

Guía de Seguridad de las TIC

CCN-STIC 1504

Procedimiento de empleo seguro

Blancco Drive Eraser v6.9



Abрил 2021



Edita:



© Centro Criptológico Nacional, 2021
NIPO: 083-21-096-7

Fecha de Edición: Abril de 2021

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN	3
2. OBJETO Y ALCANCE	3
3. ORGANIZACIÓN DEL DOCUMENTO	4
4. FASE DE DESPLIEGUE E INSTALACIÓN	5
4.1 ENTREGA SEGURA DEL PRODUCTO	5
4.2 ENTORNO DE INSTALACIÓN SEGURO	5
4.3 REGISTRO Y LICENCIAS	8
4.4 INSTALACIÓN DE LA HERRAMIENTA	8
5. FASE DE CONFIGURACIÓN	11
5.1 ADMINISTRACIÓN DEL PRODUCTO	11
5.1.1 MENU PRINCIPAL.....	11
5.1.2 CONFIGURACIÓN DE ADMINISTRADORES	12
5.2 CONFIGURACIÓN DE LAS COMUNICACIONES.....	12
5.3 CONFIGURACIÓN DE PARÁMETROS DE SEGURIDAD	14
5.4 SINCRONIZACIÓN HORARIA	15
5.5 ACTUALIZACIONES	15
5.6 AUDITORÍA	15
5.6.1 REGISTRO DE EVENTOS: INFORMES.....	15
5.6.2 ALMACENAMIENTO REMOTO	17
5.6.3 NOTIFICACIONES	18
5.7 BACKUP	19
5.8 ESTÁNDARES DE BORRADO.....	19
6. FASE DE EJECUCIÓN	20
6.1 ENVÍO O ALMACENAMIENTO DEL INFORME	22
7. FASE DE OPERACIÓN	24
8. CHECKLIST.....	25
9. REFERENCIAS	27

1. INTRODUCCIÓN

1. *Blancco Drive Eraser* es un producto de *software* que proporciona servicios de borrado seguro de datos de discos duros completos o de particiones (denominadas unidades), basándose en estándares. Puede realizar el borrado seguro de discos duros HDD y estado sólido SSD en ordenadores de escritorio, portátiles y almacenamiento masivo con adaptadores IDE, SATA, SAS, SCSI, FIBRA CANAL FC, SSD y Emmc. Además, realiza la detección, notificación y borrado de áreas ocultas (DCO, HPA) y sectores reasignados.
2. Permite un borrado automatizado, monitorización de las actividades de borrado y registro de todas las actividades de borrado, lo que facilita el cumplimiento de las Políticas de Seguridad y Retención de Información de la organización.
3. Cada procedimiento de borrado es verificado y certificado, lo que da como resultado un Certificado de Borrado (*Data Erasure Report*) firmado digitalmente y a prueba de manipulaciones.

2. OBJETO Y ALCANCE

4. Este procedimiento recoge la configuración de seguridad que debe ser aplicada en la herramienta ***Blancco Drive Eraser*, versión 6.9.**

Nota: Todas las instrucciones contenidas en este procedimiento son soportadas por las versiones 6.x.

5. El *hardware* soportado por la herramienta son equipos con arquitectura basada en x86. Los requisitos mínimos del sistema se encuentran especificados en el Manual de BDE [REF1].
6. Por otro lado, *Drive Eraser* no requiere de ningún sistema operativo específico en el equipo en el que se instala, ya que el *software* es iniciado desde un CD o USB de arranque.

3. ORGANIZACIÓN DEL DOCUMENTO

7. La estructura de apartados del documento es la siguiente:

- a) Apartado 4. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.
- b) Apartado 5. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- c) Apartado 6. En este apartado se recogen las tareas recomendadas para la fase de ejecución.
- d) Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
- e) Apartado 8. En este apartado se incluye un breve *checklist* de acciones de configuración del producto.
- f) Apartado 9. En este apartado se incluyen las referencias asociadas a este documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. *Blancco Drive Eraser*, abreviado por BDE, es suministrado a través del envío de un correo electrónico que incluye los enlaces para la descarga del software.
9. Una vez se ha completado la descarga, se debe verificar la integridad y autenticidad del fichero descargado. En la página de descarga se encuentra el **valor SHA-256** del fichero, este deberá ser comparado con el valor obtenido del fichero de la herramienta descargada, y comprobar que la descarga se ha realizado de manera correcta.

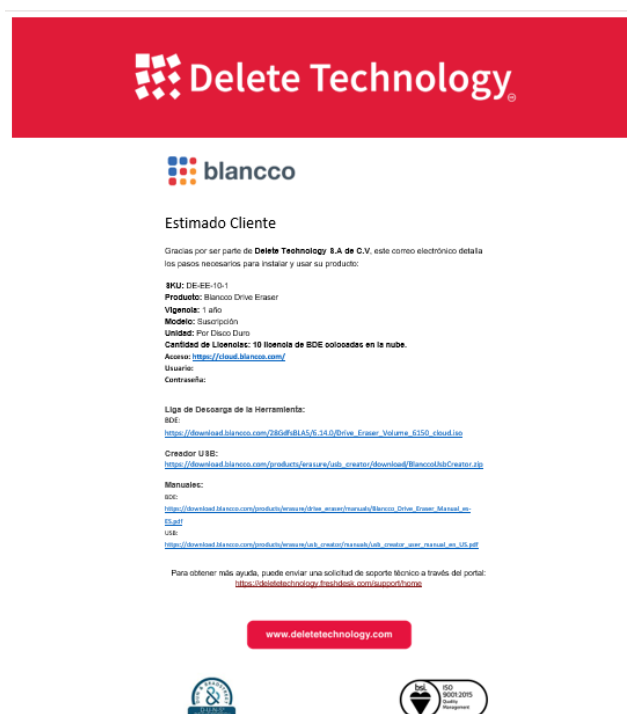


Ilustración 4-1. Ejemplo del mail de envío de licenciamiento de BDE

10. En el mismo correo electrónico se incluye el enlace de descarga de la herramienta *Blancco USB Creator*, que será usada para la creación del USB de arranque, a partir del cual se ejecutará la herramienta BDE.

4.2 ENTORNO DE INSTALACIÓN SEGURO

11. *Blancco Drive Eraser* se usa para el borrado total de HDD de ordenadores portátiles, de escritorio y servidores. Al no necesitar de ningún sistema operativo específico, solo es necesario cumplir con los requisitos mínimos *hardware* indicados en la página 11 del Manual [REF1].

12. Para poder ejecutar la herramienta se necesita crear un **USB de arranque** que se conectará al dispositivo que se quiere borrar de manera segura.
13. A continuación, se describen los pasos generales para la creación de dicho USB de arranque, aunque se puede consultar la información detallada en [REF3]:
 - a) Descargar la última versión del *software Blancco USB Creator (.exe)* y la imagen de la herramienta *Blancco Drive Eraser (.iso)*, a partir de los enlaces proporcionados en el correo electrónico.

El link de descarga del software *Blancco USB Creator* consta de un fichero .zip, el cual contiene el ejecutable (.exe).

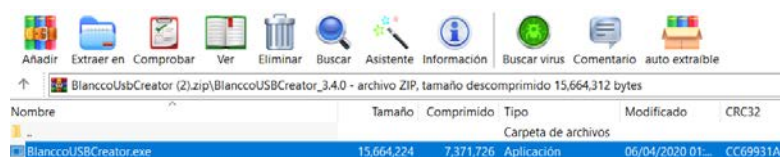


Ilustración 4-2. Muestra de archivos en el zip de Blancco USB Creator

- b) Descomprimir el fichero para poder ejecutar la herramienta.
- c) Conectar un USB.
- d) Al hacer doble clic sobre el ejecutable (.exe) se solicitará permiso para ejecutar el programa y se abrirá la herramienta.

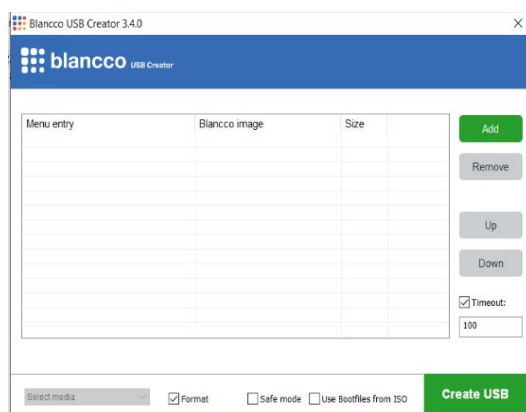


Ilustración 4-3. Pantalla principal de Blancco USB Creator

- e) En la pantalla principal de la herramienta se pulsará el botón “Add” para añadir la imagen ISO, previamente descargada.

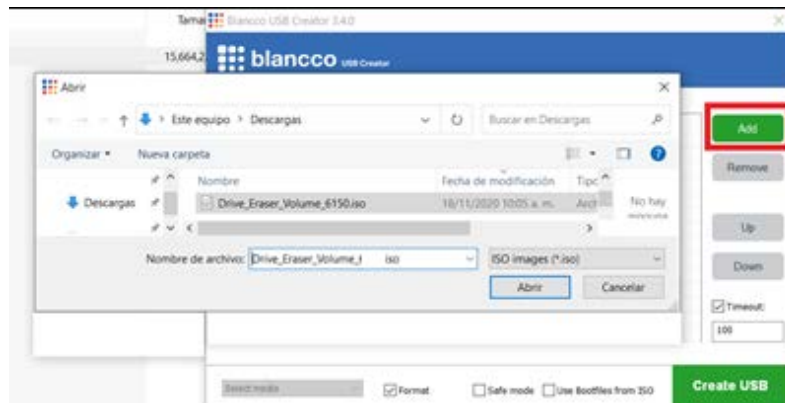


Ilustración 4-4. Selección de la imagen de BDE

- f) Una vez que se tiene seleccionada la imagen, generar el USB de arranque que se usará para realizar el borrado seguro del dispositivo.
- g) Seleccionar el USB conectado en el botón “*Select media*”, y clic en el botón “*Create USB*”.

Nota: Si se selecciona la opción “*Format*”, se formateará el USB y se eliminarán todos los datos y archivos que haya en el dispositivo.

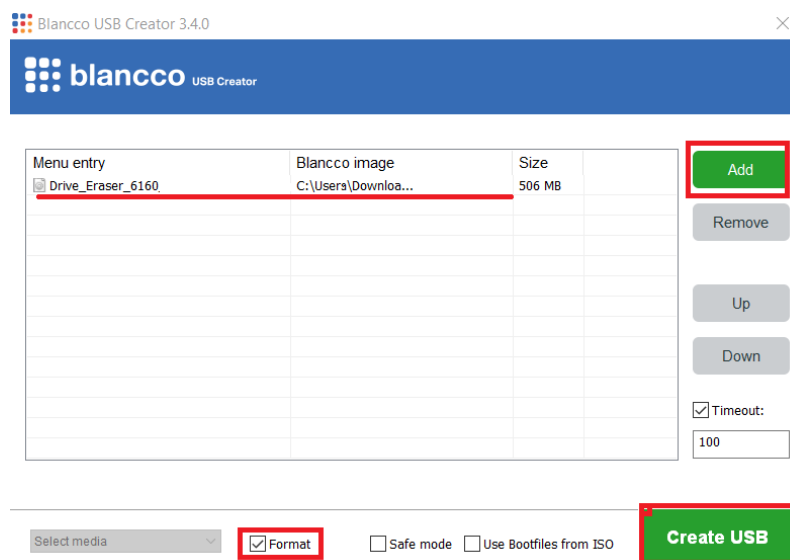


Ilustración 4-5. Creación del USB de arranque

14. Con los pasos indicados anteriormente se creará el USB de arranque. Este USB es el encargado de ejecutar la herramienta BDE para realizar el borrado seguro del dispositivo. Además, también puede almacenar los informes de borrado.
15. Para más información sobre *Blancco USB Creator* se recomienda acceder al manual de la herramienta [REF3].

4.3 REGISTRO Y LICENCIAS

16. En el correo electrónico se detalla el usuario y las credenciales para tener acceso a las licencias, junto con información adicional de la suscripción obtenida.

Estimado Cliente

Gracias por ser parte de **Delete Technology S.A de C.V**, este correo electrónico detalla los pasos necesarios para instalar y usar su producto:

SKU: DE-EE-10-1

Producto: Blancco Drive Eraser

Vigencia: 1 año

Modelo: Suscripción

Unidad: Por Disco Duro

Cantidad de Licencias: 1 licencia de **BDE** colocadas en la nube.

Acceso: <https://cloud.blancco.com/>

Usuario: ejemplo_CLIENTE

Contraseña: *****

Ilustración 4-6. Correo electrónico con usuario y credenciales.

17. Blancco cuenta con dos (2) formas diferentes de usar las licencias para el borrado seguro:

- A través de **Blancco Cloud** (*Blancco Management Console*, BMC, en la nube), haciendo uso de internet, junto con las credenciales (usuario y contraseña) proporcionadas en el correo electrónico.
- Mediante el uso de una llave **HASP** (*HASP-key*, contenedor de licencias), la cual se conectará al mismo tiempo que el USB de arranque. En esta opción, el proceso de borrado no requiere de conexión a internet, y el uso de la consola BMC será únicamente para la administración de informes (opcional).

La llave HASP deberá ser solicitada y adquirida a través del proveedor, y contendrá el licenciamiento y vigencia adquirida.

18. Es importante notar que, para poder realizar el borrado, debe haber licencias suficientes.

Nota: En el caso de hacer uso de una licencia online (*Blancco Cloud*), para tener acceso a la misma, se deberá contar con acceso a internet en el equipo donde se realizará el proceso de borrado.

4.4 INSTALACIÓN DE LA HERRAMIENTA

19. Tras seguir los pasos mencionados en el apartado 4.2, se debe conectar el USB de arranque en el equipo y se seleccionará el USB en su arranque.



Ilustración 4-7. Menú de selección del dispositivo de arranque a usar

20. Una vez que se haya montado la herramienta en el dispositivo a borrar, aparecerá la pantalla inicial de *Blancco Drive Eraser*, la cual se muestra a continuación:



Ilustración 4-8. Pantalla inicial de BDE

21. Al arrancar el software, se selecciona la opción de arranque entre las mostradas a continuación (esto dependerá del equipo a borrar).
- Eliminación de bloqueo de inmovilización durante el arranque (Opción por defecto).
 - Arranque normal (resolución segura).
 - Arranque normal (resolución nativa).
 - Arranque personalizado.
 - Mostrar mensajes de arranque.
22. Las opciones de arranque permiten que la herramienta se inicie con valores alternativos, en el caso de que surjan problemas con el arranque predeterminado.
23. Estas opciones se encuentran ocultas al inicio del arranque de la herramienta y se puede acceder a ellas pulsando la tecla de flecha arriba o abajo justo después de que aparezca la pantalla inicial de *Blancco Drive Eraser*.

24. En función del *hardware* del equipo en el que se arranque la *herramienta Blancco Drive Eraser*, pueden surgir algunos problemas durante el proceso de arranque por defecto. Estos problemas pueden observarse como pantallas en negro o equipos que no responden. En estos casos se recomienda el siguiente procedimiento:
- a) Intentar arrancar *Blancco Drive Eraser* mediante la opción **Arranque normal (resolución nativa)**.
 - b) En el caso de que surjan problemas con la opción anterior, como puede ser pantalla negra o que el equipo no responda, se recomienda arrancar *Blancco Drive Eraser* en la opción **Arranque normal (resolución segura)**.
 - c) Si surgen problemas durante la fase de arranque de la herramienta, por ejemplo, si se detiene *Blancco Drive Eraser*, se debe intentar arrancar con la opción **Mostrar mensajes de arranque**. Se debe tomar nota de los últimos mensajes mostrados en la pantalla antes del bloqueo de la herramienta y se ha de poner en contacto con la Asistencia Técnica de Blancco.
25. Para obtener más información sobre las diferentes opciones de arranque, en el Manual de *Blancco Drive Eraser* [REF1] se encuentra el capítulo “Opciones de arranque”, en el cual se explica en mayor detalle cada opción.
26. Una vez seleccionado el método de arranque se mostrará la pantalla principal de la herramienta.

5. FASE DE CONFIGURACIÓN

5.1 ADMINISTRACIÓN DEL PRODUCTO

5.1.1 MENU PRINCIPAL

27. Al arrancar la herramienta, se muestra la vista principal. Esta pantalla se encuentra dividida en tres (3) secciones diferentes: el área de encabezado, el área de proceso y el área de trabajo.

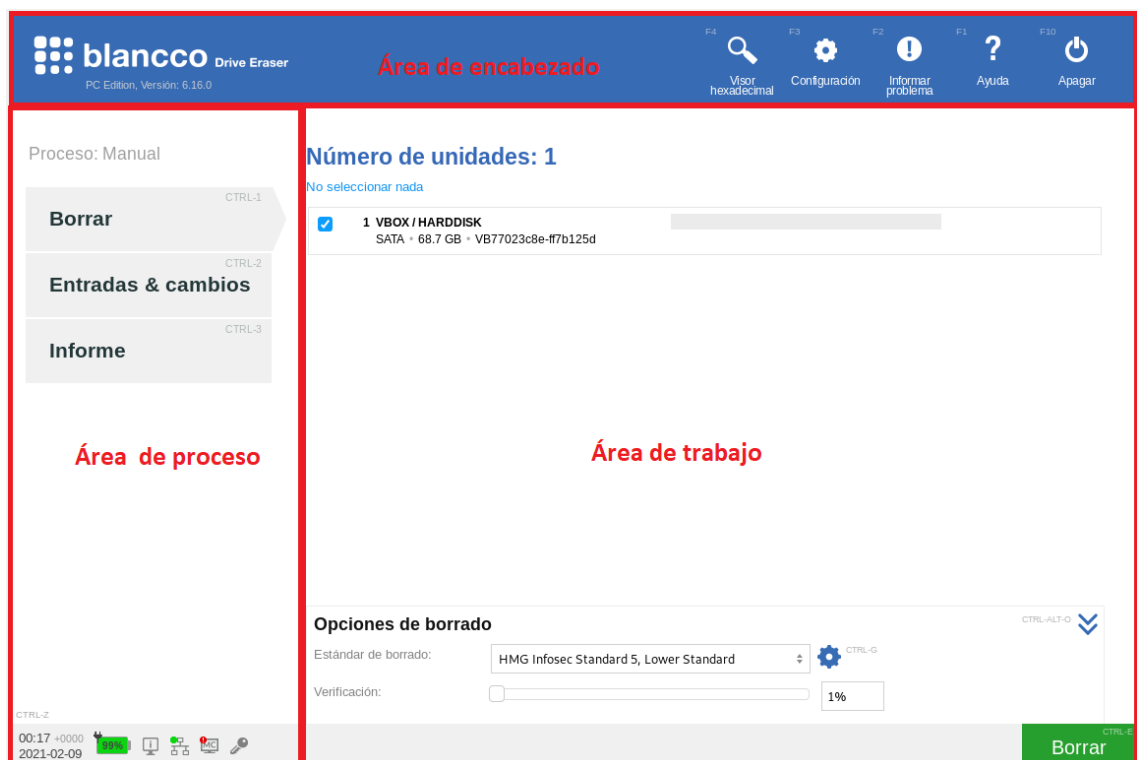


Ilustración 5-1. Pantalla principal de BDE

5.1.1.1 ÁREA DE ENCABEZADO

28. El área de encabezado contiene información acerca del *software* en uso, por ejemplo, su nombre y versión.
29. También contiene una serie de botones denominados botones de función que tienen una finalidad de carácter general, como, por ejemplo, cambiar el idioma de la interfaz de usuario, la configuración de la disposición del teclado, configuración del salvapantallas, configuración de la comunicación con la *Blancco Management Console (BMC)*, informar de un problema, menú de ayuda y apagar el equipo.

5.1.1.2 ÁREA DE PROCESO

30. El área de proceso contiene los pasos numerados necesarios para detectar y borrar las unidades del equipo (paso "*Borrar*"), actualizar el informe de borrado (paso "*Entradas & Cambios*"), visualizar y realizar copias de seguridad del informe de borrado (paso "*Informe*").

5.1.1.3 ÁREA DE TRABAJO

31. El área de trabajo contiene toda la información específica y detalles para cada paso del proceso: unidades disponibles y métodos de borrado en el paso "*Borrar*", campos adicionales para modificar informes durante el paso "*Entradas & Cambios*", información sobre el borrado y activos en el paso "*Informe*".
32. La mayoría de las acciones del usuario y la interacción con el *software* tiene lugar en el área de trabajo. Además, si un borrado genera una advertencia, se escribe un mensaje informativo de color amarillo en el informe.

5.1.1.4 MULTITAREA

33. La interfaz del usuario de *Drive Eraser* hace posible la multitarea al permitir al usuario navegar libremente entre las pestañas durante un proceso de borrado.
34. Gracias a la capacidad de multitarea, mientras el usuario está realizando el borrado de una unidad, se puede iniciar simultáneamente el borrado de otra unidad diferente.

5.1.2 CONFIGURACIÓN DE ADMINISTRADORES

35. La aplicación no dispone de diferentes tipos de usuarios, es decir, no limita las características del *software* dependiendo del usuario y sus permisos, ya que cualquier usuario que disponga del USB de arranque puede ejecutarla.
36. Sin embargo, para poder hacer uso de la herramienta es necesario contar con las credenciales de acceso a la BMC Cloud y tener disponible una licencia para realizar el borrado, o, en su defecto, contar con la llave HASP-key (contenedor de licencias) para poder realizar dicho proceso de borrado.

5.2 CONFIGURACIÓN DE LAS COMUNICACIONES

37. El proceso de borrado requerirá acceso a la consola en el caso de que las licencias se encuentren online en BMC Cloud. Por lo que, si para el acceso a internet se requiere configurar los parámetros de red, se puede acceder a "*Configuración*" a la pestaña "*Red Alámbrica*" o "*Red Inalámbrica*", dependiendo de la red. Estos

datos deberán ser proporcionados por los administradores de red de la organización.

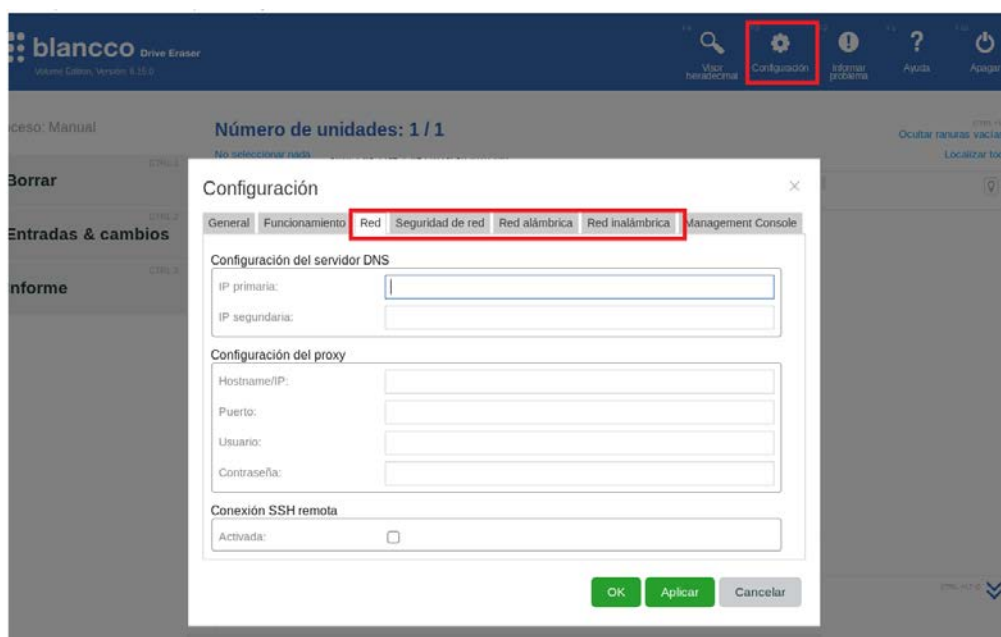


Ilustración 5-2. Gestión de datos de red

38. La conexión con la consola BMC Cloud, requiere el usuario y contraseña necesarios para comprobar que hay licencias activas para poder realizar un borrado seguro.
39. Junto con las credenciales, se han de indicar los parámetros necesarios para poder establecer la conexión: la dirección IP de la consola y el puerto de operación. Estos valores se encuentran indicados en el correo electrónico inicial (imagen 4-1).

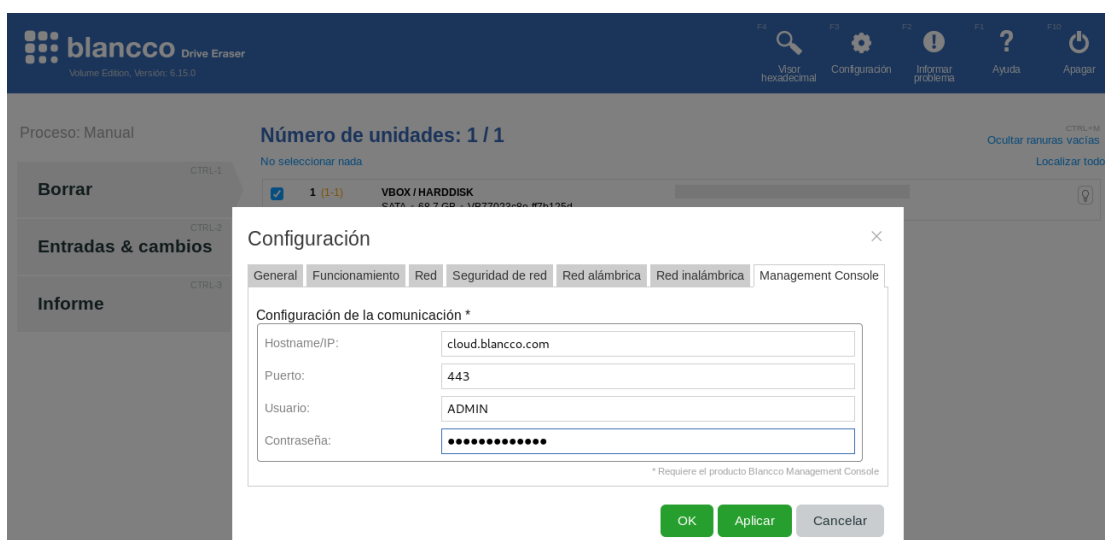


Ilustración 5-3. Configuración del usuario de BMC y sus credenciales

40. El acceso a la consola BMC Cloud puede ser necesario, también, en caso de que se quieran enviar los informes de borrado para su almacenamiento centralizado.

41. La comunicación entre el cliente y la consola, se realiza a través de HTTPS. Para ello la consola utiliza un certificado SSL de tipo ECDSA, de forma que el canal de comunicación proporciona confidencialidad e integridad a la información transmitida.
42. En caso de disponer de una consola BMC instalada en la red de la organización para el envío y almacenamiento de los informes, **se debe configurar la consola BMC con un certificado SSL que proporcione una seguridad igual o superior a 128 bits y, configurar el protocolo TLS para impedir las conexiones de clientes con una versión inferior a TLS 1.2.**

5.3 CONFIGURACIÓN DE PARÁMETROS DE SEGURIDAD

43. Desde la herramienta de configuración (BDECT, *Blancco Drive Eraser Configuration Tool*) [REF2] se pueden configurar parámetros relacionados con la seguridad. Los más destacados, son los siguientes:

- a) Clave de firma digital de Informes.

A partir de la versión 6.12 de *Blancco Drive Erase*, de forma opcional, se puede configurar una clave privada con la que firmar los informes. Esta configuración se realiza mediante la BDECT.

La clave privada puede ser importada por el usuario o generada de forma automática por BDE. Los formatos admitidos corresponden a claves RSA 2048 a 4096 bits en formato PKCS#1 y PKCS#8. **Se recomienda utilizar claves (generadas o importadas) de un tamaño mínimo de 3072 bits, para proporcionar una seguridad equivalente a 128 bits.**

- b) No validar el certificado.

Por defecto esta opción se encuentra desactivada y no se debe activar, ya que, en ese caso el cliente BDE no validaría el certificado SSL de la consola BMC en las conexiones HTTPS que establezca con ella para el envío de Informes, monitorización, etc.

- c) Contraseña (de acceso del cliente BDE a la consola BMC).

Esta contraseña debe cumplir con la política de contraseñas de la organización. Se recomienda que tenga una longitud mínima de 9 caracteres, que se componga letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, “]. De igual forma, se deben establecer, aunque sea de forma manual, parámetros de vigencia de contraseña (no superior a 180 días) y de no reutilización de las mismas.

- d) En el manual de la herramienta BDECT [REF2] se pueden encontrar parámetros de seguridad adicionales.

5.4 SINCRONIZACIÓN HORARIA

44. *Blancco Drive Eraser* toma la fecha y hora del equipo. Además, la zona horaria podrá ser configurada previamente con la herramienta *Blancco Drive Eraser Configuration Tool*. En caso de necesitar más información, se recomienda leer el manual de DECT [REF2].
45. La referencia horaria de cualquier actividad de borrado aparecerá en el informe de actividad correspondiente.

5.5 ACTUALIZACIONES

46. En caso de existir una versión nueva, esta podrá ser descargada desde la BMC, de manera manual. En caso de no contar con BMC se podrá revisar en la página <https://support.blancco.com/> si existe una nueva versión y solicitarla por correo electrónico.



Ilustración 5-4. Visualización de la actualización del *software*

5.6 AUDITORÍA

5.6.1 REGISTRO DE EVENTOS: INFORMES

47. *Blancco Drive Eraser* genera un informe con cada actividad de borrado. Estos informes serán la evidencia, en auditorías externas o internas, de que los dispositivos o discos fueron borrados de manera segura. Dichos informes pueden ser almacenados en formato XML o PDF.
48. Antes de que el borrado se haya completado, el informe simplemente contiene información acerca del *hardware* de la máquina. Una vez finalizado el borrado, este se convierte en un informe de borrado con información de activos e información de borrado combinadas. Este informe es la única prueba de que el borrado se ha inicializado y completado, de ahí su valor.
49. Por cada informe de borrado se realiza un cálculo de su valor *hash* con la función *SHA-256*. Este valor se añade al propio informe, para que el usuario final o la consola BMC puedan verificar su integridad.

50. El informe de borrado que genera *BDE* incluye, entre otros datos, los siguientes:

- a) **Detalles del *hardware* y *software*:** Información acerca del equipo borrado.
 - Nombre y versión del sistema operativo.
 - Modelo del equipo.
 - Número de serie del equipo.
- b) **Test de *hardware*:** Resultados de los tests de hardware, en el caso de haberse realizado.
- c) **Detalles del informe:** Información detallada acerca del propio informe.
 - Identificador UUID del informe.
 - Fecha y hora del informe.
 - Versión del *software*.
 - Firma Digital: Firma *RSA-SHA-256* generada con la clave privada configurada, para garantizar la autenticidad e integridad de la información contenida en el informe.

2021-02-09 01:38:49 (+0000), BLANCCO DRIVE ERASER 6.16.0, INNOTEK GMBH, VIRTUALBOX, 0

Informe de borrado de datos

Resultado de borrado

Disco: 1	Fabricante: VBOX	Modelo: HARDDISK	N.º de serie: VB77023c8e-f7fb125d
Sector(es) reasignado(s) después de borrado:	Tamaño: 69GB	Bus: SATA	Sectores: 134217728
Hora de inicio/final:	HPA: No existe	DCO: No existe	Sector(es) reasignado(s): 0
Duración:	Estdo: N/A		
Método:	0		
Pasos de borrado:	2021-02-09 01:37:12 (+0000) / 2021-02-09 01:38:38 (+0000)		
Estado:	00:01:26		
	HMG Infosec Standard 5, Lower Standard		
	1 (1 sobrescritura)		
	Borrado		

Detalles del hardware

Fabricante:	innotek GmbH
Tipo de chasis:	Other
Modelo:	VirtualBox
N.º de serie:	0
UUID:	6e92c3f8-d8b2-f41a-a9a9-dc53c5c3214e
Versión del sistema:	1.2
Procesador:	GenuineIntel, Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz, Núcleos: 1, Submodelo: 10, Velocidad nominal: 2600MHz, Velocidad máxima: N/A 12GB, Bancos de memoria ocupados: 0/0
Memoria total:	InnoTek Systemberatung GmbH VirtualBox Graphics Adapter, 32MB
Tarjeta gráfica:	Intel Corporation 82801FB/FBM/FRW/FW (ICH6 Family) High Definition Audio Controller
Tarjeta de sonido:	Intel Corporation 82801HM/HM (ICH8M/ICH8M-E) SATA Controller [AHCI mode]
Controlador de almacenamiento: 1	VBOX, HARDDISK, Firmware: 1.0, N.º de serie: VB77023c8e-f7fb125d, 69GB / 134217728 sector(es), SATA, Tamaño de sector: 512, Velocidad promedio de escritura: 784MB/s, Velocidad promedio de lectura: 599MB/s, Región accesible: 69GB / 134217728 sector(es), DCO: No existe, HPA: No existe, Estado: N/A
Disco: 1	Ethernet, Intel Corporation 82540EM Gigabit Ethernet Controller / PRO/1000 MT Desktop Adapter, 08:00:27:11:c3:ca, 10.0.2.15, 255.255.255.0, 10.0.2.2
Adaptador de red:	VBOX, Tipo: DVD-ROM, CD-ROM
Unidad de disco óptico:	VirtualBox, USB Tablet, VirtualBox, USB Tablet 1.10
Dispositivo USB:	Oracle Corporation, VirtualBox
Placa base:	innotek GmbH, Versión: VirtualBox, Fecha: 12/01/2006
BIOS:	PCI, ACPI, CD Boot
Características del BIOS:	Fabricante: innotek, Modelo: 1, N.º de serie: 0, Tipo: Unknown, Capacidad: 50000 / 50000 mWh, Voltaje: 10000 mV
Batería:	

Detalles del informe

UUID del informe:	e2149c2c-2a47-4616-ac96-b4b0356f13ec
Fecha del informe:	2021-02-09 01:38:49 (+0000)
Versión de software:	Blancco Drive Eraser 6.16.0
Firma digital:	XYYTgUpwGZGz+7weYUcMAK23RMhNqg3erVdZSE3cg7XGEWpYtLMQALduhApJ7ZdFLAnd+CUGZomEBUB+CvpeE3BEHPRRxbhKsAKuBKCmAbQUZuSSGsmYELyTH3BhwIggBr-vSML3eSdP7FkmaadLddidwafWpYpRPMPmpwrFDWdgGrVChRRFSDEBdrhNJCLYAT84hswAYPCAGDGRhUj2GN3ZYQUHESBMFP3BuutV9vMtHrDOCArPDxwCqr9WnwhvndtsdEdBmgwWYWGMA==

Por la presente declaro que el proceso de borrado de datos ha sido realizado de conformidad con las instrucciones recibidas.

OPERADOR DE BORRADO DE DATOS

SUPERVISOR

Ilustración 5-5. Ejemplo de informe de borrado

5.6.2 ALMACENAMIENTO REMOTO

51. Los informes generados por BDE se pueden almacenar en local, en el mismo dispositivo USB utilizado para el arranque de la herramienta, o se pueden enviar a la consola *Blancco Management Console*. **Se recomienda el almacenamiento local**, ya que es la opción más segura.
52. No obstante, en caso de envío a una consola BMC instalada en la red de la organización, se recomienda que dicha consola sea configurada, tal y como se ha indicado en el apartado 5.2 (TLS \geq 1.2 y certificado SSL que proporcione, al menos, 128 bits de seguridad).
53. Para el almacenamiento remoto se han de configurar, también, los parámetros de red necesarios para establecer la conexión con la consola, tal y como se ha mostrado en la imagen 5-3. Se recomienda hacer uso del puerto HTTPS **443**, para

que se autentique la identidad de la consola a través del certificado SSL, y que la información se transmita por un canal seguro.

	Date	Erase state	Disk serial	Disk capacity	Memory capacity	Product Name
<input type="checkbox"/> View	2020-11-30 15:42	Successful		1 TB	8 GB	Blancco File Eraser - Enterprise Edition
<input type="checkbox"/> View	2020-11-30 16:37	Successful	Z1090	1 TB	8 GB	Blancco Drive Eraser
<input type="checkbox"/> View	2020-11-30 16:32	Successful	WD-WCC3	1 TB	8 GB	Blancco Drive Eraser
<input type="checkbox"/> View	2020-11-30 16:24	Successful	TF9501	500 GB	8 GB	Blancco Drive Eraser
<input type="checkbox"/> View	2020-11-30 16:02	Successful	SVPCZ	1 TB	4 GB / 4 GB	Blancco Drive Eraser
<input type="checkbox"/> View	2020-11-30 15:00	Successful	SVF502	1 TB	4 GB / 4 GB	Blancco Drive Eraser

Ilustración 5-6. Almacenamiento de informes dentro de la herramienta BMC

5.6.3 NOTIFICACIONES

54. Durante el proceso de borrado pueden ocurrir diferentes errores o excepciones, que la herramienta notifica al usuario dependiendo del tipo de error y del estado del proceso de borrado:
 - a) **Borrado satisfactorio** con excepciones: Estos errores o excepciones se indican en el informe como un mensaje informativo en color **amarillo**. Además, el salvapantallas proporciona una notificación mediante un icono de éxito cuyo color cambia entre el verde y el amarillo.
 - b) **Borrado fallido**: En el informe se notifican todos los errores que han ocurrido y el salvapantallas muestran el símbolo “!” sobre un fondo rojo, como se muestra en la imagen 6-5.
 - c) **Temperatura elevada en NVMe**: La herramienta produce una notificación cuando una unidad NVMe (*Non-Volatile Memory Express*) detecta una temperatura elevada durante el proceso de borrado. En este caso, el salvapantallas muestra una notificación con el símbolo “!” parpadeando.
55. La notificación de dichas excepciones de borrado sólo puede activarse/desactivarse a través de DECT.
56. A parte de los errores que puedan surgir durante el proceso de borrado, se recomienda que el usuario esté atento a las notificaciones y ventanas emergentes proporcionadas por la herramienta, en las que se indican los posibles errores o advertencias que el usuario deberá tener en cuenta. Estos errores pueden ser fallos al enviar los informes a la BMC, número de licencia inválido, error en algún parámetro introducido, etc.

5.7 BACKUP

57. Los informes de *Blancco Drive Eraser* son generados en formato en XML y PDF y pueden ser respaldados con cualquier aplicación de *backup*. Este proceso es externo a *Blancco Drive Eraser*. **Se deben establecer procedimientos de *backup* de acuerdo con la política de seguridad de la información de la organización.**
58. También, como se ha mencionado en el apartado anterior, se tiene la opción de hacer el envío o la importación de los informes en la BMC.

5.8 ESTÁNDARES DE BORRADO

59. *Blancco Drive Eraser* basa su operación en el uso de estándares para el borrado seguro. Los estándares de borrado son emitidos por organismos de seguridad nacionales que establecen bajo qué algoritmos se debe realizar la sobrescritura de los ficheros para garantizar su eliminación correcta del disco duro.
60. El producto soporta varios estándares de sobrescritura. *Blancco Drive Eraser* tiene como predeterminado el estándar de borrado: *HMG INFOSEC Lower Standard* de 1 sobrescritura publicado por el Centro de Ciberseguridad del Reino Unido (NCSC, por sus siglas en inglés). **Se recomienda configurar aquel estándar que garantice el cumplimiento de los requisitos normativos aplicables para cada sistema u organismo.**
61. El estándar de borrado se puede configurar como se indica en la siguiente imagen:

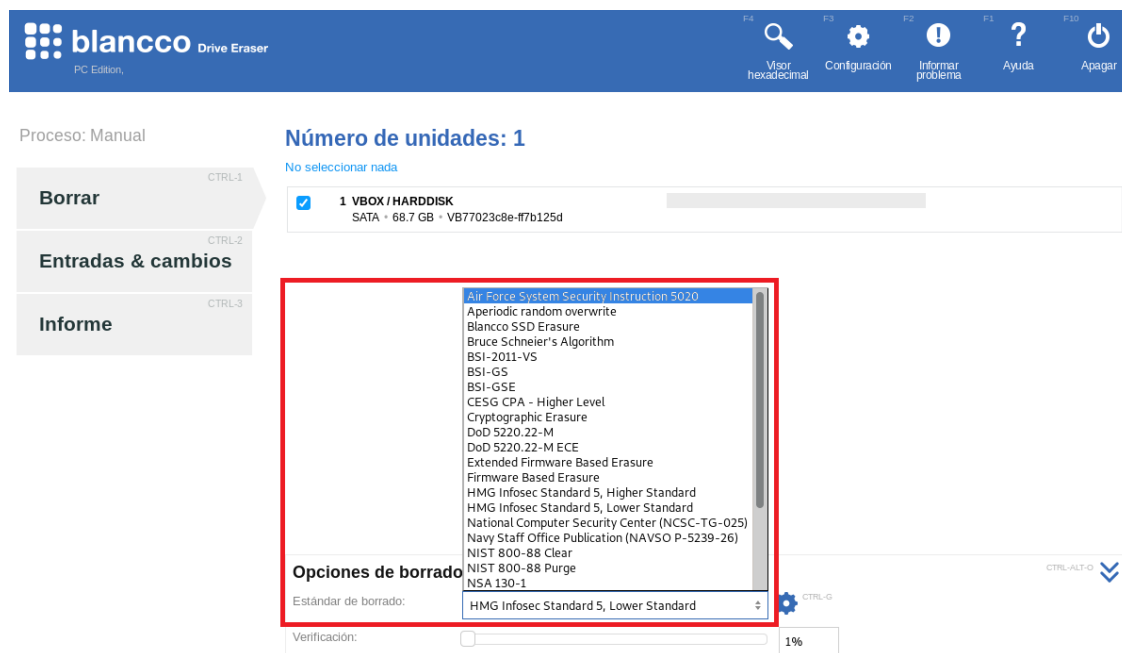


Ilustración 5-7. Selección del estándar de borrado

6. FASE DE EJECUCIÓN

62. Este apartado describe de manera general el proceso que se deberá llevar a cabo para realizar el borrado seguro con la herramienta *Blancco Drive Eraser*.
- a) Previamente se deben haber realizado las configuraciones necesarias en la imagen ISO mediante la herramienta de configuración DECT y se deberá haber creado un **USB de arranque** con la imagen ISO, tal y como se ha indicado en el apartado 4.4.
 - b) Se ejecutará el USB de arranque en el equipo a borrar.
 - c) En el Área de Trabajo se mostrarán los diferentes discos o las diferentes particiones que se pueden borrar. Se deberá seleccionar la unidad o unidades a borrar.
 - d) En el caso de hacer uso de las licencias en *Blancco Cloud (BMC)*, el equipo deberá disponer de **conexión a Internet** e indicar las credenciales de acceso.
63. Realizando los pasos anteriormente mencionados, en la parte inferior de la ventana de la aplicación se mostrarán unos iconos con un círculo verde. Esto confirmará que se tiene acceso a red, la conexión es exitosa con *Blancco Cloud* y que se cuenta con licencias disponibles para el proceso de borrado.
64. En caso de no haber licencias disponibles, el icono de la llave no contaría con el círculo verde encima.

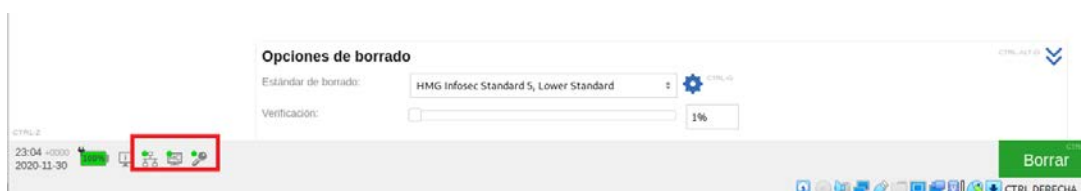


Ilustración 6-1. Visualización de los iconos de la herramienta

Nota: En caso de usar *HASP-key*, en vez de *Blancco Cloud*, se deberá conectar el dispositivo al mismo tiempo que el USB de arranque, y al pulsar “*Borrar*” se emitirá una ventana emergente como la imagen 6-2, donde solicitará la confirmación del borrado y la aceptación de los términos de la herramienta. Una vez confirmado, se iniciará el proceso de borrado, sin requerir las credenciales del usuario, ni acceso a internet.

- 1) Se hará clic en “*Borrar*” y se emitirá la siguiente ventana emergente.

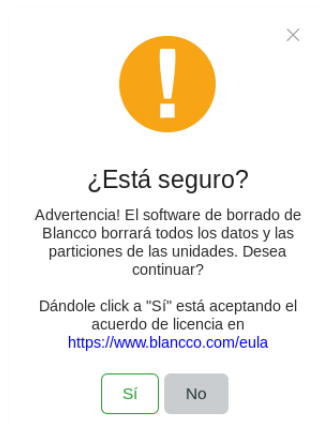


Ilustración 6-2. Confirmación del borrado

Nota: Dando clic en “Sí” se acepta el borrado del equipo, y el uso de la licencia. Por lo tanto, una vez iniciado el proceso, la información borrada no podrá ser recuperada. Además, el equipo deberá contar con energía eléctrica ya que, si se llegara a apagar por cualquier circunstancia, se tendría que realizar de nuevo el proceso de borrado y conllevaría el consumo de otra licencia.

65. Una vez aceptado el borrado se mostrará la siguiente imagen, donde se indicará el tiempo que tardará en realizarse el proceso de borrado. También permite al usuario añadir datos adicionales, y navegar entre las diferentes opciones, mientras se realiza el proceso de borrado.

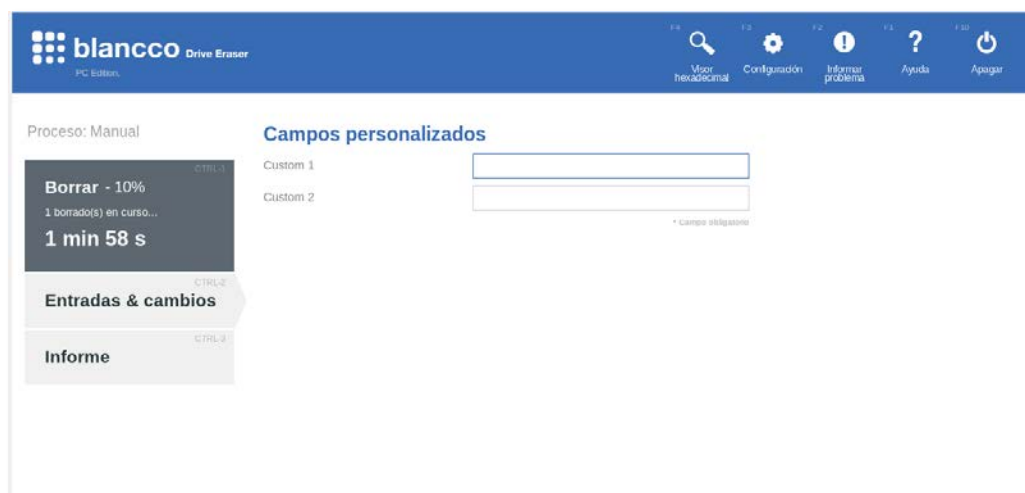


Ilustración 6-3. Posibilidad de añadir datos adicionales durante el borrado

66. Durante el proceso de borrado se podrá verificar su estado, el cual podrá ser identificado por los siguientes colores:



Ilustración 6-4. Identificadores de color del proceso

67. Además, en el salvapantallas se podrá visualizar el porcentaje de progreso del borrado, si finalizó el borrado de manera exitosa o si hubo algún fallo. Para activar o desactivar el salvapantallas deberá hacerse desde la herramienta DECT o desde “Configuración”.

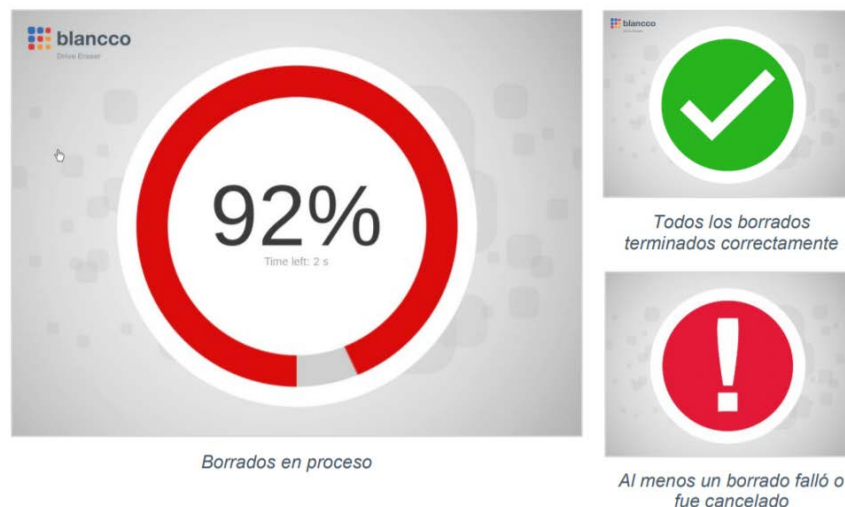


Ilustración 6-5. Pantalla con porcentaje de borrado y estado de finalización.

68. Una vez finalizado el borrado se generará un certificado de borrado, el cual contendrá el estado del proceso y las características tanto del disco borrado, como del equipo donde se realizó el proceso de borrado seguro.

6.1 ENVÍO O ALMACENAMIENTO DEL INFORME

69. Como se ha indicado en el apartado 5.6.2, el informe generado tras el proceso de borrado podrá ser enviado o guardado, a decisión del usuario final.

Nota: Si el informe no es almacenado o enviado no se tendrá el certificado de borrado y se deberá realizar de nuevo el proceso de borrado, lo que conllevaría el uso de otra licencia.

70. La herramienta BDE proporciona dos (2) diferentes métodos para almacenar el informe:

a) Botón Guardar o “Save”:

El botón “Save”, o el método abreviado Ctrl + S, se utiliza para guardar el informe en un soporte físico externo, por ejemplo, un USB. Este informe irá firmado, como se ha mencionado anteriormente, para poder verificar su integridad.

Se selecciona el dispositivo externo en el que se almacenará el informe en *Periférico de almacenamiento*, en *Nombre de archivo* se indicará el nombre deseado para guardarlo, y en *Formato* se puede seleccionar el formato en el que se almacenará.

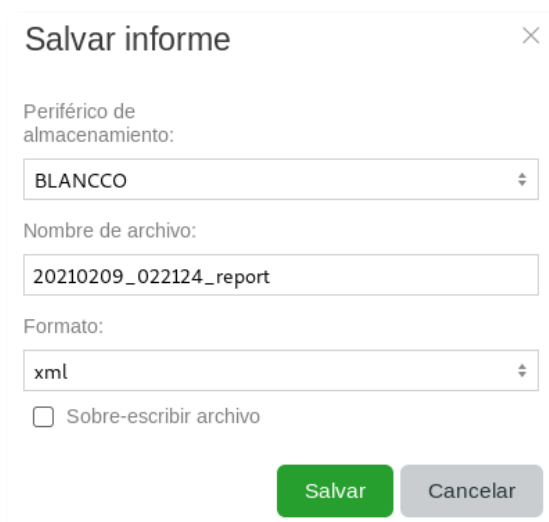


Ilustración 6-6. Guardar informe de borrado

b) Botón Enviar o “Send”

El botón “Send” se utiliza para enviar el informe a la BMC, en el caso de disponer acceso a ella.

Cuando la BMC recibe el informe, verifica su integridad y firma (en caso de que se haya configurado), permitiendo o rechazando su visualización.

7. FASE DE OPERACIÓN

71. Para la fase operativa es recomendable **actualizar el *software*** de forma periódica, mediante el uso de BMC o mediante el portal de soporte de Blancco, con el objetivo de mantener el sistema actualizado siempre a la última versión.
72. Se recomienda el **almacenamiento local de los informes**, y en el caso de almacenarlos en la consola BMC, se recomienda seguir la configuración segura de las comunicaciones, mediante el **uso de TLS 1.2 y certificados SSL** (ver apartado 5.2).
73. Además, se ha de **controlar el acceso a los informes**, de tal forma que únicamente el personal autorizado pueda acceder a ellos.
74. También, es recomendable **revisar las alarmas** que genere el producto durante su ejecución, para tener en cuenta los posibles problemas o incidencias que surjan a la hora del borrado seguro.

8. CHECKLIST

75. Para aplicar una configuración segura de *Blancco Drive Eraser*, se deberán realizar las siguientes acciones:

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Descargar y verificar el <i>software</i> del enlace de descarga suministrado por correo electrónico.	<input type="checkbox"/>	<input type="checkbox"/>	
Creación del USB de arranque.	<input type="checkbox"/>	<input type="checkbox"/>	
Tener conexión a internet	<input type="checkbox"/>	<input type="checkbox"/>	
Configurar las comunicaciones con BMC o <i>Blancco Cloud</i> .	<input type="checkbox"/>	<input type="checkbox"/>	
Especificar las credenciales de <i>Blancco Cloud</i> o contar con la llave <i>HASP-key</i> .	<input type="checkbox"/>	<input type="checkbox"/>	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Actualización de manera manual.	<input type="checkbox"/>	<input type="checkbox"/>	
Establecimiento de contraseñas de usuarios que cumpla con la política.	<input type="checkbox"/>	<input type="checkbox"/>	
No activar la validación de los certificados.	<input type="checkbox"/>	<input type="checkbox"/>	
Establecer una clave para la firma digital de los informes mediante RSA.	<input type="checkbox"/>	<input type="checkbox"/>	
Configurar el certificado SSL de la consola BMC.	<input type="checkbox"/>	<input type="checkbox"/>	

ACCIONES	SÍ	NO	OBSERVACIONES
Seleccionar el estándar de borrado acorde a los requerimientos.	<input type="checkbox"/>	<input type="checkbox"/>	
Proceso de borrado.	<input type="checkbox"/>	<input type="checkbox"/>	
En el caso de utilizar la consola, enviar los informes al recurso centralizado o guardar el informe en el USB.	<input type="checkbox"/>	<input type="checkbox"/>	
Realizar <i>backups</i> de los informes.	<input type="checkbox"/>	<input type="checkbox"/>	

9. REFERENCIAS

- REF1** *Manual de Blancco Drive Eraser*
[Blancco Drive Eraser Manual](#)
- REF2** *Manual de Blancco Drive Eraser Configuration Tool*
[Blancco Drive Eraser Configuration Tool Manual](#)
- REF3** *Manual de Blancco USB Creator*
[Blancco USB Creator Manual](#)

