centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

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

Febrero 2020

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.02.13 17:36:32 +01'00'

NIPO: 083-19-053-9

Fecha de Edición: febrero 2020

ÍNDICE

1. INTRODUCCIÓN Y OBJETO 4
2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS 5
2.1 FUNCIONALIDAD 5
2.2 CASOS DE USO 5
2.2.1. CASO DE USO 1 5
2.3 ENTORNO DE USO 6
2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO 6
2.5 CERTIFICACIÓN LINCE 6
3. ANÁLISIS DE AMENAZAS 7
3.1 RECURSOS QUE ES NECESARIO PROTEGER 7
3.2 AMENAZAS 7
3.2.1. COMUNICACIONES CON EL PRODUCTO 7
4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS) 8
4.1 ADMINISTRACIÓN CONFIABLE 8
4.2 IDENTIFICACIÓN Y AUTENTICACIÓN 8
4.3 CANALES DE COMUNICACIÓN CONFIABLES 9
4.4 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES 9
4.5 CAPACIDAD ANTI-EXPLOTACIÓN 9
4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES 10
4.7 REGISTROS AUDITORIA 10
4.8 REQUISITOS CRIPTOGRÁFICOS 10
4.9 FILTRADO DE NAVEGACIÓN 11
5. ABREVIATURAS 12

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 de Seguridad de las Tecnologías de la Información y la Comunicación (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

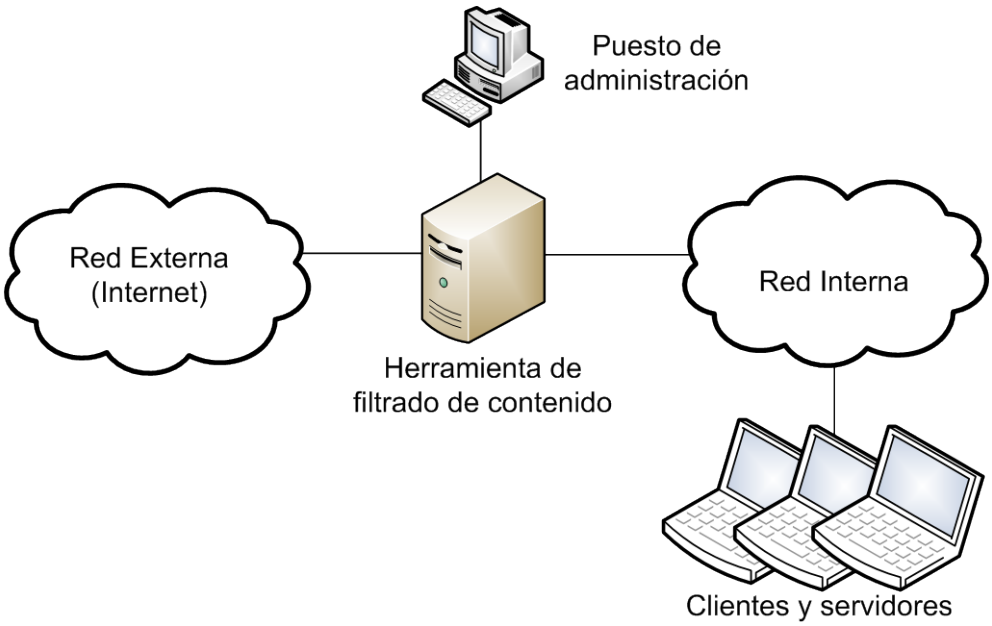
6. Las herramientas de filtrado de navegación son aplicaciones software que protegen al usuario durante el acto de navegación por Internet. Controlan los sitios web y servicios que pueden ser vistos o accedidos. Para lograrlo, hacen uso de listas de confianza o reputación basadas en direcciones URL[1], así como pueden limitar todo acceso a sitios no confiables o potencialmente peligrosos.

2.2 CASOS DE USO

7. 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

8. 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.



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

2.3 ENTORNO DE USO

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:

   - **Plataforma segura**: El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.
   - **Administración confiable**: El Administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello se asume que dicha persona estará capacitada, formada y carecerá de cualquier intención maliciosa.
   - **Flujo de información:** La información entre la red interna y externa sólo podrá realizarse a través del producto.
   - **Actualizaciones periódicas**: El software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
   - **Acceso:** El producto tiene acceso a todos los datos del sistema necesarios para llevar a cabo todas sus funciones" que entiendo que no se si aplicaría en este caso.

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 RECURSOS QUE ES NECESARIO 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.
- **AC.Datos**. Datos de configuración del producto y de auditoría generados por éste. Información que atraviese el producto entre sus interfaces de red.
- **AC.Actualizaciones**. Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

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

3.2.1. COMUNICACIONES CON EL PRODUCTO

- **A.RED. Ataque a la red.** Un atacante, desde dentro o desde fuera de la red, consigue acceder a información intercambiada a través de la red entre el producto y otras entidades autorizadas o modificar sus comunicaciones.
- **A.LOCAL. Ataque local.** Un atacante puede actuar a través de software no privilegiado ejecutado en la misma plataforma de computación donde se ejecuta el producto. Los atacantes podrían modificar de forma maliciosa los ficheros o comunicaciones que utiliza el producto.
- **A.REST. Acceso a información almacenada.** Un atacante podía acceder a información sensible almacenada en la plataforma en la que se instala y ejecuta el producto.
- **A.NODET. Actividad no detectada.** Un atacante consigue acceder, cambiar o modificar la funcionalidad de seguridad de la herramienta sin que esto sea apreciado por el administrador.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

15. 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.

4.1 ADMINISTRACIÓN CONFIABLE

16. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional**.
17. **ADM.1** El producto debe de definir al menos el rol de administrador y ser capaz de asociar un usuario con un rol.
18. **ADM.2** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades:
    a) Administración del producto de forma local y remota.
    b) Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
    c) Otros parámetros de configuración del producto.
19. **ADM.3** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones en la medida anteriormente descrita.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

20. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional**.
21. **IAU.1** El producto deberá identificar y autenticar a cada usuario antes de otorgar acceso.
22. **IAU.2** El producto debe implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
23. **IAU.3** El producto debe proteger contra lectura y modificación no autorizadas las credenciales de autenticación.
24. **IAU.4** El producto debe disponer de la capacidad de gestión de las contraseñas:
    a) La contraseña debe de poder configurarse con una longitud mínima o igual a 9 caracteres.
    b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]
25. **IAU.5** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.

4.3 CANALES DE COMUNICACIÓN CONFIABLES

26. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
27. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas o entre distintas partes del producto empleando funciones, algoritmos y protocolos que estén de acuerdo a lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).
28. **COM.2** El TOE debe permitir que estos canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas.
29. **COM.3** El producto hará uso de certificados digitales para la autenticación cuando utilice cualquiera de estos protocolos.

4.4 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

30. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL).
31. **ACT.1** El producto debe ofrecer la posibilidad de consultar la versión actual del firmware/software.
32. **ACT.2** El producto debe ofrecer mecanismos (conforme a la criptografía de empleo en el ENS) a través de hashes o firma digital para autenticar las actualizaciones de firmware/software antes de instalarlas.
33. **ACT.3.** La actualización del firmware/software se permitirá únicamente a usuarios con rol de administrador.
34. **ACT.4** El producto debe ofrecer la posibilidad de iniciar actualizaciones de forma manual y de comprobar si existen nuevas actualizaciones disponibles.
35. **ACT.5** El producto deberá estar empaquetado de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
36. **ACT.6** El producto no descargará ni modificará su propio código binario.
37. **ACT.7** El producto solamente utilizará las bibliotecas de terceras partes declaradas por el fabricante.

4.5 CAPACIDAD ANTI-EXPLOTACIÓN

38. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL).
39. **EXP.1** Capacidades anti-explotación. El producto se auto-protegerá cuando se encuentre en ejecución, de tal forma que tenga acceso exclusivo a su zona de memoria asignada.
40. **EXP.2** El producto está configurado por defecto con permisos de ficheros que lo protejan de accesos no autorizados.

4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

1. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional.**
2. **CRD.1** En el caso en que el producto almacene credenciales y/o datos sensibles, éstos no deberán almacenarse en claro.
3. **CRD.2** En el caso en el que el producto utilice sus propias credenciales de acceso, el producto obligará al cambio/establecimiento de credenciales cuando el acceso se realice utilizando credenciales por defecto o el usuario no tenga asignadas credenciales.

4.7 REGISTROS AUDITORIA

1. Estas funcionalidades de seguridad mitigan la amenaza (A.NODET).
2. **AUD.1** El producto debe generar información de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzca alguno de los siguientes eventos:
    a) *Login* y *logout* de usuarios registrados.
    b) Cambio en las credenciales de usuarios.
    c) Cambios en la configuración del producto.
    d) Eventos relativos a la funcionalidad del producto.
3. **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 (si aplica).
4. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: usuarios autorizados.
    b) Modificación: ningún usuario.
    c) Borrado: administradores.

4.8 REQUISITOS CRIPTOGRÁFICOS

5. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST).
6. **REQ. 2** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos que utilicen suites de cifrado que estén incluidas entre las autorizadas para Categoría Media del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.
7. **REQ. 3** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

4.9 FILTRADO DE NAVEGACIÓN

8. **NAV.1** El producto debe de intervenir en el flujo de información entre la red interna y la red externa, rechazando el paso de información no autorizada.
9. **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.

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