



Edita:



© Centro Criptológico Nacional, 2019  
NIPO: 083-19-053-9.

Fecha de Edición: febrero de 2019

#### **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**

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

## ÍNDICE

<b>1. INTRODUCCIÓN Y OBJETO .....</b>	<b>4</b>
<b>2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS .....</b>	<b>5</b>
2.1 FUNCIONALIDAD .....	5
2.2 ENTORNO DE USO .....	5
2.3 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO .....	5
2.4 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA) .....	6
<b>3. ANÁLISIS DE AMENAZAS .....</b>	<b>7</b>
3.1 RECURSOS QUE ES NECESARIO PROTEGER.....	7
3.2 AMENAZAS .....	7
<b>4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS).....</b>	<b>9</b>
4.1 REQUISITOS OBLIGATORIOS.....	9
<b>5. ABREVIATURAS .....</b>	<b>12</b>
<b>6. DEFINICIONES .....</b>	<b>13</b>

## 1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto para ser etiquetado como **Plataforma de confianza** en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones (CPSTIC), publicado por el departamento de Productos y Tecnologías del CCN, CCN-PYTEC.
2. Estos requisitos, que no están definidos para una familia específica de productos sino que podrán ser aplicables de manera transversal a un conjunto de familias, ya que representan las funcionalidades de seguridad mínimas que cualquier producto debe implementar para ser etiquetado como “plataforma confiable”, independientemente del fabricante y la tecnología, de cara a hacer frente a un conjunto de amenazas bien definidas. No obstante, este paquete de medidas no está completo en sí mismo, sino que extiende y se aplica en conjunción al conjunto de RFS definidos para cada una de las familias para las que es aplicable.
3. De esta forma, un determinado producto podrá entrar a formar parte del catálogo en la familia que le corresponde dentro del CPSTIC siempre y cuando cumpla con los RFS exigidos para esa familia determinada y, una vez dentro, podrá ser etiquetado como plataforma confiable si cumple además con el paquete extendido de RFS descritos en el presente documento.

## 2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

### 2.1 FUNCIONALIDAD

4. Bajo el término “plataforma” se definen todos aquellos productos o sistemas que sirven como base o soporte para la ejecución de determinados módulos software con los que es compatible.
5. De acuerdo a las garantías que ofrecen y el nivel de evaluación al que se hayan sometido, se distinguen tres tipos o niveles, cuyos requisitos se especifican en la siguiente tabla:

NIVEL 3	NIVEL 2	NIVEL 1
Certificación <i>Common Criteria</i> que incluya los RFS descritos en este documento	Requisitos nivel 3 + Evaluación criptológica CCN	Requisitos nivel 2 + Mecanismo que garantice la integridad de arranque seguro mediante hardware

6. Dependiendo de las condiciones del entorno de uso y de la información que vaya a manejar, el CCN determinará qué nivel de plataforma es el adecuado para cada caso.

### 2.2 ENTORNO DE USO

7. Para la utilización en condiciones óptimas de seguridad de estos productos, es necesaria su integración en un entorno operacional que cumpla las siguientes condiciones:
  - **Administración confiable:** El Administrador (si existe) será un miembro de plena confianza y estará capacitado y formado.

### 2.3 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

8. Típicamente las plataformas suelen presentarse en los siguientes formatos:
  - **Appliance** (hardware provisto de firmware dedicado) sobre el que se instarán las aplicaciones software requeridas.
  - **Firmware** instalable sobre un hardware genérico sobre los que se instalarán las aplicaciones requeridas.

9. Todas las funcionalidades de seguridad están contenidas y ejecutadas dentro del alcance de la plataforma.

Algunos casos típicos de plataformas son:

- Dispositivos móviles.
- Ordenadores personales de sobremesa o portátiles.
- Tabletas.
- Tarjetas inteligentes.

## 2.4 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

10. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).
11. El nivel de confianza EAL (*Evaluation Assurance Level*) conforme a CC, al que deben ser evaluados los Requisitos Fundamentales de Seguridad descritos en este documento debería ser EAL2 o superior.

### 3. ANÁLISIS DE AMENAZAS

#### 3.1 RECURSOS QUE ES NECESARIO PROTEGER

12. Los recursos que es necesario proteger mediante el uso de estos productos son:

- Datos de usuario. Dimensiones: confidencialidad e integridad.
- Parámetros sensibles de seguridad: Deberá implementar las medidas de seguridad adecuadas para proteger los Parámetros Sensibles de Seguridad (PSS) que maneja, que engloban tanto los Parámetros Críticos de Seguridad (PCS) como los Parámetros Públicos de Seguridad (PPS).
  - Parámetros Críticos de Seguridad (PCS) Dimensiones: Confidencialidad e integridad
  - Parámetros Públicos de Seguridad (PPS). Dimensiones: Integridad
- Aplicaciones software cuya instalación en la plataforma haya sido autorizada. Dimensiones: integridad y autorización.
- Sistema operativo y componente software que corra bajo las aplicaciones. Dimensiones: integridad.

#### 3.2 AMENAZAS

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

- **Instalación no autorizada.** Un usuario legítimo o atacante podría instalar aplicaciones en la plataforma que podrían no haber sido autorizadas por la organización.
- **Compromiso de parámetros sensibles de seguridad (PSS).** Un usuario del sistema (no legitimado para estas acciones) o atacante consulta o modifica los PSS almacenados y gestionados por la plataforma.
- **Compromiso de datos de usuario.** Un atacante recupera, accede o modifica datos de usuario guardados en la plataforma y protegidos por ésta.
- **Compromiso de datos de configuración.** Un usuario del sistema (no legitimado para estas acciones) o atacante es capaz de modificar los datos de configuración que son gestionados por la plataforma.
- **Arranque no autorizado.** Un atacante es capaz de burlar la protección de integridad y autenticidad del mecanismo de arranque utilizado por la plataforma y producir un arranque no autorizado.
- **Administración no autorizada.** Un atacante o usuario no autorizado accede a la administración, configuración o desarrollo de funcionalidades establecidas dentro de la plataforma.

- **Modificación del sistema operativo.** Un atacante o usuario no autorizado consigue modificar el sistema operativo o los componentes software sobre los que corren las aplicaciones.
- **Ataque hardware.** Un atacante consigue abrir el producto mediante mecanismos mecánicos sin dejar evidencia del ataque.



## 4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

14. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a ser etiquetados como “Plataforma de confianza” en el CPSTIC.

### 4.1 REQUISITOS OBLIGATORIOS

15. **REQ. 1 Protección de datos en reposo (*cifrado data at rest*)**. El producto implementará cifrado de disco para proteger los datos de usuario, y parámetros sensibles de seguridad con apoyo de claves externas cuya fortaleza dependerá del nivel de la plataforma (ver Tabla).

NIVEL 3	NIVEL 2	NIVEL 1
Algoritmos tipo B. 128 bits	Algoritmos tipo B. 128 bits	Algoritmos tipo B. 192 bits

Tabla 1 Criptografía requerida para los distintos niveles de plataformas

16. **REQ. 2 Listas blancas de aplicación**. Solamente las aplicaciones autorizadas por la organización podrán ser instaladas en el dispositivo.

17. **REQ. 3 Arranque seguro**. El arranque de la plataforma solo será posible si se cumplen estas dos condiciones:

- Ha finalizado con éxito la comprobación de la integridad y autenticidad del sistema operativo.
- Se han descifrado los datos de usuario y los parámetros sensibles de seguridad por medio de una contraseña fuerte<sup>1</sup> u otra medida de autenticación equivalente que es provista por el usuario.

18. **REQ. 4 Seguridad lógica**. La plataforma implementará mecanismos de seguridad lógica durante el arranque y bajo demanda del software y firmware, los mecanismos criptográficos y las funciones de seguridad críticas. En la siguiente se recogen los mecanismos exigidos para cada uno de los niveles.

<sup>1</sup> Las contraseñas fuertes deberán:

- Cambiarse periódicamente, con un período no superior a 180 días.
- No permitir la repetición de al menos las 5 últimas contraseñas utilizadas.
- No permitir realizar un nuevo cambio de contraseña en los 4 días posteriores al último cambio.
- Tener una longitud mínima de 9 caracteres.
- Incluir caracteres alfanuméricos y caracteres especiales como “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “\*”, “(” y “)”, al menos una letra en mayúscula y otra en minúscula, un número o más, y un signo de puntuación o más.

NIVEL 3 - NIVEL 2	NIVEL 1
<ul style="list-style-type: none"> <li>• Auto-test de arranque:               <ul style="list-style-type: none"> <li>○ Verificación de la integridad del SW/FW.</li> <li>○ Test de los mecanismos criptográficos.</li> <li>○ Test de funciones críticas (si procede).</li> </ul> </li> <li>• Auto-test condicionales:               <ul style="list-style-type: none"> <li>○ Comprobación de los PSS durante su establecimiento y entrada/salida.</li> <li>○ Verificación de la integridad y autenticidad del SW/FW durante su arranque en la plataforma.</li> <li>○ Test periódico de funciones críticas y mecanismos criptográficos (si procede).</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Auto-test de arranque:               <ul style="list-style-type: none"> <li>○ Verificación de la integridad del SW/FW (firma digital del CCN).</li> <li>○ Test de los mecanismos criptográficos.</li> <li>○ Test de funciones críticas (si procede).</li> </ul> </li> <li>• Auto-test condicionales:               <ul style="list-style-type: none"> <li>○ Comprobación de los PSS durante su establecimiento y entrada/salida.</li> <li>○ Verificación de la integridad y autenticidad del SW/FW durante su carga (firma digital del CCN).</li> <li>○ Test periódico de funciones críticas y mecanismos criptográficos (si procede).</li> </ul> </li> </ul>

Tabla 2. Descripción de medidas de seguridad lógica

19. **REQ. 5 Borrado seguro.** El sistema implementará borrado seguro bajo demanda, o bien deberá incorporar una herramienta de borrador seguro<sup>2</sup>.
20. **REQ. 6 Actualizaciones seguras.** Todas las actualizaciones deberán estar firmadas por el fabricante y esta firma será verificada por la plataforma antes de la instalación. Además deberá definirse una política de actualización y distribución de las versiones, mediante la cual el administrador autorizará la actualización segura del dispositivo.
21. **REQ. 7 Mecanismos robustos<sup>3</sup> de autenticación.** Los mecanismos robustos de autenticación deberán ser implementados mediante una política de control de acceso que establezca las acciones oportunas ante intentos de autenticación fallidos.

<sup>2</sup> Ver taxonomía de productos STIC - Anexo E.3: Herramientas de borrado seguro

<sup>3</sup> Se considera mecanismo robusto de autenticación el uso de una política de contraseña fuerte. Además, sería deseable usar un segundo factor de autenticación siempre que sea posible.

NIVEL 3	NIVEL 2	NIVEL 1
Contraseña fuerte	Doble factor	Doble factor, al menos uno de ellos Hardware

Tabla 3 Requisitos de autenticación

22. **REQ. 8 Administración segura.** La administración de la plataforma será realizada por un perfil de usuario privilegiado (rol de administrador).
23. **REQ. 9 Detección y/o protección contra intentos de intrusión.** La plataforma implementará mecanismos anti-tamper ante los intentos de manipulación del hardware (ataques mecánicos).

NIVEL 3	NIVEL 2	NIVEL 1
Mecanismos tamper evidence	Mecanismos tamper evidence	Mecanismos tamper response

Tabla 4 Requisitos anti tamper

24. **REQ. 10 Auditoría.** La plataforma confiable guardará un registro con los eventos de seguridad relevantes y asociará cada evento con la identidad del usuario que causa el evento. Este registro estará protegido de modificaciones no autorizadas y pérdida de datos de auditoría. La plataforma tendrá la capacidad de enviar el registro de auditoría a una entidad externa a través de un canal seguro.
25. **REQ. 11 Canales seguros.** La comunicación con las entidades externas se desarrollará a través de canales seguros que proveerán de confidencialidad e integridad al flujo de datos y autenticidad extremo a extremo. Dependiendo del uso y del flujo de datos, se consideran canales seguros:
- Canal CIK<sup>4</sup>. La “*Crypto Ignition Key*” (CIK) se introducirá en el producto desde un dispositivo externo a través de un canal de confianza dedicado.
  - Canal seguro para la conexión con entidades externas de administración remota o servidor de auditoría.

<sup>4</sup> No es obligatorio que la plataforma confiable cuente con una CIK. Solo en el caso de contar con una CIK, ésta se introducirá en el producto a través de un canal de confianza dedicado.

## 5. ABREVIATURAS

<b>CC</b>	Common Criteria
<b>CCN</b>	Centro Criptológico Nacional
<b>CIK</b>	Crypto Ignition Key
<b>CPSTIC</b>	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
<b>EAL</b>	Evaluation Assurance Level
<b>FW</b>	Firmware
<b>HW</b>	Hardware
<b>KEK</b>	Key Encryption Key
<b>PCS</b>	Parámetros Críticos de Seguridad
<b>PPS</b>	Parámetros Públicos de Seguridad
<b>PSS</b>	Parámetros de Seguridad Sensibles
<b>PYTEC</b>	Productos Y TECnologías.
<b>RFS</b>	Requisitos Fundamentales de Seguridad
<b>SFR</b>	Security Functional Requirements
<b>SW</b>	Software

## 6. DEFINICIONES

<b>Mecanismos tamper evidence</b>	Mecanismos de seguridad que permiten detectar a posteriori, mediante inspección, un intento de acceso físico al equipo no autorizado.
<b>Mecanismos tamper response</b>	Mecanismos de seguridad que se encargan de borrar los PSS no protegidos ante un intento de acceso físico no autorizado al equipo.
<b>Parámetros Críticos de Seguridad</b>	Elementos intervinientes en las funciones de seguridad del sistema cuya revelación compromete la seguridad del mismo. Deberán protegerse frente a un acceso, uso, revelación, modificación y sustitución no autorizados. Pertenecen a este grupo, entre otros, las claves para cifrado de tráfico (TEK), claves para cifrado de claves (KEK), claves privadas para firma y autenticación, algoritmos criptográficos Tipo A (no públicos), parámetros de autenticación frente al equipo, etc.
<b>Parámetros Públicos de Seguridad</b>	Elementos intervinientes en las funciones de seguridad del sistema cuya revelación no compromete la seguridad del sistema. Deberán protegerse, al menos, frente a la modificación y sustitución no autorizadas. Pertenecen a este grupo, entre otros, las claves públicas, vectores de inicialización, etc.
<b>Parámetros Sensibles de Seguridad</b>	Engloban tanto los Parámetros Críticos de Seguridad (PCS) como los Parámetros Públicos de Seguridad (PPS).