centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

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

Noviembre de 2022

MINISTERIO DE DEFENSA

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

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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
2023.01.03 14:56:49 +01'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-102-1

Fecha de Edición: noviembre 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 y Servicios STIC (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 MEDIA**. 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 experiencia durante la videollamada.

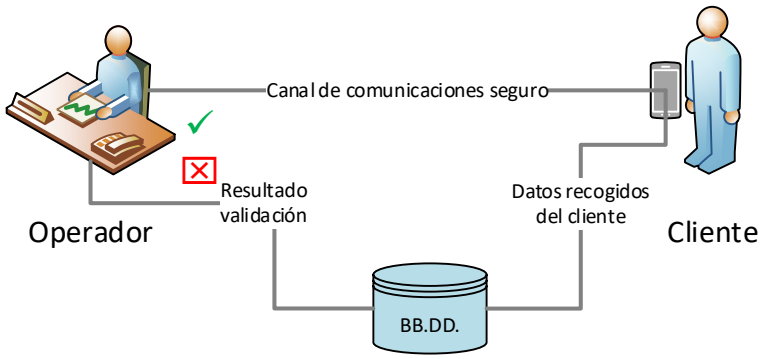

Figura 1 – Ejemplo de Caso de Uso: Proceso Asistido o síncrono

15. Los datos capturados y generados en el lado del cliente, 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.

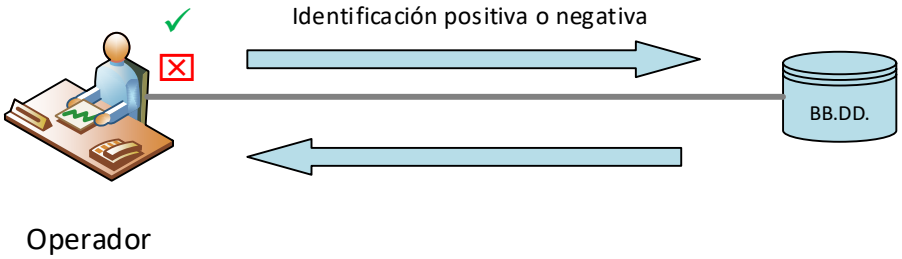

Figura 2 – Ejemplo de Caso de Uso: Proceso desasistido o asíncrono

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

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

19. Se asume que el entorno operacional cumple las siguientes condiciones:

- **Protección física.** El producto debe estar protegido físicamente por su entorno operacional y no sujeto a ataques físicos que puedan comprometer su seguridad o interferir en su correcta operación. En caso de productos software, esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.
- **Administración confiable**. Los administradores son miembros de plena confianza y velan por los mejores intereses en materia de seguridad de la organización. Dichas personas deben estar debidamente capacitadas y carecer de cualquier intención maliciosa o conflicto de intereses al administrar el producto.
- **Actualizaciones periódicas.** El *firmware/software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **Funcionalidad limitada.** El producto solo debe proporcionar la funcionalidad de *identificación mediante video* como función principal y no debe proporcionar ninguna otra funcionalidad o servicio.
- **Protección de las credenciales.** Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.
- **Plataforma confiable**. En caso de tratarse de un producto software, este se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución que la plataforma proporcione.

2.4 DELIMITACIÓN DEL ALCANCE DEL PRODUCTO

20. Estos productos pueden constar de uno o varios componentes, los cuales se presentan en forma de producto *software*.

21. 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.

2.5 CERTIFICACIÓN LINCE

22. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Categoría MEDIA, debe disponer de una **Certificación Nacional Esencial de Seguridad (LINCE) con Módulo de Evaluación Biométrica (MEB)** que incluya 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).

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.

2.5.1. EVALUACIONES

23. 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].
24. 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 ACTIVOS SENSIBLES A PROTEGER

25. Los recursos que deben protegerse mediante el uso de estos productos son:

- **AC.Administración**. Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos, que debe ser protegida en Confidencialidad, Trazabilidad, Autenticidad e Integridad.
- **AC.PSS.** Datos de configuración, registros auditoría y [***asignación****: listado de datos definidos por el fabricante]* que deben ser protegidos en Integridad.
- **AC.PSC**. [**selección**: credenciales; claves; [**asignación**: *listado de datos definidos por el fabricante*] que deben ser protegidos en Confidencialidad e Integridad.
- **AC.Actualizaciones**. Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad, que deben ser protegidos en Integridad y Autenticidad.
- **AC.Comunicaciones.** Comunicaciones del producto, establecidas entre sus propios componentes y con [**asignación**: *listado de entidades autorizadas*] que deben ser protegidas en Confidencialidad, Integridad y Autenticidad.

3.2 AMENAZAS

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

- **A.NOAUT Acceso no autorizado de administrador:** Un atacante puede obtener un acceso de administración no autorizado haciéndose pasar por un administrador ante el producto, haciéndose pasar por el producto ante un administrador, reproduciendo una sesión de administración, o realizando ataques del hombre en medio.
- **A.CRYPTO Mecanismos criptográficos débiles:** Utilización en el producto de mecanismos criptográficos o longitudes de clave débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.COM Protocolos de comunicación no autorizados:** Utilización de protocolos no autorizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones críticas del producto.
- **A.AUD Actividades no detectadas:** Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.

- **A.PSC Compromiso de parámetros de seguridad críticos:** Un atacante puede comprometer los parámetros de seguridad críticos y acceder de forma continuada al producto y a sus datos críticos.
- **A.FUN Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad declaradas del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.
- **A.NOAUTUSR Acceso no autorizado de usuario:** Un atacante puede obtener un acceso no autorizado haciéndose pasar por un usuario ante el producto, haciéndose pasar por el producto ante un usuario, reproduciendo una sesión de usuario, o realizando ataques del hombre en medio.
- **A.CRE Compromiso de credenciales:** Un atacante puede aprovecharse del uso credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.

3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD

27. En la siguiente tabla se trazan que Requisitos Fundamentales de Seguridad definidos en el apartado 4 cubren las amenazas definidas:

	A.NOAUT	A.CRYPTO	A.COM	A.AUD	A.PSC	A.FUN	A.NOAUTUSR	A.CRE
ADM.1	X							
ADM2	X							
ADM.3	X							
IAU.1	X						X	
IAU.2								X
IAU.3								X
IAU.4	X							
IAU.5								X
COM.1		X	X					
COM.2			X					
COM.4		X	X					

	A.NOAUT	A.CRYPTO	A.COM	A.AUD	A.PSC	A.FUN	A.NOAUTUSR	A.CRE
AUD.1				X				
AUD.2				X				
AUD.3				X				
AUD.4				X				
AUD.5				X				
PSC.1					X			
GEN.1						X		
GEN.2						X		
SOL.1						X		
SOL.2						X		
SOL.3						X		
DOC.1						X		
DOC.2						X		
DOC.3						X		
DOC.4						X		

4. REQUISITOS DE SEGURIDAD

28. 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.

29. La convención utilizada en las descripciones de los RFS es la siguiente:

- Selección: se deberá seleccionar al menos una opción de las indicadas en el RFS y se incluirá en la declaración de seguridad. Ejemplo:

  RFS: Administración del producto [**selección***: local; remota*]

  DS: Administración del producto local y remota

- Asignación: se deberá especificar el listado de opciones que sean de aplicación al TOE (podría no haber ninguna). Ejemplo:

  RFS: El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación:** otros usuarios del producto] antes de otorgar acceso.

  DS: El TOE deberá identificar y autenticar a cada usuario administrador, auditor y usuario avanzado antes de otorgar acceso.

4.1 ADMINISTRACIÓN CONFIABLE

30. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

31. **ADM.1** El TOE debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.

32. **ADM.2** El TOE debe ser capaz de realizar la gestión de las siguientes funcionalidades:

- Administración del producto [**selección**: *local; remota*].
- Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
- [**asignación**: otras funcionalidades administrables del producto].

33. **ADM.3** El TOE deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones descritas en **ADM.2**.

> 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 funcionalidades para las que tengan permiso.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

34. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

35. **IAU.1** El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación**: *otros usuarios del producto*] antes de otorgar acceso, salvo para las siguientes funcionalidades [**asignación**: *listado funcionalidades*].

36. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.

37. **IAU.3** El TOE 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 TOE implemente otros mecanismos de autenticación.

38. **IAU.4** El TOE debe [**selección***: bloquear; cerrar*] la sesión de un usuario después de [***asignación****: tiempo de inactividad*] de inactividad.

39. **IAU.5** Cuando el acceso se realice utilizando credenciales por defecto o el usuario no tenga asignadas credenciales, el TOE obligará al [**selección***: cambio; establecimiento*] de credenciales en el siguiente acceso.

4.3 CANALES SEGUROS

40. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

41. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas: [**selección***: servidor de auditoría;* [***asignación****: otras entidades*]] o entre distintas partes del producto, usando [**selección***: IPSec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

42. **COM.2** El TOE debe permitir que los canales de comunicación definidos en **COM.1** sean iniciados por él mismo o por las entidades autorizadas.

43. **COM.4** Protección de la información del canal de administración. El TOE deberá establecer canales seguros cuando intercambie información con el administrador remoto, usando [**selección**: *IPsec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

4.4 AUDITORÍA

44. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

45. **AUD.1** El TOE debe generar registros de auditoría cuando se produzca alguno de los siguientes eventos:

    a) Al inicio y finalización de las funciones de auditoría.

    b) *Login* y *logout* de usuarios registrados.

    c) Cambios en las credenciales de usuarios.

    d) Cambios en la configuración del producto [**asignación**: *listado de cambios*].

    e) Eventos relativos a la funcionalidad del producto [**asignación:** *listado de eventos*].

    f) Si el TOE gestiona claves criptográficas, [**selección:** generación; importación; cambio; eliminación de claves criptográficas; ningún otro].

46. **AUD.2** Los registros de auditoría contendrán al menos la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento.

47. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:

    a) Lectura: usuarios autorizados.

    b) Modificación: ningún usuario.

    c) Borrado: [**selección**: solo administradores; ningún usuario]

48. **AUD.4** El TOE debe ser capaz de almacenar en sí mismo la información de auditoría generada y [**selección**: transmitir la información de auditoría generada a una entidad externa utilizando un canal seguro COM.1; no transmitir la información de auditoría generada].

49. **AUD.5** El TOE deberá [**selección**: sobreescribir los registros siguiendo el criterio de mayor antigüedad; enviar a una entidad externa y eliminar; otra opción validada por el CPSTIC] en el caso de que el espacio para almacenamiento de los registros alcance su límite.

4.5 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

50. **PSC.1** En el caso en que el TOE almacene [***selección**: credenciales; claves privadas; [**asignación**: otros parámetros de seguridad críticos*] estos no deberán almacenarse en claro, sino que se utilizarán mecanismos de protección criptológica que cumplan con **CIF.1**.

4.6 PROTECCIÓN FRENTE A EN LA CAPTURA DE EVIDENCIAS

51. **GEN.1** El TOE 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.
52. **GEN.2** El TOE 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.
53. Nota de aplicación: el fabricante deberá describir en la declaración de seguridad los mecanismos implementados para satisfacer ambos requisitos.

4.7 VERIFICACIÓN BIOMÉTRICA

54. **SOL.1** El TOE deberá proporcionar verificación biométrica facial utilizando la imagen del solicitante y la imagen impresa en el documento de identidad.
55. **SOL.2** El TOE debe implementar medidas técnicas para detectar que la persona está viva a través de pruebas activas o pasivas.
56. **SOL.3** El TOE deberá implementar mecanismos de detección de ataques de presentación biométrica que impidan la verificación exitosa: [***selección**: Presentation Atack Detection;* PAD; *[**asignación**: otros mecanismos]*].
57. **SOL.4** El TOE debe registrar el resultado de los procesos de verificación junto con el motivo de rechazo, en caso de tratarse de un resultado negativo.

5. VALIDACIÓN DE LOS DOCUMENTOS PRESENTADOS

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

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

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

61. **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).

62. **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

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

64. 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.

65. **CIF.1** El TOE permitirá exclusivamente el empleo de mecanismos criptográficos: [***asignación**: listado de mecanismos*] autorizados de acuerdo a lo establecido en la guía CCN-STIC-807. La fortaleza de clave empleada será la indicada en esa guía para Categoría MEDIA del ENS, y de acuerdo al nivel de amenaza establecido.

66. **CIF.2** Generador de bits aleatorios. En caso de suministrar un servicio de generación de bits aleatorios (RBG) determinísticos, el TOE deberá:

    - Utilizar [**selección**: *Hash_DRBG (any), HMAC_DRBG (any) o CTR_DRBG (AES)*].
    - Usar una semilla de, al menos, una fuente de entropía que acumule entropía [**selección**: de una o varias fuentes; una fuente de entropía estudiada], con un mínimo de bits de entropía al menos igual a la mayor fortaleza de seguridad de las claves y hashes que generará, de acuerdo a la ISO/IEC 18031:2011.

67. **CIF.3** Generación de claves simétricas. En caso de generar claves simétricas, el TOE [**selección**: utilizará RBG definido en CIF.2; importará la clave del entorno operacional utilizando un mecanismo de protección de claves (key wrapping) que cumpla CIF.1].

68. **CIF.4** Generación de claves asimétricas. El TOE debe implementar mecanismos de generación de claves asimétricas que cumplan lo indicado en CIF.1.

69. **CIF.5** Acuerdo de claves. El TOE debe implementar mecanismos de acuerdo de claves que cumplan lo indicado en CIF.1.

70. **CIF.6** Funciones Resumen. El TOE debe implementar funciones resumen que cumplan lo indicado en CIF.1.

71. **CIF.7** Firma digital. El TOE debe implementar mecanismos de firma digital que cumplan lo indicado en CIF.1.

72. **CIF.8** Cifrado. El TOE debe implementar mecanismos de cifrado simétrico que cumplan lo indicado en CIF.1.

73. **CIF.9** Protección de claves. El TOE debe implementar mecanismos de protección de claves (*key wrapping*) que cumplan lo indicado en CIF.1.

74. **CIF.10** Autenticación de mensajes. El TOE debe implementar mecanismos de autenticación de mensajes (MAC) que cumplan lo indicado en CIF.1.

75. **PSC.2** Destrucción de PSC. El TOE deberá borrar todos los PSC que utilice una vez finalice su uso implementando uno de los siguientes métodos de borrado.

a) Para memoria volátil, la destrucción podrá ser realizada utilizando los siguientes métodos:

   i. Una pasada de sobrescritura utilizando alguno de los siguientes métodos:

   - Un patrón pseudoaleatorio generado por el RBG.
   - Todo cero o uno.
   - 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.

b) Para memoria no volátil:

   i. 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.

   ii. 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 y Servicios 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*
SOG-IS	*Senior Officials Group Information Systems Security*
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