centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo F.3: Protección de correo electrónico

Marzo 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN
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
2022.03.21 15:53:40 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-102-1.

Fecha de Edición: marzo de 2022

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Protección de correo electrónico** 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 para los 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 **Protección de correo electrónico** 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 '*Protección de correo electrónico*' están orientados a proporcionar seguridad a los sistemas de correo electrónico. Su objetivo es analizar el correo entrante y saliente, y bloquear correo no deseado o basura (*spam*) 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 tres (3) casos de uso para esta familia de productos, tal y como se define 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 de protección de correo electrónico recibe todos los *emails* y los analiza. Aquellos que no se retienen en cuarentena o se bloquean, se reenvían al servidor de correo de destino.

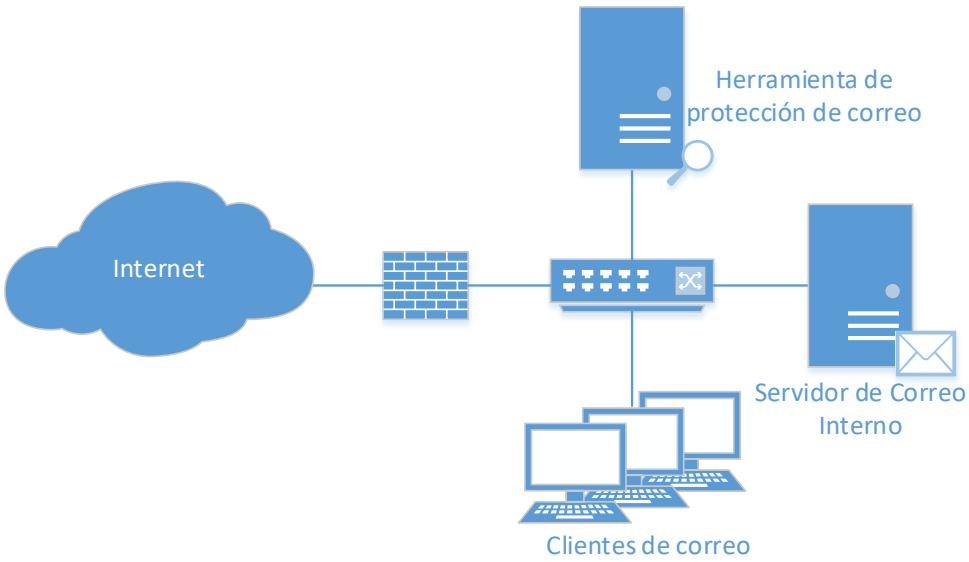

Figura 1 – Ejemplo de Caso de Uso: Modo Pasarela

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

2.2.3. CASO DE USO 3 – INCLUIDO EN EL SERVIDOR DE CORREO

10. El producto se despliega como un módulo software en el servidor en el que se encuentra alojado el servidor de correo electrónico.

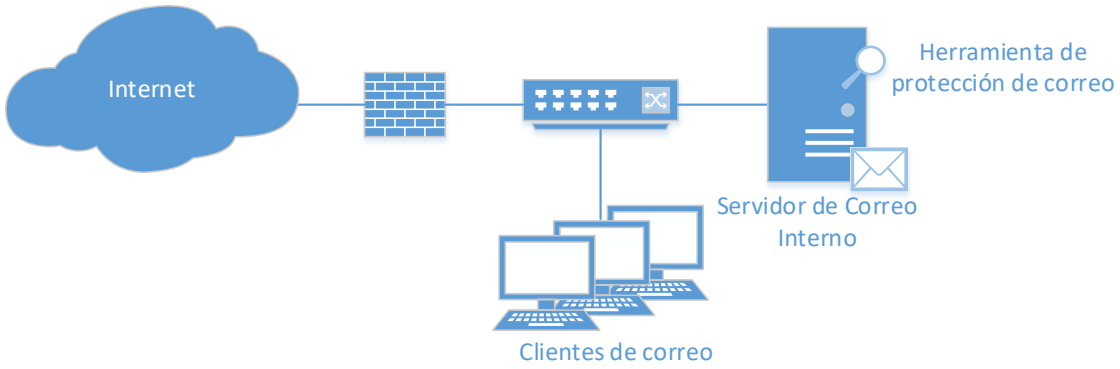

Figura 3 – Ejemplo de Caso de Uso: Herramienta de protección de correo en el servidor de correo

2.3 ENTORNO DE USO

11. 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 adicionales en diferentes capas de protección.
12. Para la utilización en condiciones óptimas de seguridad del producto, 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.

- **Plataforma segura:** En caso de tratarse de un producto *software*, este 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 dañina al administrar el producto.
- **Actualizaciones periódicas:** El firmware (si aplica) y el software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **Protección de las credenciales:** Todas las credenciales, en especial las del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

13. Este tipo de productos se presentan, tanto en formato **Equipo dedicado o *Appliance*** (*hardware* provisto de *firmware* dedicado y *software*), como en formato ***software*** (que se instala en un sistema de ficheros proporcionado por un Sistema Operativo).

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (*COMMON CRITERIA*)

14. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos TIC (Tecnologías de la Información y de las Comunicaciones).
15. En el ámbito de CC se definen un conjunto de objetivos y requisitos de seguridad, tanto funcionales (*SFR, Security Functional Requirements*) como de evaluación (*SAR, Security Assurance Requirements*), independientes de la implantación, que cada producto incluirá dentro de su declaración de seguridad (*ST, Security Target*).
16. **Los productos dentro de esta familia, deberán disponer de una declaración de seguridad (ST) certificada con un nivel de confianza EAL2 o superior (*Evaluation Assurance Level*), que contenga los RFS indicados en el apartado 4.**
17. En caso de que alguno de los requisitos indicados en el apartado 4 no se encuentre recogido en la declaración de seguridad del producto, pero este sí implemente esa función de seguridad, se podrá llevar a cabo una *evaluación STIC complementaria***,** cuyo objetivo será verificar el cumplimiento de esos requisitos.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

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

- Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos.
- Toda la información que tenga que hacer uso del producto para ser transmitida (como 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.
- Información y recursos de la red interna de la organización, susceptibles de ser objeto de ataques a través de correo electrónico.

3.2 AMENAZAS

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

- **A.RED. Ataque a la red.** Un atacante, desde dentro o desde fuera de la red, consigue acceder y/o modificar la información intercambiada entre el producto y otras entidades autorizadas o entre los distintos módulos del producto.
- **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.SEG. Acceso a las funciones de seguridad.** Un atacante podría acceder y modificar las funciones y datos de seguridad del 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.
- **A.SPM. Contenido externo potencialmente dañino**. Un atacante consigue introducir en la red interna, contenido potencialmente dañino a través del correo electrónico.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

20. 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

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

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

5. Estas funcionalidades de seguridad mitigan la amenaza (A.REST, A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
6. **IAU.1** El producto deberá identificar y autenticar a cada usuario antes de otorgar acceso.
7. **IAU.2**. El producto deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
8. **IAU.3.** El producto deberá proteger de lectura y modificación no autorizada las credenciales de autenticación.
9. **IAU.4**. El producto 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 [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]

10. **IAU.5** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.

4.3 AUDITORÍA

11. Estas funcionalidades de seguridad mitigan la amenaza (A.NODET).
12. **AUD.1** El producto deberá 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 personal autorizado.
    b) Cambio en las credenciales de usuarios.
    c) Cambios en la configuración del producto.
    d) Eventos relativos a la funcionalidad del producto.
13. **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).
14. **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.
15. **AUD.4** Si se trata de un producto *appliance*, debe ser capaz de almacenar la información de auditoría generada en sí mismo o en una entidad externa.
16. **AUD.5** Si se trata de un producto *appliance*, este debe ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno.

4.4 CANAL SEGURO

17. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
18. **COM.1** El TOE deberá establecer canales seguros (HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, SSHv2, etc.) cuando intercambie información sensible con entidades autorizadas, o entre las 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.).
19. **COM.2** El TOE debe permitir que estos canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

20. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL, A.SEG).

21. **ACT.1** El producto ofrecerá la posibilidad de consultar la versión actual del *firmware/software*, iniciar actualizaciones manualmente y comprobar si existen nuevas actualizaciones disponibles.
22. **ACT.2** El producto deberá 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.
23. **ACT.3.** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.
24. **ACT.5** En caso de tratarse de un producto *software*, este deberá estar empaquetado de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
25. **ACT.6** En caso de tratarse de un producto *software*, este no descargará ni modificará su propio código binario.
26. **ACT.7** En caso de tratarse de un producto *software*, solamente utilizará las bibliotecas de terceras partes declaradas por el fabricante.

4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

27. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional.**
28. **CRD.1.** En el caso en que el producto almacene credenciales y/o datos sensibles, éstos no deberán almacenarse en claro.

4.7 REQUISITOS CRIPTOGRÁFICOS

29. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST).
30. **CIF.1** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos criptográficos que estén incluidas entre las autorizadas para Categoría ALTA del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.
31. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

4.8 PROTECCIÓN DE CORREO ELECTRÓNICO

32. Estas funcionalidades de seguridad mitigan las amenazas (A.SPM).
33. **COR.1.** El producto debe proporcionar una política de correo electrónico que permita analizar todos los correos entrantes y salientes.
34. **COR.2.** El producto debe analizar un correo completo (cabecera y cuerpo) y sus adjuntos.
35. **COR.3.** El producto aplicará como técnicas de análisis de protección de correo, al menos, un análisis heurístico y firmas de correo no deseado conocidos.

36. **COR.4.** El producto permitirá configurar reglas para detectar patrones de texto dentro del cuerpo o de la cabecera del mensaje.

37. **COR.5.** Cuando un correo se detecte como no deseado o basura, el producto permitirá, al menos, eliminarlo o marcarlo como no deseado o basura.

38. **COR.6.** El producto permitirá usar listas blancas y negras para descartar o permitir correos electrónicos, basadas en direcciones de correo, nombres de dominio o direcciones IP.

4.9 NOTAS DE APLICACIÓN

39. En caso de que el producto no implemente la funcionalidad a la que aplica alguno de los requisitos anteriores (o algunas partes de ellos), y ésta sea proporcionada por el entorno operacional, el fabricante deberá indicarlo en la declaración de seguridad o justificarlo debidamente. En este caso, se considerará que el requisito ***no aplica***.

40. Lo anterior no es válido en caso de que tal funcionalidad solicitada en un requisito, sea proporcionada por un componente del producto que no forma parte de la configuración evaluada. En este caso ***sí aplica***, y el fabricante deberá demostrar el correcto cumplimiento del requisito por parte 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*
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