centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC
Anexo F.11: Herramientas de Videoidentificación

Marzo 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.03.21 15:54:51 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-102-1.

Fecha de Edición: marzo de 2022

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 Videoidentificación** 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), para categoría ALTA**. 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 Videoidentificación** 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

2.1 FUNCIONALIDAD

6. Según la ISO 2382-37, la biometría es "el reconocimiento automático de los individuos en función de sus características biológicas y de comportamiento".

7. El reconocimiento biométrico está basado en características físicas, fisiológicas o conductuales. Esta familia de productos utiliza únicamente la modalidad biométrica facial.

8. Los productos asociados a la familia **Herramientas de Videoidentificación** surgen para dar respuesta a la necesidad de establecer mecanismos de autenticación e identificación remota, con el fin de contribuir en la reducción de los desplazamientos de los ciudadanos para realizar trámites, sin mermar sus derechos.

9. Hoy en día, los productos de videoidentificación, y de biometría en general, son productos complejos en los que la fiabilidad, privacidad y seguridad son claves.

10. Algunas de las características de estos productos son las siguientes:

    - **Composición modular.** Estos productos suelen estar compuestos por diferentes módulos con funcionalidades diferenciadas: módulo de captura de datos y módulo de procesamiento y comparación (motor biométrico).

    - **Comparación no absoluta.** El resultado del módulo de utilización o comparación de datos biométricos no es binario, sino que emite un porcentaje de coincidencia (también llamado similitud o semejanza) o diferencia (*scoring*).

    - **Proceso asistido o desasistido.** El proceso de identificación puede ser asistido o desasistido. En el proceso asistido, el operador es parte activa del proceso y toma la decisión de identificación a partir de la información suministrada por la herramienta. En el proceso desasistido, la revisión de evidencias y decisión final de identificación es realizada a posteriori por el operador.

    - **Grabación y almacenamiento de evidencias:** Los productos permiten, además de la captura de datos y la grabación del proceso de identificación, su posterior almacenamiento e indexación en una base de datos.

2.2 CASOS DE USO

11. Dependiendo de las funcionalidades y características de despliegue del producto, se contemplan dos (2) casos de uso:

    a) Caso 1 Proceso asistido o síncrono: el operador participa en el propio proceso de identificación *on line* y toma la decisión de forma inmediata.

    b) Caso 2 Proceso desasistido o asíncrono: el operador toma la decisión a posteriori, en función de las evidencias recibidas *off line*, como proceso de *back-office*.

12. En ambos casos, la decisión se realiza en función de la revisión de todas las evidencias recabadas en el proceso de identificación.

2.2.1. CASO DE USO 1 – OPERADOR PRESENTE EN EL PROCESO DE IDENTIFICACIÓN (PROCESO ASISTIDO O SÍNCRONO)

13. El operador interactúa con el usuario a través de una videollamada.

14. El operador aprueba o rechaza la identificación en función del resultado de validación de la herramienta (*scoring*), de la revisión de las evidencias y de su valoración durante la videollamada.

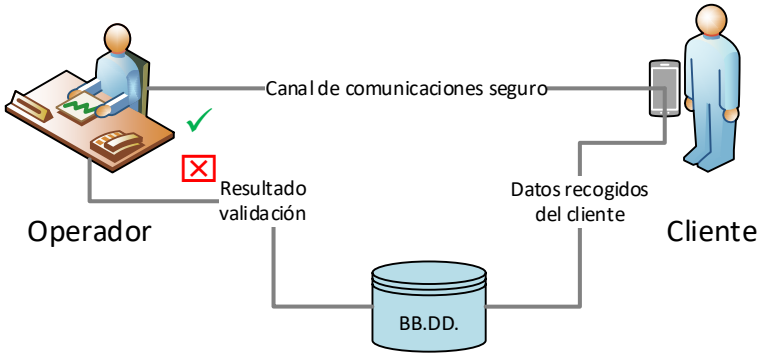

Figura 1 – Ejemplo de Caso de Uso: Proceso Asistido o síncrono

15. Los datos capturados y generados, así como el resultado del análisis del operador (identificación positiva o negativa), se almacenan en el sistema de información y se indexan en una base de datos.

2.2.2. CASO DE USO 2 – OPERADOR NO PRESENTE EN EL PROCESO DE IDENTIFICACIÓN (PROCESO DESASISTIDO O ASÍNCRONO)

16. El operador no interactúa con el usuario, solo consulta y analiza la información, almacenada previamente en los sistemas de información e indexada en la base de datos.

17. El operador accede a un panel o cuadro de mandos en el que tiene acceso a todas las evidencias (imágenes, videos y resultados de las validaciones automáticas) y

aprueba o rechaza la identificación en función del análisis realizado de las evidencias.

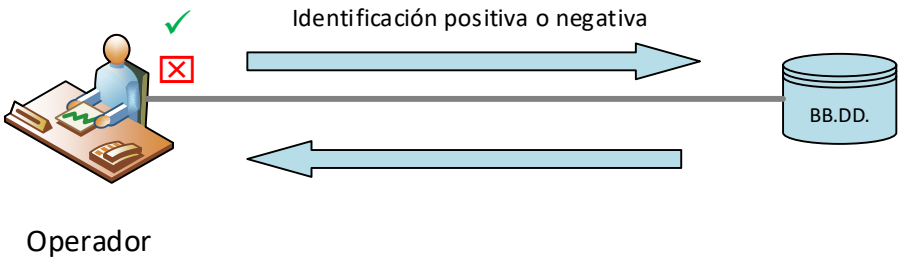

Figura 2 – Ejemplo de Caso de Uso: Proceso desasistido o asíncrono

18. Este caso de uso no considera la interacción con el usuario: la verificación se realiza en el *back-office*, a partir de los datos capturados en un proceso videoidentificación anterior.

2.3 DELIMITACIÓN DEL ALCANCE DEL PRODUCTO

19. Estos productos pueden constar de uno o varios componentes, los cuales se presentan en forma de producto *software*.
20. Las evidencias obtenidas en el proceso de identificación, así como los resultados proporcionados por la herramienta pueden ser almacenados en los sistemas de información de los Prestadores de Servicios de Confianza u organismos responsables de la adquisición para su consulta por parte de sus operadores de identificación.

2.4 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

21. Se asume que el entorno operacional cumple las siguientes condiciones:
    - **Protección física.** La herramienta se encuentra protegida por su entrono operacional y no puede ser objeto de ataques físicos que pudiesen comprometer su seguridad o interferir en su correcta operación.
    - **Administración confiable.** El usuario administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad del sistema. Por ello, se asume que dicha persona estará altamente capacitada y carecerá de cualquier intención dañina al administrar estos dispositivos.
    - **Intervención de operador.** En el proceso de videoidentificación siempre intervendrá un operador que tomará la decisión en base a la revisión de las evidencias obtenidas en el proceso de identificación, así como el *scoring* proporcionado por la herramienta.
    - **Verificación de la autenticidad e integridad de los documentos de identificación**: El sistema garantizará, mediante medidas procedimentales o

técnicas, la autenticidad e integridad de los documentos de identificación empleados para la videoidentificación del solicitante.

2.5 CERTIFICACIONES / EVALUACIONES EXIGIDAS PARA LA CUALIFICACIÓN

2.5.1. CERTIFICACIONES

22. Para que un producto de esta familia pueda ser incluido en el CPSTIC deberá disponer de alguna de las siguientes certificaciones:

    a) ***Common Criteria***. La certificación deberá ser de un nivel de aseguramiento EAL 2 y la Declaración de Seguridad (ST, por sus siglas en inglés) asociada a la certificación deberá contener los RFS (SFR en terminología *Common Criteria*) reflejados en el Apartado **4**, evaluados considerando el problema de seguridad definido en el presente documento.

    b) **Certificación Nacional Esencial de Seguridad (LINCE) con Módulo de Evaluación Biométrica (MEB)**. La Declaración de Seguridad asociada a la certificación deberá contener los RFS reflejados en el Apartado **4**, evaluados considerando el problema de seguridad definido en el presente documento. Los requisitos biométricos se evaluarán de acuerdo a la IT-14 del Organismo de Certificación del ENECSTI. Además, en el caso de que el producto implemente mecanismos para la protección criptológica de las evidencias almacenadas, los requisitos definidos en el apartado **6** deberán evaluarse fuera del alcance de la certificación LINCE inicial, en una Evaluación STIC Complementaria que incluya también el Módulo de Evaluación Criptográfica (MEC).

23. En caso de que el producto implemente algún requisito de los especificados en el Apartado **4** que no se encuentren incluidos en la certificación, se podrá llevar a cabo una *evaluación STIC complementaria***,** cuyo objetivo será verificar el cumplimiento de esos requisitos para completar el proceso de cualificación.

NOTA:

Es importante destacar que las certificaciones exigidas para los productos de esta familia únicamente ofrecen garantías de que el producto implementa las funcionalidades de seguridad incluidas en su Declaración de Seguridad y que dicha implementación es resistente a atacantes con un potencial de ataque básico y moderado, tal como se encuentra definido en las distintas metodologías consideradas. Ninguna de estas certificaciones ofrece garantías sobre la funcionalidad de verificación de la autenticidad e integridad del documento de identidad, que deberá ser garantizada mediante otros medios fuera del alcance de estas certificaciones.

2.5.2. EVALUACIONES

24. El sistema biométrico de comparación facial entre el solicitante y la foto del documento de identidad debe haber sido evaluado, según *el Face Recognition Vendor Test* (FRVT) en la categoría VISABORDER, del NIST[1] y haber obtenido una tasa de FNR[2] (*False Negative Rate*) menor o igual a 5% para un FPR[3] (*False Positive Rate*) de menor o igual a 1/1 000 000. La base de datos utilizada para la prueba debe ser la utilizada por el NIST en 2020 o superior[4].

25. Se realizará una evaluación STIC complementaria de los requisitos incluidos en el Apartado **5**.

NOTA:

Esta evaluación tiene por objeto comprobar que la herramienta realiza unas comprobaciones básicas sobre el documento. En ningún momento se considera dentro del alcance de la evaluación funcionalidad de verificación de la autenticidad e integridad del documento de identidad, que deberá ser garantizada mediante otros medios fuera del alcance de estas evaluaciones.

[1] National Institute of Standards and Technology (NIST)

[2] También denominado FNMR. *False Non-Match Rate*. Falso negativo en la comparación. Esta tasa se define para algoritmos de comparación. En sistemas finales, donde la decisión se puede tomar tras varios intentos, suele denominarse *FRR False RejectionRate*.

[3] También denominado FMR. *False Match Rate*. Falso positivo en la comparación. Esta tasa se define para algoritmos de comparación. En sistemas finales, donde la decisión se puede tomar tras varios intentos, suele denominarse FAR *False Acceptance Rate*.

[4] El CCN podrá revisar los términos exigibles al sistema en la anterior evaluación atendiendo al avance del estado del arte y/o al cambio en las condiciones de evaluación del NIST.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

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

- Comunicaciones con el producto.
- Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos.
- Información sensible:

a) Datos de configuración del producto.

b) Datos de auditoría generados.

c) Credenciales.

d) Parámetros biométricos utilizados por la herramienta como criterios de decisión, entre ellos el valor umbral que se usa de referencia para la verificación biométrica. También debe proteger el *scoring* obtenido en el proceso de comparación.

e) Evidencias biométricas (opcional, en función de la arquitectura del producto).

3.2 AMENAZAS

27. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, serían:

- **A.RED. Ataque a la red.** Un atacante, desde dentro o desde fuera de la red, consigue acceder y/o modificar la información intercambiada durante su tránsito entre el producto y otras entidades externas autorizadas o entre los distintos módulos del producto.
- **A. SEG. Acceso a configuración de seguridad y parámetros biométricos.** Un atacante podría acceder y modificar la configuración de seguridad del producto, así como los parámetros biométricos que intervienen en proceso de decisión.
- **A.NODET. Actividad no detectada.** Un atacante consigue acceder, cambiar o modificar la funcionalidad de seguridad registrada por la herramienta sin que esto sea apreciado por el administrador.
- **A.BIO. Presentación de rasgos biométricos similares**. Un atacante puede presentar algunos rasgos biométricos, por su parecido, que puedan ser verificados incorrectamente como un usuario genuino.
- **A.PAD.** Un atacante puede presentar cualquier tipo de instrumentos de ataque de presentación durante el registro y/o verificación biométrica con

objeto de suplantar una identidad o de ofuscar la propia. (Por ejemplo, un atacante puede robar rasgos biométricos de un usuario genuino y elaborar cualquier tipo de instrumentos de ataque de presentación basados en esas características biométricas).

- **A.REST. Acceso a información almacenada.** Un atacante puede acceder a información sensible almacenada en el producto.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

28. A continuación, se recogen los requisitos fundamentales de seguridad que deben incluirse en la certificación del producto.

4.1 PROTECCIÓN FRENTE A ATAQUES EN LA CAPTURA DE EVIDENCIAS

29. **GEN.1** La herramienta debe garantizar que la interacción del cliente con el sistema se ejecuta en un único dispositivo y en un único acto secuencial en el tiempo.
30. **GEN.2** La herramienta únicamente permitirá la identificación cuando esta se realice en tiempo real. En el caso de la grabación de video, este debe realizarse en directo, no se permiten archivos pregrabados.
31. Nota de aplicación: el fabricante deberá describir en la declaración de seguridad los mecanismos implementados para satisfacer ambos requisitos.

4.2 VERIFICACIÓN BIOMÉTRICA

32. **SOL.1** La herramienta deberá proporcionar verificación biométrica facial utilizando la imagen del solicitante y la imagen impresa en el documento de identidad.
33. **SOL.2** La herramienta debe implementar medidas técnicas para detectar que la persona está viva a través de pruebas activas o pasivas.
34. **SOL.3** La herramienta deberá implementar mecanismos de detección de ataques de presentación biométrica (*Presentation Atack Detection*, PAD) que impidan la verificación exitosa.

4.3 AUDITORÍA

35. **AUD.1** La herramienta debe generar información de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzca alguno de los siguientes eventos:
    a) *Login* y *logout* de personal autorizado.
    b) Cambio en las credenciales de usuarios administradores del servicio.
    c) Cambios en la configuración.
    d) Cualquier otro evento relacionado con el proceso de identificación y validación del documento de identidad.
36. **AUD.2** Los registros de auditoría deben contener, al menos, la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento (si aplica).
37. **AUD.3** La herramienta debe registrar el resultado de los procesos de verificación junto con el motivo de rechazo, en caso de tratarse de un resultado negativo.

38. **AUD.4** Los registros de auditoría solo podrán ser consultados y eliminados por usuarios con el rol de auditor o de forma automática cuando se alcance el tiempo máximo configurado en la herramienta.

4.4 COMUNICACIONES SEGURAS

39. **COM.1** La herramienta deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas (que serán especificadas en la declaración de seguridad) 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.).

4.5 ADMINISTRACIÓN CONFIABLE

40. **ADM.1** La herramienta deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones administrativas.
41. **ADM.2** La herramienta tendrá la capacidad de definir dos (2) tipos de roles de administración: configurador y auditor.

4.6 IDENTIFICACIÓN Y AUTENTICACIÓN

42. **IAU.1** La herramienta deberá identificar y autenticar a cada usuario antes de otorgar acceso.
43. **IAU.2** La herramienta deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
44. **IAU.3** La herramienta deberá proteger la confidencialidad e integridad de las credenciales de autenticación.
45. **IAU.5** La herramienta debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.

4.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

46. **CRD.1** En el caso en que la herramienta almacene credenciales y/u otros datos sensibles (que serán especificados en la declaración de seguridad), éstos no deberán almacenarse en claro sino utilizando mecanismos criptológicos autorizados en la CCN-STIC-807.

5. VALIDACIÓN DE LOS DOCUMENTOS PRESENTADOS

47. Los requisitos incluidos en este apartado serán evaluados en una evaluación STIC complementaria fuera del alcance de la certificación.

48. **DOC.1** La herramienta implementará mecanismos de detección de ataques de replicación y ataques de impresión.

49. **DOC.2** La herramienta debe ser capaz de verificar que la fecha de validez del documento no ha expirado.

50. **DOC.3** La herramienta deberá comprobar la integridad de los datos de la zona de inspección visual (VIZ) con la MRZ (zona de lectura mecanizada).

51. **DOC.4** La herramienta generará alertas al operador cada vez que detecte alguno de los ataques descritos en **DOC.1** o hayan fallado las comprobaciones de las pruebas **DOC.2** y **DOC.3**.

6. REQUISITOS FUNDAMENTALES DE SEGURIDAD OPCIONALES

52. Los requisitos incluidos en este apartado serán exigidos únicamente en el caso en el que el producto almacene internamente evidencias biométricas y declare implementar mecanismos criptológicos para su protección.

53. Si el producto almacena evidencias pero no implementa mecanismos de seguridad, los requisitos de seguridad podrían ser cubiertos por el entorno en el que está desplegada la herramienta.

54. **CIF.1** La herramienta 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.

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

56. **CIF.3** Generador de bits aleatorios. En caso de suministrar un servicio de generación de bits aleatorios (RBG) determinísticos, el producto deberá:

    - Utilizar *Hash_DRBG (any)* o *HMAC_DRBG (any).*
    - Usar una semilla de al menos una fuente de entropía que acumule entropía de varias fuentes o disponer de una fuente de entropía estudiada, con un mínimo de 256 bits de entropía.

57. **CIF.4** Generación de claves simétricas. En caso de generar claves simétricas, el producto podrá utilizar el RBG definido en CIF.3 o importarlas del entorno operacional envuelta digitalmente. En cualquier caso, todas las claves utilizadas deberán tener una fortaleza mayor o igual a 128 bits.

58. **CIF.5** Generación de claves asimétricas. En caso de generar claves asimétricas, el producto podrá utilizar los siguientes algoritmos:

    - ECC con una longitud de clave de 256 o superior.
    - FFC con una longitud de clave de 3072 o superior.
    - RSA con una longitud de clave de 3072 o superior.

59. **CIF.6** Establecimiento de claves. Para el establecimiento de claves, el producto podrá utilizar los siguientes algoritmos:

    - Esquemas basados en RSA con una longitud de clave de 3072 o superior.
    - Esquemas basados en FFC con una longitud de clave de 3072 o superior.
    - Esquemas basados en ECC con una longitud de clave de 256 o superior.

60. **CIF.7** Algoritmos HASH. Las funciones resumen o HASH que utilice el producto deberán utilizar los algoritmos SHA-2 y SHA-3 de longitud mayor o igual a 256.

61. **CIF.8** Firma digital. Para los servicios de generación/verificación de firma digital, el producto deberá utilizar uno de los siguientes algoritmos:

- *Digital Signature Algorithm (DSA)* con una longitud de clave de 3072 bits o superior.
- *Elliptic Curve Digital Signature Algorithm* (ECDSA) con una longitud de clave de 256 o superior.
- RSA con una longitud de clave de 3072 o superior.

62. **CIF.9** Cifrado de datos y claves con AES. El producto implementará cifrado de datos de acuerdo con el algoritmo AES, los modos CBC, GCM y una longitud de claves 128 bits o superior.
63. **CIF.8** Envoltura digital de claves. El producto podrá implementar envoltura digital de claves utilizando el algoritmo AES, en los modos KW, KWP, CCM, GCM y una longitud de claves 128 bits o superior.
64. **CIF.10** Autenticación de mensajes. Para los servicios de autenticación de mensajes, el producto podrá utilizar HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512.
65. **CIF.11** Destrucción de PSC. El producto deberá borrar todos los PSC que utilice una vez finalice su uso implementando uno de los siguientes métodos de borrado.
    - Para memoria volátil, la destrucción podrá ser realizada utilizando los siguientes métodos:
        i. Una pasada de sobrescritura utilizando alguno de los siguientes métodos:
            1. Un patrón pseudoaleatorio generado por el RBG.
            2. Todo ceros o unos.
            3. Algún valor que no contenga ningún parámetro de seguridad crítico (PSC).
        ii. Destrucción de la referencia a la clave directamente seguida por una llamada al "recolector de basura" de la memoria.
        iii. Apagado de la memoria.
    - Para memoria no volátil:
        - Que emplee un algoritmo de *wear-leveling*, la destrucción deberá consistir en alguno de los siguientes métodos:
            - Una sola pasada de sobrescritura consistente en ceros, unos u otro valor que no contenga ningún PSC.
            - Borrado de bloque.
        - Que no emplee un algoritmo *wear-leveling*, la destrucción deberá ejecutarse por:

- Una o más pasadas de sobrescritura consistente en ceros, unos o algún valor que no contenga ningún CSP seguidos de una lectura de verificación.
- Borrado de bloque.

Y si la lectura de verificación de los datos sobrescritos falla, el proceso deberá ser repetido de nuevo hasta alcanzar un número N (N>1) de intentos en el cual se devuelva un error.

7. ABREVIATURAS

AES	*Advanced Encryption Standard*
CBC	*Cipher Block Chaining*
CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
DSA	*Digital Signature Algorithm*
EAL	*Evaluation Assurance Level*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ENS	Esquema Nacional de Seguridad
FNR	*False Negative Rate*
FPR	*False Positive Rate*
GCM	*Galois Counter Mode*
HMAC	*Keyed-hash Message Authentication Code*
NIAP	*National Information Assurance Partnership*
PAD	*Presentation Attack Detection*
PCS	Parámetro de seguridad crítico
RBG	*Random Bits Generator*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
TOE	*Target of Evaluation*

PUBLICACIONES DE DEFENSA

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