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 F.3: Herramientas anti-spam

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 11:29:31 +01'00'

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017

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 **Herramientas *Anti-Spam*** 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 *Anti-Spam*** 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. Los productos asociados la familia Herramientas *Anti-Spam* están orientados a proporcionar seguridad a los sistemas de correo electrónico. Basado en analizar el correo entrante y saliente y bloquear correo no deseado o basura y código dañino (*malware)* antes de que pueda comprometer la red o los clientes de correo

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 contemplan dos casos de uso para esta familia de productos tal y como se definen a continuación.

2.2.1. CASO DE USO 1- MODO PASARELA

8. El dispositivo se encuentra en la misma red que el servidor de correo electrónico y todos los clientes de correo. La herramienta *Anti-Spam* recibe todos los *emails* y tras analizarlos, los que no se retienen en cuarentena o se bloquean, se reenvían al servidor de correo de destino.

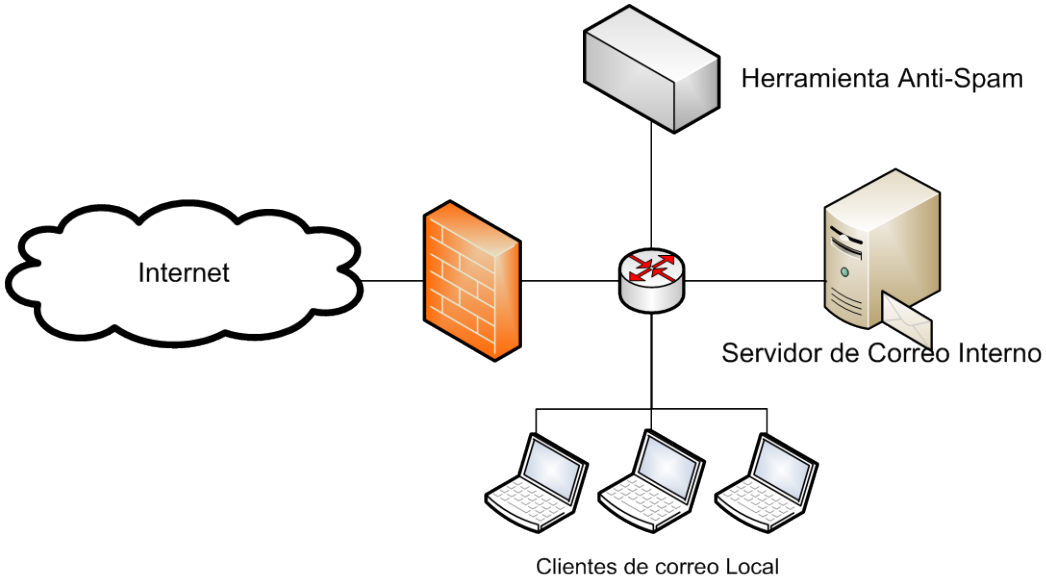

Figura 1 – Ejemplo de Caso de Uso: Modo pasarela

2.2.2. CASO DE USO 2 – MODO TRANSPARENTE

9. El dispositivo se encuentra físicamente entre el servidor de correo y todos los clientes de correo local, permitiendo la interceptación de los mensajes.

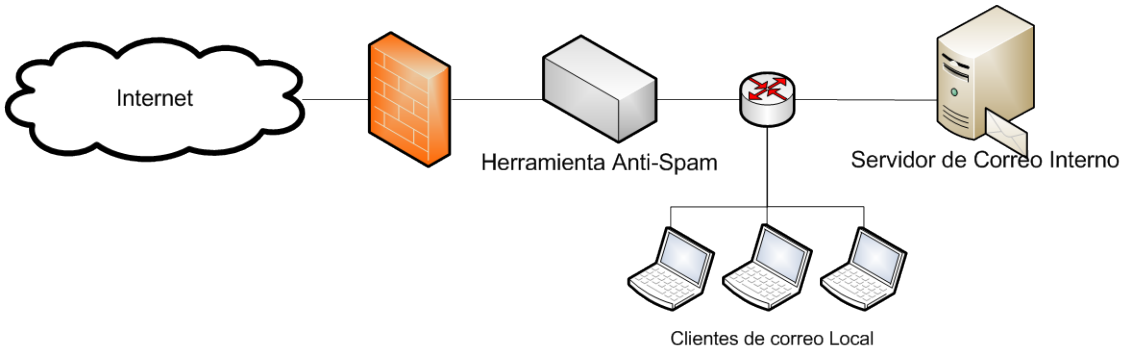

Figura 2 – Ejemplo de Caso de Uso: Modo transparente

2.3 ENTORNO DE USO

10. Por lo general, este tipo de dispositivos se encuentran en grandes o medianas empresas, así como en redes del sector público, como parte de una arquitectura de defensa en profundidad, en combinación con medidas complementarias en diferentes capas de protección.

11. 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 deberá instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.
    - **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 dañina al administrar el producto.
    - **Actualizaciones periódicas:** El firmware y el software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
    - **Política de seguridad de la Información.** La política de seguridad deberá recoger el conjunto de principios, la organización y los procedimientos impuestos por una organización para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

12. Este tipo de productos se presentan tanto en formato **Equipo dedicado o (*Appliance:*** hardware provisto de firmware dedicado y software) como en forma de aplicación **Software**. Además, debe presentar las funcionalidades estrictamente necesarias para cumplir su finalidad y acotadas al servicio específico que presten.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

13. 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).

14. 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.

15. Los productos dentro de esta familia deberán cumplir con los requisitos Fundamentales de Seguridad reflejados en el apartado 4 y con los SFR (*Security Functional Requirements*) que se especifican en alguno de los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Devices.[1]	1.0	27/02/2015	CCDB
Protection Profile for Network Devices.[2]	1.1	08/06/2012	NIAP
Protection Profile for Application Software.[3]	1.2	25/04/2016	NIAP

Tabla 1. Perfiles de protección

16. 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 alguno de los perfiles anteriormente descritos.
- **EAL2 o superior** para los RFS adicionales que no encuentren incluidos dentro de un perfil.
- **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra ningún perfil.

[1] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[2] https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.1.pdf
[3] https://www.commoncriteriaportal.org/files/ppfiles/pp_app_v1.2.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

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

    - Comunicaciones con el producto.
    - Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos.
    - 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

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

    - **Errores en la administración**. Un administrador, involuntariamente, puede instalar o configurar el producto de forma incorrecta y dejar los mecanismos de seguridad sin efecto.
    - **Fallo en las funcionalidades de seguridad del producto**. Los mecanismos de seguridad del producto pueden fallar y comprometer sus funcionalidades de seguridad.
    - **Acciones no autorizadas**. Un usuario podría obtener acceso no autorizado a los recursos. Un usuario, proceso o entidad externa dañina, se podría enmascarar como una entidad autorizada, para obtener un acceso no autorizado a los recursos del producto.
    - **Actualizaciones no autorizadas.** Se podría proporcionar al producto de una actualización dañina que comprometa su seguridad.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

19. 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 REQUISITOS CRIPTOGRÁFICOS

20. **REQ. 1** Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807 Criptología de empleo en el ENS (Categoría ALTA).

4.2 CORREO BASURA (*SPAM*)

21. **REQ. 2** El producto deberá poder escanear todos los correos entrantes y salientes e identificar los correos identificados como correo basura.
22. **REQ. 3** El producto deberá permitir bloquear o introducir una marca a los correos identificados como correo basura.
23. **REQ. 4** El producto utilizará listas blancas y negras de direcciones y dominios de correo para identificar correos como correo basura.
24. **REQ. 5** El producto analizará el contenido de los mensajes para identificar correos como correo basura.

4.3 PRODUCTO *APPLIANCE*

25. **REQ. 6** En caso de que el producto sea un equipo dedicado (*Appliance),* deberá estar certificado con uno de los siguientes perfiles de protección publicados certificados de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Devices.[4]	1.0	27/02/2015	CCDB
Protection Profile for Network Devices.[5]	1.1	08/06/2012	NIAP

Tabla 2. Perfiles de protección

[4] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[5] https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.1.pdf

26. **REQ. 7** En caso de que el producto no esté certificado bajo ningún perfil de los anteriores, la declaración de seguridad deberá contener al menos los SFR (*Security Functional* Requirements) del perfil *Collaborative Protection Profile for Network Devices v1.0* con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.4 PRODUCTO SOFTWARE

27. **REQ. 8** En caso de que el producto sea únicamente Software, deberá estar certificado con el siguiente perfile de protección certificado de acuerdo a la norma *Common Criteria:*

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Application Software.[6]	1.2	25/04/2016	NIAP

Tabla 3. Perfil de protección

28. **REQ. 9** En caso de que el producto no esté certificado contra el perfil indicado, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) de éste con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior.**

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

5. ABREVIATURAS

CC	*Common Criteria*
CCDB	*Common Criteria Development Board*
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*
TIC	*Tecnologías de Información y las Comunicaciones*