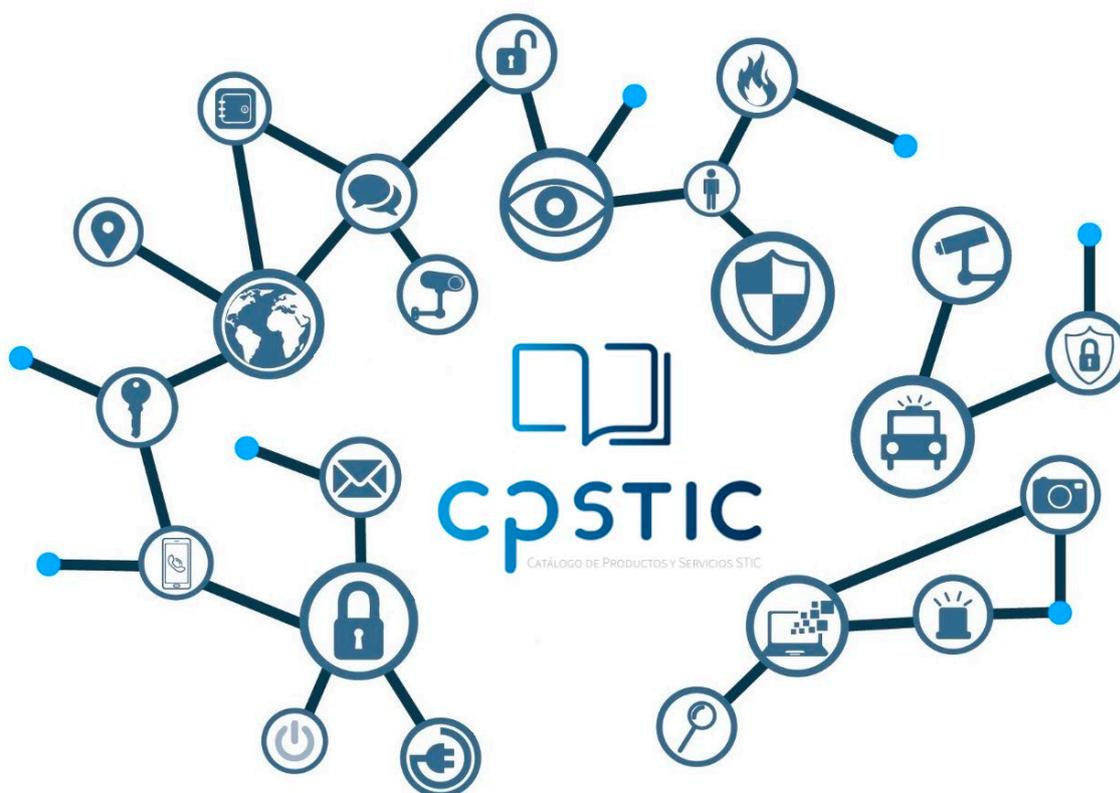


Guía de Seguridad de las TIC CCN-STIC 140

Taxonomía de productos STIC - Anexo B.5 - M: Herramientas de filtrado de navegación



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

1. INTRODUCCIÓN Y OBJETO	3
2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS	4
2.1 FUNCIONALIDAD	4
2.2 CASOS DE USO.....	4
2.2.1. CASO DE USO 1.....	4
2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN.....	5
2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO	5
2.5 CERTIFICACIÓN LINCE.....	6
3. ANÁLISIS DE AMENAZAS	7
3.1 ACTIVOS SENSIBLES A PROTEGER	7
3.2 AMENAZAS	7
3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD.....	8
4. REQUISITOS DE SEGURIDAD	10
4.1 ADMINISTRACIÓN CONFIABLE	10
4.2 IDENTIFICACIÓN Y AUTENTICACIÓN	11
4.3 CANALES SEGUROS	11
4.4 CRIPTOGRAFÍA.....	12
4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES	12
4.6 AUDITORIA	12
4.7 CAPACIDADES ANTI-EXPLOTACIÓN.....	13
4.8 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES	13
4.9 FILTRADO DE NAVEGACIÓN	14
5. ABREVIATURAS.....	15

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia Herramientas de filtrado de navegación 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) 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 **Herramientas de filtrado de navegación** 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

- Las herramientas de filtrado de navegación son aplicaciones software que protegen al usuario durante el acto de navegación por Internet. Controlan los sitios web y servicios que pueden ser vistos o accedidos. Para lograrlo, hacen uso de listas de confianza o reputación basadas en direcciones URL¹, así como pueden limitar todo acceso a sitios no confiables o potencialmente peligrosos.

2.2 CASOS DE USO

- Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contempla un caso de uso para esta familia de productos tal y como se define a continuación.

2.2.1. CASO DE USO 1

- La herramienta se ejecuta sobre una plataforma que separa la red externa de la interna, de forma que todo el tráfico de red tenga que pasar por la herramienta.

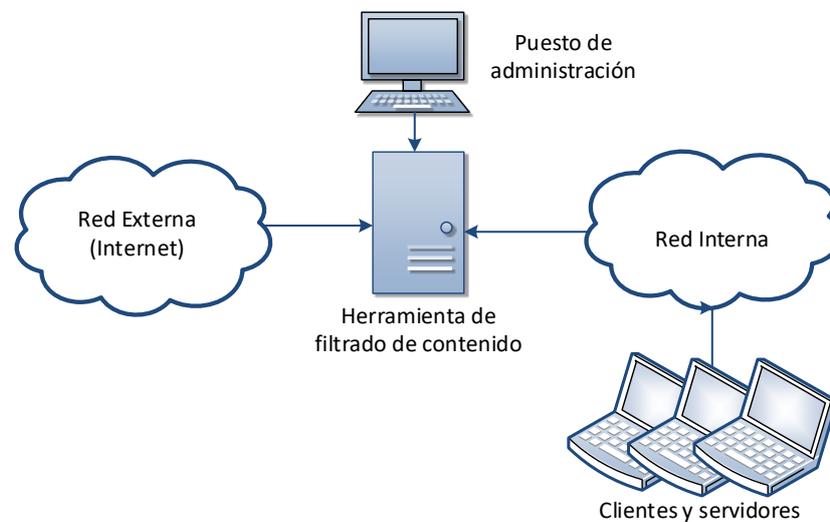


Figura 1. Caso de uso 1

¹Uniform Resource Locator. Localizador Uniforme de Recursos cuyo formato general es esquema://máquina.directorio.archivo

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

9. Para la utilización en condiciones óptimas de seguridad de los sistemas para la prevención de fuga de datos, 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 *Filtrado de Navegación* 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

10. Este tipo de productos se presentan en formato **software**, instalándose 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.
11. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2, éstas quedan fuera del alcance analizado, y deberán ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 CERTIFICACIÓN LINCE

12. 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)² que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.

² 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 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

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.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.INT Compromiso de la integridad del software/firmware:** 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.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.RED Ataque a la red:** Un atacante consigue acceder a la red pudiendo realizar mapeos de las máquinas que residen en ella y obtener datos de dirección IP, servicios o cualquier otra información que le permita lanzar ataques a dichas máquinas y servicios.

3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD

15. 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.INT	A.PSC	A.NOAUTUSR	A.CRE	A.RED
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							

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.INT	A.PSC	A.NOAUTUSR	A.CRE	A.RED
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					
EXP.1						X				
EXP.2						X				
EXP.3						X				
PSC.1							X			
CIF.1		X	X							
NAV.1										X
NAV.2										X
NAV.3										X

4. REQUISITOS DE SEGURIDAD

16. 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.

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 por el producto 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 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.

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 CRIPTOGRAFÍA

33. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
34. **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.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

35. **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*].
36. **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.
37. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.
38. **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).
39. **ACT.5** En el caso de que el TOE sea una aplicación software, este no descargará ni modificará su propio código binario.

4.6 AUDITORIA

40. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
41. **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].
42. **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.
43. **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]

4.7 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*].

4.8 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**.

4.9 FILTRADO DE NAVEGACIÓN

48. **NAV.1** El producto debe intervenir en el flujo de información entre la red interna y la red externa, rechazando el paso de información no autorizada.
49. **NAV.2** El flujo de información intercambiada entre la red externa e interna deberá contener los siguientes atributos de seguridad: origen, destino, aplicación y categoría de la petición.
50. **NAV.3** El flujo de información intercambiada entre la red externa e interna, se evaluará según reglas predefinidas por el administrados del producto.

5. ABREVIATURAS

CC	<i>Common Criteria</i>
CCN	<i>Centro Criptológico Nacional</i>
CPSTIC	<i>Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones</i>
EAL	<i>Evaluation Assurance Level</i>
ENS	<i>Esquema Nacional de Seguridad</i>
NIAP	<i>National Information Assurance Partnership</i>
RFS	<i>Requisitos Fundamentales de Seguridad</i>
SFR	<i>Security Functional Requirements</i>
URL	<i>Uniform Resource Locator</i>

