GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 1501

# Configuración segura de Herramienta de Borrado Seguro EraseIT Loop

Octubre 2018

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.10.26 09:33:48 +02'00'


NIPO: 083-19-010-5

Fecha de Edición: octubre 2018
Recovery Labs ha participado en la realización y modificación del presente documento y sus anexos.

# PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Octubre de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

# ÍNDICE



# ANEXOS

# 1. INTRODUCCIÓN

1. Las herramientas de borrado seguro son aplicaciones software diseñadas para impedir que se recupere información no autorizada de dispositivos de almacenamiento que hayan almacenado datos sensibles y que vayan a ser reutilizados o reciclados.
2. Para posibilitar la reutilización de estos dispositivos sin comprometer la confidencialidad de la información previamente almacenada, se utilizan técnicas estándar de borrado seguro, que tradicionalmente consisten en sobrescribir un determinado número de veces todos los sectores del disco siguiendo un patrón establecido.
3. EraseIT Loop es una herramienta software que borra de forma segura, definitiva e irreversible todos los datos de los dispositivos de almacenamiento de un equipo informático, incluido el disco de sistema, lo que permite su reciclaje o reutilización de manera segura. El proceso de borrado se realiza mediante sobrescritura de datos.
4. EraseIT Loop es capaz de detectar dispositivos de almacenamiento masivo con diferentes interfaces de conexión: IDE, SATA, SCSI y USB y sobrescribir los datos contenidos en el dispositivo seleccionado por el usuario. Además, se pueden parametrizar diversos estándares de borrado (DoD, CCN Wipe, NATO, etc.) o establecer uno como predefinido en la personalización.

## 2. ALCANCE

5. El presente documento define el procedimiento de empleo seguro de la herramienta EraseIT Loop en sistemas afectados por el Esquema Nacional de Seguridad hasta categoría Alta donde se maneje información sensible.
6. La herramienta es capaz de realizar el borrado seguro en dispositivos de almacenamiento de datos que empleen un sistema de grabación magnética con una de las siguientes interfaces de conexión:
    a) IDE,
    b) SATA,
    c) SCSI,
    d) USB.
7. Este procedimiento no es válido para los dispositivos que empleen como sistema de almacenamiento de datos memorias no volátiles como:
    a) discos de estado sólido,
    b) memorias *flash,*
    c) memorias *nand.*
8. No se deberá utilizar la herramienta para borrar:
    a) Cintas magnéticas.
    b) Unidades de lectura asociadas a los dispositivos de almacenamiento, como el caso de las unidades USB tipo U3.

## 3. ENTORNO

9. A pesar de que la aplicación arranca desde un USB, no existe una cadena de confianza que permita un arranque seguro, por lo que deberá asegurarse que la herramienta se ejecuta en un equipo aislado (sin conexión a red) y libre de malware.
10. El personal que utilice la herramienta EraseIT deberá haber sido instruido previamente sobre el procedimiento de borrado seguro.
11. La herramienta deberá instalarse sobre una plataforma que cumpla los siguientes requisitos mínimos:
    a) Procesador Pentium II.
    b) Memoria RAM 128 MB o superior.
    c) Un lector de puerto USB.
    d) Capacidad de arrancar desde el sistema presente en un USB.
12. Deberá configurarse el equipo en BIOS para que permita el arranque desde USB.

# 4. EJECUCIÓN

## 4.1 ARRANQUE

13. La herramienta EraseIT Loop se suministra en una memoria USB auto-arrancable.
14. En el arranque de la aplicación se deberán seguir los siguientes pasos:
    a) Se configura la BIOS del equipo para que realice el arranque desde el USB.
    b) Se reinicia el equipo y se introduce el USB de EraseIT Loop antes de que comience el proceso de arranque.
    c) Se esperará hasta que el programa de borrado se cargue en memoria y muestre la pantalla de presentación, sin acceder a otras áreas del sistema operativo ni del equipo. Este proceso puede tardar unos minutos.


**Figura 1 Arranque de la herramienta**

## 4.2 SELECCIÓN DE DISPOSITIVO

15. En el siguiente paso, se seleccionan los dispositivos que van a ser borrados de forma segura, tal y como se muestra a continuación:


**Figura 2 - Pantalla de selección de dispositivo**

16. Una vez seleccionados los dispositivos[1], continuamos con el proceso presionando siguiente, llegamos a una pantalla de **confirmación**. El sistema nos advertirá en el caso de que alguno de los discos seleccionados ya haya sido previamente borrado de forma segura y nos posibilita la visualización del informe de borrado correspondiente.


**Figura 3 - Pantalla de confirmación de dispositivos**

[1] No hay que seleccionar el USB en el que se encuentra la herramienta EraseIT Loop.

## 4.3 MÉTODO DE BORRADO

17. Durante la siguiente fase se selecciona el método de borrado dentro de la pestaña “Método predefinido”. EraseIT implementa los métodos estándares de borrado más habituales del mercado con diferentes niveles de complejidad y ofrece al usuario la posibilidad de seleccionar cuál de ellos utilizar.


Figura 4 - Pantalla de selección del método de borrado

18. Igualmente permite la opción de configurar un método de borrado personalizado, accediendo a la pestaña “Método definido por el usuario”, para lo que habrá que definir:

    a) El número de pasadas, con o sin verificación. Este número indica cuántas veces se sobrescribe cada uno de los bloques en los que se divide el dispositivo.

    b) El patrón de sobrescritura en cada una de ellas.

19. Con los medios actuales, una sola pasada de borrado imposibilita cualquier recuperación posterior de datos mediante técnicas estándar de análisis forense.

20. No obstante, es recomendable añadir una pasada de comprobación posterior en el caso que tras el borrado se quiera reutilizar los dispositivos. Si el dispositivo tuviera problemas de lectura en algún sector y por tanto no pudiera utilizarse normalmente, estos serían detectados en la pasada de comprobación.

## 4.4 VERIFICACIÓN DE BORRADO

21. Al finalizar el borrado de los dispositivos, la aplicación genera un informe de borrado con toda la información obtenida durante el proceso y lo almacena en

cada uno de los discos borrados como “marca de borrado”. De esta forma EraseIT puede identificar durante la detección de los dispositivos si alguno de ellos ya fue borrado previamente.

22. Para verificar que el dispositivo se ha borrado de forma satisfactoria, el usuario de la herramienta deberá comprobar que el informe generado indica que el borrado se ha realizado con éxito y sin ningún error.

23. En caso de detectarse algún error o detectarse el disco cómo defectuoso (ANEXO A. Control de errores durante el borrado), se deberá proceder a la destrucción física del dispositivo para asegurar el borrado seguro de la información que contiene.


**Figura 5 - Pantalla de visualización de informe de borrado**

24. Para visualizar el informe, el usuario deberá hacer clic en “Mostrar” en la primera línea del resumen que aparece al finalizar el proceso.


**Figura 6 -Pantalla resumen de borrado**

25. Pulsando "guardar" (Figura 7) podrá grabar el informe de borrado. Aparecerá una pantalla para seleccionar el dispositivo en el que se desea almacenar el informe de borrado como la que se muestra a continuación.


**Figura 7 - Selección de dispositivo de almacenamiento de informe**

26. Hay que tener en cuenta que si se realiza el borrado de dispositivos a través de USB y no se desconectan, aparecerán como unidades donde almacenar el informe, por eso se solicita haberlos desconectado en la pantalla anterior.

27. El informe de borrado podrá ser almacenado en la misma memoria USB donde reside la herramienta EraseIT Loop o en otra distinta. En ese caso habría que introducir la nueva memoria, hacer clic en "Refrescar" y, una vez que la aplicación la haya reconocido, hacer clic en "Guardar".

### 4.4.1. VISUALIZADOR DE INFORMES DE BORRADO (VIS.EXE)

28. El visualizador de informes (Figura 8) de borrado se suministra junto a la herramienta de borrado EraseIT Loop y permite:
    a) Visualizar los informes de borrado seguro generados por la aplicación EraseIT Loop
    b) Enviar los informes a la extranet[2] EraseIT Loop.
29. Para emplear esta herramienta es necesario un equipo con Microsoft Windows y los informes generados por la herramienta de borrado EraseIT Loop.
30. Se recomienda utilizar el visor para visualizar los informes de borrado seguro generados por la aplicación EraseIT Loop, evitando el uso de la extranet de EraseIT Loop.

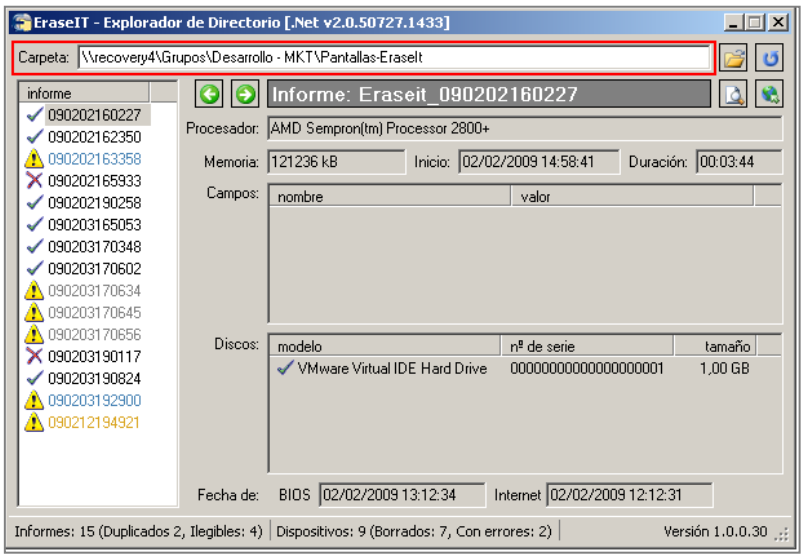


**Figura 8 - Ejemplo de Vis.exe con informes**

Seleccionar un informe del listado;

Abrir la carpeta (contenida en el equipo del usuario) donde se guardan los informes

Actualizar el listado de informes

Acceder a la vista preliminar de un informe

Enviar los informes seleccionados a la extranet de EraseIT Loop. (Esta acción sólo es posible si se dispone de conexión a Internet.)

[2] La extranet de EraseIT Loop pertenece al fabricante de la herramienta (Recovery Labs)

## 5. REFERENCIAS

**REF 1** *Security Target for the Secure Data Erasure Software – Erase IT Core* v 1.5

**REF 2** Informe de certificación 2010-6-INF-615 v2

**REF 3** CCN-STIC-105 Catálogo de Productos de Seguridad TIC

## 6. ABREVIATURAS

| | |
|---|---|
| **ENS** | Esquema Nacional de Seguridad. |
| **IDE** | *Integrated Device Electronics* |
| **SATA** | *Serial Advanced Technology Attachment* |
| **SCSI** | *Small Computer System Interface* |
| **USB** | *Universal Serial Bus* |

## ANEXO A. CONTROL DE ERRORES DURANTE EL BORRADO

31. Si durante el proceso de sobrescritura la herramienta detectara errores de escritura en los sectores del dispositivo, dado que el objetivo es borrar el mayor número de sectores posible, se realizarán 3 reintentos de sobrescritura. Si fuera imposible el acceso a dicho sector se aumentará el número de errores en el dispositivo actual y se continuará con los sectores siguientes. En caso de que se contabilicen más de 5 sectores inaccesibles se marcará dicho dispositivo como inaccesible a escritura y, por tanto, como defectuoso.
32. Si durante el proceso de verificación la herramienta detectara errores en los sectores del dispositivo, se realizarán 3 reintentos de lectura. Si se repitieran los errores de acceso a dicho sector, se aumentará el número de errores de verificación en el dispositivo actual y se continuará con los sectores siguientes. En caso de que se contabilicen más de 15 sectores inaccesibles se marcará dicho dispositivo como inaccesible a lectura y, por tanto, como defectuoso.