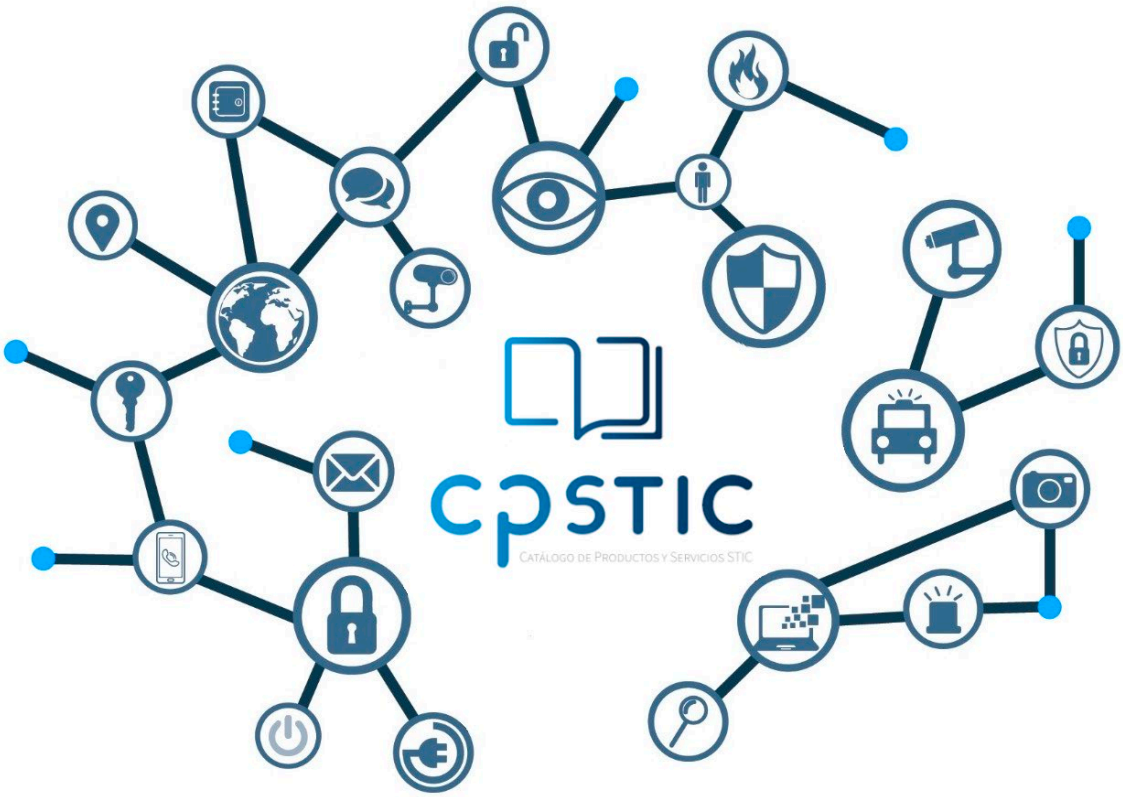
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo I.1-M: Cámaras IP



Septiembre 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 criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.10.03 16:52:56 +02'00'

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

NIPO: 083-23-071-5
Fecha de Edición: septiembre 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 los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Cámaras IP** 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) 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 **Cámaras IP** 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. El video en red, que también se denomina vigilancia IP, funciona como una red IP cableada o inalámbrica. La red se utiliza para transmitir video digital, audio digital y otros datos.
7. Un sistema de video en red permite supervisar y grabar video desde cualquier lugar de la red, ya sea, por ejemplo, una red de área local (LAN) o una red de área amplia (WAN) como Internet.
8. Los componentes esenciales de un sistema de video en red son la cámara de red, el codificador de video (que se emplea para conectar cámaras analógicas a una red IP), la red, el servidor, el dispositivo de almacenamiento y el software de gestión de video (VMS). Tanto la cámara de red como el codificador de video funcionan con un ordenador y tienen capacidades que no tiene ninguna cámara analógica de CCTV.

Figura 1 Sistema de vídeo en red.

9. En este contexto, las cámaras IP deberán implementar las siguientes funciones básicas:
   - Captación y grabación de vídeo.
   - Accesibilidad remota, para realizar las siguientes operaciones:
     - Configuración del equipo.
     - Visualización del vídeo en directo.
   - Gestión de eventos y análisis de vídeo, con capacidad de programar ciertas acciones como respuesta a determinados eventos.

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 y como se definen a continuación.

2.2.1. CASO DE USO 1 – CÁMARA IP EN MODO STAND ALONE

11. En este caso de uso la cámara IP se utiliza de manera individual. La cámara de red permite a usuarios remotos visualizar video en directo o grabado. El video se puede guardar en una ubicación local o remota. Con la autorización correspondiente, se puede acceder al video desde cualquier lugar con acceso a una red IP.

Figura 2 Esquema de cámara IP en modo *stand alone*

2.2.2. CASO DE USO 2- CÁMARA IP CON GESTOR DE VÍDEO CENTRALIZADO

12. En instalaciones profesionales o sistemas que constan de muchas cámaras, es aconsejable utilizar una solución centralizada de gestión de video. Las soluciones de gestión de video se componen de distintas plataformas de hardware y software que se pueden configurar de distintas formas. Por ejemplo, la grabación puede tener lugar localmente en las cámaras o centralizada en una sola ubicación.
13. Las funcionalidades más habituales de un sistema de gestión de video son, entre otras, las siguientes:
    a) **Grabación**. Función principal del sistema. Suelen poder realizar varias grabaciones simultáneas.
    b) **Visualización**. Casi todos los sistemas de gestión de video ofrecen la posibilidad de que varios usuarios visualicen las imágenes de varias cámaras a la vez.
    c) **Gestión y análisis de eventos**. Pueden recibir, procesar y asociar eventos de distintas fuentes. Una vez que se desencadena un evento, puede registrarlo, asociarlo a un clip de video, alertar a un operador, etc.

d) **Administración y gestión**. Incluye la instalación, las actualizaciones de firmware, la seguridad y el registro de auditoria. También se lleva a cabo la configuración de los parámetros de las cámaras.

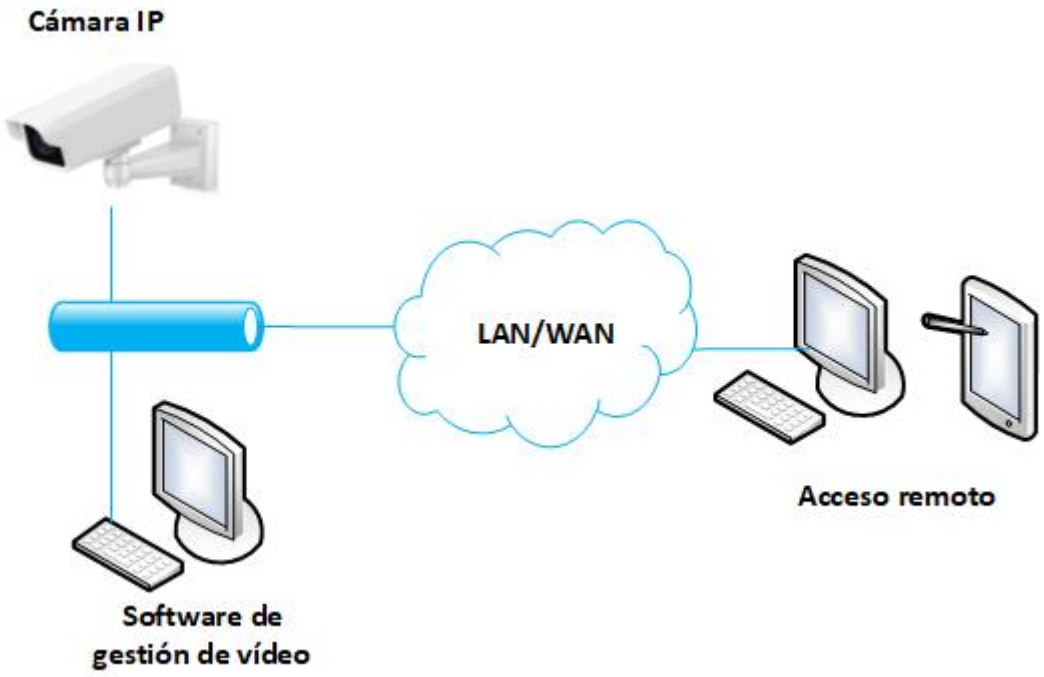


Figura 3 Esquema de cámara IP con gestor de vídeo centralizado

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

14. Este tipo de dispositivos son de uso generalizado en cualquier tipo de ámbito, debido a su trascendencia para la protección de instalaciones de organismos públicos y privados y su facilidad de integración con redes de comunicaciones estándar.
15. Para la utilización en condiciones óptimas de seguridad de estos dispositivos, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

- **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.

- **Protección de las credenciales**: Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

16. Este tipo de productos se presentan en formato de **Equipo dedicado** o ***Appliance*** (hardware provisto de firmware dedicado) con las funcionalidades necesarias para cumplir su finalidad y acotadas al servicio específico que presten. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, éstas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 CERTIFICACIÓN LINCE

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

[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

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

    - **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

20. 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 y A.PSS Compromiso de parámetros de seguridad críticos y/o sensibles:** un atacante puede comprometer los parámetros de seguridad críticos y/o sensibles y acceder de forma continuada al producto y a sus datos críticos y/o sensibles.
- **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.CRE Compromiso de credenciales:** Un atacante puede aprovecharse del uso de credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.

3.3 TRAZABILIDAD AMENAZAS/ REQUISITOS DE SEGURIDAD

21. 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.PSS	A.PSC	A.FUN	A.NOAUTUSR	A.CRE
ADM.1	X									
ADM2	X									
ADM.3	X									
IAU.1	X								X	
IAU.2										X
IAU.3										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					

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSS	A.PSC	A.FUN	A.NOAUTUSR	A.CRE
AUD.2					X					
AUD.3					X					
AUD.4					X					
AUD.5					X					
PSS.1						X				
PSC.1							X			
PSC.2							X			
PRO.1								X		
CIF.1		X	X							
CAM.1								X		
CAM.2	X						X	X		
CAM.3								X		

4. REQUISITOS DE SEGURIDAD PARA CÁMARAS IP

22. 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.

23. 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.

5.1 ADMINISTRACIÓN CONFIABLE

24. Podrán ser cubiertas por el TOE o por su entorno operacional.

ADM.1 El TOE debe definir, al menos, el perfil de administrador y ser capaz de asociar usuarios a perfiles.

ADM.2 El TOE debe ser capaz de realizar la gestión de las siguientes funcionalidades:

- Administración del producto [**selección***: local; remota*].
- [**asignación**: *otras funcionalidades administrables del producto*].

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.

5.2 IDENTIFICACIÓN Y AUTENTICACIÓN

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*].

IAU.2 El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.

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.

5.3 CANALES SEGUROS

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*].

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.

COM.3 El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en COM.1.

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*].

5.4 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

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*].

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.

ACT.3 La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

5.5 AUDITORÍA

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*].

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.

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*]

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*].

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.

5.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

PSS.1 En el caso en que el TOE almacene [***asignación****: parámetros de seguridad sensibles*] estos deberán almacenarse protegidos en integridad, utilizando mecanismos de protección criptológica que cumplan con CIF.1.

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.

PSC.2 Destrucción de PSC. El TOE deberá 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 sobrescritura utilizando alguno de los siguientes métodos:

      - Un patrón pseudoaleatorio generado por el RBG.
      - Todo cero o uno.
      - 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:

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

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

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

5.7 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

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

5.8 CRIPTOGRAFÍA

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.

5.9 CÁMARAS IP

CAM.1 El TOE deberá ser capaz de realizar las siguientes acciones: [***asignación****: funciones realizadas por el TOE*] cuando detecte alguno de los siguientes eventos: *[**asignación**: listado de eventos]*.

CAM.2 El TOE deberá implementar medidas antitamper que evidencien intentos de manipulación física.

CAM.3 El TOE deberá detectar ataques de denegación de servicio e implementar las siguientes medidas reactivas: *[**asignación**: listado de medidas]*.

5. ABREVIATURAS

CCN	*Centro Criptológico Nacional*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones*
ENS	*Esquema Nacional de Seguridad*
IP	*Internet Protocol*
RFS	*Requisitos Fundamentales de Seguridad*
TOE	*Target of evaluation*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL