione **No guardar**.

Guardar los registros después

Con **No guardar**, o si la copia falló, los registros permanecen en memoria hasta que se reinicie el PC.

1. Conecte una unidad USB.
2. En la página de finalización, seleccione **Guardar registros…**.
3. Seleccione la unidad y guarde los registros.

4. Compruebe que los archivos están en la unidad antes de apagar el PC.

Resultado: Los registros y el informe están en la unidad USB.

> **Información para el soporte**
>
> Si no dispone de una unidad, la página de resultados muestra un código en **Información para el soporte**. Fotografíelo con su teléfono y envíelo al soporte técnico de O&O. El código no contiene datos personales ni sustituye al informe o al certificado de borrado.

Próximos pasos

- Verificar un certificado de borrado

Administrar informes

Localice el informe de un borrado, compruebe el resultado y decida si desea conservarlo, exportarlo o eliminarlo.

1. Seleccione **Informes**. La lista muestra la fecha, la duración, el alcance, el método y el estado de cada informe guardado.
2. Seleccione **Filtro** para reducir la lista por **Tipo**, **Estado** y **Período**. **Restablecer** muestra todos los informes de nuevo.
3. Abra un informe.
4. Compruebe el resultado general y el de cada destino. Revise también las advertencias y errores del registro.
5. Si el informe tiene un certificado de borrado, compruebe la firma. Consulte Verificar un certificado de borrado.

Resultado. El estado **OK** indica que se borraron todos los destinos**.Advertencia**, **Error** o **Cancelado** indican que quedaron destinos sin borrar.

Importar y exportar informes

- **Importar** añade a la lista informes de otra carpeta o equipo, por ejemplo, los guardados tras borrar todo el equipo. Al importarlos, O&O SafeErase indica cuántos certificados son válidos, se han modificado, carecen de firma o faltan.
- **Exportar a Excel** guarda los datos en una hoja de cálculo para su análisis. La hoja no sustituye al informe ni al certificado firmado.

Conserve juntos el informe XML y sus archivos JSON y `.oose`.

Borrar informes

Eliminar el informe de forma segura borra un informe**.Eliminar todo de forma segura** borra todos los informes. También se borran los certificados correspondientes. La cadena de certificados conserva una nota de eliminación firmada.

> **Los informes eliminados no se pueden restaurar**
>
> El borrado de informes es irreversible. Antes de eliminarlos, archive los que deba conservar como prueba.

Próximos pasos

- Configure la carpeta, el guardado automático y la anonimización de los informes: Configuración
- Verificar un certificado de borrado

Verificar un certificado de borrado

Verifique que el certificado de borrado que acompaña al informe no se ha modificado. Así podrá utilizar el informe como prueba del resultado.

Requisito previo. El informe XML y sus archivos JSON y `.oose` deben estar en la misma carpeta. Si proceden de otro equipo, impórtelos primero.

1. Seleccione **Informes** y abra el informe.
2. Consulte la línea **Firma**. Allí encontrará el estado, el certificado de firma, su huella digital SHA-256 y el sello de tiempo.
3. Compare el estado con la tabla de abajo.
4. Compruebe el resultado de la eliminación en el mismo informe.

Resultado. La firma permite comprobar la autenticidad del certificado. El resultado del informe indica si se borraron todos los destinos. Compruebe ambos.

Estado	Significado
Certificado de borrado válido	El certificado no se ha modificado desde que se firmó.
Certificado de borrado válido, sin sello de tiempo	El certificado no se ha modificado. Ningún servicio de sellado de tiempo ha confirmado la hora de la firma.
Certificado de borrado modificado	El contenido ya no coincide con la firma. Mantenga el archivo sin cambios para una investigación.
Certificado de borrado sin firmar	El certificado carece de una firma verificable. El informe indica el motivo.
Hueco en la cadena de certificados de borrado	Falta un certificado anterior y no hay una nota de eliminación.
Sin firmar (informe antiguo)	El informe procede de una versión anterior que no generaba certificados de borrado.

Verificar en la línea de comandos

Puede verificar un certificado desde la línea de comandos sin borrar datos y sin necesidad de una licencia.

```
.\OOSafeEraseCmd.exe verify "C:\Reports\Report_example.oose"
```

El código de salida indica el resultado. Consulte Línea de comandos. Para comprobar la continuidad de la cadena, los certificados anteriores deben estar disponibles en el equipo.

Próximos pasos

- Informes y certificados de borrado
- Configure los datos del operador, el certificado de firma y los sellos de tiempo en Configuración.

Configuración

Esta página enumera todas las opciones del diálogo de configuración con su significado y valor predeterminado. Abra el diálogo en la parte inferior de la navegación y confirme los cambios con **Aceptar**.

Las opciones que un administrador ha establecido por directiva de grupo están bloqueadas y marcadas en consecuencia. Algunas páginas están ocultas en el Modo Fortaleza.

Aplicación

General

Opción	Significado	Predeterminado
Idioma	Idioma de la interfaz. El cambio se aplica al reiniciar el programa.	Usar la configuración del sistema
Modo de visualización	Modo claro, modo oscuro o uno de los dos modos de alto contraste.	Usar la configuración del sistema
Minimizar al área de notificación	Minimiza la ventana en el área de notificación durante el borrado.	Desactivado
Cerrar la aplicación desde el menú contextual después de la eliminación	Cierra la aplicación al finalizar un borrado iniciado desde el menú contextual del Explorador de archivos. Los informes se guardan automáticamente.	Desactivado

Integración con Windows

Estas opciones se encuentran en **General**. Seleccione **Aceptar** para aplicarlas. Windows solicitará permisos de administrador. Las opciones no aparecen en el Modo Fortaleza.

Opción	Significado	Predeterminado
Menú contextual del Explorador	Agrega **Eliminar de forma segura** y **Borrar espacio libre** al menú contextual del Explorador de archivos; vea Borrar desde el Explorador de archivos.	Según lo establecido en este PC
Papelera de reciclaje	Agrega **Vaciar la Papelera de reciclaje de forma segura** al menú contextual de la Papelera de reciclaje. Solo se puede cambiar cuando el programa se ejecuta como administrador.	Según lo establecido en este PC

Sin derechos de administrador, la página ofrece **Reiniciar como administrador**.

LiveUpdate

Opción	Significado	Predeterminado
Buscar actualizaciones automáticamente	Comprueba periódicamente si hay una versión nueva y ofrece instalarla.	Activado
No mostrar la actualización actual	Oculta el aviso de la actualización que está disponible actualmente. Las actualizaciones posteriores se muestran de nuevo.	Desactivado
No mostrar más actualizaciones	Oculta todos los avisos de actualización. Todavía puede buscar actualizaciones en la información del programa.	Desactivado

Avanzado

Opción	Significado	Predeterminado
Desbloquear unidad	Lo que sucede cuando una unidad a borrar está en uso: **Preguntar siempre**, **Ignorar siempre** o **Desbloquear siempre**. Desbloquear una unidad en uso puede causar pérdida de datos en los programas que la usan.	Preguntar siempre
Habilitar el registro	Escribe un registro detallado del servicio O&O SafeErase para soporte. Cuando está apagado, solo se registran las advertencias y los errores. El servicio se reinicia después de un cambio.	Desactivado

Eliminación

Método de eliminación

Elija el método de borrado predeterminado para las tareas nuevas. Puede seleccionar otro al revisar cada tarea.

Opción	Predeterminado
Método de borrado	**NIST 800-88 Clear / BSI CON.6 (1× datos aleatorios)**

Archivos y carpetas

Opción	Significado	Predeterminado
Seguir enlaces en carpetas	Borra también los destinos de puntos de unión y enlaces simbólicos en las carpetas seleccionadas. Nunca se siguen enlaces a puntos de montaje, ubicaciones de red, raíces de unidades, carpetas de Windows o de programas ni carpetas de perfiles de usuario.	Desactivado

Espacio libre

Estas opciones controlan las subtareas de limpieza del espacio libre. Si alguna está desactivada, se muestra una advertencia. Si están todas desactivadas, no se puede limpiar el espacio libre.

Opción	Significado	Predeterminado
Eliminar el espacio libre de forma segura	Sobrescribe las áreas que ningún archivo ocupa.	Activado
DeepErase en clústeres	Sobrescribe el espacio sin utilizar al final de los clústeres ocupados (NTFS).	Activado
Eliminar enlaces a archivos eliminados	Elimina las entradas de archivos eliminados del sistema de archivos (MFT en NTFS, entradas de directorio en FAT).	Activado

SSD

Opción	Significado	Predeterminado
Eliminar SSD con SolidErase	Borra las unidades SSD detectados con SolidErase en lugar del método seleccionado; consulte Métodos de borrado y unidades SSD.	Activado

Análisis e informes

Recomendación

Opción	Significado	Predeterminado
Recomendar un borrado seguro después de	Intervalo tras el cual se recomienda volver a limpiar los datos del navegador, los datos de Windows y el espacio libre. Las opciones son 7, 14, 30, 60 o 90 días, o **Nunca**.	30 días

Navegador

Cada navegador compatible tiene su propio ajuste. En Privacidad solo se limpian los navegadores seleccionados. Para seleccionar un navegador, debe estar instalado.

Opción	Predeterminado
Opción independiente por navegador	Todas activadas

Cookies que se conservarán

La lista de dominios cuyas cookies se guardan cuando se borran las cookies; consulte Conservar las cookies de determinados sitios web. **Añadir…** agrega un dominio, **Eliminar** lo elimina de la lista.

Opción	Predeterminado
Lista de dominios	Vacía. Se borran todas las cookies.

Informes

Opción	Significado	Predeterminado
Guardar informes automáticamente	Guarda el informe de cada operación en la carpeta de informes.	Desactivado
Anonimizar los nombres de archivos y carpetas	Sustituye los nombres de los archivos y carpetas por asteriscos en los informes nuevos, por ejemplo `C:\*\*\*`. El certificado de borrado también omite los datos del operador. Los informes existentes se conservan sin cambios.	Desactivado
Escribir registro completo	Escribe todos los elementos procesados en el informe, no solo advertencias y errores.	Activado
Mostrar un máximo de 10.000 entradas en el informe	Limita el número de entradas de archivo que se muestran en un informe.	Activado
Ubicación	Carpeta en la que se guardan los informes. Utilice **Examinar…** para elegir otra carpeta en la que tenga permiso de escritura.	`Documents\OO Software\OO SafeErase\Reports` en el perfil del usuario

Certificado de borrado

Los detalles del operador se escriben en cada certificado de borrado. Todos los campos están vacíos por defecto (**Sin indicar**).

Opción	Significado
Nombre	Nombre de la persona que realiza el borrado.
Cargo o función	Función que desempeña la persona responsable del borrado.
Organización	Empresa u organización.
Ubicación	Lugar del borrado.
Contacto (teléfono o correo electrónico)	Contacto para preguntas sobre el borrado.

Firma de los certificados de borrado

Opción	Significado	Predeterminado
Certificado de firma	Muestra el certificado con el que firma el servicio y su huella digital SHA-256. Es un dato de consulta.	Clave de esta instalación
Certificado de la empresa (huella digital)	Huella digital de un certificado con clave privada en el almacén de certificados de este equipo. El servicio firma entonces con él en lugar de con la clave de esta instalación.	Vacía
Añadir un sello de tiempo (RFC 3161)	Una autoridad de sellado de tiempo confirma cuándo se firmó cada certificado de borrado. Solo se envía un valor hash de la firma. Para certificados creados sin conexión el sello puede obtenerse posteriormente.	Desactivado
Autoridad de sellado de tiempo (URL)	Dirección de la autoridad de sellado de tiempo, por ejemplo, un prestador cualificado conforme a eIDAS.	Si se deja vacío, se utiliza DigiCert.

Línea de comandos

`OOSafeEraseCmd.exe` permite borrar archivos, carpetas, espacio libre, unidades y el contenido de la Papelera de reciclaje mediante scripts y tareas programadas. Se instala en la carpeta de O&O SafeErase si se selecciona el componente **Línea de comandos**, activado de forma predeterminada. El instalador no añade esa carpeta a `PATH`.

Abra el símbolo del sistema o PowerShell como administrador. Ejecute el programa desde la carpeta de instalación o indique la ruta completa. En PowerShell, si está en esa carpeta, anteponga `.\` al nombre del ejecutable. En **Herramientas**, la opción **Línea de comandos** abre esta página. Sin conexión a Internet se muestra la misma ayuda que con `--help`.

```
.\OOSafeEraseCmd.exe <command> [options]
```

Los comandos borran datos reales

`wipe-file` y `secure-move` borran sin pedir confirmación. Los demás comandos de borrado piden confirmación una vez y `--yes` omite esa pregunta. Pruebe primero sus scripts con datos de prueba. La opción `--analyze-only` solo existe para los comandos que se indican más abajo y no sirve como modo de prueba general.

Comandos

Comando	Finalidad
`wipe-file`	Borrar un solo archivo.
`wipe-folder`	Borrar una carpeta y todo su contenido.
`wipe-freespace`	Limpiar el espacio libre de un volumen.
`wipe-disk`	Borra un disco entero.
`wipe-region`	Borrar una partición o región de un disco.
`list`	Borrar todos los archivos y carpetas que aparecen en un archivo de texto.
`wipe-trash`	Vaciar de forma segura la Papelera de reciclaje del usuario.
`list-trash`	Mostrar el contenido de la Papelera de reciclaje del usuario sin borrar nada.
`secure-move`	Copiar archivos o carpetas en una carpeta de destino y borrar después el origen de forma segura.
`list-disks`	Enumerar los discos y sus particiones con el número, el número de serie y el tamaño, sin borrar nada.
`list-methods`	Enumera los métodos de borrado.
`verify <file>`	Verificar un certificado de borrado (`.oose` o `.json`) o el certificado que acompaña a un informe XML.
`license`	Mostrar, activar o comprobar la licencia.

Los nombres `wipe-directory` , `wipe-partition` , `wipe-recyclebin` y `list-recyclebin` también funcionan.

Opciones comunes

Opción	Significado
`--method`, `-m <method>`	Método de borrado. Consulte Métodos. El predeterminado es `Random`.
`--verbose`	Salida detallada.
`--quiet`, `-q`	Sin salida de progreso. Las preguntas que necesitan una respuesta todavía se muestran.
`--help`, `-h`, `/?`	Muestra la ayuda.
`--version`	Muestra la versión.

El programa comprueba todas las opciones antes de borrar datos. Finaliza con el código 1 si una opción no corresponde al comando o está repetida, si falta un valor o si no reconoce el método.

Opciones por comando

Comando	Opción	Significado
`wipe-file`	`--file`, `-f <path>`	Archivo para borrar.
`wipe-folder`	`--directory`, `-d <path>` (o `--folder`, `-f`)	Carpeta a borrar.
`list`	`--list-file`, `-l <path>`	Archivo de texto con una ruta por línea; las líneas que comienzan con `#` son comentarios. Si una línea no es una ruta válida, nada se borra.
`wipe-file`, `wipe-folder`, `list`	`--force`	Permite borrar también en las carpetas de Windows, de programas o de perfiles de usuario. Consulte Rutas de archivos y carpetas.
`wipe-folder`, `list`	`--follow-links`	Borra también los destinos de puntos de unión y enlaces simbólicos. De forma predeterminada solo se eliminan los enlaces. Nunca se siguen enlaces a puntos de montaje, ubicaciones de red, raíces de unidades, carpetas de Windows o de programas ni carpetas de perfiles de usuario.
`wipe-freespace`	`--volume`, `-v <path>`	Volumen, por ejemplo `C:\`.
`wipe-freespace`	`--free-space`, `--cluster-tips`, `--fs-records`	Permiten sobrescribir el espacio libre, el espacio sobrante en clústeres y las entradas del sistema de archivos, respectivamente. Si no especifica ninguna, solo se sobrescribe el espacio libre.
`wipe-disk`, `wipe-region`	`--disk`, `-d <id>`	Número de disco como se muestra por `list-disks`, por ejemplo `0` para `\\.\PhysicalDrive0`.
`wipe-region`	`--region`, `-r <id>`	Número de la partición o región como se muestra por `list-disks`.
`wipe-disk`, `wipe-region`	`--serial <serial number>`	Solo permite el borrado si coincide el número de serie del disco.
`wipe-disk`, `wipe-region`	`--expect-size <bytes>`	Solo permite el borrado si coincide el tamaño exacto del disco en bytes.
`wipe-disk`	`--format`	Al finalizar, crea una partición y aplica un formato rápido. Utiliza GPT y NTFS en discos internos y exFAT en unidades USB y

Comando	Opción	Significado
		tarjetas de memoria, con MBR hasta 2 TB. No está disponible en el Modo Fortaleza.
`wipe-disk`, `wipe-region`	`--ignore-ssd`	Oculta el aviso relativo a las unidades SSD.
`wipe-trash`, `list-trash`	`--all-users`	Selecciona las papeleras de todos los usuarios en todas las unidades.
`list-trash`	`--drives-only`	Solo enumera unidades con elementos en la Papelera de reciclaje.
`wipe-disk`, `wipe-region`, `list`, `wipe-trash`	`--analyze-only`	Analiza los destinos sin borrar datos.
`wipe-folder`, `list`, `wipe-disk`, `wipe-region`, `wipe-trash`	`--yes`, `-y`	No preguntar antes de borrar; ver Confirmaciones.
`secure-move`	`--source`, `-s <paths>`	Rutas de origen, separadas por punto y coma.
`secure-move`	`--target`, `-t <path>`	Carpeta de destino.

Métodos

Nombre para `--method`	Pasadas	Método
`Random` (alias `NistClear` y `BsiCon6`)	1	NIST 800-88 Clear / BSI CON.6 con datos aleatorios. Es el método predeterminado.
`Zeros`	1	Sobreescribir con ceros.
`Solid`	1	SolidErase para SSD.
`Nsa3`	3	US DoD 5220.22-M (heredado).
`Bsi`	6	Procedimiento anterior del BSI (heredado), distinto de BSI CON.6.
`Nsa7`	7	US DoD 5220.22-M ECE (heredado).
`Gutmann`	35	Método de Gutmann (heredado).

Véase Métodos de borrado y unidades SSD.

Licencia

La línea de comandos utiliza la licencia de O&O SafeErase del equipo. Para borrar datos necesita una licencia activada o un período de prueba vigente. A diferencia de la interfaz gráfica, la línea de comandos permite borrar unidades durante la prueba. Los comandos de borrado indican los días restantes en la salida de error, salvo si se especifica `--quiet`. Los comandos `license`, `list-disks`, `list-methods`, `verify`, `--help` y `--version` funcionan sin licencia.

Comando	Significado
`license status`	Muestra la licencia en este equipo.
`license activate <license key>`	Active una licencia con su clave de licencia. Útil en un ordenador sin la ventana del programa, por ejemplo un servidor.
`license validate`	Compruebe la licencia con el servicio de licencias O&O.

Rutas de archivos y carpetas

`wipe-file`, `wipe-folder` y `list` comprueban cada ruta antes de borrarla y muestran la ruta completa que se borra:

- Una ruta relativa como `old_data` se interpreta a partir de la carpeta actual.

- `C:` solo, `C:folder` y `\folder` se rechazan, porque dependen de una carpeta actual que no es visible. Dé la ruta completa, por ejemplo `C:\Data\Old`.
- Se rechaza la raíz de una unidad o recurso compartido, por ejemplo `C:\` o `\\server\share`. Para borrar una unidad completa, use `wipe-disk` o `wipe-region`.
- Windows, las carpetas de programa y los perfiles de usuario, y las carpetas que los contienen, solo se borran con `--force`.

Confirmaciones

Antes de borrar, `wipe-folder`, `list`, `wipe-disk`, `wipe-region` y `wipe-trash --all-users` muestran los elementos seleccionados y esperan a que pulse una tecla. Ctrl+C cancela la operación. La opción `--yes` omite esta pregunta.

Para borrar un disco o una partición que contiene un sistema operativo debe escribir el código de seguridad que aparece en la consola, igual que en la interfaz gráfica. El modificador `--yes` no sustituye ese código. El disco o la partición donde se está ejecutando Windows no se puede borrar desde Windows. Utilice el Modo Fortaleza.

Si se requiere una confirmación pero nadie puede responder, por ejemplo porque la entrada se redirige en una tarea programada, nada se borra y el comando termina con el código de salida 5.

Discos y particiones

`list-disks` muestra cada disco con su número, modelo, tamaño, número de serie y particiones, y marca el disco con el Windows en ejecución. Para cada disco, también muestra las opciones `--serial` y `--expect-size` con los valores correctos.

Los números de disco pueden cambiar, por ejemplo al conectar una unidad USB. En los scripts, utilice `--serial` y `--expect-size` con `wipe-disk` y `wipe-region`. Si el número identifica ahora otro disco, no se borrará nada y el comando terminará con el código 1.

En una SSD, `wipe-disk` y `wipe-region` advierten que la sobrescritura no llega a las zonas reservadas por el controlador. Consulte Métodos de borrado y unidades SSD. La opción `--ignore-ssd` oculta el aviso.

Certificados de borrado y servicio

Si el servicio de O&O SafeErase se está ejecutando, la línea de comandos le encarga el borrado, igual que la aplicación. El servicio comprueba la solicitud y genera un certificado de borrado firmado. Al finalizar, la consola muestra dónde se ha guardado. El borrado mediante el servicio siempre requiere una consola con permisos de administrador.

Si el servicio no se está ejecutando, la línea de comandos lo indica y realiza el borrado en su propio proceso con los permisos de la consola. En este caso no genera un certificado. Sin permisos de administrador solo se pueden borrar archivos y carpetas que la cuenta pueda eliminar. Los discos, las particiones y el espacio libre requieren permisos de administrador.

Si la versión de la línea de comandos difiere de la del servicio, por ejemplo tras una actualización incompleta, no se borra nada y se devuelve el código 4. Vuelva a instalar O&O SafeErase.

Scripts y tareas programadas

- Ejecute `OOSafeEraseCmd.exe` indicando su ruta completa.
- Ejecute la tarea programada con los privilegios más altos, de modo que se ejecute como administrador.
- Añada `--yes` a cada comando que pregunte; de lo contrario, termina con el código de salida 5 sin borrar.
- Identifique los discos con `--serial` y `--expect-size`. Un disco o partición con un sistema operativo no se puede borrar de un script, porque requiere el código de seguridad.
- Compruebe el código de salida para determinar el resultado. Los avisos y errores se escriben en la salida de error.

```
# Borrar el disco 3 sin confirmación solo si sigue siendo el mismo disco
$cmd = "<program folder>\OOSafeEraseCmd.exe"
& $cmd wipe-disk --disk 3 --yes --serial "4C530001230" --expect-size 64023257088
if ($LASTEXITCODE -ne 0) {
 Write-Error "Erasing failed with exit code $LASTEXITCODE"
}
```

Ejemplos

```
# Borrar un archivo con el método predeterminado
.\OOSafeEraseCmd.exe wipe-file --file "C:\temp\secret.txt"

# Borrar una carpeta con el método Gutmann
.\OOSafeEraseCmd.exe wipe-folder --directory "C:\temp\old_data" --method Gutmann

# Limpiar el espacio libre de C: y el espacio sobrante en los clústeres
.\OOSafeEraseCmd.exe wipe-freespace --volume "C:\" --free-space --cluster-tips

# Mostrar los discos con su número, número de serie y tamaño
.\OOSafeEraseCmd.exe list-disks

# Borrar el disco 2 (una memoria USB) y formatearlo al finalizar
.\OOSafeEraseCmd.exe wipe-disk --disk 2 --format

# Borrar la partición 1 del disco 2
.\OOSafeEraseCmd.exe wipe-region --disk 2 --region 1

# Borrar sin confirmación todas las rutas enumeradas en un archivo
.\OOSafeEraseCmd.exe list --list-file "C:\scripts\files_to_delete.txt" --yes

# Vaciar la Papelera de reciclaje de forma segura
.\OOSafeEraseCmd.exe wipe-trash

# Activar una licencia
.\OOSafeEraseCmd.exe license activate <license key>

# Verificar un certificado de borrado
.\OOSafeEraseCmd.exe verify "C:\Reports\Report_20261019_083000.oose"
```

Códigos de salida

Código	Significado
0	Operación correcta. Para `verify`, indica que el certificado es válido, incluso sin sello de tiempo.
1	Uso incorrecto: opción inválida, desconocida o repetida, archivo o destino no encontrado, ruta de acceso rechazada o un disco que no coincide con `--serial` o `--expect-size`. Nada se borró.
2	No hay una licencia válida. El producto no se ha activado, ha terminado el período de prueba o la licencia ha dejado de ser válida.
3	La operación falló.
4	Las versiones de la línea de comandos y el servicio no coinciden.
5	Se requiere una confirmación, pero la entrada se redirige. Nada fue borrado.
6	Operación finalizada sin sobrescribir todos los elementos. En algún caso solo se eliminó un enlace, uno de los nombres de un enlace físico o un marcador de posición de la nube. La salida identifica los elementos afectados.
7	Prohibido por una política de su administrador (`wipe-disk`, `wipe-freespace`).
20	`verify`: se ha modificado el certificado.
21	`verify`: hay una interrupción en la cadena de certificados.
22	`verify`: certificado sin firmar o informe de una versión anterior sin certificado.
99	Error inesperado.
130	Cancelado, por ejemplo con Ctrl+C o un código de seguridad incorrecto.

Comandos de oosecmd

Las versiones anteriores incluían `oosecmd.exe`. La herramienta actual, `OOSafeEraseCmd.exe`, utiliza otros argumentos. La siguiente tabla indica cómo adaptar los scripts existentes.

oosecmd	OOSafeEraseCmd.exe
Archivos y carpetas sin parámetro, `--match`	`wipe-file --file <path>`, `wipe-folder --directory <path>`. Para varias rutas, utilice `list --list-file <file>`.
`--security <level>`	`--method <method>`: `highest` → `Gutmann`, `high` → `Nsa7`, `medium` → `Bsi`, `low` → `Nsa3`, `lowest` → `Random`, `zero` → `Zeros`
`--freespace <drive>`	`wipe-freespace --volume <drive>:\`
`--deletedrive <number>`	`wipe-disk --disk <number>`
`--deletevolume <drive letter>`	`wipe-region --disk <number> --region <number>`; `list-disks` muestra los números
`--showdisks`, `-w`	`list-disks`
`--tempfiles recyclebin`	`wipe-trash`
`--tempfiles`, `--internetfiles`	Sin comando equivalente. Borre los rastros del navegador y de Windows desde la interfaz gráfica.
`--analyse`, `--autoclean`	Sin comando
`--register "user:… company:… serial:…"`	`license activate <license key>`
`--createreport`, `-r`, `--reportname`	Sin opción equivalente. Si se está ejecutando el servicio, se genera un certificado de borrado. Consulte Certificados de borrado y servicio.
`--yes`, `-y`	`--yes`, `-y`
`--silent`, `-s`	`--quiet`, `-q`
`--verbose`, `-v`	`--verbose`; `-v` ahora significa `--volume`

Los rastros del navegador y de Windows solo pueden borrarse desde la interfaz gráfica. Consulte Borrar rastros del navegador y de Windows.

Glosario

Este glosario explica los términos utilizados en O&O SafeErase y en esta ayuda.

Término	Significado
Clúster	La unidad más pequeña en la que un sistema de archivos asigna espacio en una unidad.
Espacio sobrante en clústeres	Espacio sin utilizar al final del último clúster de un archivo. Puede contener restos de archivos anteriores. **Borrar restos de clúster (DeepErase)** sobrescribe ese espacio.
DeepErase	Subtarea de limpieza del espacio libre que sobrescribe el espacio sobrante en los clústeres ocupados.
Método de borrado	Determina el patrón de sobrescritura y el número de pasadas. Consulte Métodos de borrado y unidades SSD.
Certificado de borrado	Archivo firmado (`.oose`) que acompaña a un informe y permite detectar si se ha modificado. Consulte Informes y certificados de borrado.
Modo Fortaleza	Modo de ejecución de O&O SafeErase en el entorno de recuperación de Windows, donde el sistema no bloquea archivos. Es necesario para borrar la unidad del sistema o todo el equipo.
Espacio libre	Áreas de una unidad que ningún archivo ocupa. Pueden contener el contenido de archivos que se eliminaron normalmente.
MFT	Tabla maestra de archivos: el directorio de una unidad NTFS. Guarda nombres y referencias de archivos eliminados y el contenido de archivos muy pequeños.
Pasada	Una sobrescritura completa de los datos. Algunos métodos usan varias pasadas con diferentes patrones.
Cadena de certificados	Secuencia de certificados de borrado de un equipo. Cada uno hace referencia al anterior, lo que permite detectar si falta uno.
Informe	Archivo XML que identifica los destinos, el método de borrado y el resultado.
Borrado seguro	Sobrescribir los datos antes de liberar el espacio, para que no puedan recuperarse.
SolidErase	Método de O&O para las unidades SSD. Realiza una sola pasada con datos aleatorios para evitar ciclos de escritura innecesarios.
SSD	Unidad de estado sólido: una unidad con memoria flash. Su controlador decide dónde se almacenan físicamente los datos.
Sello de tiempo	Confirmación, por un servicio de sellado de tiempo (RFC 3161), del momento en que se firmó un certificado de borrado.
Rastros de uso	Datos que dejan los navegadores, Windows y otros programas durante su uso, como el historial, las cookies, la caché o los archivos temporales.
TRIM	Un comando con el que Windows indica a un SSD qué áreas ya no están en uso.

Término	Significado
Windows RE	Entorno de recuperación de Windows. Instalación mínima de Windows en una partición independiente, utilizada para reparaciones y para el Modo Fortaleza.

Solución de problemas

Localice el síntoma y siga los pasos indicados. Si el problema persiste, contacte con el soporte técnico de O&O.

Una función está bloqueada

Causa. La función requiere una licencia o permisos de administrador, o no está disponible en el Modo Fortaleza. El aviso de la tarjeta o la página correspondiente indica el motivo.

Solución:

1. Si el aviso ofrece **Reiniciar como administrador**, selecciónelo.
2. En la versión de prueba, ingrese una licencia para borrar unidades y usar el Modo Fortaleza; ver Instalación y activación.
3. Borre los rastros del navegador y de Windows desde Windows. Esta función no está disponible en el Modo Fortaleza.

El espacio libre no se puede limpiar

Causa: O&O SafeErase no se ejecuta como administrador, o todas las subtareas para el espacio libre están desactivadas.

Solución:

1. Seleccione **Reiniciar como administrador**.
2. Si la página muestra que la eliminación de espacio libre está desactivada, seleccione **Abrir configuración** y active al menos una opción en **Espacio libre**.

Un archivo no se ha borrado

Causa: Otro programa mantiene el archivo abierto, o Windows niega el acceso.

Solución:

1. Abra el registro del borrado y lea la advertencia para el archivo.
2. Cierre el programa que utiliza el archivo. Si no sabe qué programa es, reinicie Windows.
3. Vuelva a borrar el archivo.

No se puede cerrar un navegador

Causa: El navegador, o uno de sus procesos en segundo plano, no se cierra cuando O&O SafeErase se lo pide.

Solución:

1. Guarde su trabajo en el navegador y ciérrelo usted mismo.
2. Compruebe en el Administrador de tareas que ningún proceso del navegador sigue ejecutándose.
3. Seleccione **Borrar los rastros seleccionados** de nuevo.

No se admite una versión de navegador

Causa: La versión del navegador instalado es más nueva o antigua que las versiones que O&O SafeErase puede limpiar. Sus rastros no se borran.

Solución. Instale la actualización más reciente de O&O SafeErase y seleccione **Volver a comprobar**.

Una unidad no se borró porque ha cambiado

Causa: Un disco se conectó o desconectó después de la selección, y los números de disco han cambiado.

Solución:

1. Seleccione **Actualizar**.
2. Seleccione la unidad de nuevo y compruebe su nombre, número y capacidad.
3. Inicie el borrado de nuevo.

El disco borrado no aparece en el Explorador de archivos

Causa: Después de un borrado completo, el disco no tiene partición.

Solución. Inicialice el disco y cree una partición en la Administración de discos de Windows, o active **Inicializar y formatear después** para el próximo borrado. Consulte Borrar unidades y particiones.

El modo Fortaleza no se inicia

Causa. El Modo Fortaleza no está configurado, se configuró con otra versión, Windows RE está desactivado o hay un borrado en curso.

Solución:

1. Seleccione **Borrar todo el equipo** y compruebe la tarjeta **Modo Fortaleza**.
2. Seleccione **Configurar el Modo Fortaleza** o **Volver a crear**. El asistente puede reparar Windows RE si está desactivado.

3. Espere hasta que los borrados en ejecución hayan terminado, luego seleccione **Iniciar el Modo Fortaleza**.

El recurso compartido de red no se puede utilizar para los registros

Causa. El Modo Fortaleza no tiene conexión de red, a menudo porque falta el controlador del adaptador. También puede ocurrir que el servidor no esté disponible, las credenciales sean incorrectas o la cuenta no tenga permiso de escritura.

Solución:

1. Consulte la causa indicada en el mensaje.
2. Corrija la ruta del recurso compartido, el nombre de usuario o la contraseña.
3. Si no hay red, seleccione una unidad USB en su lugar.

> **Los registros en la memoria se pierden al reiniciar**
>
> Si no se pudieron guardar los registros, seleccione **Guardar registros…** antes de apagar o reiniciar el PC; consulte Guardar los registros.

Falta un informe

Causa. El guardado automático está desactivado, no hay permiso de escritura en la carpeta de informes o un filtro oculta el informe.

Solución:

1. En **Informes**, seleccione **Filtro > Restablecer**.
2. Compruebe la carpeta de informes y el guardado automático en Configuración > Informes.

El servicio y el programa no coinciden

Causa: El programa y el servicio O&O SafeErase tienen diferentes versiones, por ejemplo, después de una actualización incompleta.

Solución. Vuelva a instalar O&O SafeErase con el instalador actual. El programa y el servicio se instalan juntos.

Preguntas frecuentes

Respuestas cortas a preguntas frecuentes. Cada respuesta enlaza a la página con los detalles.

¿Puedo deshacer un borrado seguro?

No. Ni siquiera O&O Software puede recuperar los datos sobrescritos. Cancelar el proceso tampoco recupera los datos que ya se han sobrescrito. Antes de empezar, haga una copia de los datos que necesite. Consulte Cómo funciona el borrado seguro.

¿Cómo elimino los restos de archivos que ya he borrado?

Limpie el espacio libre de la unidad para sobrescribir los restos de archivos eliminados y conservar los archivos existentes. Consulte Limpiar el espacio libre.

¿La limpieza del espacio libre elimina mis archivos existentes?

No. Solo se sobrescriben las áreas que ningún archivo ocupa. Para borrar una unidad incluyendo sus archivos, use Borrar unidades y particiones.

¿La recomendación en la página de inicio significa que se encontraron datos?

No. La recomendación solo indica cuánto tiempo ha pasado desde la última limpieza segura. No analiza el equipo ni inicia un borrado. Consulte Interfaz de usuario.

¿Por qué me desconecto de los sitios web después de una limpieza?

Borrar las cookies elimina los datos de sesión. Para mantener la sesión iniciada en determinados sitios, añádalos a Cookies que se conservarán.

¿Por qué el informe muestra SolidErase en lugar del método que elegí?

Las unidades SSD se borran con SolidErase cuando esta configuración está activada. El informe muestra el método realmente utilizado; consulte Métodos de borrado y unidades SSD.

¿Qué método de borrado debo usar?

El método predeterminado, NIST 800-88 Clear / BSI CON.6, sobrescribe los datos una vez con datos aleatorios. Eso es suficiente para los discos duros actuales. Los métodos con más pasadas tardan mucho más tiempo; ver Métodos de borrado y unidades SSD.

¿Borrar todo el equipo también borra las unidades USB conectadas?

Solo si las selecciona. En cambio, los discos internos se borran siempre. Guarde los registros en una unidad que no se vaya a borrar. Consulte Borrar todo el equipo.

¿Un certificado válido demuestra que se han borrado todos los datos?

La firma acredita que el certificado no ha cambiado desde que se firmó. Consulte también el resultado del informe para saber si se borraron todos los destinos. Véase Verificar un certificado de borrado.

¿Cómo ayuda O&O SafeErase a cumplir el RGPD?

O&O SafeErase permite borrar datos personales de forma irreversible y documentar el borrado mediante certificados firmados. Cada organización debe determinar qué medidas necesita. El programa no sustituye una evaluación de protección de datos.

¿Qué puedo hacer con la versión de prueba?

Puede borrar archivos, carpetas y rastros de uso, así como limpiar el espacio libre. El borrado de unidades y particiones y el Modo Fortaleza requieren una licencia. Consulte Instalación y activación.

¿Dónde está la versión de línea de comandos?

`OOSafeEraseCmd.exe` está en la carpeta de programa de O&O SafeErase si el componente fue instalado; vea Línea de comandos.

Novedades de la versión 22

O&O SafeErase 22 incorpora una nueva interfaz y documenta los borrados con certificados firmados. A continuación se detallan los cambios respecto a la versión 21.

Funciones nuevas

- **Nueva interfaz**. Panel de navegación a la izquierda, página de inicio con historial y recomendaciones, revisión de cada tarea antes del borrado y nueva vista de progreso. Incluye modos claro, oscuro y de alto contraste y admite lectores de pantalla. Consulte Interfaz de usuario.
- **Certificados de borrado firmados**. Cada informe puede incluir un certificado firmado, un sello de tiempo RFC 3161 opcional y una cadena de certificados. Configure los datos del operador en **Configuración > Informes**. Consulte Informes y certificados de borrado.
- **Borrar todo el equipo**. Se pueden guardar los registros en un recurso compartido de red y documentar el número de inventario, el destino del soporte y la necesidad de protección de los datos. Tras el borrado se muestra un código para el soporte técnico. Consulte Borrar todo el equipo.
- **Inicializar y formatear después**. Al terminar el borrado de un disco completo, O&O SafeErase puede crear y formatear una partición. Consulte Borrar unidades y particiones.
- **Más navegadores**. Además de Chrome, Edge y Firefox, se admiten Brave, Vivaldi, Opera y Opera GX, incluidos todos sus perfiles.
- **Cookies que se conservarán**. Puede indicar qué sitios deben conservar sus cookies durante la limpieza. Consulte Conservar las cookies de determinados sitios web.
- **Línea de comandos**. `OOSafeEraseCmd.exe` permite borrar desde scripts, utiliza la licencia del programa, genera certificados de borrado mediante el servicio y permite verificarlos. No admite los parámetros de la antigua herramienta `oosecmd.exe`. Consulte Línea de comandos.

Cambios

- **Nuevo método predeterminado:** NIST 800-88 Clear / BSI CON.6 sobrescribe los datos una vez con datos aleatorios. Los métodos DoD, el procedimiento anterior BSI y el método Gutmann están marcados como **(Legacy)**. Ver Métodos de borrado y unidades SSD.
- **Enlaces en carpetas**. Por defecto ya no se siguen los puntos de unión ni los enlaces simbólicos. Puede activar este comportamiento con **Seguir enlaces en carpetas**.
- **Integración con Windows**. Las opciones del menú contextual ahora se configuran en **Configuración > General**.
- **Habilitar el registro**. Esta opción controla ahora el registro del servicio de O&O SafeErase.
- **Modo Fortaleza** se encuentra ahora bajo **Borrar todo el equipo**.
- El instalador incluye el entorno de ejecución de .NET que necesita el programa.

Funciones retiradas

- Se ha eliminado la comprobación de seguridad, que buscaba en el PC datos recuperables. En su lugar, la página de inicio muestra el historial de limpieza.
- Las cookies de Adobe Flash Player e Internet Explorer ya no se limpian.
- La comprobación de actualización y la información de soporte se han movido de **Herramientas** a la información del programa.

Soporte técnico y otros recursos de O&O

Aquí encontrará los datos de contacto del soporte técnico de O&O y la información que conviene incluir para agilizar la respuesta a su consulta.

Contactar con el soporte técnico de O&O

Utilice el formulario de la página de soporte de O&O o escriba a support@oo-software.com. Puede utilizar la misma página para consultas sobre licencias y pedidos.

Incluya esta información:

- La versión y la edición del producto y la versión de Windows. Puede consultarlas en la información del programa, al pie del panel de navegación.
- La tarea y el tipo de destino, por ejemplo, un archivo, el espacio libre, una unidad o todo el equipo.
- El mensaje de error exacto y los pasos que conducen a él.
- El informe y el registro del borrado.
- Si el borrado se ejecutó en Windows o en el Modo Fortaleza.

Después de borrar todo el equipo, la página de resultados muestra en **Información para el soporte** un código con un breve resumen técnico. Si no dispone de una unidad para guardar los registros, envíe una foto del código.

> **Nota**
>
> Los informes pueden contener nombres de archivos y unidades y datos del operador. Revíselos antes de enviarlos. No publique claves de licencia ni contraseñas en capturas de pantalla o mensajes públicos.

Licencias y actualizaciones

O&O SafeErase es un software comercial. Puede probarlo durante el período de prueba; el uso continuo requiere una licencia válida. El borrado de unidades y particiones y el Modo Fortaleza no están disponibles en la versión de prueba.

Las actualizaciones de una misma versión principal, por ejemplo de 22.0 a 22.1, suelen ser gratuitas. El cambio de versión principal requiere otra clave de licencia. Consulte cómo introducir la clave y buscar actualizaciones en Instalación y activación.

Más de O&O

O&O Software desarrolla herramientas para Windows, entre ellas programas de copia de seguridad, optimización y privacidad. Consulte el catálogo de productos de O&O.