GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo B.5: Herramientas de filtrado de navegación

Noviembre 2017

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.11.27 11:17:19 +01'00'

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017

ÍNDICE

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). 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

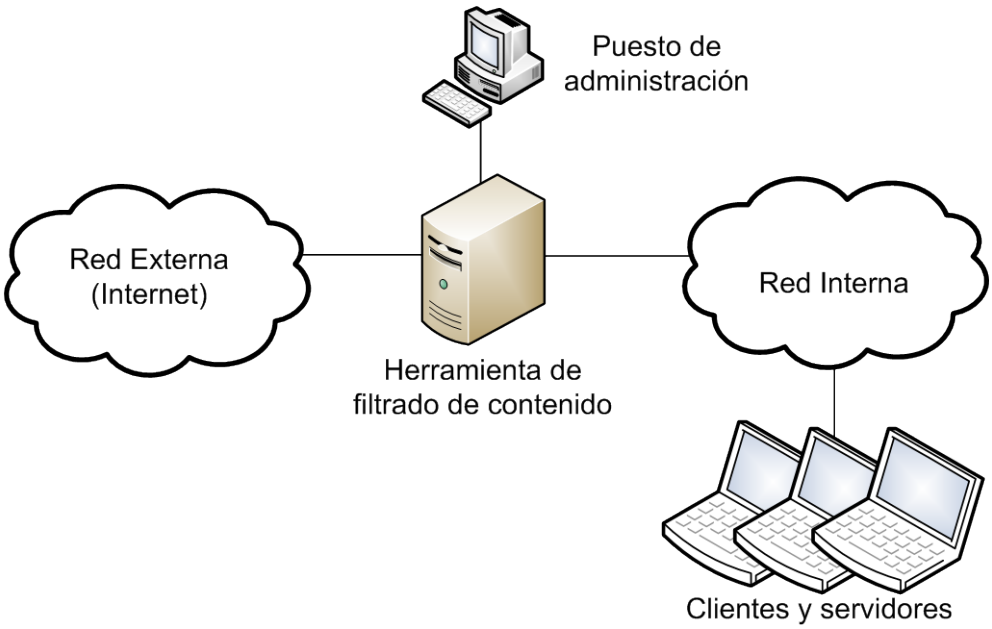
6. Las herramientas de filtrado de navegación son aplicaciones software que protegen al usuario durante el acto de navegación por Internet. Controlan los sitios web y servicios que pueden ser vistos o accedidos. Para lograrlo, hacen uso de listas de confianza o reputación basadas en direcciones URL[1], 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.

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.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

11. El estándar *Common Criteria* (CC)proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).

12. En el ámbito de CC se elaboran unos perfiles de seguridad que definen, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de seguridad, tanto funcionales como de evaluación, independientes de la implantación.

13. Los productos dentro de esta familia deberán cumplir con los SFR (*Security Functional Requirements*) que se especifican en el siguiente perfil de protección certificado de acuerdo a la norma *Common Criteria,* junto con los restantes requisitos fundamentales de seguridad recogidos en la sección 4:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Application Software.[2]	1.2	25/04/2016	NIAP

Tabla 1. Perfil de protección

[2] https://www.commoncriteriaportal.org/files/ppfiles/pp_app_v1.2.pdf

14. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:

    - **El determinado por el perfil de protección** para aquellos SFR incluidos en los perfiles exigidos cuando los productos se encuentren certificados contra el perfil exigido.
    - **EAL2 o superior** para los RFS adicionales que no encuentren incluidos dentro del perfil.
    - **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra el perfil.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

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

- Comunicaciones con el producto.
- Toda la información que tenga que hacer uso del producto para ser transmitida (cómo contraseñas, parámetros de configuración, actualizaciones críticas).
- Datos de configuración del producto y de auditoría generados por éste.
- Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

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

- **Ataque a la red.** Un atacante, que acceda al canal de comunicación, puede modificar las comunicaciones entre los distintos módulos del producto.
- **Monitorización del tráfico.** Un atacante, desde dentro o desde fuera de la red, consigue acceder a información intercambiada entre los distintos módulos de la aplicación.
- **Ataque local.** Un atacante puede actuar a través de Software 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.
- **Acceso físico.** Un atacante podía acceder a información sensible almacenada en el sistema.
- **Registros Auditoria.** Un usuario o proceso podría causar la pérdida o modificación de registros de auditoría del producto de forma dañina.
- **Auditoria**. Un atacante puede no ser detectado, si las acciones de los usuarios no se registran como auditables.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

17. 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 PERFIL DE PROTECCIÓN

18. **REQ. 1** El producto debe cumplir con los SFR (*Security Functional Requirements*) que se especifican el siguiente perfil de protección certificados de acuerdo a la norma *Common Criteria*:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Application Software.[3]	1.2	25/04/2016	NIAP

Tabla 2. Perfil de protección

19. **REQ. 2** En caso de que el producto no esté certificado contra el perfil indicado, la declaración de seguridad deberá contener al menos los SFR de éste con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

20. **REQ. 3** El producto deberá identificar y autentificar la identidad de todos los usuarios, antes de otorgar acceso a la funcionalidad producto.
21. **REQ. 4** El producto deberá tener asociado cada usuario a un perfil, que contenga un conjunto de permisos predefinidos por el administrador.

4.3 FLUJO INFORMACIÓN

22. **REQ. 5** 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.
23. **REQ. 6** El flujo de información intercambiada entre la red externa e interna deberá contener los siguientes atributos de seguridad: origen, destino, aplicación, categoría de la petición.
24. **REQ. 7** El flujo de información intercambiada entre la red externa e interna, se evaluará según reglas predefinidas por el administrados del producto.

[3] https://www.commoncriteriaportal.org/files/ppfiles/pp_app_v1.2.pdf

4.4 INICIO Y RECUPERACIÓN

25. **REQ. 8** Desde la puesta en marcha del producto o una recuperación debido a una interrupción en el servicio, no se deben comprometer de ninguna de las redes conectadas en el producto.

4.5 PROTECCIÓN RECURSOS

26. **REQ. 9** El producto se debe proteger contra intentos de usuarios no autorizados, que tengan el fin de evitar, desactivar o alterar las funciones de seguridad del producto.

4.6 REGISTROS AUDITORIA

27. **REQ. 10** Se debe proporcionar un medio para almacenar los eventos relacionados con la seguridad, de forma que permita interpretarse por un usuario.
28. **REQ. 11** 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.
29. **REQ. 12** Se registrarán en la auditoria los siguientes eventos:
    a. Iniciar o detener la auditoria de la aplicación
    b. Cambios en el grupo de usuario que tiene el rol de administrador.
    c. Utilización por parte del usuario de los mecanismos de autenticación.
    d. Cualquier utilización de los mecanismos de autenticación del producto
    e. Todas las decisiones en cuanto a las peticiones en el intercambio de información entre la red interna y externa.
    f. Cambio de hora o fecha.
    g. Cambios de la configuración del producto
30. **REQ. 13** Los registros de auditoría, no podrán modificarse por ningún usuario.
31. **REQ. 14** Sólo podrán leer los registros de auditoría los usuarios autorizados.
32. **REQ. 15** Los administradores serán los únicos usuarios que puedan borrar registros de auditoría.

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*