Compumax

GUÍA DE USUARIO · COMPUMAX SECURE ERASE 3.0

Borrado seguro de datos y restauración del equipo

Borre de forma permanente todos los datos del equipo y compruébelo con un certificado.

Contenido

1. Introducción 3

2. Características y alcance de la herramienta 4

2.1 Qué hace 4

2.2 Métodos de borrado 4

2.3 Discos probados 5

3. Dónde guarda sus datos el equipo 6

3.1 Configuración de la BIOS 6

3.2 Chip de seguridad (TPM) 7

4. Antes de empezar 7

5. Descargar la herramienta y crear la USB 7

6. Arrancar el equipo desde la USB 9

7. Borrar el disco 10

7.1 Elegir el disco 10

7.2 Elegir el método 10

7.3 Datos del reporte y hora (opcional) 11

7.4 Confirmar y esperar 12

7.5 Resultado y apagado 13

8. El certificado de sanitización 13

9. Restaurar el equipo 15

9.1 Restaurar Windows 15

9.2 Configurar Windows por primera vez 16

9.3 Restaurar Linux (Ubuntu) 16

10. Restablecer el equipo sin borrado seguro 18

10.1 Restablecer este equipo (Windows) 18

10.2 Recuperación Compumax 18

11. Solución de problemas 19

12. Glosario y soporte 20

1. Introducción

Antes de reciclar, vender, donar o devolver un equipo, hay que borrar los datos que guardó su usuario: archivos, cuentas, contraseñas y redes. Eliminar archivos o formatear el disco no basta, porque los datos se pueden recuperar con programas comunes.

Compumax Secure Erase (CSE) es una herramienta que se graba en una memoria USB y arranca el equipo sin usar Windows. Desde ahí le ordena al disco que borre todas sus celdas, comprueba que no quedaron datos y genera un **certificado en PDF** como constancia.

Esta guía explica todo el proceso, desde la descarga de la herramienta hasta la reinstalación del sistema operativo:

1. Revisar qué partes del equipo guardan datos y cómo se borra cada una (sección 3).
2. Descargar la herramienta y grabarla en una USB (sección 5).
3. Arrancar el equipo desde la USB y borrar el disco (secciones 6 y 7).
4. Guardar el certificado y comprobar que no fue alterado (sección 8).
5. Reinstalar Windows o Linux para volver a usar el equipo (sección 9).

> **Advertencia**
>
> El borrado es **permanente**. Después de él, los datos no se pueden recuperar por ningún medio, ni siquiera con ayuda de Compumax. Haga una copia de seguridad antes de empezar.

El certificado indica el **nivel de borrado** que se logró: **Purga**, el más alto, o **Limpieza**. La diferencia entre los dos se explica en el glosario (sección 12).

2. Características y alcance de la herramienta

2.1 Qué hace

Arranca con Secure Boot activo
No hay que cambiar la configuración de seguridad de la BIOS. La herramienta se basa en Debian 13 y usa su firma oficial.

No usa Windows ni el disco
Arranca desde la USB y funciona solo en la memoria del equipo. No necesita internet.

Borrado por el propio disco
Le ordena al disco que se borre con sus comandos de firmware (NVMe Sanitize, Format NVM, ATA Secure Erase). Tarda segundos.

Verifica el resultado
Después de borrar, revisa una muestra de 100 zonas repartidas en todo el disco (1000 en las sobrescrituras) y comprueba que no quedaron datos.

Certificado en PDF
Guarda en la USB un certificado con el equipo, el disco, el método, el nivel logrado, la verificación y el estado de salud del disco.

Registro a prueba de cambios
Junto al PDF guarda un registro (.log). Su huella SHA-256 va impresa en el certificado para comprobar que no se alteró.

Protege la USB y el sistema
La USB nunca aparece en la lista y no se puede borrar: ahí se guardan los certificados. Un disco en uso no se borra. Durante el borrado se ignoran Ctrl+C, la tapa y las teclas de suspensión.

Modo cerrado
Solo muestra la aplicación de borrado. Desde ella solo se puede borrar, reiniciar o apagar.

> **La herramienta borra el disco**
> La configuración de la BIOS y el chip TPM se borran aparte (sección 3). Después del borrado el equipo queda sin sistema operativo; la sección 9 explica cómo reinstalarlo.

2.2 Métodos de borrado

La herramienta ofrece cuatro métodos. Se recomienda el primero: es el más completo y tarda segundos. Los demás sirven cuando el disco no tiene borrado por firmware o cuando se prefiere sobrescribir el disco.

Método (nombre en pantalla)	Qué hace	Nivel	Duración
Borrado por firmware (recomendado)	El propio disco borra todas sus celdas, incluidas las de reserva (NVMe Sanitize o Format NVM con borrado criptográfico).	Purga [1]	Segundos
Borrado lógico por firmware	El disco borra los datos de usuario con un formateo seguro (Format NVM o ATA Secure Erase).	Limpieza	Segundos a 1 min

Método (nombre en pantalla)	Qué hace	Nivel	Duración
Sobrescritura de una pasada	Escribe ceros en todo el disco y comprueba 1000 zonas. Sirve aunque el disco no tenga borrado por firmware.	Limpieza	10 a 22 min [2]
Sobrescritura DoD 5220.22-M (3 pasadas)	Tres pasadas completas (ceros, unos y patrón aleatorio) y comparación de 1000 zonas con el patrón escrito.	Limpieza	46 min a 1 h 25 min [2]

[1] Si el disco es SATA, o no tiene Sanitize ni borrado criptográfico, el resultado es Limpieza. La herramienta lo avisa antes de empezar y el certificado lo indica.
[2] Medido en discos de 500 GB a 1 TB. La duración depende del tamaño y la velocidad del disco; la herramienta muestra un estimado antes de empezar y lo ajusta durante el borrado. En un SSD, las sobrescrituras no alcanzan las celdas de reserva del disco: por eso logran Limpieza y no Purga.

Temperatura del disco

Las sobrescrituras escriben el disco completo durante casi una hora o más y pueden calentar un SSD sin disipador. El estado de salud del disco antes y después queda en el certificado. El **Borrado por firmware** tarda segundos y no tiene este efecto.

2.3 Discos probados

Estos discos se probaron con la herramienta y el método **Borrado por firmware**, en un equipo con Secure Boot activo. En cada prueba se verificó el borrado y se comprobó la huella del certificado.

Disco	Tipo	Comando que aplica la herramienta	Nivel	Duración medida
ADATA LEGEND 700 512 GB	NVMe	Sanitize Block Erase	Purga	5 s
ADATA LEGEND 850 512 GB	NVMe	Sanitize Block Erase	Purga	3-4 s
ADATA LEGEND 900 512 GB	NVMe	Sanitize Block Erase	Purga	2-3 s
Crucial T500 500 GB	NVMe	Format NVM con borrado criptográfico	Purga	1 s
Hikvision Desire P 1 TB	NVMe	Sanitize Block Erase	Purga	6 s
MX NVMe SSD 512 GB	NVMe	Sanitize Block Erase	Purga	5 s
Netac NV2000 512 GB	NVMe	Sanitize Block Erase	Purga	5 s
Patriot P300 512 GB	NVMe	Sanitize Block Erase	Purga	9-10 s
WD Blue SN580 1 TB	NVMe	Sanitize Block Erase	Purga	8 s
WD Green SN350 500 GB	NVMe	Sanitize Block Erase	Purga	17 s
WD Green SN3000 500 GB	NVMe	Sanitize Block Erase	Purga	6 s

¿Y si mi disco no está en la lista?

Igual puede usar la herramienta. Funciona con cualquier disco SSD NVMe o SATA: detecta los comandos de borrado que el disco tiene, aplica el mejor y el certificado dice el nivel que se logró (Purga o Limpieza).

Discos mecánicos (HDD)

La herramienta no se ha probado en discos mecánicos (HDD), por lo que no se garantiza el resultado en ellos. Los equipos Compumax usan discos SSD.

3. Dónde guarda sus datos el equipo

Sus datos no son solo los archivos: también son la configuración, las redes, las contraseñas y las cuentas. Esta tabla muestra todas las partes del equipo que pueden guardarlos y cómo se borra cada una.

Parte del equipo	Qué datos guarda	Cómo se borra
Disco SSD	Archivos, sistema operativo, cuentas, redes Wi-Fi, contraseñas guardadas y las huellas registradas en el lector de huella	Compumax Secure Erase, método **Borrado por firmware** (secciones 5 a 7). El certificado indica el nivel logrado.
Configuración de la BIOS	De fábrica no guarda datos suyos. Solo los guarda si usted puso una contraseña, cambió el orden de arranque o agregó claves de Secure Boot.	Solo en ese caso: restablecerla desde la BIOS (sección 3.1)
Chip de seguridad (TPM)	Las llaves con las que Windows protege sus datos: el cifrado del disco (BitLocker) y el inicio de sesión con PIN, huella o rostro (Windows Hello)	Borrar el TPM desde Windows antes de borrar el disco, o desde la BIOS (sección 3.2)

La memoria RAM no guarda datos

La memoria RAM se borra sola al apagar el equipo, por eso no aparece en la tabla.

Si va a vender, donar, devolver o reciclar el equipo, haga los pasos de las secciones 3.1 y 3.2 **antes** de borrar el disco. No hacen falta para usar la herramienta de borrado.

3.1 Configuración de la BIOS

Solo hace falta si usted puso una contraseña en la BIOS o cambió su configuración. Los nombres y la ubicación de los menús cambian según el modelo; busque opciones parecidas a las que se indican.

1. Encienda el equipo y presione varias veces la tecla de entrada a la BIOS: **Supr**, **F2** o **Esc**.
2. **Contraseñas:** en el menú de seguridad (Security), quite la contraseña de administrador (Administrator o Supervisor Password) y la de arranque (User o Power-On Password). Normalmente se quitan dejando la contraseña nueva en blanco.
3. **Secure Boot:** en el menú de arranque seguro (Secure Boot), elija la opción que restaura las claves de fábrica (Restore Factory Keys o Install Default Secure Boot Keys). No desactive Secure Boot.
4. **Valores de fábrica:** en el menú de salida (Save & Exit o Exit), elija cargar los valores predeterminados (Load Setup Defaults o Load Optimized Defaults).
5. Guarde los cambios y salga (normalmente con **F10**).

3.2 Chip de seguridad (TPM)

Según el modelo, el TPM viene integrado en el procesador o es un chip de la placa base. En todos los casos se borra de la misma forma y el chip no se daña: queda como salió de fábrica.

Bórrelo **antes de borrar el disco**, mientras Windows todavía arranca:

1. Abra **Seguridad de Windows** y entre a **Seguridad del dispositivo**.
2. Abra los detalles del **procesador de seguridad** y elija **Solución de problemas del procesador de seguridad**.
3. Elija **Borrar TPM** y confirme. El equipo se reinicia; si en el reinicio pide presionar una tecla para confirmar, hágalo.

Si Windows ya no arranca, el TPM se borra desde la BIOS: en el menú de seguridad, busque una opción como Clear TPM, TPM Clear, Reset PTT o fTPM NV Clear.

> **Antes de borrar el TPM**
>
> Si el disco tiene BitLocker, después de borrar el TPM Windows pedirá la clave de recuperación. Si de todas formas va a borrar el disco, no la necesitará.

4. Antes de empezar

Tenga a mano:

- El equipo Compumax que va a borrar, **conectado al cargador**.
- Una memoria USB de **8 GB o más**. Todo lo que tenga se borrará al grabar la herramienta.
- Otro computador con Windows para descargar y grabar la herramienta.

Y revise que:

- Hizo una **copia de seguridad** de los datos que quiera conservar. El borrado no tiene vuelta atrás.
- Si va a entregar el equipo a otra persona, ya borró la BIOS y el TPM (sección 3).
- Si el disco tiene BitLocker, no hace falta desactivarlo: el borrado elimina también los datos cifrados.
- Si el equipo tiene Windows, anotó su **edición** (Home o Pro), que aparece en **Configuración** → **Sistema** → **Información**. La necesitará para reinstalarlo (sección 9.1).

> **No hace falta desactivar Secure Boot**
>
> Compumax Secure Erase arranca con Secure Boot activo. No cambie esa opción en la BIOS.

5. Descargar la herramienta y crear la USB

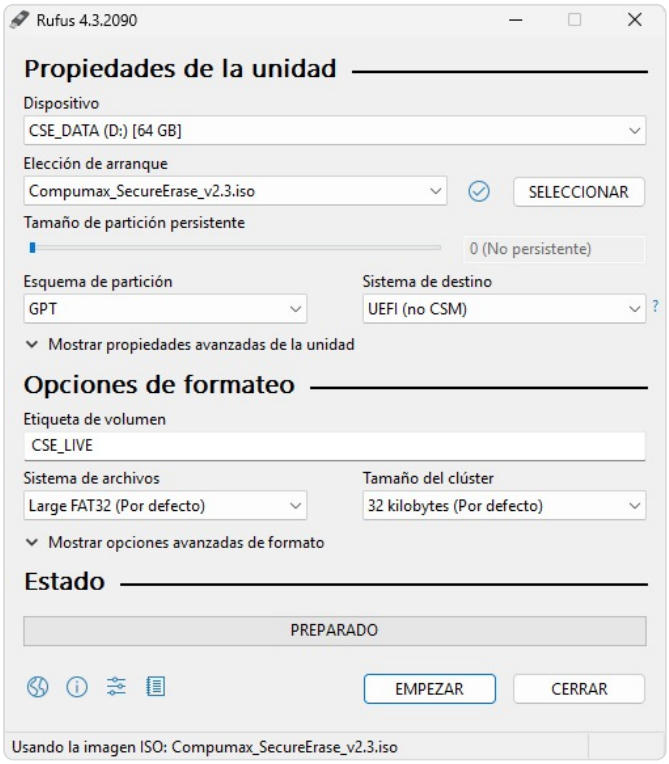
Para grabar la herramienta en la USB se usa **Rufus**, un programa de terceros que no necesita instalación.

1. En el otro computador, entre a **www.compumax.com.co/soporte**, abra **Restauración y Borrado Seguro** y descargue **Compumax_SecureErase_v3.0.zip**. Haga clic derecho sobre el archivo y elija **Extraer todo**. Queda el archivo **Compumax_SecureErase_v3.0.iso**.
2. Descargue Rufus desde su página oficial, **rufus.ie**.

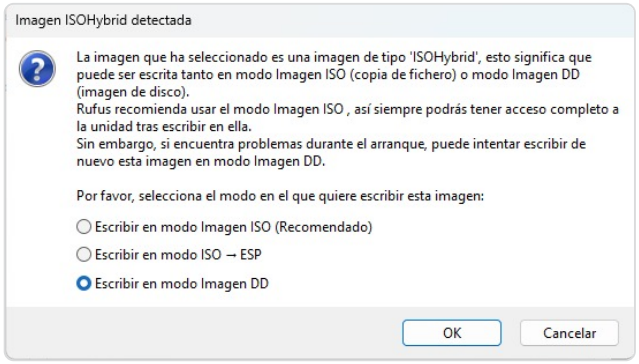
3. Conecte la USB y abra Rufus. Si Windows pregunta si permite cambios en el equipo, acepte.
4. En **Dispositivo**, elija la USB. En **Elección de arranque**, presione **Seleccionar** y elija el archivo .iso. Deje las demás opciones como están y presione **Empezar**.
5. Rufus pregunta en qué modo escribir la imagen. Elija **Escribir en modo Imagen DD** y acepte.
6. Cuando termine, cierre Rufus. Desconecte la USB y vuelva a conectarla.
7. En el Explorador de archivos debe aparecer una unidad llamada **CSE_DATA** de unos 512 MB. Ahí quedarán los certificados.

Use el modo Imagen DD

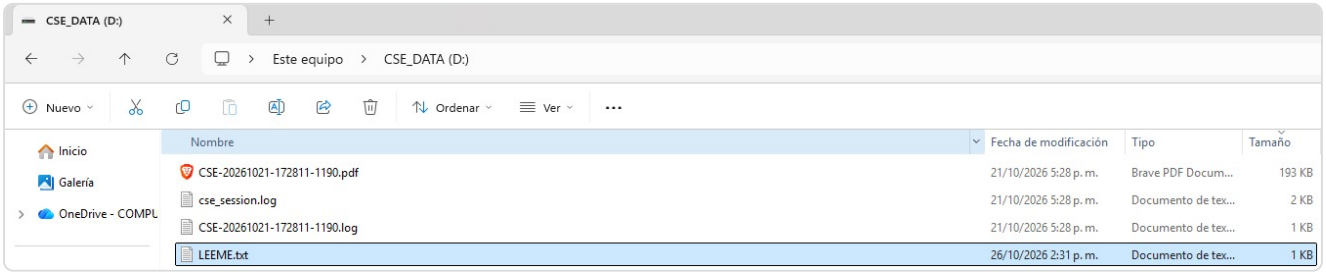
Si la USB se graba en modo ISO, la herramienta arranca pero **no puede guardar el certificado**: al final del borrado avisa que el PDF quedó en memoria y se pierde al apagar. Si pasa, vuelva a grabar la USB en modo DD.



Rufus listo para grabar: la USB en Dispositivo y el archivo .iso elegido



Pregunta del modo de escritura: elija Escribir en modo Imagen DD



La unidad CSE_DATA en el Explorador de archivos: cada borrado deja su certificado (.pdf) y su registro (.log)

Una misma USB sirve para borrar muchos equipos. Los certificados se acumulan en **CSE_DATA**.

6. Arrancar el equipo desde la USB

1. Apague el equipo que va a borrar y conecte la USB.
2. Encienda el equipo y presione varias veces la **tecla del menú de arranque** hasta que aparezca la lista de dispositivos. En los equipos Compumax es una de las teclas entre **F7** y **F12**. Si no sabe cuál, pruébelas una por una al encender el equipo.
3. Elija la USB (suele aparecer con UEFI y la marca de la memoria) y presione Enter.
4. Espere unos segundos a que cargue la herramienta. Cuando aparezca la pantalla de bienvenida, presione cualquier tecla.



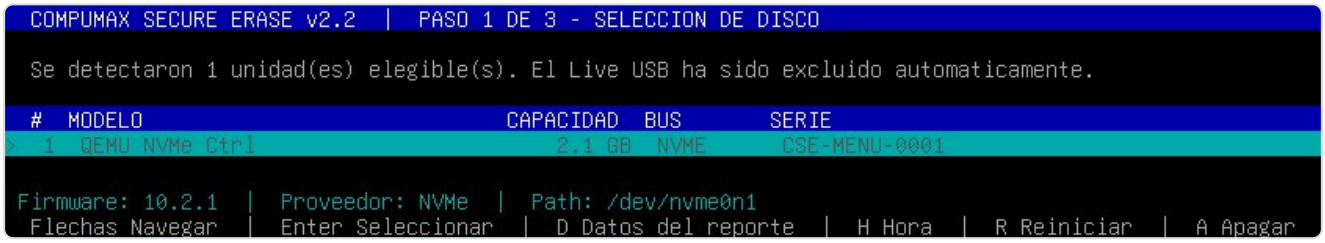
Pantalla de bienvenida de Compumax Secure Erase

La herramienta se maneja solo con el teclado. En la parte de abajo de cada pantalla aparecen las teclas disponibles. El ratón y el panel táctil no se usan.

7. Borrar el disco

El borrado tiene tres pasos en pantalla: elegir el disco, elegir el método y confirmar.

7.1 Elegir el disco

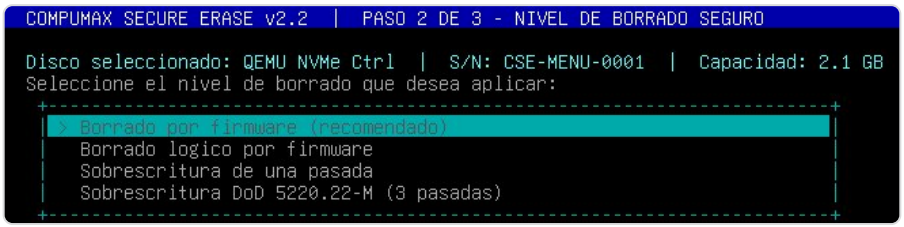


Paso 1 de 3: lista de discos y teclas disponibles

1. Revise la lista. Aparecen el modelo, la capacidad, el tipo (NVMe o SATA) y el número de serie de cada disco. La USB nunca aparece: la herramienta la excluye.
2. Con las flechas, elija el disco que va a borrar y presione **Enter**.

Teclas de esta pantalla: **D** datos del reporte, **H** hora, **R** reiniciar y **A** apagar. Las teclas D y H son opcionales y se explican en la sección 7.3.

7.2 Elegir el método

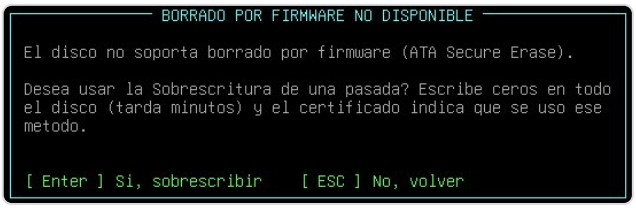


Paso 2 de 3: métodos de borrado

1. Deje marcado **Borrado por firmware (recomendado)** y presione **Enter**. Debajo de la lista, la herramienta explica qué hace cada método.
2. Si quiere otro método, elíjalo con las flechas (ver la tabla de la sección 2.2). Con **B** vuelve a la lista de discos.

Si el disco no tiene borrado por firmware

La herramienta lo avisa y ofrece la **Sobrescritura de una pasada**. Presione **Enter** para usarla o **ESC** para volver.



Aviso cuando el disco no tiene borrado por firmware

Si el disco es SATA

El borrado por firmware de un SATA logra Limpieza, no Purga. La herramienta lo avisa antes de empezar y el certificado dice Borrado lógico por firmware y Limpieza.

Algunos discos SATA vienen bloqueados (frozen). En ese caso la herramienta suspende el equipo 3 segundos y lo despierta sola para desbloquear el disco.

7.3 Datos del reporte y hora (opcional)

Si no va a usar estas opciones, pase a la sección 7.4. Sin ellas, el certificado sale de 2 páginas con los datos del equipo, del disco y del borrado.

Tecla D: datos del reporte

Sirve para entregar el certificado a un cliente o a otra área. En la lista de discos, presione **D** y llene los datos:

- **Cliente:** entidad, ciudad, nombre, documento, cargo y contacto.
- **Técnico:** nombre, documento, cargo y contacto.
- **Disco:** fabricante, si la herramienta no lo detecta.



Datos del reporte (tecla D)

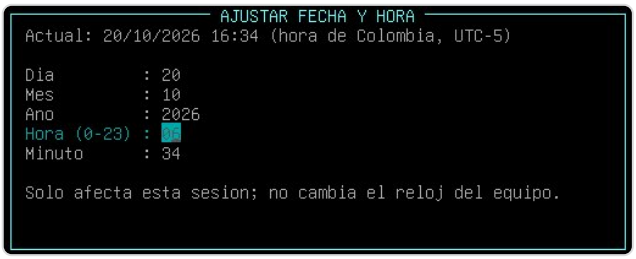
Muévase con las flechas o Tab y guarde con **Enter**. Los campos vacíos no salen en el certificado.

Con estos datos, el certificado sale de **3 páginas**: la tercera es una constancia de conformidad con espacio para las firmas del cliente y del técnico.

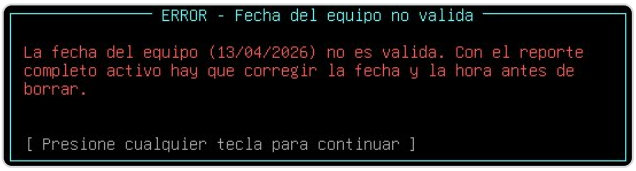
Tecla H: fecha y hora

La fecha y la hora del certificado salen del reloj del equipo (hora de Colombia, UTC-5). Si están mal, presione **H** en la lista de discos y corríjalas. El cambio solo vale para esta sesión: no modifica el reloj de la BIOS.

Si activó el reporte completo (tecla D) y el reloj del equipo está atrasado, la herramienta **no deja borrar hasta corregir la hora**. Pasa en equipos con la pila del reloj agotada o con la placa cambiada.



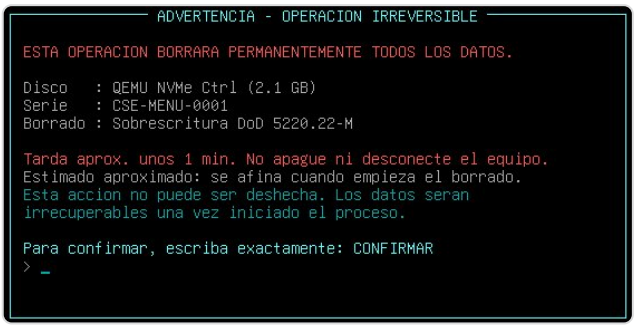
Ajuste de fecha y hora (tecla H)



Aviso cuando la fecha no es válida con el reporte completo

7.4 Confirmar y esperar

1. Revise el disco, el número de serie y el método que muestra la advertencia.
2. Escriba **CONFIRMAR** en mayúsculas y presione **Enter**. Con **ESC** cancela y no se borra nada.
3. Espere. En pantalla se ven el avance, el tiempo transcurrido y el registro de eventos. **No apague ni desconecte el equipo.**



Paso 3 de 3: confirmación final



Borrado en progreso: avance, eventos y generación del certificado

Durante el borrado

- Una vez que empieza, el borrado no se puede cancelar.
- No apague el equipo, no cierre la tapa y no desconecte la USB ni el cargador.
- El borrado por firmware tarda segundos; las sobrescrituras, de minutos a más de una hora.
- Si el equipo se apaga a mitad, el disco no queda certificado: arranque de nuevo y repita el borrado.

7.5 Resultado y apagado



Resultado del borrado y opciones para terminar

1. Revise el resultado: **BORRADO SEGURO COMPLETADO EXITOSAMENTE**, el método, las zonas verificadas, el estado de salud (SMART) y el nombre del certificado.
2. Elija **[A] Apagar el equipo** y presione Enter. Así el certificado queda guardado en la USB.
3. Con el equipo apagado, retire la USB. Para borrar otro disco, elija **[R] Reiniciar el equipo** en vez de apagar.

> **Si el borrado falla**
>
> La pantalla y el certificado dicen **BORRADO FALLIDO** y la causa. Repita el borrado; si vuelve a fallar, contacte a soporte con el PDF y el archivo .log (sección 12).

8. El certificado de sanitización

Conecte la USB a un computador con Windows y abra la unidad **CSE_DATA**. Por cada borrado hay dos archivos con el mismo nombre (el folio):

- **CSE-AAAAMMDD-HHMMSS-XXXX.pdf**: el certificado.
- **CSE-AAAAMMDD-HHMMSS-XXXX.log**: el registro técnico del borrado.

Copie los dos archivos a un lugar seguro.

Qué dice el certificado

- **Resultado:** Borrado verificado o Borrado fallido, con el tipo de borrado y el **nivel de sanitización** (Purga o Limpieza).
- **Equipo:** fabricante, modelo, placa, BIOS y procesador.
- **Disco:** fabricante, modelo, número de serie, capacidad, tipo de medio y firmware.
- **Método:** descripción, inicio, fin y duración (hora de Colombia, UTC-5).
- **Verificación:** zonas revisadas y resultado, y si el disco confirmó el borrado.
- **Anexo técnico:** comando ejecutado, estado de salud del disco (SMART) antes y después, y la huella SHA-256 del registro.
- **Constancia de conformidad** con firmas, solo si se llenaron los datos del reporte (tecla D).


Compumax

FOLIO
CSE-20261006-114250-CNWL
Emitido el 6 de octubre de 2026

Certificado de Sanitización de Datos
Compumax Secure Erase v2.2

BORRADO VERIFICADO
Se comprobó que no quedan datos en las zonas revisadas del disco.

TIPO DE BORRADO
Borrado por firmware
Nivel de sanitización: Purga

EQUIPO

Fabricante	Compumax Computer
Modelo	Onix Series CX10
Placa base	NC14N
BIOS versión	ADLN202P_V10.135.02
BIOS fecha	03/10/2025
Procesador	Intel(R) N200
Número de serie	No disponible
UUID	No disponible

UNIDAD DE ALMACENAMIENTO

Fabricante	ADATA
Modelo	ADATA LEGEND 850
Número de serie	2O422LA7CNWL
Capacidad	512.1 GB
Tipo de medio	Flash (SSD) · NVMe PCIe
Firmware	W0802A0

CONFIRMACIÓN DEL DISCO

El disco confirmó el borrado completo	Sí

MÉTODO

Descripción	Borrado por bloques ejecutado por el firmware del disco
Tipo de borrado	Borrado por firmware
Inicio	2026-10-06 11:42:50 (UTC-5)
Fin	2026-10-06 11:42:53 (UTC-5)
Duración	00:00:03

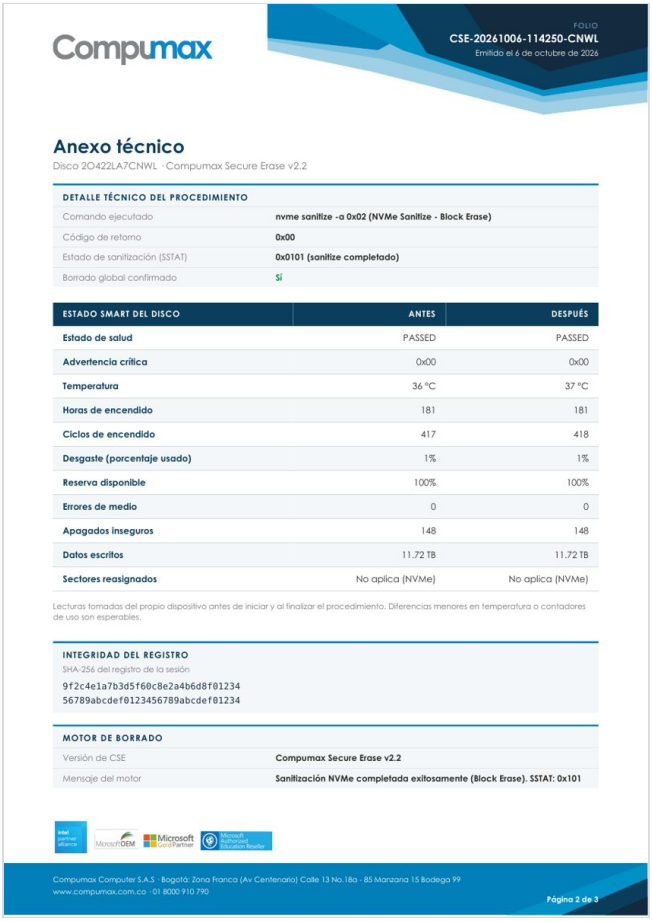
VERIFICACIÓN

Comprobación posterior	Lectura de 100 zonas del disco (inicio, final y distribuidas)
Zonas revisadas	100 / 100
Resultado	Sin datos en las zonas revisadas

Certificado generado automáticamente por Compumax Secure Erase. El borrado fue confirmado por el firmware de la unidad y verificado por muestreo de sectores.

Compumax Computer S.A.S · Bogotá: Zona Franca (Av Centenario) Calle 13 No.18a - 85 Manzana 15 Bodega 99
www.compumax.com.co · 01 8000 910 790
Página 1 de 3

Página 1: resultado, equipo, disco, método y verificación


Compumax

FOLIO
CSE-20261006-114250-CNWL
Emitido el 6 de octubre de 2026

Anexo técnico
Disco 2O422LA7CNWL · Compumax Secure Erase v2.2

DETALLE TÉCNICO DEL PROCEDIMIENTO

Comando ejecutado	nvme sanitize -a 0x02 (NVMe Sanitize - Block Erase)
Código de retorno	0x00
Estado de sanitización (SSTAT)	0x0101 (sanitize completado)
Borrado global confirmado	Sí

ESTADO SMART DEL DISCO	ANTES	DESPUÉS
Estado de salud	PASSED	PASSED
Advertencia crítica	0x00	0x00
Temperatura	36 °C	37 °C
Horas de encendido	181	181
Ciclos de encendido	417	418
Desgaste (porcentaje usado)	1%	1%
Reserva disponible	100%	100%
Errores de medio	0	0
Apagados inseguros	148	148
Datos escritos	11.72 TB	11.72 TB
Sectores reasignados	No aplica (NVMe)	No aplica (NVMe)

Lecturas tomadas del propio dispositivo antes de iniciar y al finalizar el procedimiento. Diferencias menores en temperatura o contadores de uso son esperables.

INTEGRIDAD DEL REGISTRO
SHA-256 del registro de la sesión
9f2c4e1a7b3d5f60c8e2a4b6d8f01234
56789abcdef0123456789abcdef01234

MOTOR DE BORRADO

Versión de CSE	Compumax Secure Erase v2.2
Mensaje del motor	Sanitización NVMe completada exitosamente (Block Erase). SSTAT: 0x101

Compumax Computer S.A.S · Bogotá: Zona Franca (Av Centenario) Calle 13 No.18a - 85 Manzana 15 Bodega 99
www.compumax.com.co · 01 8000 910 790
Página 2 de 3

Página 2: anexo técnico, estado del disco y huella SHA-256 del registro

Certificado de muestra con datos de prueba. Con el reporte completo se agrega una tercera página con la constancia de conformidad y las firmas.

Comprobar que el certificado no se alteró

1. Abra el PDF y busque, en el anexo técnico, **Integridad del registro**. Ahí está la huella SHA-256 del archivo .log.
2. Abra PowerShell en la carpeta donde copió los archivos y escriba (con el nombre de su folio):

```
Get-FileHash .\CSE-20261006-114250-CNWL.log -Algorithm SHA256
```

3. Compare la huella que muestra PowerShell con la impresa en el PDF. Si son iguales, el registro no se modificó desde el borrado.

9. Restaurar el equipo

El borrado no daña ninguna pieza: el disco queda vacío y el equipo vuelve a funcionar como nuevo al instalar el sistema operativo.

El borrado también elimina las herramientas de recuperación que venían en el disco (sección 10), así que el sistema se instala desde una USB nueva. Siga la sección del sistema que va a instalar:

- **Windows:** secciones 9.1 y 9.2.
- **Linux (Ubuntu):** sección 9.3.

Necesita una USB de **8 GB o más** y el otro computador con internet. Puede usar la misma USB de la herramienta, pero **antes copie a otro lugar** el certificado PDF y el archivo .log de **CSE_DATA**: al grabar la USB de instalación se borra todo lo que tiene.

> **¿Dónde está el número de serie?**
> En la etiqueta del equipo. También aparece en el certificado del borrado, en los datos del equipo.

9.1 Restaurar Windows

1. En el otro computador, entre a **https://www.microsoft.com/es-es/software-download/windows11**. En **Crear medios de instalación de Windows 11**, presione **Descargar ahora** y abra el archivo descargado. Acepte los términos, deje el idioma y la edición recomendados y elija **Unidad flash USB**. La herramienta descarga Windows y graba la USB.
2. Conecte la USB al equipo borrado, enciéndalo y elíjala en el menú de arranque (tecla entre F7 y F12, sección 6).
3. Siga el instalador. Si pide una clave de producto, elija **No tengo clave de producto**.
4. Si pregunta qué edición instalar, elija **la de su licencia** (Home o Pro). Con otra edición, Windows no se activa.
5. Cuando pregunte dónde instalar, elija el disco del equipo (aparece como espacio sin asignar) y presione **Siguiente**. El equipo se reinicia varias veces; no retire la USB hasta que aparezcan las pantallas de configuración (sección 9.2).

> **La licencia se activa sola**
> Si el equipo se compró con licencia de Windows, la licencia está guardada en la BIOS, no en el disco: el borrado no la elimina. Windows se activa solo al conectarse a internet, siempre que sea la misma edición. En un equipo sin licencia de Windows, la activación queda a cargo del usuario.

Instalar los drivers

1. Con Windows ya instalado y conectado a internet, entre a **https://www.compumax.com.co/soporte**, escriba el **número de serie** del equipo y presione **Buscar Drivers**.
2. Descargue e instale los drivers de la lista y reinicie el equipo. Si para su modelo también hay manual o actualización de BIOS, aparecen ahí mismo.

9.2 Configurar Windows por primera vez

Al terminar la instalación, Windows hace unas preguntas antes de mostrar el escritorio. Las pantallas cambian un poco según la versión de Windows.

> **Si va a entregar el equipo a otra persona**
>
> No haga estos pasos. Deténgase en la primera pantalla (país o región) y apague el equipo: así la persona que lo reciba los hace con sus propios datos. Para apagarlo, presione **Shift + F10** (en algunos portátiles, **Fn + Shift + F10**), escriba este comando en la ventana que se abre y presione Enter:
>
> ```
> shutdown /s /t 0
> ```

Si el equipo es para usted, siga estos pasos:

1. Elija el país o región (**Colombia**) y presione **Sí**.
2. Elija la distribución de teclado **Latinoamericano**. Cuando ofrezca agregar una segunda distribución, elija **Omitir**.
3. Conéctese a internet (Wi-Fi o cable) o siga sin internet. Con internet, Windows descarga actualizaciones y la configuración tarda bastante más; la conexión se puede hacer después, desde el escritorio. Para seguir sin internet, vea el recuadro **Configurar Windows sin internet**, más abajo.
4. Escriba un nombre para el equipo, si lo pide. Con internet, inicie sesión con una cuenta de Microsoft; sin internet, escriba el nombre del usuario.
5. Cree una contraseña o un PIN para entrar al equipo. No lo deje sin contraseña.
6. Revise las opciones de privacidad, elija las que prefiera y presione **Aceptar**. Al final aparece el escritorio.

> **Configurar Windows sin internet**
>
> Si la pantalla de conexión no deja continuar sin internet:
>
> 1. En esa pantalla, presione **Shift + F10** (en algunos portátiles, **Fn + Shift + F10**). Se abre una ventana negra.
> 2. Escriba este comando y presione Enter:
>
>    ```
>    oobe\bypassnro
>    ```
>
> 3. El equipo se reinicia y vuelve a la primera pantalla. Repita el país y el teclado.
> 4. En la pantalla de conexión, elija **No tengo internet** y después **Continuar con la configuración limitada**. Siga con el paso 4.
>
> Si Windows responde que no reconoce el comando, su versión ya no lo permite: conéctese a internet para continuar.

9.3 Restaurar Linux (Ubuntu)

Linux se restaura con **Ubuntu 26.04 LTS**, que se descarga gratis. Instalado con internet, Ubuntu descarga solo los controladores que el equipo necesita.

1. En el otro computador, entre a **https://ubuntu.com/download/desktop** y descargue **Ubuntu 26.04 LTS** (la versión para Intel o AMD de 64 bits).

2. Grabe la imagen en la USB con **Rufus** (sección 5): elija la USB y el archivo .iso de Ubuntu y presione **Empezar**. Si Rufus pregunta el modo, deje el **modo Imagen ISO (recomendado)**.
3. Conecte la USB al equipo borrado, enciéndalo y elíjala en el menú de arranque (tecla entre F7 y F12, sección 6). En el menú de Ubuntu, presione Enter en la primera opción para iniciar el instalador.
4. **Conecte el equipo a internet** por cable o Wi-Fi cuando el instalador lo pida. Este paso es el que trae los controladores: no lo omita.
5. Si el instalador ofrece **instalar software de terceros** para gráficos y Wi-Fi, márquelo.
6. En el tipo de instalación, elija la opción que **borra el disco e instala Ubuntu**. El disco ya está vacío.
7. Elija la zona horaria (**Bogotá**), cree el usuario con su contraseña y espere a que termine. Al final, reinicie y retire la USB cuando lo pida.

Si algo no funciona después de instalar

Casi siempre es porque se instaló sin internet. Conecte el equipo por cable, abra **Software y actualizaciones → Controladores adicionales**, instale los que aparezcan y reinicie. Si sigue igual, contacte a soporte (sección 12).

10. Restablecer el equipo sin borrado seguro

Este capítulo es para quien se queda con el equipo y solo quiere reinstalar Windows, por ejemplo porque está lento o tiene un problema de software.

No sirve para vender, donar, devolver o reciclar el equipo

- Estos métodos reinstalan Windows, pero **no son un borrado seguro**: no garantizan que los datos anteriores queden irrecuperables y no generan certificado. Para entregar el equipo, use Compumax Secure Erase (secciones 5 a 8).
- Funcionan con las herramientas de recuperación guardadas en el disco. Después de usar Compumax Secure Erase ya no existen: en ese caso, restaure el equipo con la sección 9.
- Solo aplican a equipos con Windows.

Antes de empezar, haga una copia de seguridad de sus archivos y conecte el equipo al cargador.

10.1 Restablecer este equipo (Windows)

Se usa cuando Windows todavía arranca. Tarda unos 30 minutos.

1. Abra **Configuración** → **Sistema** → **Recuperación**.
2. En **Restablecer este equipo**, presione **Restablecer PC**.
3. Elija **Quitar todo** y, después, **Reinstalación local** (o **Descarga de la nube** si prefiere que Windows se descargue de internet).
4. Revise el resumen y presione **Restablecer**. El equipo se reinicia varias veces.
5. Cuando aparezcan las pantallas de configuración, siga la sección 9.2.

10.2 Recuperación Compumax

Casi todos los equipos Compumax con Windows traen una herramienta de recuperación propia que deja el equipo como salió de fábrica. Sirve incluso cuando Windows no arranca. Si su equipo no la trae, la opción no aparece en el paso 2: use la sección 10.1 o restaure el equipo con la sección 9.1.

1. Abra el menú de recuperación de Windows:
   - Si Windows arranca: **Configuración** → **Sistema** → **Recuperación** → **Inicio avanzado** → **Reiniciar ahora**.
   - Si Windows no arranca: después de dos arranques fallidos, el equipo muestra la pantalla de **Reparación automática**. Presione **Opciones avanzadas**.
2. Elija **Solucionar problemas** y, después, **Compumax Computer**.
3. En la herramienta de Compumax, presione el icono de la **hoja**, arriba a la izquierda, y confirme con **Yes**. Desde aquí ya no se pueden salvar los archivos.
4. Acepte los términos de garantía y espere. Tarda unos 15 minutos; no apague el equipo.
5. Al terminar, presione **OK** y luego **Continuar**. Cuando aparezcan las pantallas de configuración, siga la sección 9.2.

11. Solución de problemas

Lo que ve	Qué significa	Qué hacer
El equipo no arranca desde la USB y entra a Windows	No se eligió la USB en el menú de arranque	Reinicie y presione la tecla del menú de arranque varias veces desde que enciende (sección 6). Si la USB no aparece, vuelva a grabarla (sección 5).
La USB no aparece en la lista de discos de la herramienta	Es lo normal	La herramienta oculta la USB desde la que arrancó para que nunca se borre por error.
Al final dice PDF NO PERSISTENTE: quedó en RAM	La USB se grabó en modo ISO, no en modo DD, y el certificado no se pudo guardar	Vuelva a grabar la USB con Rufus en **modo Imagen DD** (sección 5, paso 5) y repita el borrado.
Aparece Borrado por firmware no disponible	El disco no tiene borrado por firmware	Presione Enter para usar la Sobrescritura de una pasada (nivel Limpieza), o ESC para volver.
Antes de borrar, el equipo se suspende unos segundos y vuelve solo	El disco SATA estaba bloqueado (frozen) y la herramienta lo desbloquea	No toque el equipo. Es parte del proceso.
Aparece Fecha del equipo no válida	Activó el reporte completo y el reloj del equipo está atrasado (pila agotada o placa cambiada)	Presione H y escriba la fecha y la hora correctas (sección 7.3).
El disco no aparece en la lista o dice en uso	El disco está dañado, no se detecta, o está en uso por el sistema	Apague el equipo, revise la conexión del disco y vuelva a arrancar. Si sigue igual, contacte a soporte.
El certificado dice BORRADO FALLIDO	El disco rechazó el borrado o la verificación encontró datos	Repita el borrado. El certificado indica la causa; si se repite, contacte a soporte con el PDF y el archivo .log.
El certificado dice Limpieza en vez de Purga	El disco no tiene un borrado por firmware de nivel Purga (por ejemplo, los discos SATA)	Es el resultado correcto para ese disco: los datos quedaron borrados. Revise la lista de discos probados (sección 2.3).
Después de una sobrescritura larga, el certificado muestra un aviso de temperatura	Las sobrescrituras escriben el disco completo y lo calientan	Deje enfriar el equipo. Prefiera el Borrado por firmware, que tarda segundos.
Después de reinstalar, Windows dice que no está activado	Se instaló una edición distinta a la de la licencia, o todavía no se conectó a internet	Conéctese a internet y espere unos minutos. Si sigue igual, reinstale Windows con la edición de su licencia (sección 9.1).
En el menú de recuperación no aparece Compumax Computer	El equipo no trae la Recuperación Compumax, o el disco ya se borró con la herramienta	Use Restablecer este equipo (sección 10.1) o reinstale Windows desde una USB (sección 9.1).

12. Glosario y soporte

Glosario

Término	Significado
Limpieza	Borrado que impide recuperar los datos con programas de recuperación comunes.
Purga	Borrado que impide recuperar los datos incluso con equipos de laboratorio especializados, sin dañar el disco. Es el nivel más alto que se logra sin destruir el disco.
Borrado por firmware	Orden que ejecuta el propio disco (su controladora), no el computador. Alcanza zonas que el sistema operativo no ve, como las celdas de reserva.
ISO	Archivo con la imagen completa de la herramienta, listo para grabar en una USB.
Secure Boot	Protección de la BIOS que solo deja arrancar software firmado. Compumax Secure Erase arranca con Secure Boot activo.
SHA-256	Huella digital de un archivo. Si el archivo cambia en un solo carácter, la huella cambia.

Soporte

Compumax Computer S.A.S · Línea nacional **01 8000 910 790** · Teléfono **601 580 6600** · Correo **contactanos@compumax.com** · Lunes a viernes, de 8:00 a. m. a 5:00 p. m.
Más canales de contacto en **www.compumax.com.co/contactenos**.

Al contactar a soporte por un borrado, tenga a mano el certificado PDF y el archivo .log.

Marcas

© Compumax Computer S.A.S. Todos los derechos reservados. Windows es una marca registrada de Microsoft Corporation. Ubuntu es una marca registrada de Canonical Ltd. Las demás marcas y nombres de productos mencionados pertenecen a sus respectivos dueños.