Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo I.3: Control de acceso físico

Julio de 2026

Edita:

Centro Criptológico Nacional, 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.07.22 09:02:29 +02'00'

Fecha de Edición: julio de 2026

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Control de acceso físico** 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 **Categorías Media y 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 ***Control de acceso físico*** 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. Este tipo de sistemas están diseñados para gestionar, controlar y registrar el acceso de personas a espacios físicos protegidos, mediante la evaluación de credenciales y la aplicación de políticas de autorización definidas.
7. Suelen estar compuestos de varios componentes, tanto *hardware* como *software*:
    a) **Lectores RFID**: se comunican con las *smartcards* usadas por los usuarios para acceder a los espacios protegidos, a las que identifican y autentican a través de varios factores (sobre todo, claves y PINs).
    b) **Unidades de control de acceso (UCA)**: autorizan o deniegan el acceso de los usuarios (previamente autenticados de forma exitosa) a los espacios protegidos, basándose en la política de control de acceso previamente configurada a través del software de gestión.
    c) **Software de gestión**: permiten la configuración y administración del sistema, centrándose sobre todo en la configuración de la política de control de accesos a implementar en las UCAs. Además, suelen permitir otras funcionalidades como la gestión del ciclo de vida de las credenciales y claves, la revocación de permisos o la renovación de *smartcards*.

2.2 CASOS DE USO

8. Independientemente de la zona concreta donde se instale el sistema, se contempla un único caso de uso.

2.2.1. CASO DE USO 1 – CONTROL DE ACCESOS CENTRALIZADO

9. El sistema permite el acceso a la zona protegida si el usuario se identifica y autentica de forma exitosa, y la política de control de accesos autoriza su acceso.
10. Las políticas de control de accesos se configuran de forma centralizada, a través del software de gestión, y son aplicadas a los distintos sistemas que protegen las zonas protegidas. En caso de haber más de una zona protegida, el sistema permitirá la aplicación de políticas distintas a cada una de las zonas a proteger.

Figura 1: Caso de uso 1 - Control de accesos centralizado

2.3 DELIMITACIÓN DEL ALCANCE DEL PRODUCTO

11. Tal y como se describe en el apartado 2.1, este tipo de sistemas suelen estar compuestos de varios componentes, los cuales pueden presentarse de diferentes formas:

    a) **Lectores RFID**: se presentan como dispositivos *hardware* o *appliances* provisto de *firmware* y *software* dedicados.

    b) **Unidades de control de acceso (UCA)**: pueden presentarse como *hardware* o *appliances* provisto de firmware y software dedicados, **máquina virtual** (el hipervisor sobre el que corra el producto no formará parte del alcance de la certificación) o **aplicación *software***.

    c) **Software de gestión**: puede presentarse como **máquina virtual** (el hipervisor sobre el que corra el producto no formará parte del alcance de la certificación), **aplicación *software*** o **SaaS**.

12. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, estas quedan fuera del alcance analizado, y deberán ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

3. INCLUSIÓN EN EL CPSTIC

3.1 PRODUCTOS

3.1.1. ENS CATEGORÍA MEDIA

13. Para que un **producto** de esta familia pueda ser incluido en el CPSTIC bajo la categoría Media del ENS, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)[1] que incluya los RFS reflejados en el apartado 5, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.
14. El alcance de la evaluación deberá incluir el módulo de evaluación básico de 25 días de esfuerzo. Los módulos de Evaluación Criptográfica (MEC) y de Revisión de Código Fuente (MCF) serán opcionales.
15. Adicionalmente, la realización de una Evaluación de Mecanismos Criptográficos nacional (MEMeC) de nivel CL1 se considerará equivalente a incluir el módulo de Evaluación Criptográfica (MEC) bajo el alcance de la evaluación.

3.1.2. ENS CATEGORÍA ALTA

16. Para que un **producto** de esta familia pueda ser incluido en el CPSTIC bajo la categoría Alta del ENS, deberá estar certificados de acuerdo a la norma *Common Criteria*. Dicha certificación deberá evidenciar el problema de seguridad definido en el presente documento e incluir los Requisitos Fundamentales de Seguridad recogidos en el apartado 6. Consulte el apartado 8 para verificar la trazabilidad entre los Requisitos Fundamentales de Seguridad recogidos en el apartado 6 y los SFRs de los principales perfiles de protección de Common Criteria aplicables a este tipo de productos.
17. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:
    a) **El determinado por el perfil de protección** para aquellos SFR incluidos en los perfiles exigidos cuando los productos se encuentren certificados contra alguno de los perfiles anteriormente descritos.
    b) **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra ningún perfil.
18. En caso de que alguno de los requisitos indicados en el apartado 6 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.

[1] Toda la información relativa a esta metodología se encuentra disponible en la web del Organismo de Certificación (https://oc.ccn.cni.es)

3.2 PRODUCTOS DESPLEGADOS EN LA NUBE

19. Para que un **producto desplegado en la nube** de esta familia pueda ser incluido en el CPSTIC, deberá superar una Evaluación de Productos en la nube (CICLON) que incluya los RFS reflejados en el apartado 6, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento. Deberá de tenerse en cuenta la aplicabilidad de los RFS reflejados en el apartado 6 en el caso de que el TOE sea un producto desplegado en la nube, definida en el apartado 7.
20. La categoría de ENS en la que se incluirá el **producto desplegado en la nube** dependerá de la Certificación de Conformidad del ENS que posea el sistema sobre el que se despliega éste junto al Porcentaje de Garantía Compuesto (PGC) de CICLON.

4. PROBLEMA DE SEGURIDAD

4.1 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

21. Para la utilización en condiciones óptimas de seguridad de esta familia de productos, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

- **Usuarios confiables bajo el control del usuario final**: Los usuarios con privilegios deben estar debidamente capacitados y carecer de cualquier intención maliciosa o conflicto de intereses dentro de su respectivo dominio de uso que puedan alterar o comprometer la integridad del producto.

  Nota de aplicación: Un ***dominio de uso*** es el entorno delimitado dentro de un sistema o infraestructura que establece los límites de operación permitidos para los usuarios, definiendo qué recursos pueden gestionar, que acciones pueden ejecutar y en qué condiciones. Por lo tanto, cualquier acción fuera del dominio de uso establecido debe entenderse como potencialmente maliciosa.

  Nota de aplicación: Con intención de que el concepto *dominio de uso* aplicado en este documento no conduzca a error, se presentan los siguientes ejemplos:

  1) **Usuario con permisos y acceso a una API explotable ante buffer overflow y posibilidad de escalar privilegios.** Dentro del dominio de uso este usuario podría modificar parámetros permitidos y realizar sus tareas administrativas. Sin embargo, si explota una vulnerabilidad de tipo buffer overflow para ejecutar código arbitrario y escalar privilegios fuera de lo que sus permisos o dominio de uso le permite, estaría actuando de forma maliciosa. No obstante, la API tendría una no-conformidad sobre la vulnerabilidad detectada. En ningún caso, esta vulnerabilidad se vería cubierta por que el usuario tiene permisos de administración.
  2) **Usuario con permisos privilegiados a un dashboard con un RCE explotable.** En este caso el usuario autorizado con acceso al panel de control para monitorear datos de la empresa, dentro de su dominio de uso podría visualizar registros, generar informes y configurar parámetros dentro de los límites establecidos. Sin embargo, si este usuario explota una vulnerabilidad de ejecución de código remoto para ejecutar comandos arbitrarios en el servidor con privilegios elevados, estaría fuera de su dominio de uso de forma maliciosa.

- **Protección física.** El *software* de gestión 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. Esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.

- **Actualizaciones periódicas.** El *firmware/software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **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.** El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución que la plataforma proporcione.

  Nota de aplicación: Esta hipótesis se considerará aplicable únicamente en los casos en los que el producto sea proporcionado como un software a instalar sobre un dispositivo de usuario final.

- **Usuarios confiables bajo el control de la plataforma**: Los usuarios con privilegios en la plataforma deben estar debidamente capacitados y carecer de cualquier intención maliciosa o conflicto de intereses dentro de su respectivo dominio de uso que puedan alterar o comprometer la integridad del producto.

  Nota de aplicación: Esta hipótesis se considerará aplicable únicamente en los casos en los que el producto sea proporcionado como un software a instalar sobre un dispositivo de usuario final.

- **Publicación de actualizaciones**: Las actualizaciones de firmware/software serán publicadas junto a su hash de identificación unívoco en el repositorio oficial del fabricante, considerando dicha información como confiable.

  Nota de aplicación: Esta hipótesis se considerará aplicable únicamente en los casos en los que el producto use hashes publicados para comprobar la autenticidad de los paquetes de actualización.

- **Asignación de PIN**: Los usuarios con privilegios deben proporcionar a cada usuario final el PIN asignado a su *smartcard* a través de un canal seguro.

  Nota de aplicación: Esta hipótesis se considerará aplicable únicamente en el caso en el que la *smartcard* no pueda ser proporcionada sin PIN, con el objetivo de que el usuario lo establezca durante el primer acceso.

4.2 ACTIVOS SENSIBLES A PROTEGER

22. Los recursos que deben protegerse mediante el uso de esta familia de productos incluyen:

    - **AC.PSS.** Datos de configuración, registros auditoría y [***asignación****: listado de datos definidos por el fabricante]* que deben ser protegidos en Integridad.

- **AC.PSC**. Credenciales, credenciales de *smartcards*, claves privadas, y [**asignación**: *listado de datos definidos por el fabricante*] almacenados que deben ser protegidos en Confidencialidad e Integridad.

  Nota de aplicación: el activo "claves privadas" aplicará a las claves privadas usadas por el TOE para autenticarse en las comunicaciones.

- **AC.Comunicaciones.** Comunicaciones del producto, establecidas entre entidades autorizadas, que deben ser protegidas en Confidencialidad, Integridad y Autenticidad.

  Nota de aplicación: las entidades autorizadas hacen referencia a componentes del TOE, componentes del entorno operacional y usuarios (tanto administradores como no administradores) con acceso al TOE como el cliente final del producto.

- **AC.AUTMECH**. Mecanismos de autenticación y políticas de control de acceso gestionadas, que deben ser protegidos en Integridad.

4.3 AMENAZAS

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

    - **A.NOAUT Acceso a cambios en configuración no autorizado del producto**: Un atacante puede obtener un acceso no autorizado al TOE, ya sea haciéndose pasar por un usuario legítimo o escalando privilegios a nivel de administración, permitiéndole modificar configuraciones clave, gestionar accesos o modificar elementos críticos del sistema (registros de auditoría, credenciales y claves privadas) alterando de esta forma la integridad del producto. Esta amenaza afecta a los activos *AC.PSS* y *AC.PSC*.

    - **A.MITM Ataques *Man In The Middle*:** Un atacante puede interceptar y modificar la comunicación entre dos entidades autorizadas comprometiendo la confidencialidad, integridad y autenticidad de los datos transmitidos. Esta amenaza afecta a los activos *AC.PSS*, *AC.PSC* y *AC.Comunicaciones*.

    - **A.ACT Actualización maliciosa**: Un atacante puede obtener un acceso no autorizado al TOE por medio de una actualización maliciosa que comprometa la integridad y autenticidad del producto. Esta amenaza afecta a los activos *AC.PSS*, *AC.PSC* y *AC.Comunicaciones*.

    - **A.MAN Manipulación previa al arranque**: Un atacante puede obtener un acceso no autorizado al TOE por medio de un arranque del mismo a través de un firmware/software alterado que comprometa la integridad del producto. Esta amenaza afecta a los activos *AC.PSS*, *AC.PSC* y *AC.Comunicaciones*.

    - **A.MEM Ataques de corrupción de memoria**: Un atacante puede explotar vulnerabilidades de gestión de memoria para inyectar y ejecutar código malicioso dentro del espacio de memoria del producto, comprometiendo la

integridad del producto. Esta amenaza afecta a los activos *AC.PSS*, *AC.PSC* y *AC.Comunicaciones*.

- **A.AFNOAUT Acceso físico no autorizado**: Un atacante podría obtener acceso no autorizado a una zona protegida mediante el robo o uso indebido de una *smartcard* válida, la obtención del PIN asociado mediante coacción al usuario legítimo, o la manipulación física de los dispositivos de lectura del sistema de control de acceso. Esta amenaza afecta al activo *AC.AUTMECH*

4.4 TRAZABILIDAD AMENAZAS Y REQUISITOS DE SEGURIDAD

24. En la siguiente tabla se trazan qué Funciones de Seguridad definidas en los apartados 5 y 6 cubren las amenazas definidas en el apartado 4.3:

	A.NOAUT	A.MITM	A.ACT	A.MAN	A.MEM	A.AFNOAUT
ADM	X					X
IAU	X					
COM	X	X				
CIF	X	X	X			
ACT			X			
AUD	X					
PSC	X					
PRO				X		
EXP	X				X	
STM	X					
CERT	X	X	X			
CAF						X

5. REQUISITOS FUNDAMENTALES DE SEGURIDAD ENS CATEGORÍA MEDIA

25. 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 bajo la categoría Media del ENS.

26. 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.

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

- Selección múltiple: 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 múltiple***: local; remota*]

  DS: Administración del producto local y remota

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

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

  DS: Administración del producto local

- 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.

5.1 ADMINISTRACIÓN

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

29. **ADM.1** El TOE debe definir el rol [**asignación**: *nombre del rol o roles de administrador*] como rol de administrador, y el rol [**asignación**: *nombre del rol o roles no administrativos*] como rol no administrativo para los usuarios de las interfaces de gestión. Además, el TOE debe ser capaz de asociar uno o más roles a estos usuarios.

30. **ADM.2M/CAF** El TOE debe permitir realizar de forma [**selección múltiple**: *local; remota*] las siguientes funcionalidades de gestión a través de las interfaces de gestión:

    - Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad en las interfaces de gestión.

- Configuración de políticas de control de accesos basadas en:
  - Zonas protegidas.
  - Horarios.
  - Accesos de emergencia.
  - [**asignación**: *otros parámetros aplicables*].
- Gestión de *smartcards*:
  - Revocación.
  - Renovación.
  - Reemisión.
- [**asignación**: *otras funcionalidades administrables del producto*].

31. **ADM.3** El TOE debe asegurar que solamente usuarios con permisos de administrador son capaces de realizar las funciones descritas en **ADM.2M/CAF**.

> 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.

5.2 IDENTIFICACIÓN Y AUTENTICACIÓN

32. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
33. **IAU.1M** El TOE debe identificar y autenticar a cada usuario administrador y [**asignación**: otros usuarios con roles no administrativos del producto] antes de otorgar acceso a las interfaces de gestión, salvo para las siguientes funcionalidades [**asignación**: listado funcionalidades].
34. **IAU.2M** El TOE debe implementar [**selección múltiple**: *bloqueo de usuarios durante [**asignación**: tiempo de bloqueo] tras [**asignación**: número de intentos] intentos fallidos; bloqueo de usuarios permanente tras [**asignación**: número de intentos] intentos fallidos; 2FA; [**asignación**: cualquier otro mecanismo de prevención de ataques por fuerza bruta validado por CCN]*] para protegerse ante ataques de autenticación por fuerza bruta a las interfaces de gestión.

> Nota de aplicación: en caso de implementar un bloqueo de usuarios temporal, el umbral mínimo debe ser de 30 segundos cada 3 intentos fallidos o equivalente en cuanto al número de contraseñas que se podrían intentar diariamente.

35. **IAU.3M** El TOE debe disponer de la capacidad de gestión de las contraseñas para los usuarios de las interfaces de gestión:
    a) La longitud de la contraseña debe ser mayor o igual a 8 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.

36. **IAU.4** El TOE debe [**selección única***: bloquear; cerrar*] la sesión de un usuario en la correspondiente interfaz de gestión después de [***asignación****: tiempo de inactividad inferior o igual a 30 minutos*] de inactividad.

Nota de aplicación: el tiempo máximo de inactividad debe ser de 30 minutos. En caso de que este tiempo no sea configurable, se permitirá un tiempo superior a 30 minutos únicamente si se trata de una interfaz de monitorización continua que requiera que el usuario tenga la sesión abierta para detectar posibles amenazas.

37. **IAU.5** Cuando el acceso se realice utilizando credenciales por defecto o el usuario no tenga asignadas credencialesa través de las interfaces de gestión, el TOE debe obligar al [**selección única***: cambio; establecimiento*] de credenciales en el siguiente acceso.

Nota de aplicación: este requisito será considerado aplicable únicamente a aquellos usuarios que sean creados desde el TOE una vez que se haya llevado a cabo el proceso de instalación y configuración segura del TOE.

5.3 CANALES SEGUROS

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

39. **COM.1** El TOE debe establecer canales seguros cuando intercambie información sensible con entidades autorizadas: [**selección múltiple***: servidor de auditoría;* [***asignación****: otras entidades*]] o entre distintas partes del producto, usando [**selección múltiple***: IPSec; SSHv2 o superior; TLS 1.2 o superior; DTLS 1.2 o superior; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****: listado de mecanismos, cipher suites o curvas elípticas autorizadas por el CCN para cada protocolo*].

40. **COM.2** El TOE no debe iniciar canales de comunicación adicionales a los definidos en **COM.1**.

41. **COM.3** El TOE debe hacer uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en **COM.1** y **COM.4**.

42. **COM.4** El TOE debe establecer canales seguros cuando intercambie información con los usuarios remotos, usando [**selección múltiple**: *IPsec; SSHv2 o superior; TLS 1.2 o superior; DTLS 1.2 o superior; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos: [**asignación**: listado de mecanismos, cipher suites o curvas elípticas autorizadas por el CCN para cada protocolo].

5.4 CRIPTOGRAFÍA

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

44. **CIF.1M** El TOE debe permitir exclusivamente el empleo de mecanismos criptográficos: [**asignación**: listado de mecanismos] autorizados por el CCN para para Categoría MEDIA del ENS, de acuerdo con el nivel de amenaza establecido.

5.5 INSTALACIÓN Y ACTUALIZACIÓN

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

46. **ACT.1** El TOE debe ofrecer la posibilidad de consultar la versión actual del firmware/software y poder [**selección única**: *actualizarse automáticamente; actualizarse manualmente; iniciar actualizaciones manualmente*] y [**selección única**: *comprobar si existen nuevas actualizaciones disponibles; ningún otro*].

47. **ACT.2M** El TOE debe utilizar [**selección única***: hashes publicados; mecanismos de firma digital*] que estén autorizados por el CCN para autenticar las actualizaciones *firmware/software* antes de instalarlas.

48. **ACT.3** El TOE debe permitir la actualización del *firmware/software* únicamente a usuarios con rol de administrador en la interfaz de gestión correspondiente.

49. **ACT.4** El TOE debe estar empaquetado de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).

    Nota de aplicación: el requisito **ACT.4** se considerará aplicable únicamente en los casos en los que el producto sea proporcionado como un software a instalar sobre un dispositivo de usuario final. En caso de que el TOE se distribuya como una máquina virtual compuesta de un software *core* instalado sobre un sistema operativo convencional, estos requisitos también se considerarán aplicables y aplicarán únicamente a dicho software *core*.

50. **ACT.5** El TOE no debe descargar, modificar, reemplazar o actualizar su propio código binario.

    Nota de aplicación: el requisito **ACT.5** se considerará aplicable únicamente en los casos en los que el producto sea proporcionado como un software a instalar sobre un dispositivo de usuario final. En caso de que el TOE se distribuya como una máquina virtual compuesta de un software *core* instalado sobre un sistema operativo convencional, estos requisitos también se considerarán aplicables y aplicarán únicamente a dicho software *core*.

    Además, este requisito no considerado aplicable en el caso de que el TOE se actualice automáticamente, tal y como permite en **ACT.1**.

5.6 AUDITORÍA

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

52. **AUD.1M/CAF** El TOE debe generar registros de auditoría cuando se produzca alguno de los siguientes eventos:

    a) *Login* y *logout* de usuarios registrados en las interfaces de gestión.

    b) Cambios en las credenciales de usuarios en las interfaces de gestión.

    c) Cambios en la configuración del producto tras llevar a cabo las acciones definidas en **ADM.2M/CAF**.

    d) Eventos relativos a la funcionalidad del producto:

        i. Accesos aprobados y denegados.

        ii. Intentos fallidos.

        iii. Bloqueo por fuerza bruta.

        iv. Detección de tampering.

        v. Detección de coacción.

        vi. [**asignación:** *listado de eventos*].

53. **AUD.2** Los registros de auditoría generados por el TOE deben contener, al menos, la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento.

> Nota de aplicación: en caso de que el resultado de un evento presente más de un valor posible (típicamente, exitoso o fallido), **AUD.1** debe contemplar la generación de auditoría para todos los resultados posibles del evento.

54. **AUD.3** El TOE debe aplicar la siguiente política de control de acceso a los registros de auditoría:

    a) Lectura: usuarios autorizados.

    b) Modificación: ningún usuario.

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

> Nota de aplicación: en este requisito se deben declarar aquellos usuarios del TOE que puedan gestionar los registros de auditoría a través de las interfaces de gestión. En caso de que los registros de auditoría se puedan gestionar únicamente a través de ficheros del sistema operativo sobre el que se instale el TOE, se deberá indicar que ningún usuario puede leer, modificar o borrar dichos registros.

55. **AUD.4** El TOE debe transmitir los registros de auditoría generados a una entidad externa utilizando un canal seguro declarado en **COM.1** y [**selección única**:

almacenar los registros de auditoría en sí mismo; no almacenar los registros de auditoría en sí mismo].

56. **AUD.5** El TOE deberá [**selección única**: *sobrescribir 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.

5.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

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

58. **PSC.1M** El TOE debe almacenar las [**selección múltiple***: credenciales; claves privadas; [**asignación**: otros parámetros de seguridad críticos definidos en el activo AC.PSC*] utilizando mecanismos criptográficos que cumplan con **CIF.1M**.

5.8 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

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

60. **PRO.1** El TOE debe ser capaz de realizar un test durante el arranque o encendido del producto, [**selección múltiple***: periódicamente durante la operación normal del producto; a petición de un usuario autorizado; ninguna*] para verificar la integridad del software/firmware, [***selección múltiple**: el correcto funcionamiento de los mecanismos criptográficos; [**asignación**: otros]; ninguno*].

5.9 CAPACIDADES ANTI-EXPLOTACIÓN

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

62. **EXP.1** Cuando el TOE se encuentre en ejecución, este no debe solicitar la asignación de ninguna dirección explícita de memoria del sistema, ni asignar memoria con permisos simultáneos de escritura y ejecución.

63. **EXP.2** El TOE debe estar configurado por defecto con permisos de ficheros que lo protejan de accesos no autorizados.

64. **EXP.3** El TOE debe estar compilado con protecciones contra *stack-based buffer overflow* habilitadas.

> Nota de aplicación: en caso de que el TOE se distribuya como una máquina virtual compuesta de un software *core* instalado sobre un sistema operativo convencional, estos requisitos también se considerarán aplicables y aplicarán únicamente a dicho software *core*.

5.10 CONTROL DE ACCESO FÍSICO

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

66. **CAF.1** El TOE (lector RFID) debe identificar y autenticar a cada usuario final a través de su *smartcard* y PIN.

67. **CAF.2** El TOE debe implementar [**selección múltiple**: *bloqueo de usuarios durante [**asignación**: tiempo de bloqueo] tras [**asignación**: número de intentos] intentos fallidos; bloqueo de usuarios permanente tras [**asignación**: número de intentos] intentos fallidos; [**asignación**: cualquier otro mecanismo de prevención de ataques por fuerza bruta validado por CCN]*] para protegerse ante ataques de autenticación por fuerza bruta en los accesos de los usuarios finales a través de PIN.

> Nota de aplicación: en caso de implementar un bloqueo de usuarios temporal, el umbral mínimo debe ser de 30 segundos cada 3 intentos fallidos o equivalente en cuanto al número de contraseñas que se podrían intentar diariamente.

68. **CAF.3** El TOE debe forzar a establecer un PIN de [**asignación**: *número de dígitos mayor o igual que 4*] dígitos.

69. **CAF.4** El TOE debe implementar *anti-passback*, evitando que se pueda acceder físicamente de nuevo una vez registrado un acceso.

70. **CAF.5** El TOE debe implementar medidas de detección *anti-tamper* que eviten casos de manipulación física de los componentes del TOE expuestos.

71. **CAF.6** El TOE debe implementar medidas de protección contra usuarios finales coaccionados.

72. **CAR.7** El TOE debe aplicar las políticas de control de accesos configuradas antes de autorizar el acceso a los usuarios finales.

73. **CAR.8** El TOE debe denegar el acceso a usuarios finales cuya *smartcard* haya sido revocada.

6. REQUISITOS DE SEGURIDAD ENS CATEGORÍA ALTA

74. 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 bajo la categoría Alta del ENS.

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

- Selección múltiple: 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 múltiple***: local; remota*]

  DS: Administración del producto local y remota

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

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

  DS: Administración del producto local

- 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.

6.1 ENS CATEGORÍA MEDIA

76. El producto deberá de cumplir con todos los requisitos fundamentales de seguridad descritos en la sección 5, salvo aquellos que cuenten con la nomenclatura *SF.XM*. En estos casos, los requisitos a cumplir serán aquellos incluidos en la presente sección con la nomenclatura *SF.XA*.

6.2 ADMINISTRACIÓN

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

78. **ADM.2A/CAF** El TOE debe permitir realizar de forma [**selección múltiple**: *local; remota*] las siguientes funcionalidades de gestión a través de las interfaces de gestión:

- Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad en las interfaces de gestión.
- Configuración de políticas de control de accesos basadas en:
  - Zonas protegidas.
  - Horarios.
  - Accesos de emergencia.
  - [**asignación**: *otros parámetros aplicables*].

- Gestión de *smartcards*:
  - Revocación.
  - Renovación.
  - Reemisión.
- Gestión de claves criptográficas.
- [**asignación**: otras funcionalidades administrables del producto].

6.3 IDENTIFICACIÓN Y AUTENTICACIÓN

79. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
80. **IAU.1A** El TOE debe identificar y autenticar a cada usuario antes de otorgar acceso a las interfaces de gestión.
81. **IAU.2A** El TOE debe de implementar un doble factor de autenticación (2FA) en los inicios de sesión de los usuarios en las interfaces de gestión.
82. **IAU.3A** El TOE debe disponer de la capacidad de gestión de las contraseñas para los usuarios de las interfaces de gestión:
    a) La longitud de la contraseña debe ser mayor o igual a 12 caracteres.
    b) La contraseña debe estar compuesta de, al menos, una letra minúscula, una letra mayúscula, un número y un carácter especial [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”].

Nota de aplicación: este requisito podría ser modificado en el caso de que el TOE implemente otros mecanismos de autenticación.

83. **IAU.6** El TOE debe permitir que los usuarios cierren su propia sesión.

6.4 CRIPTOGRAFÍA

84. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
85. **CIF.1A** El TOE debe permitir exclusivamente el empleo de mecanismos criptográficos: [**asignación**: listado de mecanismos] autorizados por el CCN para para Categoría ALTA del ENS, de acuerdo con el nivel de amenaza establecido.

6.5 INSTALACIÓN Y ACTUALIZACIÓN

86. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
87. **ACT.2A** El TOE debe utilizar mecanismos de firma digital que estén autorizados por el CCN para autenticar las actualizaciones *firmware/software* antes de instalarlas.

6.6 AUDITORÍA

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

89. **AUD.1A/CAF** 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 en las interfaces de gestión.

    c) Cambios en las credenciales de usuarios en las interfaces de gestión.

    d) Cambios en la configuración del producto tras llevar a cabo las acciones definidas en **ADM.2A/CAF**.

    e) Eventos relativos a la funcionalidad del producto:

        i. Accesos aprobados y denegados.

        ii. Intentos fallidos.

        iii. Bloqueo por fuerza bruta.

        iv. Detección de tampering.

        v. Detección de coacción.

        vi. [**asignación:** *listado de eventos*].

6.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

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

91. **PSC.1A** El TOE debe almacenar las [**selección múltiple***: credenciales; claves privadas; [**asignación**: otros parámetros de seguridad críticos definidos en el activo AC.PSC*] utilizando mecanismos criptográficos que cumplan con **CIF.1A**.

92. **PSC.2** El TOE debe 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 sobreescritura utilizando alguno de los siguientes métodos:

            1. Un patrón pseudoaleatorio generado por el RBG.

            2. Todo cero o uno.

            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.

b) Para memoria no volátil:

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

1. Una sola pasada de sobrescritura consistente en ceros, unos u otro valor que no contenga ningún PSC.

2. Borrado de bloque.

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

1. Una o más pasadas de sobrescritura consistente en ceros, unos o algún valor que no contenga ningún PSC seguidos de una lectura de verificación.

2. 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.

6.8 SELLOS DE TIEMPO

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

94. **STM.1** El TOE debe ser capaz de sellar los registros de auditoria con una fuente de tiempo fiable.

95. **STM.2** El TOE debe [**selección única***: permitir que los usuarios administradores establezcan la fecha y hora manualmente; obtener los sellos de tiempo de la plataforma sobre la que se instala; sincronizarse con un servidor NTP*].

6.9 COMUNICACIONES

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

97. **COM.DTLSC.1** El TOE debe verificar que el identificador presentado por el servidor en los campos [**selección múltiple**: *Common Name (CN); Subject Alternative Name (SAN)*] concuerdan con el identificador esperado. En caso contrario, debe finalizar la conexión.

98. **COM.DTLSC.2** El TOE no debe establecer el canal de comunicación si el certificado del servidor no es válido [**selección única**: *sin ningún mecanismo de anulación por parte del administrador.; excepto con la siguiente anulación del administrador: si el TOE no logra determinar el estado de revocación, el TOE permitirá que el administrador proporcione una autorización de anulación para establecer la conexión por cada certificado.*].

99. **COM.DTLSC.3** El TOE debe prohibir el uso de las siguientes extensiones:
    a) Early data extension.
    b) Post-handshake client authentication.
100. **COM.DTLSC.4** El TOE debe [**selección única**: *no usar PSKs; usar únicamente PSK en la reanudación de sesiones (sesión resumption) DTLS 1.3 con forward secrecy*].
101. **COM.DTLSC.5** El TOE debe [**selección única**: *soportar renegociación segura en DTLS 1.2 a través del uso de la extensión "renegotiation_info"; rechazar intentos de renegociación en [**selección múltiple**: DTLS 1.2; DTLS 1.3]*].
102. **COM.DTLSC.6** El TOE debe [**selección única**: *terminar la sesión DTLS; descartar silenciosamente el registro*] si el MAC recibido del servidor en el *handshake* es inválido.
103. **COM.DTLSC.7** El TOE debe detectar y descartar silenciosamente los mensajes repetidos para:
    a) Registros DTLS previamente recibidos.
    b) Registros DTLS demasiado antiguos para encajar en la *sliding window*.

> Nota de aplicación: los requisitos **COM.DTLSC.1**, **COM.DTLSC.2**, **COM.DTLSC.3**, **COM.DTLSC.4**, **COM.DTLSC.5**, **COM.DTLSC.6** y **COM.DTLSC.7** se considerarán aplicable en caso de que se declare un canal DTLS (independientemente de si el canal requiere autenticación mutua o no) en **COM.1** o **COM.4** en el que el TOE actúe como cliente, aplicándolos por separado a cada canal DTLS declarado en ambos requisitos.

104. **COM.DTLSC.8** El TOE debe soportar comunicaciones DTLS con autenticación mutua de cliente usando certificados X.509v3.

> Nota de aplicación: el requisito **COM.DTLSC.8** se considerará aplicable en caso de que se declare un canal DTLS con autenticación mutua en **COM.1** o **COM.4** en el que el TOE actúe como cliente, aplicándolos por separado a cada canal DTLS declarado en ambos requisitos.

105. **COM.DTLSS.1** El TOE debe denegar las conexiones de los clientes que usen versiones de DTLS inferiores a 1.2.
106. **COM.DTLSS.2** El TOE no debe continuar intentos de *handshake* en los que no puede validar correctamente la *cookie* devuelta por el cliente en el mensaje *ClientHello*.
107. **COM.DTLSS.3** El TOE debe autenticarse a sí mismo usando certificados X.509v3.
108. **COM.DTLSS.4** El TOE debe [**selección única**: *terminar la sesión DTLS; descartar silenciosamente el registro*] si el MAC recibido del cliente en el *handshake* es inválido.
109. **COM.DTLSS.5** El TOE debe detectar y descartar silenciosamente los mensajes repetidos para:

a) Registros DTLS previamente recibidos.

b) Registros DTLS demasiado antiguos para encajar en la *sliding window*.

110. **COM.DTLSS.6** El TOE debe [**selección única**: *no soportar session resumption o session tickets; soportar session resumption basados en session IDs de acuerdo al RFC 5246 (TLS1.2); soportar session resumption basados en session tickets de acuerdo al RFC 5077]*.

111. **COM.DTLSS.7** El TOE debe prohibir el uso de la extensión *early data*.

112. **COM.DTLSS.8** El TOE debe [**selección única**: *no usar PSKs; usar únicamente PSK en la reanudación de sesiones (sesión resumption) DTLS 1.3 con forward secrecy*].

113. **COM.DTLSS.9** El TOE debe [**selección única**: *soportar renegociación segura en DTLS 1.2 a través del uso de la extensión "renegotiation_info"; rechazar intentos de renegociación en [**selección múltiple**: DTLS 1.2; DTLS 1.3]*].

> Nota de aplicación: los requisitos **COM.DTLSS.1**, **COM.DTLSS.2**, **COM.DTLSS.3**, **COM.DTLSS.4**, **COM.DTLSS.5**, **COM.DTLSS.6**, **COM.DTLSS.7**, **COM.DTLSS.8** y **COM.DTLSS.9** se considerarán aplicables en caso de que se declare un canal DTLS (independientemente de si el canal requiere autenticación mutua o no) en **COM.1** o **COM.4** en el que el TOE actúe como servidor, aplicándolos por separado a cada canal DTLS declarado en ambos requisitos.

114. **COM.DTLSS.10** El TOE debe soportar comunicaciones DTLS con autenticación mutua de cliente usando certificados X.509v3 y rechazar la conexión si el cliente no proporciona ningún certificado de cliente o si el certificado de cliente no puede ser validado correctamente por el TOE (excepto en el caso de los mecanismos de anulación que puedan estar definidos en **COM.DTLSS.10**).

115. **COM.DTLSS.11** El TOE no debe establecer por defecto el canal de comunicación si el certificado del cliente no es válido. Además, el TOE [**selección única**: *no debe implementar algún mecanismo de anulación por parte del administrador; debe requerir autorización del administrador para establecer la conexión si el TOE falla a la hora de determinar el estado de revocación] del certificado presentado por el cliente*].

116. **COM.DTLSS.12** El TOE no debe establecer un canal DTLS si el campo *Common Name (CN)* o el *Subject Alternative Name (SAN)* contenidos en el certificado del cliente no concuerda con el identificador esperado.

> Nota de aplicación: los requisitos **COM.DTLSS.10**, **COM.DTLSS.11** y **COM.DTLSS.12** se considerarán aplicables en caso de que se declare un canal DTLS con autenticación mutua en **COM.1** o **COM.4** en el que el TOE actúe como servidor, aplicándolos por separado a cada canal DTLS declarado en ambos requisitos.

117. **COM.TLSC.1** El TOE debe verificar que el identificador presentado por el servidor en los campos [**selección múltiple**: *Common Name (CN); Subject Alternative Name (SAN)*] concuerdan con el identificador esperado. En caso contrario, debe finalizar la conexión.

118. **COM.TLSC.2** El TOE no debe establecer el canal de comunicación si el certificado del servidor no es válido [**selección única**: *no debe implementar algún mecanismo de anulación por parte del administrador; debe requerir autorización del administrador para establecer la conexión si el TOE falla a la hora de determinar el estado de revocación del certificado presentado por el cliente*].

119. **COM.TLSC.3** El TOE debe prohibir el uso de las siguientes extensiones:

    a) Early data extension.

    b) Post-handshake client authentication.

120. **COM.TLSC.4** El TOE debe [**selección única**: *no usar PSKs; usar únicamente PSK en la reanudación de sesiones (sesión resumption) TLS 1.3 con forward secrecy*].

121. **COM.TLSC.5** El TOE debe [**selección única**: *soportar renegociación segura en TLS 1.2 a través del uso de la extensión "renegotiation_info"; rechazar intentos de renegociación en [**selección múltiple**: TLS 1.2; TLS 1.3]*].

> Nota de aplicación: los requisitos **COM.TLSC.1**, **COM.TLSC.2**, **COM.TLSC.3**, **COM.TLSC.4** y **COM.TLSC.5** se considerarán aplicables en caso de que se declare un canal TLS (independientemente de si el canal requiere autenticación mutua o no) en **COM.1** o **COM.4** en el que el TOE actúe como cliente, aplicándolos por separado a cada canal TLS declarado en ambos requisitos.

122. **COM.TLSC.6** El TOE debe soportar comunicaciones TLS con autenticación mutua de cliente usando certificados X.509v3.

> Nota de aplicación: el requisito **COM.TLSC.6** se considerará aplicable en caso de que se declare un canal TLS con autenticación mutua en **COM.1** o **COM.4** en el que el TOE actúe como cliente, aplicándolos por separado a cada canal TLS declarado en ambos requisitos.

123. **COM.TLSS.1** El TOE debe denegar las conexiones de los clientes que usen versiones de TLS inferiores a 1.2.

124. **COM.TLSS.2** El TOE debe autenticarse a sí mismo usando certificados X.509v3.

125. **COM.TLSS.3** El TOE debe [**selección única**: *no reanudar sesiones; soportar session resumption basados en session IDs de acuerdo al RFC 5246 (TLS1.2); soportar session resumption basados en session tickets de acuerdo al RFC 5077 (TLS 1.2), soportar session resumption de acuerdo al RFC 8446 (TLS 1.3)*].

126. **COM.TLSS.4** El TOE debe prohibir el uso de la extensión *early data*.

127. **COM.TLSS.5** El TOE debe [**selección única**: *no usar PSKs; usar únicamente PSK en la reanudación de sesiones (sesión resumption) TLS 1.3 con forward secrecy*].

128. **COM.TLSS.6** El TOE debe [**selección única**: *soportar renegociación segura en TLS 1.2 a través del uso de la extensión "renegotiation_info"; rechazar intentos de renegociación en [**selección múltiple**: TLS 1.2; TLS 1.3]*].

> Nota de aplicación: los requisitos **COM.TLSS.1**, **COM.TLSS.2**, **COM.TLSS.3**, **COM.TLSS.4**, **COM.TLSS.5** y **COM.TLSS.6** se considerarán aplicables en caso de que se declare un canal TLS (independientemente de si el canal requiere autenticación mutua o no) en **COM.1** o **COM.4** en el que el TOE actúe como servidor, aplicándolos por separado a cada canal TLS declarado en ambos.

129. **COM.TLSS.7** El TOE debe soportar comunicaciones TLS con autenticación mutua de cliente usando certificados X.509v3 y rechazar la conexión si el cliente no proporciona ningún certificado de cliente o si el certificado de cliente no puede ser validado correctamente por el TOE (excepto en el caso de los mecanismos de anulación que puedan estar definidos en **COM.TLSS.8**).

130. **COM.TLSS.8** El TOE no debe establecer por defecto el canal de comunicación si el certificado del cliente no es válido. Además, el TOE [**selección única**: *no debe implementar algún mecanismo de anulación por parte del administrador; debe requerir autorización del administrador para establecer la conexión si el TOE falla a la hora de determinar el estado de revocación] del certificado presentado por el cliente*].

131. **COM.TLSS.9** El TOE no debe establecer un canal TLS si el identificador contenido en los campos *Common Name* o *Subject Alternative Name* del certificado del cliente no concuerda con el identificador esperado para dicho cliente. Si el identificador es un *Fully Qualified Domain Name (FQDN)*, el TOE debe comparará los identificadores según la RFC 6125. De lo contrario, el TOE analizará el identificador del certificado y lo comparará con el identificador esperado del cliente.

> Nota de aplicación: los requisitos **COM.TLSS.7**, **COM.TLSS.8** y **COM.TLSS.9** se considerarán aplicables en caso de que se declare un canal TLS con autenticación mutua en **COM.1** o **COM.4** en el que el TOE actúe como servidor, aplicándolos por separado a cada canal TLS declarado en ambos requisitos.

132. **COM.IPSEC.1** El TOE deberá implementar la arquitectura IPSEC de acuerdo a lo especificado en la RFC 4301, en modo túnel.

133. **COM.IPSEC.2** El TOE deberá asegurar que el protocolo IKE implementa autenticación extremo a extremo utilizando firma electrónica, con certificados X.509v3.

134. **COM.IPSEC.3** El TOE deberá asegurar que los tiempos de vida de las asociaciones de seguridad (SA) de los protocolos IKE podrán ser configurados por un administrador en base al número de paquetes, volumen de tráfico y/o tiempo transcurrido.

135. **COM.IPSEC.4** El TOE deberá generar el valor secreto X utilizado en el intercambio de claves Diffie-Hellman ("x" en gx mod p) con una longitud de bits de al menos el doble de los "bits de seguridad" asociados con el grupo DH negociado.

136. **COM.IPSEC.5** El TOE deberá implementar protocolo IPSEC ESP como se define en RFC 4303 utilizando mecanismos de protección de integridad, autenticidad, y confidencialidad autorizados por el CCN.

137. **COM.IPSEC.6** El TOE deberá generar nonces para el intercambio en IKE. La probabilidad de repetir un nonce durante la vida de una determinada SA IPSec será menor o igual que $1/(2^{128})$.

138. **COM.IPSEC.7** El TOE deberá validar que el certificado del servidor contiene, en los campos Sujeto (Subject Distinguished Name) o Nombre Alternativo del Titular (Subject Alternative Name), el identificador del servidor configurado para la conexión. En caso contrario, finalizará la conexión.

> Nota de aplicación: los requisitos **COM.IPSEC.X** serán considerados aplicables en caso de que se declare un canal IPSec en **COM.1** o **COM.4**, aplicándolos por separado a cada canal IPSec declarado en ambos requisitos.

139. **COM.NTP.1** El TOE debe soportar solamente las siguientes versiones de NTP: [**selección múltiple**: *NTP v3; NTP v4*].

140. **COM.NTP.2** El TOE debe actualizar la hora del sistema usando [**selección múltiple**:

    a) Un canal de comunicación [**selección múltiple**: *IPSec; DTLS*] con el servidor NTP;

    b) Autenticación usando [**selección múltiple**: *HMAC-SHA-256; HMAC-SHA-384; HMAC-SHA-512; AES-CMAC-128; AES- CMAC-256*]].

141. **COM.NTP.3** El TOE no debe actualizar la hora del sistema si se recibe desde direcciones *broadcast* y/o *multicast*.

142. **COM.NTP.4** El TOE debe soportar la configuración de, al menos, 3 fuentes de tiempo NTP en el entorno operacional.

> Nota de aplicación: los requisitos **COM.NTP.X** serán considerados aplicables en caso de que se seleccione la opción "*sincronizarse con un servidor NTP*" en el requisito **STM.2**.

143. **COM.SSH.1** El TOE debe implementar SSH v2 actuando como [**selección múltiple**: *cliente; servidor*] de acuerdo a los RFCs 4251, 4252, 4253 y 4254.

144. **COM.SSH.2** En caso de que el TOE actúe como servidor SSH, el TOE debe soportar los siguientes métodos de autenticación en las sesiones de usuario: [**selección múltiple**: *contraseña; interactiva por teclado; clave pública con [**selección múltiple**: ecdsa-sha2-nistp256; ecdsa-sha2-nistp384; ecdsa-sha2-nistp521; x509v3-ecdsa-sha2-nistp256; x509v3-ecdsa-sha2-nistp384; x509v3-ecdsa-sha2-nistp521]*].

145. **COM.SSH.3** El TOE debe descartar los paquetes con un tamaño mayor a [**asignación**: *número de bytes entre 35000 y 1 GB*] en una conexión de transporte SSH.

146. **COM.SSH.4** El TOE debe usar SSH KDF como se define en [**selección múltiple**: *RFC 4253 (Sección 7.2); RFC 5656 (Sección 4)*].

> Nota de aplicación: el RFC elegido en la selección dependerá del esquema de intercambio de clave definido en **COM.1** o **COM.4** para cada canal de comunicaciones SSH definido en dichos requisitos.

147. **COM.SSH.5** El TOE debe asegurar que [**selección única**: *se regenera una clave de sesión; se termina la conexión*] en caso de que se alcance alguno de los siguientes umbrales:

    a) Una hora de conexión.

    b) No más de 1 GB de datos transmitidos.

    c) No más de 1GB de datos recibidos.

> Nota de aplicación: los requisitos **COM.SSH.X** serán considerados aplicables en caso de que se declare un canal SSH en **COM.1** o **COM.4**, aplicándolos por separado a cada canal SSH declarado en ambos requisitos.

6.10 CERTIFICADOS

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

149. **CERT.1** El TOE debe validar certificados de acuerdo a las siguientes reglas:

    a) Validación de certificados conforme al RFC 5280 y validación de la ruta de certificación soportando un mínimo de 3 certificados por ruta.

    b) La ruta de certificación debe terminar con el certificado de una CA de confianza designado como ancla de confianza.

    c) El TOE debe validar la ruta de certificación asegurando que los certificados de todas las CAs que conforman la ruta de certificación contienen la extensión *basicConstraints* con el flag *CA* establecido a *TRUE*.

    d) El TOE debe validar el estado de revocación del certificado usando [**selección múltiple**: *el protocolo Online Certificate Status Protocol (OCSP) como se especifica en el RFC 6960; una Lista de Revocación de Certificados (CRL) como se especifica en la sección 6.3 del RFC 5280; una Lista de Revocación de Certificados (CRL) como se especifica en la sección 5 del RFC 5759*].

    e) El TOE debe validar el campo *extendedKeyUsage* de acuerdo a las siguientes reglas:

        i. Los certificados usados para las actualizaciones confiables y verificaciones de integridad de código ejecutable cuentan con el

valor *Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3)* en el campo *extendedKeyUsage*.

ii. Los certificados presentados por un servidor en comunicaciones TLS deben contar con el valor *Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1)* en el campo *extendedKeyUsage*.

iii. Los certificados presentados por un cliente en comunicaciones TLS deben contar con el valor *Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2)* en el campo *extendedKeyUsage*.

iv. Los certificados OCSP presentados para respuestas OCSP deben contar con el valor *OCSP Signing purpose* (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) en el campo *extendedKeyUsage*.

150. **CERT.2** El TOE debe considerar un certificado como certificado de CA solo si la extensión *basicConstraints* está presente en el certificado y el flag *CA* está establecido con el valor *TRUE.*

151. **CERT.3** El TOE debe usar certificados X.509v3 como define el RFC 5280 para soportar autenticación en los protocolos [**selección múltiple**: *DTLS; HTTPS; IPSec; SSH; TLS; ningún protocolo*] y [**selección múltiple**: *firmas de código para actualizaciones software; [**asignación**: otros usos]; ningún uso adicional*].

152. **CERT.4** En el caso en el que el TOE no pueda establecer una conexión para determinar la validez de un certificado, el TOE debe [**selección única**: *permitir que el administrador decida si aceptar o no el certificado; aceptar el certificado; no aceptar el certificado*].

> Nota de aplicación: los requisitos **CERT.1**, **CERT.2**, **CERT.3** y **CERT.4** se considerarán aplicables en el caso de que el TOE valide certificados en comunicaciones (TLS, DTLS o IPSec) o en actualizaciones.

153. **CERT.5** El TOE debe generar una *Certificate Request* como especifica el RFC 2986 y ser capaz de proporcionar la siguiente información en la petición: clave púbica y [**selección múltiple**: *información específica del dispositivo; Common Name; Organization; Organization Unit; Country*].

154. **CERT.6** El TOE debe validar la cadena de certificados desde la *Root CA* hasta recibir la *CA Certificate Response*.

> Nota de aplicación: los requisitos **CERT.5** y **CERT.6** se considerarán aplicables en el caso de que el TOE permita la generación de certificados X509.

7. ANEXO I: TRAZABILIDAD REQUISITOS DE SEGURIDAD PARA LINCE Y CICLON

155. En la siguiente tabla se trazan qué Funciones de Seguridad definidas en los apartados 5 y 6 se considerarán aplicables en una certificación de producto a través de LINCE y en una evaluación de productos desplegados en la nube a través de CICLON:

	LINCE	CICLON
ADM	X	X
IAU	X	X
COM	X	X
CIF	X	X
ACT	X	
AUD	X	X
PSC	X	X
PRO	X	
EXP	X	
STM	X	X
CERT	X	X
CAF	X	

8. ANEXO II: TRAZABILIDAD CON COMMON CRITERIA

156. Para aquellos casos en los que el producto haya superado una certificación Common Criteria, se deberá de llevar a cabo una **evaluación STIC complementaria**. Para determinar el conjunto de requisitos a probar en dicha evaluación, se facilita la tabla incluida en el presente anexo.

157. En esta tabla se traza la equivalencia entre los Requisitos Fundamentales de Seguridad definidos en los apartados 5 y 6 y los SFRs de los perfiles de Protección *Collaborative Protection Profile for Network Devices v3.0*[2], *Collaborative Protection Profile for Network Devices v2.2e*[3], *Protection Profile for Application Software v1.4*[4] y *Functional Package for Secure Shell (SSH) v1.0*[5].

158. Debe tenerse en cuenta que la tabla de equivalencias dependerá de las *asignaciones* y *selecciones* realizadas, tanto en la Declaración de Seguridad de Common Criteria como en el conjunto de requisitos a probar en la evaluación STIC complementaria. La equivalencia de requisitos deberá ser justificada y validada por CPSTIC.

159. Debe tenerse en cuenta que las celdas de la tabla que se encuentren vacías supondrán que el Perfil de Protección de Common Criteria correspondiente no incluye un requisito que satisfaga el RFS correspondiente del presente documento.

160. Para realizar esta trazabilidad, se deberá tener en cuenta la siguiente tabla:

RFS Anexo I.3	SFR Collaborative Protection Profile for Network Devices v3.0e	SFR Collaborative Protection Profile for Network Devices v2.2e	SFR Protection Profile for Application Software v1.4	SFR Functional Package for Secure Shell (SSH) v1.0
ADM.1	FMT_SMR.2	FMT_SMR.2		
ADM.2M/CAF	FMT_SMF.1	FMT_SMF.1		
ADM.2A/CAF	FMT_SMF.1 FMT_MOF.1/Services FMT_MOF.1/AutoUpdate FMT_MTD.1/CryptoKeys	FMT_SMF.1 FMT_MOF.1/Services FMT_MOF.1/AutoUpdate FMT_MTD.1/CryptoKeys		
ADM.3	FMT_MTD.1.1/CoreData	FMT_MTD.1.1/CoreData		
IAU.1M	FIA_UIA_EXT.1	FIA_UIA_EXT.1		
IAU.1A				
IUA.2M	FIA_AFL.1	FIA_AFL.1		

[2] https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/NDcPP_v3_0e.pdf
[3] https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/CPP_ND_V2.2E.pdf
[4] https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/PP_APP_V1.4.pdf
[5] https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/pkg_ssh_v1.0.pdf

RFS Anexo I.3	SFR Collaborative Protection Profile for Network Devices v3.0e	SFR Collaborative Protection Profile for Network Devices v2.2e	SFR Protection Profile for Application Software v1.4	SFR Functional Package for Secure Shell (SSH) v1.0
IAU.2A				
IAU.3M	FIA_PMG_EXT.1.1	FIA_PMG_EXT.1		
IAU.3A	FIA_PMG_EXT.1.1	FIA_PMG_EXT.1		
IAU.4	FTA_SSL_EXT.1 FTA_SSL.3.1	FTA_SSL_EXT.1 FTA_SSL.3		
IAU.5			FMT_CFG_EXT.1.1	
IAU.6	FTA_SSL.4	FTA_SSL.4		
COM.1	FTP_ITC.1.1 FCS_DTLSC_EXT.1.1 FCS_DTLSC_EXT.1.4 FCS_DTLSS_EXT.1.1 FCS_DTLSS_EXT.1.4 FCS_TLSC_EXT.1.1 FCS_TLSC_EXT.1.4 FCS_TLSS_EXT.1.1 FCS_TLSS_EXT.1.3 FCS_IPSEC_EXT.1.4 FCS_IPSEC_EXT.1.6 FCS_IPSEC_EXT.1.11 FCS_IPSEC_EXT.1.13	FTP_ITC.1.1 FCS_DTLSC_EXT.1.1 FCS_DTLSC_EXT.1.4 FCS_DTLSS_EXT.1.1 FCS_DTLSS_EXT.1.4 FCS_TLSC_EXT.1.1 FCS_TLSC_EXT.1.4 FCS_TLSS_EXT.1.1 FCS_TLSS_EXT.1.3 FCS_IPSEC_EXT.1.4 FCS_IPSEC_EXT.1.6 FCS_IPSEC_EXT.1.11 FCS_IPSEC_EXT.1.13	FTP_DIT_EXT.1	FCS_SSH_EXT.1.4 FCS_SSH_EXT.1.5 FCS_SSH_EXT.1.6
COM.2	FTP_ITC.1.2	FTP_ITC.1.2		

RFS Anexo I.3	SFR Collaborative Protection Profile for Network Devices v3.0e	SFR Collaborative Protection Profile for Network Devices v2.2e	SFR Protection Profile for Application Software v1.4	SFR Functional Package for Secure Shell (SSH) v1.0
	FTP_ITC.1.3	FTP_ITC.1.3		
COM.3	FCS_DTLSS_EXT.1.3 FCS_TLSS_EXT.1.2	FCS_DTLSS_EXT.1.3 FCS_TLSS_EXT.1.2		
COM.4	FTP_TRP.1/Admin FCS_DTLSC_EXT.1.1 FCS_DTLSC_EXT.1.4 FCS_DTLSS_EXT.1.1 FCS_DTLSS_EXT.1.4 FCS_TLSC_EXT.1.1 FCS_TLSC_EXT.1.4 FCS_TLSS_EXT.1.1 FCS_TLSS_EXT.1.3 FCS_IPSEC_EXT.1.4 FCS_IPSEC_EXT.1.6 FCS_IPSEC_EXT.1.11 FCS_IPSEC_EXT.1.13	FTP_TRP.1/Admin FCS_DTLSC_EXT.1.1 FCS_DTLSC_EXT.1.4 FCS_DTLSS_EXT.1.1 FCS_DTLSS_EXT.1.4 FCS_TLSC_EXT.1.1 FCS_TLSC_EXT.1.4 FCS_TLSS_EXT.1.1 FCS_TLSS_EXT.1.3 FCS_IPSEC_EXT.1.4 FCS_IPSEC_EXT.1.6 FCS_IPSEC_EXT.1.11 FCS_IPSEC_EXT.1.13		FCS_SSH_EXT.1.4 FCS_SSH_EXT.1.5 FCS_SSH_EXT.1.6
COM.DTLSC.1	FCS_DTLSC_EXT.1.2	FCS_DTLSC_EXT.1.2		
COM.DTLSC.2	FCS_DTLSC_EXT.1.3	FCS_DTLSC_EXT.1.3		
COM.DTLSC.3	FCS_DTLSC_EXT.1.7			

RFS Anexo I.3	SFR Collaborative Protection Profile for Network Devices v3.0e	SFR Collaborative Protection Profile for Network Devices v2.2e	SFR Protection Profile for Application Software v1.4	SFR Functional Package for Secure Shell (SSH) v1.0
COM.DTLSC.4	FCS_DTLSC_EXT.1.8			
COM.DTLSC.5	FCS_DTLSC_EXT.1.9			
COM.DTLSC.6	FCS_DTLSC_EXT.1.10	FCS_DTLSC_EXT.2.2		
COM.DTLSC.7	FCS_DTLSC_EXT.1.12	FCS_DTLSC_EXT.2.3		
COM.DTLSC.8	FCS_DTLSC_EXT.2.1	FCS_DTLSC_EXT.2.1		
COM.DTLSS.1	FCS_DTLSS_EXT.1.1	FCS_DTLSS_EXT.1.2		
COM.DTLSS.2	FCS_DTLSS_EXT.1.2			
COM.DTLSS.3	FCS_DTLSS_EXT.1.3			
COM.DTLSS.4	FCS_DTLSS_EXT.1.5	FCS_DTLSS_EXT.1.5		
COM.DTLSS.5	FCS_DTLSS_EXT.1.6	FCS_DTLSS_EXT.1.6		
COM.DTLSS.6	FCS_DTLSS_EXT.1.7	FCS_DTLSS_EXT.1.7		
COM.DTLSS.7	FCS_DTLSS_EXT.1.9			
COM.DTLSS.8	FCS_DTLSS_EXT.1.10			
COM.DTLSS.9	FCS_DTLSS_EXT.1.11			
COM.DTLSS.10	FCS_DTLSS_EXT.2.1	FCS_DTLSS_EXT.2.1		
COM.DTLSS.11	FCS_DTLSS_EXT.2.2	FCS_DTLSS_EXT.2.2		
COM.DTLSS.12	FCS_DTLSS_EXT.2.3	FCS_DTLSS_EXT.2.3		
COM.TLSC.1	FCS_TLSC_EXT.1.2	FCS_TLSC_EXT.1.2		

RFS Anexo I.3	SFR Collaborative Protection Profile for Network Devices v3.0e	SFR Collaborative Protection Profile for Network Devices v2.2e	SFR Protection Profile for Application Software v1.4	SFR Functional Package for Secure Shell (SSH) v1.0
COM.TLSC.2	FCS_TLSC_EXT.1.3	FCS_TLSC_EXT.1.3		
COM.TLSC.3	FCS_TLSC_EXT.1.7			
COM.TLSC.4	FCS_TLSC_EXT.1.8			
COM.TLSC.5	FCS_TLSC_EXT.1.9			
COM.TLSC.6	FCS_TLSC_EXT.2.1	FCS_TLSC_EXT.2.1		
COM.TLSS.1	FCS_TLSS_EXT.1.1	FCS_TLSS_EXT.1.2		
COM.TLSS.2				
COM.TLSS.3	FCS_TLSS_EXT.1.2			
COM.TLSS.4	FCS_TLSS_EXT.1.4	FCS_TLSS_EXT.1.4		
COM.TLSS.5	FCS_TLSS_EXT.1.6			
COM.TLSS.6	FCS_TLSS_EXT.1.7			
COM.TLSS.7	FCS_TLSS_EXT.2.1	FCS_TLSS_EXT.2.1		
COM.TLSS.8	FCS_TLSS_EXT.2.2	FCS_TLSS_EXT.2.2		
COM.TLSS.9	FCS_TLSS_EXT.2.3	FCS_TLSS_EXT.2.3		
COM.IPSEC.1	FCS_IPSEC_EXT.1.1	FCS_IPSEC_EXT.1.1		
COM.IPSEC.2	FCS_IPSEC_EXT.1.13	FCS_IPSEC_EXT.1.13		
COM.IPSEC.3	FCS_IPSEC_EXT.1.7	FCS_IPSEC_EXT.1.7		
COM.IPSEC.4	FCS_IPSEC_EXT.1.9	FCS_IPSEC_EXT.1.9		

RFS Anexo I.3	SFR Collaborative Protection Profile for Network Devices v3.0e	SFR Collaborative Protection Profile for Network Devices v2.2e	SFR Protection Profile for Application Software v1.4	SFR Functional Package for Secure Shell (SSH) v1.0
COM.IPSEC.5	FCS_IPSEC_EXT.1.4	FCS_IPSEC_EXT.1.4		
COM.IPSEC.6	FCS_IPSEC_EXT.1.10	FCS_IPSEC_EXT.1.10		
COM.IPSEC.7	FCS_IPSEC_EXT.1.14	FCS_IPSEC_EXT.1.14		
COM.NTP.1	FCS_NTP_EXT.1.1	FCS_NTP_EXT.1.1		
COM.NTP.2	FCS_NTP_EXT.1.2	FCS_NTP_EXT.1.2		
COM.NTP.3	FCS_NTP_EXT.1.3	FCS_NTP_EXT.1.3		
COM.NTP.4	FCS_NTP_EXT.1.4	FCS_NTP_EXT.1.4		
COM.SSH.1				FCS_SSH_EXT.1.1
COM.SSH.2				FCS_SSH_EXT.1.2
COM.SSH.3				FCS_SSH_EXT.1.3
COM.SSH.4				FCS_SSH_EXT.1.7
COM.SSH.5				FCS_SSH_EXT.1.8
CIF.1M				
CIF.1A				
ACT.1	FPT_TUD_EXT.1.1 FPT_TUD_EXT.1.2	FPT_TUD_EXT.1.1 FPT_TUD_EXT.1.2	FPT_TUD_EXT.1.1 FPT_TUD_EXT.1.2	
ACT.2M	FPT_TUD_EXT.1.3	FPT_TUD_EXT.1.3	FPT_TUD_EXT.1.4 FPT_TUD_EXT.2.3	
ACT.2A	FPT_TUD_EXT.1.1	FPT_TUD_EXT.1.1	FPT_TUD_EXT.1.4	

RFS Anexo I.3	SFR Collaborative Protection Profile for Network Devices v3.0e	SFR Collaborative Protection Profile for Network Devices v2.2e	SFR Protection Profile for Application Software v1.4	SFR Functional Package for Secure Shell (SSH) v1.0
			FPT_TUD_EXT.2.3	
ACT.3	FMT_MOF.1/ManualUpdate	FMT_MOF.1/ManualUpdate		
ACT.4			FPT_TUD_EXT.2.2	
ACT.5			FPT_TUD_EXT.1.3	
AUD.1M/CAF	FAU_GEN.1.1	FAU_GEN.1.1		
AUD.1A/CAF	FAU_GEN.1.1	FAU_GEN.1.1		
AUD.2	FAU_GEN.1.2 FAU_GEN.2	FAU_GEN.1.2 FAU_GEN.2		
AUD.3	FAU_STG.1	FAU_STG.1		
AUD.4	FAU_STG_EXT.1.1 FAU_STG_EXT.1.2	FAU_STG_EXT.1.1 FAU_STG_EXT.1.2		
AUD.5	FAU_STG_EXT.1.4 FAU_STG_EXT.1.5	FAU_STG_EXT.1.3		
PSC.1M	FPT_SKP_EXT.1 FPT_APW_EXT.1	FPT_SKP_EXT.1 FPT_APW_EXT.1	FCS_STO_EXT.1	
PSC.1A	FPT_SKP_EXT.1 FPT_APW_EXT.1	FPT_SKP_EXT.1 FPT_APW_EXT.1	FCS_STO_EXT.1	
PSC.2	FCS_CKM.4	FCS_CKM.4		
EXP.1			FPT_AEX_EXT.1.1 FPT_AEX_EXT.1.2	

RFS Anexo I.3	SFR Collaborative Protection Profile for Network Devices v3.0e	SFR Collaborative Protection Profile for Network Devices v2.2e	SFR Protection Profile for Application Software v1.4	SFR Functional Package for Secure Shell (SSH) v1.0
EXP.2			FMT_CFG_EXT .1.2	
EXP.3			FPT_AEX_EXT. 1.5	
PRO.1	FPT_TST_EXT. 1	FPT_TST_EXT. 1		
STM.1	FPT_STM_EXT .1.1	FPT_STM_EXT .1.1		
STM.2	FPT_STM_EXT .1.2	FPT_STM_EXT .1.2		
CERT.1	FIA_X509_EXT .1.1/Rev	FIA_X509_EXT .1.1/Rev	FIA_X509_EXT .1.1	
CERT.2	FIA_X509_EXT .1.2/Rev	FIA_X509_EXT .1.2/Rev	FIA_X509_EXT .1.2	
CERT.3	FIA_X509_EXT .2.1	FIA_X509_EXT .2.1	FIA_X509_EXT .2.1	
CERT.4	FIA_X509_EXT .2.2	FIA_X509_EXT .2.2	FIA_X509_EXT .2.2	
CERT.5	FIA_X509_EXT .3.1	FIA_X509_EXT .3.1		
CERT.6	FIA_X509_EXT .3.2	FIA_X509_EXT .3.2		
CAF.1				
CAF.2				
CAF.3				
CAF.4				
CAF.5				
CAF.6				
CAF.7				
CAF.8				

9. ABREVIATURAS

2FA	*Two-Factor Authentication*
AES	*Advanced Encryption Standard*
CA	*Certification Authority*
CCN	*Centro Criptológico Nacional*
CICLON	*Certificación Iterativa Cloud Nacional*
CL	*Certification Level*
CMAC	*Cipher-based Message Authentication Code*
CN	*Common Name*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones*
CRL	*Lista de Revocación de Certificados*
DH	*Diffie-Hellman*
DN	*Distinguised Name*
DS	*Declaración de Seguridad*
DTLS	*Datagram Transport Layer Security*
EAL	*Evaluation Assurance Level*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ENS	*Esquema Nacional de Seguridad*
ESP	*Encapsulating Security Payload*
FQDN	*Fully Qualified Domain Name*
HMAC	*Hash-based Message Authentication Code*
HTTPS	*HyperText Transfer Protocol Secure*
ID	*Identifier*
IKE	*Internet Key Exchange*
IPSec	*Internet Protocol Security*
KDF	*Key Derivation Function*
LINCE	*Certificación Nacional Esencial de Seguridad*
MAC	*Message Authentication Code*
MCF	*Módulo de Revisión de Código Fuente*
MEC	*Módulo de Evaluación Criptográfica*
MEMeC	*Metodología de Evaluación de Mecanismos Criptográficos*
NIST	*National Institute of Standards and Technology*

NTP	*Network Time Protocol*
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
PGC	*Porcentaje de Garantía Compuesto*
PIN	*Personal Identification Number*
PSC	*Parámetro de seguridad crítico*
PSK	*Pre-Shared Key*
PSS	*Parámetro de seguridad sensible*
RCE	*Remote Command Execution*
RFC	*Request for Comments*
RFID	*Radio Frequency Identification*
RFS	*Requisitos Fundamentales de Seguridad*
SA	*Security Association*
SaaS	*Software-as-a-Service*
SAN	*Subject Alternative Name*
SFR	*Security Functional Requeriments*
SHA	*Secure Hash Algorithm*
SSH	*Secure Shell*
STIC	*Seguridad de las Tecnologías de Información y las Comunicaciones*
TLS	*Transport Layer Security*
TOE	*Target of Evaluation*
UCA	*Unidad de control de acceso*