

# Guía de Seguridad de las TIC CCN-STIC 140

## Taxonomía de productos STIC - Anexo E.3-M Herramientas de borrado seguro



Noviembre de 2022





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

cpage.mpr.gob.es



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

Fecha de Edición: noviembre de 2022

#### LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

#### AVISO LEGAL

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>3</b>
<b>2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS .....</b>	<b>4</b>
2.1 FUNCIONALIDAD .....	4
2.2 CASOS DE USO.....	4
2.2.1. CASO DE USO 1.....	4
2.2.2. CASO DE USO 2.....	5
2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN.....	5
2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO.....	6
2.5 CERTIFICACIÓN LINCE.....	6
<b>3. ANÁLISIS DE AMENAZAS .....</b>	<b>7</b>
3.1 ACTIVOS SENSIBLES A PROTEGER .....	7
3.2 AMENAZAS .....	7
3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD.....	8
<b>4. REQUISITOS DE SEGURIDAD .....</b>	<b>10</b>
4.1 ADMINISTRACIÓN CONFIABLE .....	10
4.2 IDENTIFICACIÓN Y AUTENTICACIÓN .....	10
4.3 CANALES SEGUROS .....	11
4.4 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLE .....	12
4.5 AUDITORÍA .....	12
4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES .....	13
4.7 CRIPTOGRAFÍA.....	13
4.8 BORRADO SEGURO.....	13
4.9 NOTAS DE APLICACIÓN GENERAL .....	13
<b>5. ABREVIATURAS.....</b>	<b>14</b>

## 1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia de Herramientas de borrado seguro 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 a las que sea de aplicación el **Esquema Nacional de Seguridad (ENS) para categoría MEDIA**. Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.
3. Además, la aplicación de estos criterios permitirá:
  - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
  - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
  - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.
4. Por lo tanto, los productos catalogados dentro de la familia de **Herramientas de borrado seguro** 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. Las herramientas de borrado seguro son aplicaciones software diseñadas para impedir que se recupere información no autorizada de dispositivos de almacenamiento que hayan almacenado datos sensibles y que vayan a ser reutilizados o reciclados.
7. Durante un proceso de borrado no seguro, la información no se borra completamente del dispositivo de almacenamiento, sino que simplemente se marca como disponible ese espacio de memoria y se borra la entrada que lo indexa en la tabla de direccionamiento, por lo que puede ser recuperada total o parcialmente mediante la aplicación de sencillas técnicas de análisis forense. Esta recuperación podrá llevarse a cabo hasta que no se haya sobrescrito el espacio liberado en su totalidad.
8. Para posibilitar la reutilización de estos dispositivos sin comprometer la confidencialidad de la información previamente almacenada, se utilizan técnicas estándar de borrado seguro, que tradicionalmente consisten en sobrescribir un determinado número de veces el sector del disco siguiendo un patrón establecido.
9. Los estándares más comunes son: Standard Overwrite, British HMG IS5 Baseline, Russian GOST R 50739-95, NSA 130-2, British HMG IS5 Enhanced, US DoD 5220.22-M, NCSC-TG-025, Navso P-5329-26, US Air Force 5020, Bruce Schneier, Canadian OPS-II, German VSITR, Gutmann, etc. Todos ellos aportan diferentes niveles de seguridad, dependiendo del número de pasadas y del patrón utilizado.

### 2.2 CASOS DE USO

10. Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contemplan dos casos de uso para esta familia de productos tal como se definen a continuación.

#### 2.2.1. CASO DE USO 1

11. Se realiza una gestión centralizada, que permite monitorizar y administrar varias instancias de la herramienta de borrado seguro sobre un grupo heterogéneo de sistemas.

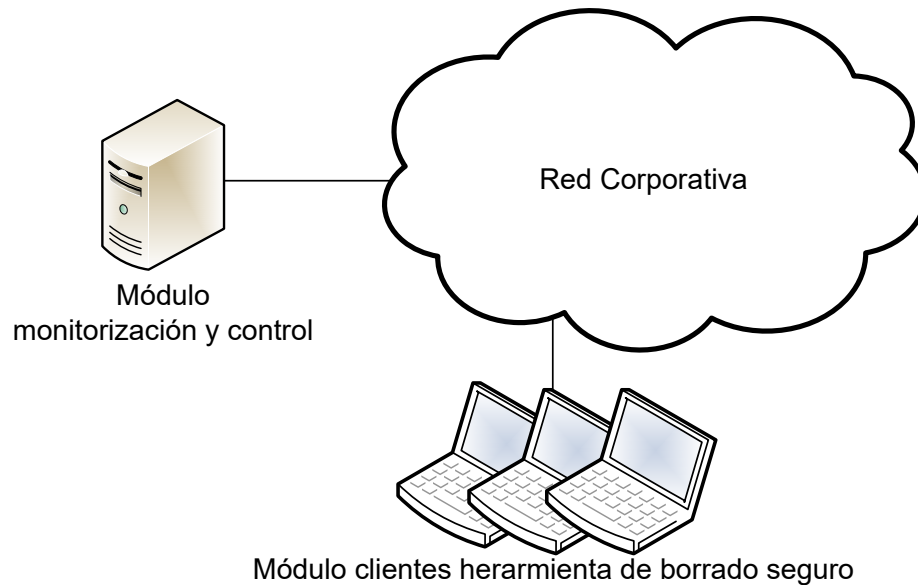


Figura 1-Caso de uso 1

## 2.2.2. CASO DE USO 2

12. La gestión es autónoma en cada equipo, la monitorización y control de ejecución de la herramienta de borrado seguro forma parte de la propia aplicación local.

## 2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

13. Este tipo de herramientas suele utilizarse en dispositivos de almacenamiento que almacenen información sensible, tanto de empresas como del sector público, en combinación con medidas complementarias para preservar la confidencialidad de la información.
14. Para la utilización en condiciones óptimas de seguridad de las herramientas de borrado seguro, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:
  - **Protección física.** El producto debe estar protegido físicamente por su entorno operacional y no sujeto a ataques físicos que puedan comprometer su seguridad o interferir en su correcta operación. En caso de productos software, esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.
  - **Administración confiable.** Los administradores son miembros de plena confianza y velan por los mejores intereses en materia de seguridad de la organización. Dichas personas deben estar debidamente capacitadas y carecer de cualquier intención maliciosa o conflicto de intereses al administrar el producto.
  - **Actualizaciones periódicas.** El *firmware/software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

- **Funcionalidad limitada.** El producto solo debe proporcionar la funcionalidad de *Herramienta de borrado seguro* como función principal y no debe proporcionar ninguna otra funcionalidad o servicio.
- **Protección de las credenciales.** Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.
- **Plataforma confiable.** En caso de tratarse de un producto software, este se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución que la plataforma proporcione.

## 2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

15. Este tipo de productos son herramientas que suelen presentarse en formato de *software* que se instala en un sistema de ficheros proporcionado por un sistema operativo. Se ejecuta en una plataforma que puede ser el sistema operativo, un entorno de ejecución o una combinación de las anteriores.

## 2.5 CERTIFICACIÓN LINCE

16. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Categoría Media, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)<sup>1</sup> que incluya los RFS reflejados en el apartado 4, evaluados considerando el problema de seguridad definido en el presente documento.
17. El alcance de la evaluación deberá incluir el módulo de evaluación básico de 25 días de esfuerzo. Los Módulos de Revisión de Código Fuente (MCF) y de Evaluación Criptográfica (MEC) serán opcionales.

---

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

### 3. ANÁLISIS DE AMENAZAS

#### 3.1 ACTIVOS SENSIBLES A PROTEGER

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

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

#### 3.2 AMENAZAS

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

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



- **A.PSC Compromiso de parámetros de seguridad críticos:** Un atacante puede comprometer los parámetros de seguridad críticos y acceder de forma continuada al producto y a sus datos críticos.
- **A.NOAUTUSR Acceso no autorizado de usuario:** Un atacante puede obtener un acceso no autorizado haciéndose pasar por un usuario ante el producto, haciéndose pasar por el producto ante un usuario, reproduciendo una sesión de usuario, o realizando ataques del hombre en medio.
- **A.CRE Compromiso de credenciales:** Un atacante puede aprovecharse del uso credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.
- **A.BOR. Acceso a información borrada.** Un atacante podría acceder a información sensible previamente borrada por el producto.

### 3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD

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

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

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSC	A.NOAUTUSR	A.CRE	A.BOR
AUD.4					X				
AUD.5					X				
PSC.1						X			
CIF.1		X	X						
BOR.1									X
BOR.2									X
BOR.3									X

## 4. REQUISITOS DE SEGURIDAD

21. 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.
22. La convención utilizada en las descripciones de los RFS es la siguiente:
  - **Selección:** se deberá seleccionar al menos una opción de las indicadas en el RFS y se incluirá en la declaración de seguridad. Ejemplo:

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

DS: Administración del producto local y remota
  - **Asignación:** se deberá especificar el listado de opciones que sean de aplicación al TOE (podría no haber ninguna). Ejemplo:

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

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

### 4.1 ADMINISTRACIÓN CONFIABLE

23. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
24. **ADM.1** El TOE debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.
25. **ADM.2** El TOE debe ser capaz de realizar la gestión de las siguientes funcionalidades:
  - Administración del producto [**selección:** *local; remota*].
  - Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
  - [**asignación:** otras funcionalidades administrables del producto].
26. **ADM.3** El TOE deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones descritas en **ADM.2**.

Nota de aplicación: en el caso de que existan distintos tipos de administrador, cada uno de ellos con distintos permisos, deberá probarse que únicamente pueden realizar aquellas funcionalidades para las que tengan permiso.

### 4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

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

28. **IAU.1** El TOE deberá identificar y autenticar a cada usuario administrador y [asignación: *otros usuarios del producto*] antes de otorgar acceso, salvo para las siguientes funcionalidades [asignación: *listado funcionalidades*].
29. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
30. **IAU.3** El TOE debe disponer de la capacidad de gestión de las contraseñas:
  - a) La contraseña debe poder configurarse con una longitud mínima o igual a 12 caracteres.
  - b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “\$”, “%”, “^”, “&”, “\*”, “(”, “].

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

31. **IAU.4** El TOE debe [selección: *bloquear; cerrar*] la sesión de un usuario después de [asignación: *tiempo de inactividad*] de inactividad.
32. **IAU.5** Cuando el acceso se realice utilizando credenciales por defecto o el usuario no tenga asignadas credenciales, el TOE obligará al [selección: *cambio; establecimiento*] de credenciales en el siguiente acceso.

### 4.3 CANALES SEGUROS

33. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
34. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas: [selección: *servidor de auditoría; [asignación: otras entidades]*] o entre distintas partes del producto, usando [selección: *IPSec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [asignación: *listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].
35. **COM.2** El TOE debe permitir que los canales de comunicación definidos en **COM.1** sean iniciados por él mismo o por las entidades autorizadas.
36. **COM.3** El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en **COM.1**.
37. **COM.4** Protección de la información del canal de administración. El TOE deberá establecer canales seguros cuando intercambie información con el administrador remoto, usando [selección: *IPsec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [asignación: *listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

#### 4.4 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLE

38. **ACT.1** El TOE ofrecerá la posibilidad de consultar la versión actual del firmware/software y podrá [**selección:** actualizarse automáticamente; iniciar actualizaciones manualmente] y [**selección:** comprobar si existen nuevas actualizaciones disponibles; ningún otro].
39. **ACT.2** El TOE deberá utilizar [**selección:** *hashes publicados; firma digital*] que estén autorizados en la guía CCN-STIC-807 para autenticar las actualizaciones *firmware/software* antes de instalarlas.
40. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

#### 4.5 AUDITORÍA

41. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
42. **AUD.1** El producto debe generar registros de auditoría cuando se produzca alguno de los siguientes eventos:
  - a) Al inicio y finalización de las funciones de auditoría.
  - b) *Login y logout* de usuarios registrados.
  - c) Cambios en las credenciales de usuarios.
  - d) Cambios en la configuración del producto [**asignación:** *listado de cambios*].
  - e) Eventos relativos a la funcionalidad del producto: [**asignación:** *listado de eventos*].
  - f) Si el TOE gestiona claves criptográficas, [**selección:** generación; importación; cambio; eliminación de claves criptográficas; ningún otro].
43. **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.
44. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:
  - a) Lectura: usuarios autorizados.
  - b) Modificación: ningún usuario.
  - c) Borrado: [**selección:** solo administradores; ningún usuario]
45. **AUD.4** El TOE debe ser capaz de almacenar en sí mismo la información de auditoría generada y [**selección:** transmitir la información de auditoría generada a una entidad externa utilizando un canal seguro COM.1; no transmitir la información de auditoría generada].

46. **AUD.5** El TOE deberá [**selección**: 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.

#### 4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

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

#### 4.7 CRIPTOGRAFÍA

48. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
49. **CIF.1** El TOE permitirá exclusivamente el empleo de mecanismos criptográficos: [**asignación**: *listado de mecanismos]* autorizados de acuerdo a lo establecido en la guía CCN-STIC-807. La fortaleza de clave empleada será la indicada en esa guía para Categoría MEDIA del ENS, y de acuerdo al nivel de amenaza establecido.

#### 4.8 BORRADO SEGURO

50. **BOR. 1** La herramienta deberá ser capaz de borrar los datos almacenados en los dispositivos seleccionados haciendo imposible la recuperación de datos tras el borrado.
51. **BOR. 2** Permitirá seleccionar el estándar de borrado, estableciendo de esta manera diferentes niveles de seguridad.
52. **BOR. 3** La herramienta permitirá verificar que el proceso de borrado se ha realizado correctamente y notificará el resultado del proceso de verificación. El producto permitirá verificar la integridad de esta información mediante mecanismos de chequeo de integridad implementados con funciones hash compatibles con **CIF.1**.

#### 4.9 NOTAS DE APLICACIÓN GENERAL

53. 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 evaluará si dada la misión y capacidades del producto, se puede considerar que el requisito **no aplica**.
54. 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.

## 5. ABREVIATURAS

<b>CC</b>	<i>Common Criteria</i>
<b>CCN</b>	<i>Centro Criptológico Nacional</i>
<b>CPSTIC</b>	<i>Catálogo de Productos y Servicios de Seguridad de las Tecnologías de Información y las Comunicaciones</i>
<b>EAL</b>	<i>Evaluation Assurance Level</i>
<b>ENS</b>	<i>Esquema Nacional de Seguridad</i>
<b>RFS</b>	<i>Requisitos Fundamentales de Seguridad</i>
<b>SFR</b>	<i>Security Functional Requirements</i>
<b>TLS</b>	<i>Transport Layer Security</i>
<b>TOE</b>	<i>Target of Evaluation</i>

