GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo E.3: Herramientas de borrado seguro

Noviembre 2017

Edita:

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
2017.11.27 11:26:50 +01'00'

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017

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

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Herramientas de borrado seguro** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado desde el punto de vista de la seguridad para ser empleado en los sistemas de información del sector público a los que sea de aplicación el Esquema Nacional de Seguridad (ENS). Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.
3. Además, la aplicación de estos criterios permitirá:
4. Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
   - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
   - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.
5. Por lo tanto, los productos catalogados dentro de la familia **Herramientas de borrado seguro** conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.
6. En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la sección siguiente. Dichos productos podrían optar a ser incluidos de manera adicional como Productos Cualificados en otra(s) familia(s) del CPSTIC si cumpliesen los RFS correspondientes.

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

7. 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.
8. Durante un proceso de borrado no seguro, la información no se borra completamente del dispositivo de almacenamiento, sino que simplemente se marca como disponible ese espacio de memoria y se borra la entrada que lo indexa en la tabla de direccionamiento, por lo que puede ser recuperada total o parcialmente mediante la aplicación de sencillas técnicas de análisis forense. Esta recuperación podrá llevarse a cabo hasta que no se haya sobrescrito el espacio liberado en su totalidad.
9. 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 el sector del disco siguiendo un patrón establecido.
10. Los estándares más comunes son: *Standard Overwrite, British HMG IS5 Baseline, Russian GOST R 50739-95, NSA 130-2, British HMG IS5 Enhanced, US DoD 5220.22-M, NCSC-TG-025, Navso P-5329-26, US Air Force 5020, Bruce Schneier, Canadian OPS-II, German VSITR, Gutmann,* etc. Todos ellos aportan diferentes niveles de seguridad, dependiendo del número de pasadas y del patrón utilizado.

2.2 CASOS DE USO

11. Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contemplan dos casos de uso para esta familia de productos tal como se definen a continuación.

2.2.1. CASO DE USO 1

12. Se realiza una gestión centralizada, que permite monitorizar y administrar varias instancias de la herramienta de borrado seguro sobre un grupo heterogéneo de sistemas.

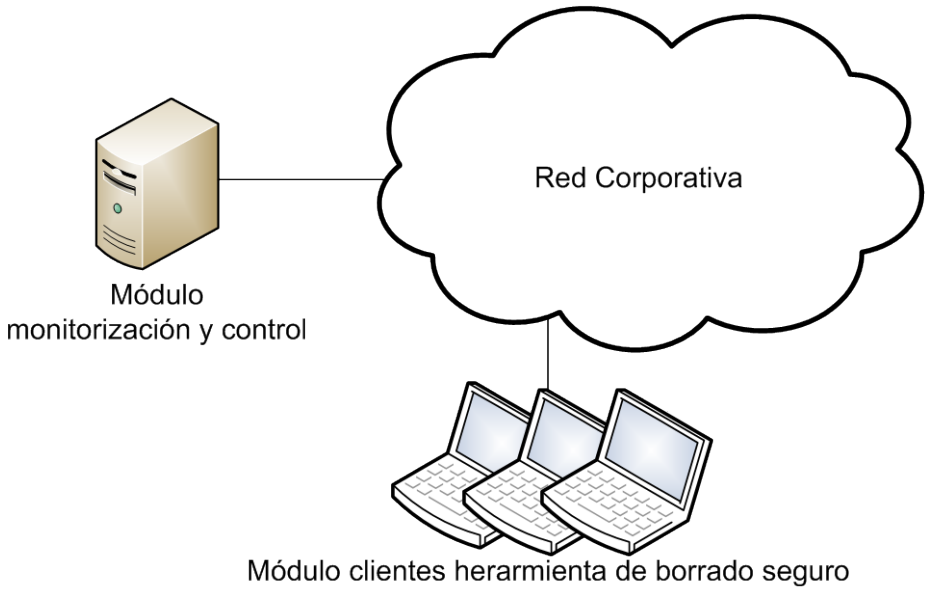

Figura 1-Caso de uso 1

2.2.2. CASO DE USO 2

13. La gestión es autónoma en cada equipo, la monitorización y control de ejecución de la herramienta de borrado seguro forma parte de la propia aplicación local.

2.3 ENTORNO DE USO

14. Este tipo de herramientas suele utilizarse en dispositivos de almacenamiento que almacenen información sensible, tanto de empresas como del sector público, en combinación con medidas complementarias para preservar la confidencialidad de la información.
15. Para la utilización en condiciones óptimas de seguridad de las herramientas de borrado seguro, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Plataforma segura:** El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.
    - **Administración confiable:** El administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello se asume que dicha persona estará capacitada y carecerá de cualquier intención dañina.
    - **Configuración del sistema:** Los dispositivos de almacenamiento deberán exponer toda su capacidad al S.O[1]. Además, la BIOS[2] del equipo deberá estar

[1] Sistema Operativo
[2] *Basic Input/Output System*

correctamente configurada, de tal forma que no impida el borrado del dispositivo.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

16. Este tipo de productos suele presentarse en formato de software instalable o aplicación portable que se ejecuta desde algún dispositivo de almacenamiento (CD, USB[3], HDD[4]) y se carga en la RAM[5] del equipo informático desde el que se realizarán las operaciones de borrado seguro.

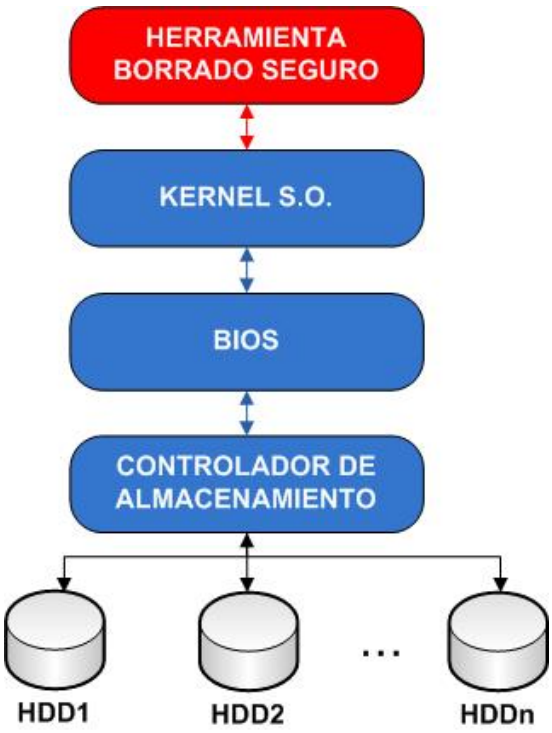

Figura 2 – Arquitectura lógica del sistema

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

17. No se ha utilizará ningún perfil de protección *Common Criteria* de referencia para esta familia de productos.
18. El nivel de confianza EAL (*Evaluation Assurance Level*) conforme a CC, al que deben ser evaluados los Requisitos Fundamentales de Seguridad descritos en este documento debería ser EAL1 o superior.

[3] *Universal Serial Bus*
[4] *Hard Disk Drive*
[5] *Random Access Memory*

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

19. Los recursos que es necesario proteger mediante el uso de esta familia de productos, incluyen:

    - Toda la información que debe ser borrada y que está contenida en los dispositivos de almacenamiento. Deberá ser protegida de divulgación no autorizada.
    - Datos de configuración del producto y de auditoría generados por éste.
    - Actualizaciones de la herramienta.

3.2 AMENAZAS

20. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, atendiendo a los casos de uso expuestos en la sección 2.2, serían:

    - **Divulgación de información no autorizada:** Un atacante que tenga acceso al dispositivo de almacenamiento después del borrado de datos podría ser capaz de recuperarlos y comprometer la confidencialidad de los datos almacenados inicialmente.
    - **Acceso no autorizado:** Un atacante consigue acceder a la herramienta y modificar su configuración.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

21. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia.

4.1 AUDITORÍA Y REGISTROS DE SEGURIDAD

22. **REQ. 1** Por cada acción que realice, el producto generará un registro de auditoría que contenga, como mínimo, la siguiente información:
    - Tipo de acción.
    - Resultado.
    - Hora y fecha.
    - Usuario.
    - Disco, fichero o directorio sobre el que se realiza la acción.
    - Estándar de borrado. En caso de que el producto permita la selección entre varios estándares.
23. **REQ. 2** La gestión de los registros sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de auditor/rol de administrador).
24. **REQ. 3** El producto debe proporcionar una forma de acceso a los registros de auditoría para facilitar su revisión a los usuarios autorizados.
25. **REQ. 4** El producto permitirá exportar los datos de auditoría a un formato legible.
26. **REQ. 5** El producto deberá generar un registro de evento de seguridad en caso de borrado, creación o modificación de registros de auditoría.
27. **REQ. 6** En el caso de que permita almacenamiento remoto de los registros de auditoría, se utilizará un protocolo de comunicaciones del tipo IPsec[6], TLS[7], TLS/HTTPS[8] para establecer un canal de comunicaciones seguro entre él y las entidades que provean estos servicios adicionales.

4.2 ADMINISTRACIÓN DEL PRODUCTO

28. **REQ. 7** El producto presentará al menos dos tipos de perfiles: administradores y usuarios, a los que se asociarán diferentes permisos. (Estos perfiles podrán estar vinculados con perfiles del propio sistema operativo).
29. **REQ. 8** Los usuarios podrán realizar tareas de borrado, selección de método de borrado, consulta de informes de verificación.

[6] *Internet Protocol Security*
[7] *Transport Layer Security*
[8] *Hypertext Transfer Protocol Secure*

30. **REQ. 9** Los administradores, además de realizar las tareas propias del resto de usuarios, podrán:
    a. Parar y arrancar el servicio.
    b. Gestionar usuarios, incluyendo creación, baja y asignación de privilegios.
31. **REQ. 10** En el caso de que se permita la administración remota, se utilizará un protocolo de comunicaciones del tipo IPsec, TLS, TLS/HTTPS para establecer un canal de comunicaciones seguro entre él y las entidades que provean estos servicios adicionales.

4.3 BORRADO SEGURO

32. **REQ. 11** La herramienta deberá ser capaz de borrar los datos almacenados en los dispositivos seleccionados haciendo imposible la recuperación de datos tras el borrado.
33. **REQ. 12** Permitirá seleccionar el estándar de borrado, estableciendo de esta manera diferentes niveles de seguridad.
34. **REQ. 13** La herramienta permitirá verificar que el proceso de borrado se ha realizado correctamente y notificará el resultado del proceso de verificación. El producto permitirá verificar la integridad de esta información mediante mecanismos de chequeo de integridad implementados con funciones hash.

5. ABREVIATURAS

BIOS	*Basic Input / Output System*
CC	*Common Criteria*
CCN	*Centro Criptológico Nacional*
CD	*Compact Disk*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones*
EAL	*Evaluation Assurance Level*
ENS	*Esquema Nacional de Seguridad*
HDD	*Hard Disk Drive*
HTTPS	*Hypertext Transfer Protocol Secure*
IPSEC	*Internet Protocol Security*
RAM	*Random Access Memory*
RFS	*Requisitos Fundamentales de Seguridad*
TLS	*Transport Layer Security*
SHA	*Secure Hash Algorithm*
USB	*Universal Serial Bus*