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 A.2: Dispositivos biométricos

Noviembre 2017

Edita:

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

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
2017.11.27 11:10:33 +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

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Dispositivos biométricos** 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 las 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 **Dispositivos biométricos** 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. Los dispositivos de control de acceso biométricos, permiten realizar un reconocimiento automático de individuos basado en sus características biológicas y de conducta, para lo que implementarán funcionalidades de registro y/o verificación como las que se definen a continuación:

   - **Registro biométrico**. Durante el proceso de registro, el producto captura los datos biométricos de un usuario "en crudo" y extrae los rasgos biométricos con los que trabaja, que se combinan con la identidad del usuario y se almacenan como una plantilla biométrica en una base de datos.

   - **Verificación biométrica.** Durante el proceso de verificación, el usuario introduce su identidad y presenta sus rasgos biométricos en el producto. El producto recupera de la base de datos la plantilla biométrica asociada a la identidad, la compara con las características biométricas extraídas de los rasgos biométricos capturados y genera la similitud entre los dos datos. En base a esta similitud, el usuario es aceptado o rechazado.

7. Algunos ejemplos de modalidades utilizadas por sistemas de reconocimiento biométrico son: huellas digitales, cara, iris, huella de palma de la mano, vena de palma de la mano, vena de dedo, habla, firma, etc.

8. La siguiente figura, inspirada por los estándares ISO/IEC JTC1 SC37 biometrics[1], es una representación genérica de un sistema biométrico (aunque existen otras configuraciones). En ella se ilustran las diferentes funcionalidades en las que se basan los procesos de registro y verificación biométricos.

[1]ISO/IEC JTC 1/SC 37 Biometría es un subcomité de estandarización del Comité Técnico Conjunto número 1(*Joint Technical Committee*) de la Organización Internacional de Estandarización y de la Comisión electrotécnica Internacional (International *Organization for Standardization* (ISO) *and the International Electrotechnical Commission (IEC))* que desarrolla y facilitar estándares en el campo de la biometría. https://www.iso.org/committee/313770.html

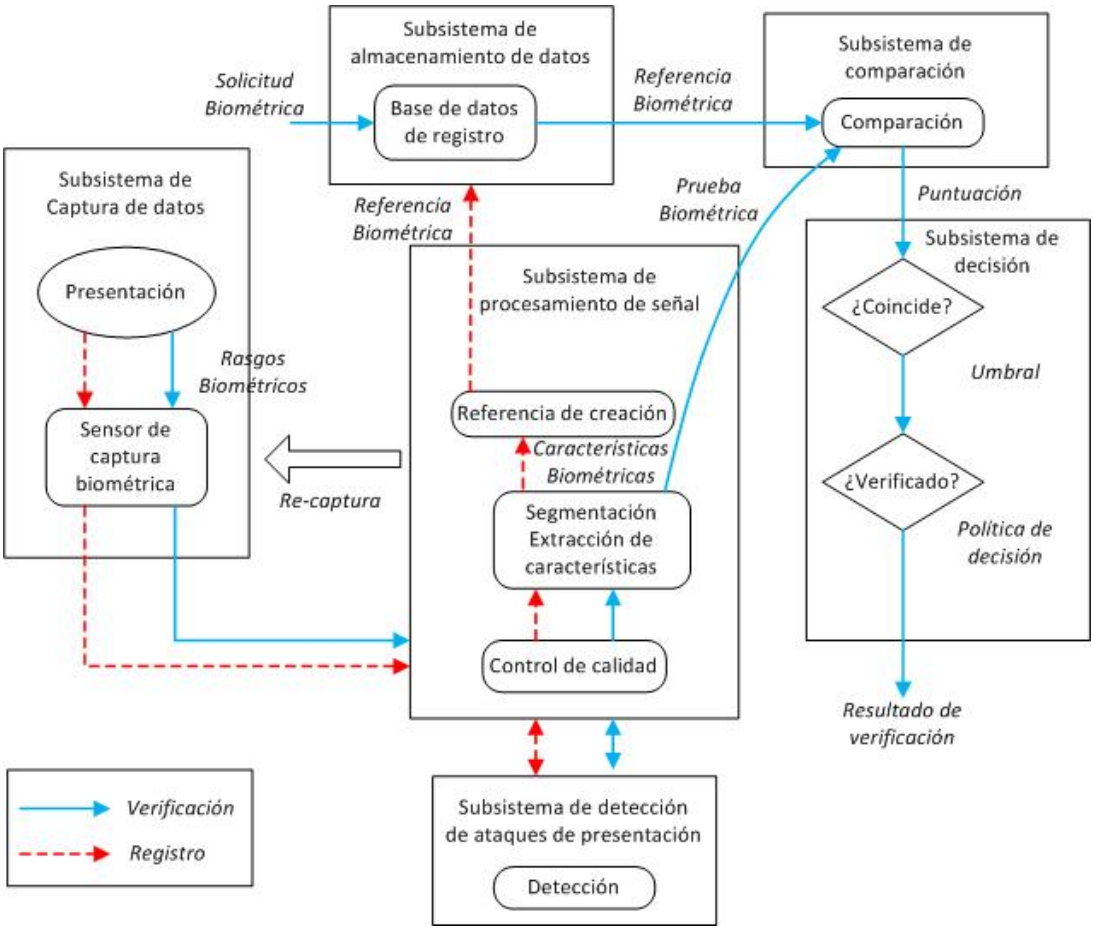

Figura 1 - Esquema de sistema biométrico

9. Cuando se utiliza en un sistema de seguridad, el producto biométrico necesita tener en cuenta el riesgo de que las funcionalidades biométricas sean alteradas. Uno de los puntos de entrada más importantes para un atacante es el subsistema de captura biométrica, donde puede presentar rasgos biométricos artificiales o anormales en el punto de presentación y recogida de las características biométricas, con objeto de interferir con la política del sistema.

10. Esto se recoge en la norma ISO/IEC 30107-1:2016[2], donde se define como ataque de presentación: "la presentación de datos biométricos al subsistema de captura con el objeto de interferir en la operación del sistema biométrico".

11. Esto puede llevarse a cabo presentando al sistema un artefacto o una característica humana, que se denominan instrumentos de ataque de presentación.

12. Por otra parte, se denomina Detección de Ataque de Presentación[3] (PAD, en sus siglas en inglés) a la determinación automática de un ataque de presentación. El subsistema PAD juega in papel importante en la seguridad de los dispositivos biométricos, especialmente cuando no están supervisados.

[2]https://www.iso.org/standard/53227.html
[3]PAD *Presentation Attack Detection*

2.2 CASOS DE USO

13. Los productos biométricos son utilizados para la autenticación de usuarios en dispositivos móviles como teléfonos inteligentes (*smartphones*) registro de usuarios en ordenadores (*login)*, accesos a cajeros automáticos en bancos, control de entrada de edificios o estancias, o controles de seguridad de fronteras.
14. De acuerdo a su configuración, se distinguen dos tipos de caso de uso de productos biométricos: integrados y separados.

2.2.1. CASO DE USO 1 – TIPO INTEGRADO

15. En el tipo integrado los componentes de los productos biométricos no están físicamente separados, p. ej.: los componentes no están conectados utilizando cables USB o de red.

2.2.2. CASO DE USO 2 – TIPO SEPARADO

16. En el tipo separado los componentes de los productos biométricos están físicamente separados, p. ej.: los componentes están conectados utilizando cables USB o redes.

2.3 ENTORNO DE USO

17. Para la utilización en condiciones óptimas de seguridad de estos productos, es necesaria su integración en un entorno operacional que cumpla las siguientes condiciones:
    - **Administración confiable:** El Administrador (si existe) será un miembro de plena confianza y estará capacitado y formado.
    - **Protección de las comunicaciones.** Las comunicaciones entre la base de datos y el producto deberán estar protegidas.
    - **Entorno controlado.** Se asumirá que el producto se usará en un entono controlado y observable (p.ej.: los ataques que requieran mucho tiempo, acceso repetido durante la fase de explotación o uso de herramientas complejas (en el sentido de herramientas visibles y aparatosas) no se consideran realizables).

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

18. El alcance estará definido por el hardware, firmware[4], software y funcionalidades de seguridad del producto biométrico.

[4] *Firmware* funciona como el nexo de unión entre las instrucciones (*software*) que llegan al dispositivo desde el exterior y las diversas partes electrónicas (*hardware*)

19. Todas las funcionalidades de seguridad están contenidas y ejecutadas dentro del alcance del dispositivo biométrico.

    Algunos casos típicos de dispositivos biométricos son:

    - Producto completamente integrado.
    - Producto software.
    - Producto basado en sensores de detección de ataque de presentación.

20. Las siguientes figuras muestran un ejemplo de cada uno de estos casos. Los bloques sombreados son los que se incluyen dentro del producto.

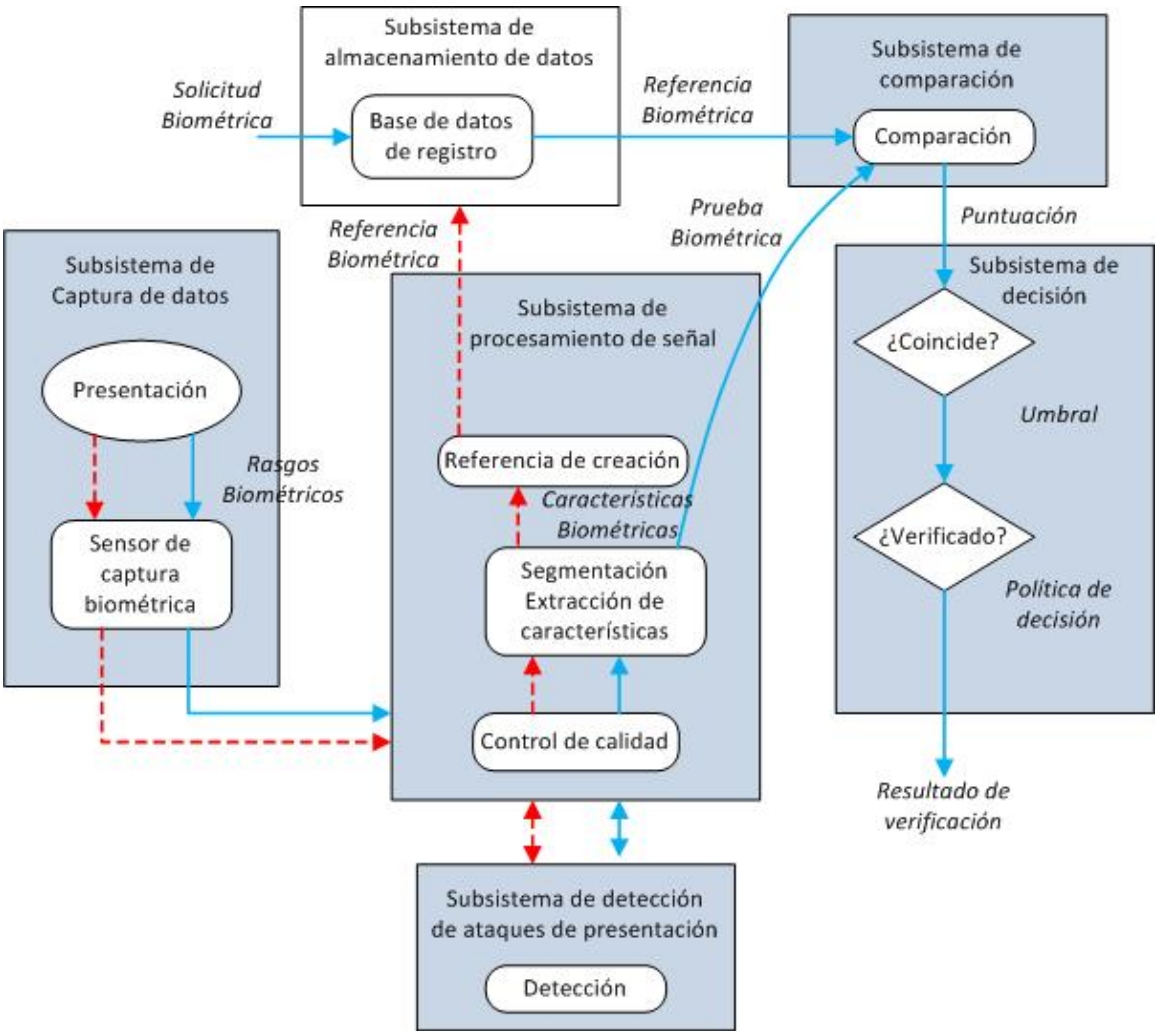

Figura 2 – Esquema de producto completamente integrado

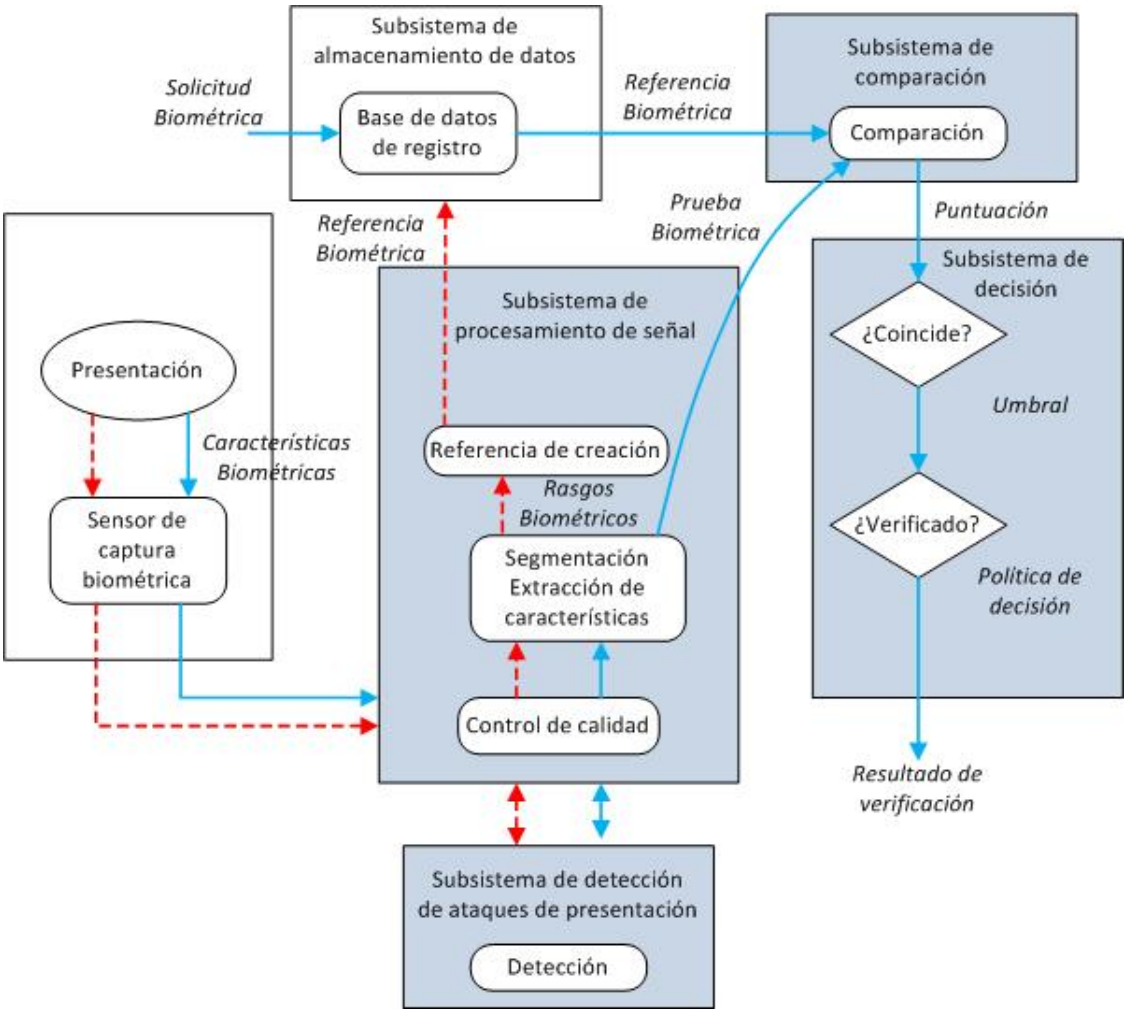

Figura 3 – Esquema de producto íntegramente software

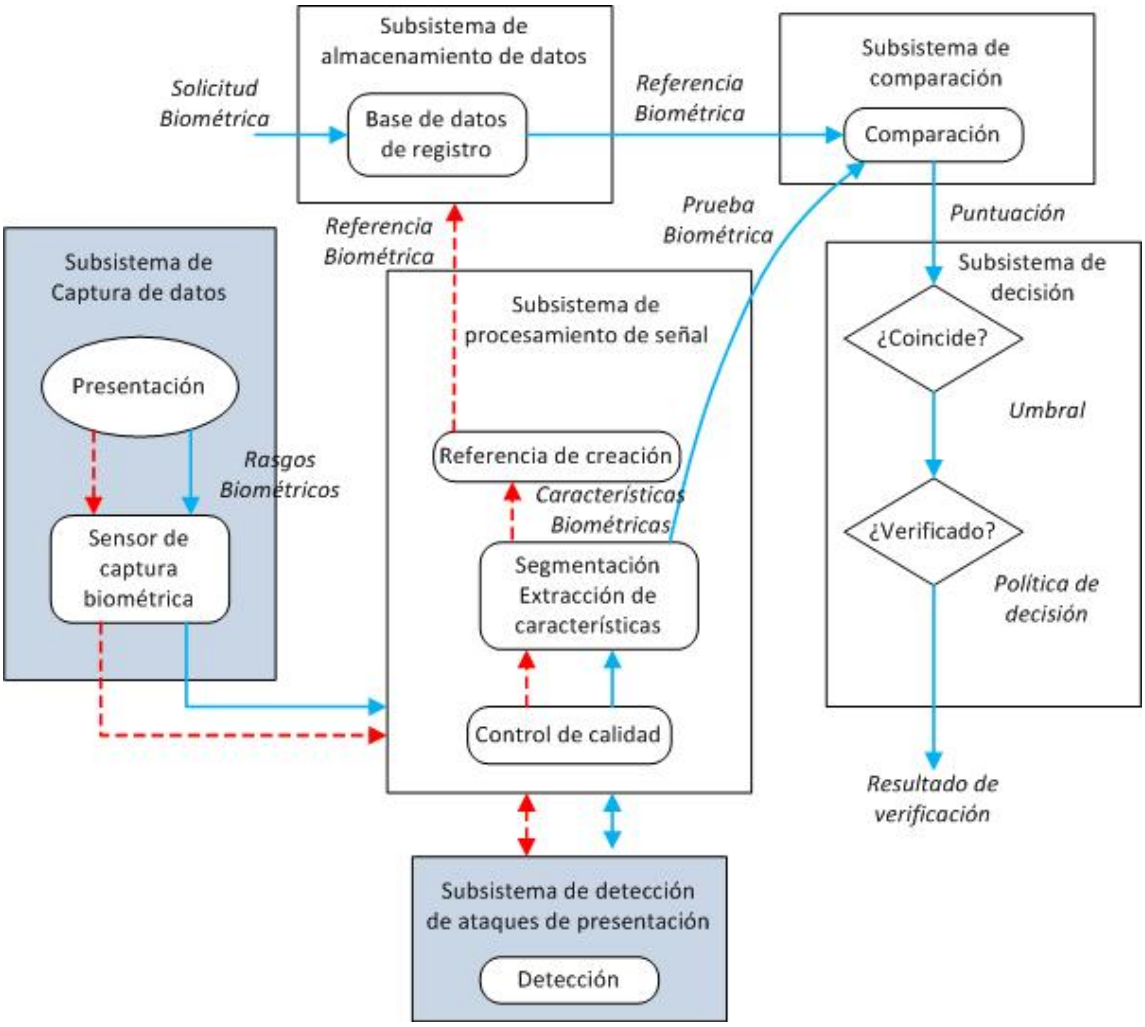

Figura 4 – Esquema de producto basado en sensores de detección de ataque de presentación

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

21. El estándar *Common Criteria*(CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).
22. En el ámbito de CC se elaboran unos *Essential Security Requirement* (ESR) que definen, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de seguridad, independientes de la implantación.
23. Los RFS recogidos en el presente documento están basados en los siguientes ESR:
    - *Biometric Product Essential Security Requirements v1.0* (10-Nov.-2016)[5].
24. Desarrollados por el CCDB Working Group for Biometric Product Security, una comunidad técnica del ámbito del Common Criteria.

[5]https://www.commoncriteriaportal.org/communities/bio-esr.pdf

25. 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 EAL2 o superior**.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

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

    - Cualquier activo al que los usuarios tengan acceso después de una verificación biométrica exitosa.
    - Características biométricas, plantillas y parámetros relacionados con la seguridad, como el valor umbral que se usa y se referencia para la verificación biométrica.
    - Datos de los registros (*logs*) producidos por el sistema biométrico (si son generados por el sistema biométrico).

3.2 AMENAZAS

27. Las principales amenazas a las que estaría expuesto el producto son:

    - Un atacante puede presentar algunos rasgos biométricos e intentar ser verificado incorrectamente como un usuario genuino.
    - Un atacante puede presentar algunos rasgos biométricos con objeto de enmascarar su propia identidad durante los procesos de registro o identificación.
    - Un atacante puede presentar cualquier tipo de instrumentos de ataque de presentación durante el registro y verificación biométrica con objeto de suplantar una identidad. (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).
    - Un atacante puede presentar cualquier tipo de instrumentos de ataque de presentación con el objetivo de enmascarar su propia identidad durante los procesos de registro o verificación.
    - Un atacante puede desarrollar cualquier tipo de ataque físico o lógico con objeto de enmascarar su propia identidad durante los procesos de verificación o registro con el objetivo de suplantar una identidad.

28. Para ello, el atacante deberá contar con los siguientes recursos:

    - Una cantidad de tiempo arbitraria para examinar y atacar el producto biométrico, en particular para elaborar rasgos biométricos artificiales y presentarlos al producto.
    - Software/conocimiento/equipamiento disponible comercialmente y/o públicamente y, además si está disponible comercialmente, muestras del producto biométrico para probar y atacar.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

29. 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 REQUISITOS OBLIGATORIOS

30. **REQ.1.** El producto biométrico registrará usuarios con una tasa de error menor a una exigida. (p.ej.: Tasa de fallos en el registro o FTE[6])

31. **REQ.2.** El producto biométrico verificará usuarios con una tasa de error menor que una exigida. (p.ej.: Tasa de falsos aceptados o FAR[7] y Tasa de falsos rechazados o FRR[8]).

32. **REQ.3.** El producto biométrico deberá prevenir el registro y la verificación exitosa cuando se usen instrumentos de ataque de presentación.

33. **REQ.4.** El producto biométrico deberá hacer frente a ataques lógicos y físicos.

4.2 REQUISITOS OPCIONALES

34. Los requisitos recogidos en esta sección no serán exigibles, a pesar de que algunos productos de esta tecnología ya los implementan:

35. **REQ.5.** Los productos biométricos evitarán el registro de usuarios cuyas características biométricas extraídas de sus rasgos biométricos y su plantilla biométrica ya almacenada se haya determinado que son del mismo usuario.

36. **REQ.6.** El producto biométrico deberá asegurar comunicaciones seguras con la base de datos.

37. **REQ.7.** El producto biométrico deberá proteger la base de datos contra modificaciones o espionaje.

[6] *Failure To Enroll*
[7] *False Accept Rate*
[8] *False Reject Rate*

5. ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
EAL	*Evaluation Assurance Level*
ESR	*Essential Security Requirements*
FAR	*False Accept Rate*
FRR	*False Reject Rate*
FTE	*Failure To Enroll*
PAC	*Presentation Attack Detection*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
SW	Software
USB	*Universal Serial Bus*