centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo E.7M: Gestión de metadatos

Julio de 2023

MINISTERIO DE DEFENSA

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

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.07.13 12:56:20 +02'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2023

NIPO: 083-23-071-5
Fecha de Edición: julio de 2023

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1 INTRODUCCIÓN Y OBJETO

1. El presente documento describe las hipótesis, activos, amenazas y Requisitos Fundamentales de Seguridad (RFS), que deberán ser tenidos en cuenta en la realización de la Declaración de seguridad asociada a la evaluación LINCE, exigidos a un producto de la familia de "Gestión de metadatos" para ser incluido en el listado 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 ***Gestión de metadatos*** 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

2 Las herramientas de gestión de metadatos son aplicaciones *software* diseñadas para impedir que se exfiltre información no autorizada. Pueden usarse para borrar metadatos o sobrescribir valores definidos previamente, así como aplicar las políticas de metadatos definidas por una organización.

3 Las soluciones trabajan en base a plantillas que permiten definir los campos de los metadatos que serán borrados, re-emplazados con un valor concreto o que conservarán su valor original.

2.2 CASOS DE USO

6. 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: GESTIÓN AUTÓNOMA

7. La monitorización y control de ejecución de la herramienta de gestión de metadatos forma parte de la propia aplicación local, por lo que se gestiona de forma autónoma.

2.2.2 CASO DE USO 2: GESTIÓN CENTRALIZADA

8. Gestión centralizada de los servicios que se despliegan que permite monitorizar, administrar y controlar las políticas de metadatos sobre un grupo heterogéneo de usuarios y/o sistemas.

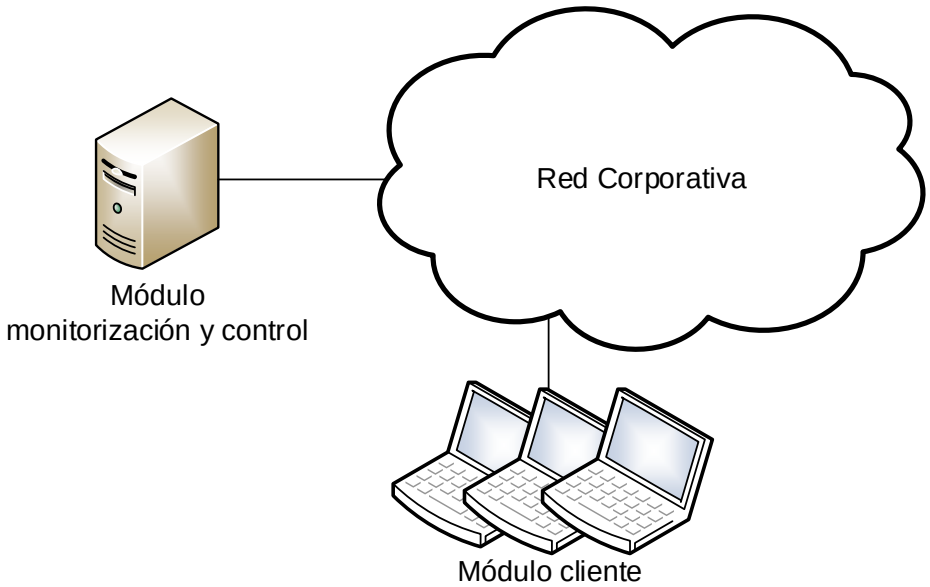

Figura 1 – Ejemplo de Caso de Uso: Gestión centralizada

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

9. Este tipo de herramientas suele utilizarse sobre los ficheros, documentos ofimáticos o archivos multimedia (imagen, audio, video…), en combinación con medidas complementarias, para preservar la fuga de información sensible asociada a los metadatos.

10. Para la utilización en condiciones óptimas de seguridad de las herramientas de gestión de metadatos 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 *software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
    - **Funcionalidad limitada.** El producto solo debe proporcionar la funcionalidad de gestión de metadatos 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 CERTIFICACIÓN LINCE

11. 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)[1] que incluya los RFS reflejados en el apartado **¡Error! No se encuentra el origen de la referencia.**, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.

12. El alcance de la evaluación deberá incluir el módulo de evaluación básico de 25 días de esfuerzo y el Módulo de Evaluación Criptográfica (MEC). El Módulo de Revisión de Código Fuente (MCF) será opcional.

[1] 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

13. Los activos 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

14. 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.COM1 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.INT Compromiso de la integridad del software:** Un atacante puede intentar comprometer la integridad del producto a través de un software sin privilegios ejecutado en la misma plataforma en la que se ejecuta el producto.
- **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.FUN Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad declaradas del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.
- **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.CON Compromiso de credenciales:** Un atacante puede aprovecharse del uso credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.
- **A.MDEXF Exfiltración de Metadatos:** Un atacante puede aprovechar el intercambio de información entre unidades de una misma o distinta organización, para extraer de forma no autorizada la información sensible contenida en los metadatos de los ficheros. Esta información podría ser utilizada para preparar un ataque contra los sistemas y/o los usuarios de la organización.

3.3 TRAZABILIDAD AMENAZAS/ REQUISITOS DE SEGURIDAD

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

	A.NOAUT	A.CRYPTO	A.COM1	A.ACT	A.AUD	A.INT	A.PSC	A.FUN	A.NOAUTUSR	A.CON	A.MDEXF
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						
ACT.4				X						
ACT.5				X						
AUD.1					X					
AUD.2					X					
AUD.3					X					
AUD.4					X					
AUD.5					X					
EXP.1						X				
EXP.2						X				
EXP.3						X				
PSC.1							X			
PSC.2							X			
PRO.1								X		

CIF.1		X	X							
MDT.1										X
MDT.2										X
MDT.3										X
MDT.4										X
MDT.5										X

4 REQUISITOS DE SEGURIDAD (RFS)

16. A continuación, se recoge el listado de requisitos de seguridad que servirán de referencia, agrupados por tipología.

17. 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

18. Estas funcionalidades podrán ser cubiertas el TOE o por su entorno operacional.

19. **ADM.1** El TOE debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.

20. **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*].

21. **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

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

23. **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*].
24. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
25. **IAU.3** El TOE deberá 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.

26. **IAU.4** El TOE debe [**selección***: bloquear; cerrar*] la sesión de un usuario después de [***asignación**: tiempo de inactividad*] de inactividad.
27. **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

28. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
29. **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*].
30. **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.
31. **COM.3** El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en **COM.1**.
32. **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 CONFIABLES

33. **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*].
34. **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.
35. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.
36. **ACT.4** En el caso de que el TOE sea una aplicación *software*, esta deberá estar empaquetada de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
37. **ACT.5** En el caso de que el TOE sea una aplicación *software*, este no descargará ni modificará su propio código binario.

4.5 AUDITORÍA

38. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
39. **AUD.1** El TOE debe generar registros de auditoría y cuando se produzca alguno de los siguientes eventos:
    a) Al inicio y finalización de las funciones de auditoría.
    b) *Login* y *logout* de usuarios.
    c) Cambio 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*].
40. **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.
41. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: solo usuarios autorizados.
    b) Modificación: ningún usuario.
    c) Borrado: [**selección**: *solo administradores; ningún usuario*]

42. **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*].
43. **AUD.5** El TOE deberá [**selección**: *sobreescribir 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 CAPACIDADES ANTI-EXPLOTACIÓN

44. **EXP.1** Cuando el TOE se encuentre en ejecución, este no solicitará la asignación de ninguna dirección explícita de memoria del sistema, ni asignará memoria con permisos simultáneos de escritura y ejecución.
45. **EXP.2** El TOE está configurado por defecto con permisos de ficheros que lo protejan de accesos no autorizados.
46. **EXP.3** En el caso de que el TOE sea una aplicación *software*, este solamente utilizará las bibliotecas de terceras partes declaradas [***asignación****: listado de librerías*].

4.7 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.

4.8 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.

4.9 PROTECCIÓN DE METADATOS

50. **MTD.1** El TOE [**selección***: monitorizará constantemente los directorios definidos por el administrador, monitorizará los archivos adjuntos en los correos de salida antes de su envío, aplicará las reglas a los archivos a petición del usuario, [****asignación****: listado de otras acciones*]
51. **MTD.2** El TOE permitirá la creación de plantillas que definan cómo se procesarán los metadatos. Estas plantillas podrán tener las siguientes opciones para los distintos campos de metadatos:

a) Borrar el contenido de un campo

b) Sobre-escribir el contenido de un campo con un valor definido

c) Mantener los valores originales

d) Añadir en los campos establecidos el valor establecido en una plantilla

52. **MTD.3** El TOE permitirá a los administradores establecer reglas para el procesado de los metadatos de los archivos

53. **MTD.4** El TOE procesará los archivos de metadatos con los siguientes formatos: [***asignación**: listado de formatos de ficheros admitidos*] siguiendo las reglas establecidas por el administrador.

54. **MTD.5** El TOE será capaz de generar información sobre el procesado de los metadatos para generar y visualizar estadísticas con respecto a la ejecución de las reglas establecidas.

4.10 NOTAS DE APLICACIÓN

55. 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***.

56. 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.

57. En el Caso de Uso 2 – Gestión Centralizada, los requisitos deberán aplicarse tanto al Cliente (Agente) como al Módulo de Monitorización y Control (Gestor Central). Por tanto, el alcance de la certificación deberá incluir ambos: el Cliente (Agente) y el Módulo de Monitorización y Control (Gestor Central).

5 ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de Información y las Comunicaciones
EAL	*Evaluation Assurance Level*
ENS	Esquema Nacional de Seguridad
SCL	Servidor de Control de Llamadas
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
TOE	*Target of Evaluation*