centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo E.6: Módulo de Seguridad Hardware (HSM)

Octubre 2021

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 15:56:55 +01'00'

NIPO: 083-21-130-1.

Fecha de Edición: octubre de 2021.

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 **Módulo de Seguridad Hardware (HSM)** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos y Servicios 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 **Módulo de Seguridad Hardware (HSM)**, 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. Un Módulo de Seguridad Hardware (en inglés *Hardware Security Module*, **HSM***)* es un dispositivo criptográfico basado en *hardware* que genera, almacena y protege claves criptográficas y suele aportar aceleración *hardware* para operaciones criptográficas.

7. Uno de los mayores problemas derivados del uso de la criptografía, es la complejidad de la gestión del ciclo de vida de las claves criptográficas. Debido a que la seguridad del sistema criptográfico recae, en gran parte, en la seguridad de la clave, esta debe ser gestionada de la manera **más segura** posible. Actualmente, la alternativa más recomendable para realizar dicha gestión segura de las claves criptográficas son los productos HSM.

8. En los últimos años, debido a la creciente migración de las organizaciones a un entorno digital, los proveedores han creado soluciones HSM basadas en la nube (*HSM As a Service*), permitiendo hacer uso de la funcionalidad HSM necesaria, sin requerir un mantenimiento específico del dispositivo *hardware* por parte del usuario. Los usuarios adquieren una suscripción únicamente para las funcionalidades que van a requerir, teniendo la posibilidad de aumentar o disminuir dicha suscripción. Además, los proveedores no cuentan con acceso a la información almacenada por parte del usuario, solo se encargan del mantenimiento, actualizaciones y copias de seguridad del HSM, sin tener acceso a los datos del usuario.

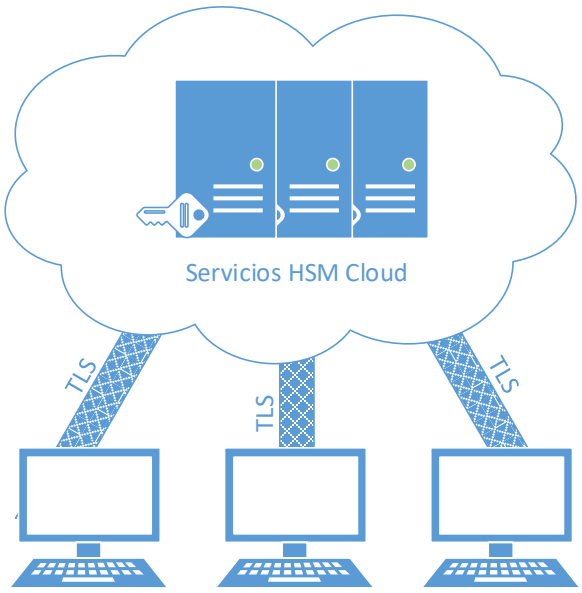

Figura 1. ***HSM-as-a-Service***

9. El **criptoprocesador** es el componente principal de un dispositivo HSM. Este permite la realización de las operaciones criptográficas de manera más eficiente y rápida, a diferencia del resto de dispositivos *hardware*. Además, es el encargado de generar dos (2) tipos diferentes de claves: **claves maestras** y **claves de datos**. Las claves de datos son las que se utilizan para cifrar los datos, mientras que las claves maestras se usan para proteger (cifrar) las claves de datos.

10. A parte de dicho criptoprocesador, estos dispositivos cuentan, de manera general, con los siguientes componentes:

    a) **Servicios de seguridad**, encargados de realizar el resto de funciones de seguridad no criptográficas del HSM, como por ejemplo, la autenticación de usuarios.

    b) **Memoria no volátil**, donde se almacenan de manera segura las claves maestras, la configuración y otros datos sensibles del HSM.

    c) ***Firmware* y componentes *hardware* generales,** como procesador, la memoria RAM, la caché, entre otros.

    d) **Interfaz y control.** Componente a través del cual el HSM se comunica con las aplicaciones y servicios externos.

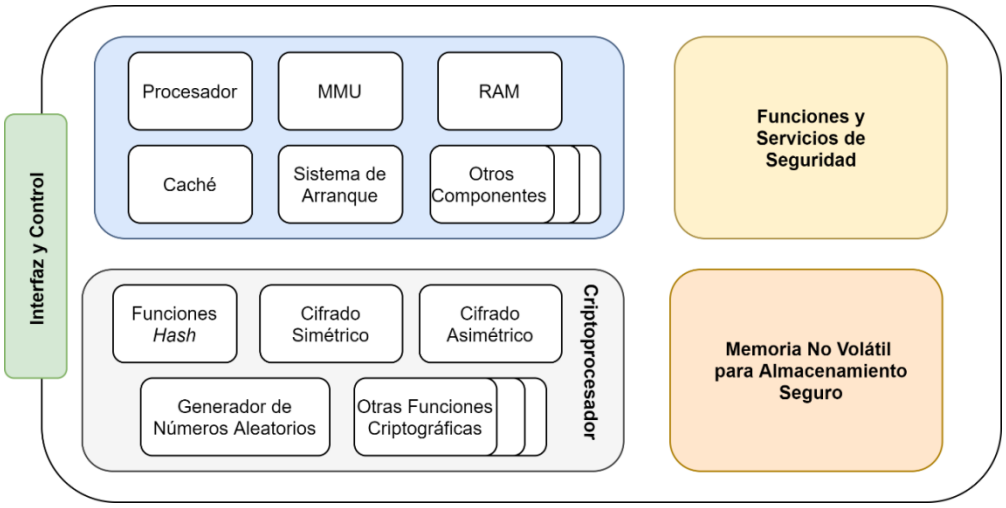

Figura 2. Arquitectura general de HSM.

11. Algunas de las características de los productos HSM son las siguientes:

    - **Alta seguridad física.** Los dispositivos HSM cuentan con un nivel alto de seguridad física frente a amenazas externas. Son *tamper-resistant*, para evitar la captura de señales internas del dispositivo por usuarios no autorizados.
    - **Gestión del ciclo de vida de las claves criptográficas.** Permiten la creación, gestión y mantenimiento de las credenciales a lo largo de su ciclo de vida.

- Comprobación de la integridad de las funciones de seguridad y criptográficas.

2.2 CASOS DE USO

12. Dada la naturaleza y el objetivo de este tipo de productos, se contemplan dos (2) casos de uso para esta familia, tal y como se indica a continuación.

2.2.1. CASO DE USO 1: HSM INDEPENDIENTE

13. Un HSM Independiente es un dispositivo físicamente protegido que integra e interconecta varios chips IC (Circuitos Integrados). Este tipo de HSM funciona de forma independiente.

2.2.2. CASO DE USO 2: HSM INTEGRADO

14. Un HSM integrado es un dispositivo que integra e interconecta varios chips IC y que puede no disponer de protección física. Este tipo de HSM se puede integrar con otros equipos que son los que le protegen físicamente. El HSM integrado puede, por ejemplo, ser una tarjeta criptográfica dedicada.

2.3 ENTORNO DE USO

15. Para la utilización en condiciones óptimas de seguridad del HSM, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Administración confiable:** Los usuarios administradores serán miembros de plena confianza y que velan por los mejores intereses en materia de seguridad de la organización. Dichas personas deberán estar debidamente capacitadas y carecerán de cualquier intención maliciosa o conflicto de intereses al administrar el producto.
    - **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.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

16. Este tipo de productos se presentan en formato *hardware* provisto de un firmware y/o software con las funcionalidades necesarias para cumplir su finalidad y acotadas al servicio específico que presten.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (*COMMON CRITERIA*)

17. 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).

18. 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*).
19. Los productos dentro de esta familia, deberán disponer de una declaración de seguridad (ST) certificada con un nivel de confianza EAL2 o superior (*Evaluation Assurance Level*), que contenga los SFR indicados en el apartado 4.
20. En caso de que alguno de los requisitos indicados anteriormente no se encuentre recogido en la declaración de seguridad del producto, pero este 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

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

- Comunicaciones con el producto.
- Claves criptográficas y otros parámetros de seguridad críticos (CSP) almacenados por el producto.
- Datos de configuración del producto y de auditoría generados por éste.
- Información de usuarios y/o de la organización almacenada en el producto.
- Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

22. 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 entre el producto y otras entidades autorizadas o entre los distintos módulos del producto.
- **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 puede acceder a información sensible almacenada en la plataforma en la que se instala y ejecuta el producto.
- **A. SEG. Acceso a las funciones de seguridad.** Un atacante podría acceder y modificar las funciones y datos de seguridad del 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.FIS. Acceso físico no autorizado**. Un atacante podría intentar obtener información sensible a través de un acceso físico al dispositivo, comprometiendo la disponibilidad de la información almacenada y de los servicios prestados.
- **A.FAIL. Fallo de la funcionalidad de seguridad.** Un componente del producto puede fallar durante el proceso de arranque o durante la

operación, provocando el compromiso o fallo de la funcionalidad de seguridad, y dejando al producto expuesto a posibles atacantes.

- **A.CRED. Acceso a claves criptográficas**. Un atacante o usuario no autorizado puede intentar acceder y atacar el dispositivo HSM para obtener las credenciales y claves criptográficas almacenadas por el producto.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

23. 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 ADMINISTRACIÓN CONFIABLE

24. Estas funcionalidades de seguridad mitigan la amenaza (A.SEG).
25. **ADM.1** El producto debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.
26. **ADM.2** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades:
    - Administración del producto de forma local (en caso de que se instale dentro de la red de la organización) y remota.
    - Configuración del tiempo de terminación de sesión o bloqueo, al detectar inactividad.
    - Desbloquear el acceso a causa de fallos en la autenticación o autorización.
    - Modificar atributos de las claves.
    - Otros parámetros de configuración del producto.
27. **ADM.3** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones anteriormente descritas (ADM.2).
28. **ADM.4** Para la administración remota, se utilizará un protocolo de comunicaciones que esté de acuerdo con lo indicado en el requisito COM.1 para el establecimiento del canal de comunicación seguro. Además, se deberá permitir que el administrador remoto inicie la comunicación a través de dicho canal seguro.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

29. Estas funcionalidades de seguridad mitigan la amenaza (A.REST, A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
30. **IAU.1** El producto deberá identificar y autenticar a cada usuario antes de otorgar acceso.
31. **IAU.2** El producto deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
32. **IAU.3** El producto deberá proteger de lectura y modificación no autorizada las credenciales de autenticación.

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

4.3 AUDITORÍA

34. Estas funcionalidades de seguridad mitigan la amenaza (A.NODET).
35. **AUD.1** El producto deberá generar registros 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) Cambios en la configuración de usuarios.
    c) Cambios en la configuración del producto.
    d) Eventos relativos a la funcionalidad del producto. Al menos: generación, destrucción, importación, exportación y modificación de claves criptográficas.
    e) Detección de una intrusión, ataque físico.
36. **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 (si aplica).
37. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: Sólo usuarios autorizados.
    b) Modificación: Ningún usuario.
    c) Borrado: solo administradores.
38. **AUD.4** El producto deberá ser capaz de almacenar la información de auditoría generada en sí mismo o en una entidad externa.
39. **AUD.5** El producto deberá ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno.

4.4 CANAL SEGURO

40. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
41. **COM.1** Protección de la información en tránsito. El producto deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas empleando funciones, algoritmos y protocolos que estén de acuerdo con lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).
42. **COM.2** El producto debe permitir que estos canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

43. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL, A.SEG).
44. **ACT.1** El producto ofrecerá la posibilidad de consultar la versión actual del *firmware/software*, iniciar actualizaciones manualmente y comprobar si existen nuevas actualizaciones disponibles.
45. **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.
46. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

4.6 PROTECCIÓN FÍSICA

47. Estas funcionalidades de seguridad mitigan la amenaza (A.FIS).
48. **HDW.1** El producto deberá:
    a) Implementar mecanismos que evidencien el intento de apertura (*tamper-evidence*) ante un intento de acceso no autorizado.
    b) Implementar encapsulado opaco que impida la observación directa o manipulación del módulo criptográfico.
    c) Ser capaz de determinar cuándo ha ocurrido un intento de apertura (*tamper-evidence*).
    d) Mantener las funcionalidades de seguridad ante un ataque de intento de apertura.
49. **HDW.2** Si el producto cuenta con agujeros de ventilación, puertas o aberturas que permitan el acceso físico al interior, estos se deberán diseñar de forma que no sea posible obtener información sobre los componentes internos del módulo criptográfico mediante la observación directa.

4.7 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

50. Estas funcionalidades de seguridad mitigan la amenaza (A.FAIL).
51. **PRO.1** El producto deberá implementar auto chequeos que verifiquen: la integridad del *software/firmware*, la correcta operación de los mecanismos criptográficos y otras funciones críticas, si procede. Estos auto chequeos deberán ejecutarse durante el arranque del dispositivo, periódicamente durante la operación, y a petición del usuario.
52. **PRO.2** El producto debe preservar un estado seguro cuando cualquiera de los auto chequeos falle.

4.8 REQUISITOS CRIPTOGRÁFICOS

53. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST). Los siguientes requisitos aplican en función de las operaciones criptográficas que lleve a cabo el producto.

54. **CIF.1** El producto permitirá exclusivamente el empleo de funciones, algoritmos y protocolos criptográficos que estén incluidas entre las autorizadas para categoría ALTA del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.

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

    a) Utilizar Hash_DRBG (any), HMAC_DRBG (any) o CTR_DRBG (AES).

    b) 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 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.

56. **CIF.4** Generación de claves asimétricas. En el caso de generar claves asimétricas, el producto podrá utilizar los siguientes algoritmos:

    a) ECC con una longitud de clave de 256 o superior.

    b) FFC con longitud de clave de 3072 o superior.

    c) RSA con longitud de clave de 3072 o superior.

57. **CIF.5** Establecimiento de claves. Para el establecimiento de claves, el producto podrá utilizar los siguientes algoritmos:

    a) Esquemas basados en RSA con una longitud de clave de 3072 o superior.

    b) Esquemas basados en FFC con una longitud de clave de 3072 o superior.

    c) Esquemas basados en ECC con una longitud de clave de 256 o superior.

    d) Esquemas basados en DH grupos 15, 19, 20, 21, 28, 29 o 30.

58. **CIF.6** 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.

59. **CIF.7** Firma digital. Para los servicios de verificación de firma digital, el producto deberá utilizar uno de los siguientes algoritmos:

    a) *Digital Signature Algorithm* (DSA) con una longitud de clave de 3072 bits o superior.

    b) *Elliptic Curve Digital Signature Algorithm* (ECDSA) con una longitud de clave de 256 o superior.

    c) RSA con una longitud de clave de 3072 o superior.

60. **CIF.8** Cifrado de datos y claves con AES. El producto implementará cifrado de datos de acuerdo con el algoritmo AES en los modos CBC, GCM, XTS y longitud de claves 128 bits o superior.

61. **CIF.9** Autenticación de mensajes. Para los servicios de autenticación de mensajes, el producto podrá utilizar HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 y HMAC-SHA-512.

62. **CIF.10** El producto deberá implementar los siguientes métodos de borrado de claves:

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

        - Un patrón de sobrescritura de una pasada utilizando un patrón pseudoaleatorio generado por el RBG del producto o algún valor que no contenga ningún parámetro de seguridad crítico (PSC).
        - Destrucción de la referencia a la clave directamente seguida por una llamada al "recolector de basura" de la memoria.

    b. Para memoria no volátil:

        - Que emplee un algoritmo de *wear-leveling*, la destrucción deberá consistir en alguno de los siguientes métodos:

            1. Una pasada de sobrescritura utilizando alguno de los siguientes métodos:
                a. Un patrón pseudoaleatorio generado por el RBG.
                b. Algún valor que no contenga ningún parámetro de seguridad crítico (PSC).
            2. Borrado de bloque.

        - Que no emplee un algoritmo *wear-leveling*, la destrucción deberá ejecutarse por:

            1. Una o más pasadas de sobrescritura que no contenga ningún CSP seguidos de una lectura de verificación.
            2. Borrado de bloque.

    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.

63. **CIF.11** Destrucción del material criptográfico. Todos los parámetros intermedios y claves criptográficas serán destruidas cuando finalice su uso, utilizando los métodos de borrado seguro establecidos.

64. **CIF.12** Generación de claves simétricas. Las claves simétricas generadas por el producto se obtendrán utilizando el RBG especificado, con longitud mayor o igual a 128 bits.

65. **CIF.13** Envoltura digital de claves. Para la implementación de envoltura digital de claves, el producto podrá utilizar AES en los modos KW, KWP, GCM, CCM, con longitud de claves de 128 bits o superior.

66. **CIF.14** Generación de *salt*, *nonce* y vector de inicialización.

    a) Las *salt* utilizadas por el producto serán generadas por un DRBG propio o suministrado por la plataforma que cumpla el requisito CIF.3.

    b) En el caso de que el producto utilice *nonce*, estos deberán ser únicos y con una longitud mínima de 64 bits.

    c) El producto creará los vectores de inicialización de la siguiente manera:

    d) Para el modo CBC: los vectores de inicialización deberán ser no repetidos.

    e) Para el modo CCM: los *nonce* deberán ser no repetidos.

    f) XTS: No utilizará vectores de inicialización. Los Tweak Values deberán ser enteros no negativos, asignados consecutivamente y comenzando por un entero no negativo arbitrario.

    g) GCM: Los vectores de inicialización deberán ser no repetidos. El número de invocaciones de GCM no excederá de 2^{32} para una clave secreta dada.

4.9 REQUISITOS HSM

67. Estas funcionalidades de seguridad mitigan las amenazas (A.CRED, A.REST).

68. **HSM.1** Las claves secretas o privadas no estarán disponibles en texto plano fuera de la frontera del producto. Esto incluye la protección de las claves durante su generación, almacenamiento y uso en las funciones criptográficas, y significa que incluso los usuarios autorizados para el acceso a estas claves o los administradores no pueden acceder al valor en claro de la clave secreta o privada.

69. **HSM.2** Transmisión, importación y exportación de claves. Las claves secretas o privadas solo podrán importarse, exportarse o transmitirse cifradas o envueltas y a través de un canal seguro (con protección de integridad y autenticación). Para las claves públicas se garantizará la integridad.

70. **HSM.3** El producto deberá permitir establecer políticas de control de acceso granulares para especificar las acciones (uso, acceso, borrado,…) permitidas a los usuarios (sujetos) sobre las claves (objetos) o sobre funciones relacionadas con ellas (por ejemplo, *backups*, modificación de atributos, etc.).

71. **HSM.4** El producto deberá reautenticar al usuario para el acceso a la clave privada bajo las siguientes condiciones:

    a) Después de expirar el tiempo establecido cómo atributo en las claves privadas.

b) Después de superar un número de usos establecido cómo atributo en las claves privadas.

c) Después de revocar una autorización para acceder a la clave privada.

d) Otras condiciones particulares definidas por el fabricante.

72. **HSM.5** Protección de la integridad de las claves almacenadas. El producto debe disponer de mecanismos que detecten la existencia de un error de integridad en las claves de usuario almacenadas en contenedores, en cuyo caso debe impedir el uso de los datos alterados, reportando el error.

73. **HSM.6** Cualquier operación de *backup* o restauración debe preservar la confidencialidad e integridad de las claves privadas o secretas, y la integridad de las claves públicas.

74. **HSM.7** El producto debe utilizar un RBG (*Random Bit Generator*)[1] de tipo físico, no físico, determinista o híbrido para suministrar bits, octetos de bits o números. En caso de que el RBG sea determinista, deberá cumplir los requisitos indicados en CIF.3.

5. NOTAS DE APLICACIÓN

75. 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. En este caso, se considerará que el requisito ***no aplica***.

76. Lo anterior no es válido en caso de que tal funcionalidad solicitada en un requisito, sea proporcionada por un componente del producto que no forma parte de la configuración evaluada. En este caso ***sí aplica***, y el fabricante deberá demostrar el correcto cumplimiento del requisito por parte del producto.

[1] RBG Físico: se basa en una fuente de ruido basada en procesos aleatorios físicos.
RBG No físico: se basa en una fuente de ruido basada en procesos aleatorios no físicos, como interacciones humanas (movimientos de ratón, pulsaciones de teclado, etc.)
RBG Determinista: utiliza una semilla aleatoria para producir una salida pseudoaleatoria.
RBG Híbrido: combina los principios del RBG físico y determinista.

6. 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
HSM	*Hardware Security Module*
IC	Circuitos Integrados
NIAP	*National Information Assurance Partnership*
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