centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo E.3: Herramientas de borrado seguro

Junio 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

© Centro Criptológico Nacional, 2021
NIPO: 083-21-130-1

Fecha de Edición: Junio de 2021

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.06.23 16:46:23 +02'00'

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 Y OBJETO 4
2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS 5
2.1 CASOS DE USO 5
2.1.1. CASO DE USO 1 5
2.1.2. CASO DE USO 2 6
2.2 ENTORNO DE USO 6
2.3 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO 7
2.4 ALINEAMIENTO CON CRITERIOS COMUNES (*COMMON CRITERIA*) 7
3. ANÁLISIS DE AMENAZAS 8
3.1 RECURSOS QUE ES NECESARIO PROTEGER 8
3.2 AMENAZAS 8
4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS) 9
4.1 CANALES DE COMUNICACIÓN CONFIABLE 9
4.2 REQUISITOS CRIPTOGRÁFICOS 9
4.3 ADMINISTRACIÓN CONFIABLE 9
4.4 IDENTIFICACIÓN Y AUTENTICACIÓN 10
4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLE 10
4.6 AUDITORÍA 11
4.7 BORRADO SEGURO 11
4.8 NOTAS DE APLICACIÓN 12
5. ABREVIATURAS 13

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 para 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:
    - 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.
4. 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.
5. 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

6. 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.

7. 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.

8. 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.

9. 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.

2.1 CASOS DE USO

10. 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.

2.1.1. CASO DE USO 1

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

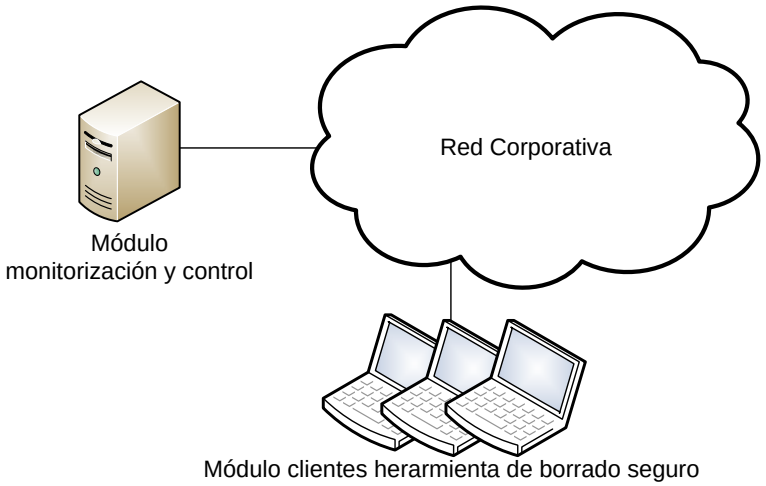

Figura 1-Caso de uso 1

2.1.2. CASO DE USO 2

12. 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.

2.2 ENTORNO DE USO

13. Para la utilización en condiciones óptimas de seguridad de las herramientas Antivirus/EPP, 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.
    - **Acceso:** El producto tiene acceso a todos los datos del sistema necesarios para llevar a cabo todas sus funciones.
    - **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, formada y carecerá de cualquier intención dañina al administrar el producto.
    - **Actualizaciones periódicas:** El software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

2.3 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

14. Este tipo de productos son herramientas que suelen presentarse en formato de *software* que se instala en un sistema de ficheros proporcionado por un sistema operativo. Se ejecutan en una plataforma que puede ser el sistema operativo, un entorno de ejecución o una combinación de las anteriores.

2.4 ALINEAMIENTO CON CRITERIOS COMUNES (*COMMON CRITERIA*)

15. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos TIC (Tecnologías de la Información y de las Comunicaciones).

16. En el ámbito de CC se definen un conjunto de objetivos y requisitos de seguridad, tanto funcionales (*SFR, Security Functional Requirements*) como de evaluación (*SAR, Security Assurance Requirements*), independientes de la implantación, que cada producto incluirá dentro de su declaración de seguridad (*ST, Security Target*).

17. Los productos dentro de esta familia, deberán disponer de una declaración de seguridad (ST) certificada con un nivel de confianza EAL (*Evaluation Assurance Level*) EAL2 o superior, que contenga los SFR indicados en el apartado 4.

18. En caso de que alguno de los requisitos indicados en la tabla anterior no se encuentre recogido en la declaración de seguridad del producto, pero sí implemente esa función de seguridad, se podrá llevar a cabo una **evaluación STIC complementaria,** cuyo objetivo será verificar el cumplimiento de esos requisitos.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

19. Los recursos que deben protegerse mediante el uso de estos productos incluyen:

- **AC.Comunicación.** Comunicaciones del producto.
- **AC.Datos.** Información almacenada en la plataforma sobre la que se instala y ejecuta el producto.
- **AC.Actualizaciones.** Actualizaciones del producto y la plataforma susceptible de afectar a la configuración y funcionalidad.

3.2 AMENAZAS

20. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, atendiendo al caso de uso expuesto en la sección 2.1, serían:

- **A.RED. Ataque a la red.** Un atacante, desde dentro o desde fuera de la red, consigue acceder a información intercambiada a través de la red entre el producto y otras entidades autorizadas o modificar sus comunicaciones.
- **A.LOCAL. Ataque local.** Un atacante puede actuar a través de software no privilegiado ejecutado en la misma plataforma de computación donde se ejecuta el producto. Los atacantes podrían modificar de forma maliciosa los ficheros o comunicaciones que utiliza el producto.
- **A.REST. Acceso a información almacenada.** Un atacante podía acceder a información sensible almacenada en la plataforma en la que se instala y ejecuta el producto.
- **A.NODET. Actividad no detectada.** Un atacante consigue acceder, cambiar o modificar la funcionalidad de seguridad de la herramienta sin que esto sea apreciado por el administrador.
- **A.BOR. Acceso a información borrada.** Un atacante podría acceder a información sensible previamente borrada por el producto.

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 para categoría ENS ALTA.

4.1 CANALES DE COMUNICACIÓN CONFIABLE

22. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).

23. **COM. 1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas (auditoría, administración, etc.) o entre distintas partes del producto empleando funciones, algoritmos y protocolos que estén de acuerdo a lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).

24. **COM.2** El producto debe permitir comunicaciones, a través de canales seguros, iniciadas por sí mismo o por entidades autorizadas.

25. **COM.3** El producto hará uso de certificados digitales para la autenticación cuando utilice cualquiera de estos protocolos.

4.2 REQUISITOS CRIPTOGRÁFICOS

26. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST).

27. **CIF.1** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos que utilicen suites de cifrado que estén incluidas entre las autorizadas para Categoría ALTA del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.

28. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

4.3 ADMINISTRACIÓN CONFIABLE

29. Estas funcionalidades de seguridad mitigan la amenaza (A. REST). Podrán ser cubiertas por el producto o por su entorno operacional.

30. **ADM.2** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades del producto:

    - Administración de producto de forma local.
    - Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.

- Otros parámetros de configuración del producto.

Nota de aplicación: En este punto se espera que el fabricante enumere todas las tareas de administración que puedan ser realizadas.

31. **ADM.3** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones anteriormente descritas.

    Nota de aplicación: en el caso de que existan distintos tipos de administrador, cada uno de ellos con distintos permisos, deberá probarse que únicamente pueden realizar aquellas funcionales para las que tengan permiso.

4.4 IDENTIFICACIÓN Y AUTENTICACIÓN

32. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). Podrán ser cubiertas por el producto o por su entorno operacional.
33. **IAU.1** El producto debe identificar y autenticar a cada usuario antes de permitir acciones que modifiquen la configuración del producto.
34. **IAU.2** El producto debe implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
35. **IAU.3** El producto debe proteger de lectura y modificación no autorizada las credenciales de autenticación, claves o información sobre las claves.
36. **IAU.4** El producto debe disponer de la capacidad de gestión de las contraseñas:

    a) La contraseña debe poder configurarse con una longitud mínima o igual a 12 caracteres.
    b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “].

    Nota de aplicación: este requisito podría ser modificado en el caso de que el producto implemente otros mecanismos de autenticación. Será estudiado caso por caso.

37. **IAU.5** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLE

38. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL).
39. **ACT.1** El producto debe ofrecer la posibilidad de consultar la versión actual del *firmware/software* e iniciar actualizaciones manualmente.

40. **ACT.2** El producto deberá ofrecer mecanismos (conforme a la criptografía de empleo en el ENS) a través de hashes o firma digital para autenticar las actualizaciones de *firmware/software* antes de instalarlas.
41. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

4.6 AUDITORÍA

42. Esta funcionalidad de seguridad mitiga la amenaza (A.NODET).
43. **AUD. 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.
44. **AUD. 2** La gestión de los registros sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de auditor/rol de administrador).
45. **AUD. 3** El producto debe proporcionar una forma de acceso a los registros de auditoría para facilitar su revisión a los usuarios autorizados.
46. **AUD. 4** El producto permitirá exportar los datos de auditoría a un formato legible.
47. **AUD. 5** El producto deberá generar un registro de evento de seguridad en caso de borrado, creación o modificación de registros de auditoría.

4.7 BORRADO SEGURO

48. Esta funcionalidad de seguridad mitiga la amenaza (A.BOR).
49. **BOR.1** La herramienta deberá ser capaz de borrar los datos almacenados en los dispositivos seleccionados haciendo imposible la recuperación de datos tras el borrado.
50. **BOR.2** Permitirá seleccionar el estándar de borrado, estableciendo de esta manera diferentes niveles de seguridad.
51. **BOR.3** 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.

4.8 NOTAS DE APLICACIÓN

52. En caso de que el producto no implemente la funcionalidad a la que aplica alguno de los requisitos anteriores (o algunas partes de ellos), y ésta sea proporcionada por el entorno operacional, el fabricante deberá indicarlo en la declaración de seguridad o justificarlo debidamente.

5. ABREVIATURAS

CC	*Common Criteria*
CCN	*Centro Criptológico Nacional*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones*
EAL	*Evaluation Assurance Level*
ENS	*Esquema Nacional de Seguridad*
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*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL