

Guía de Seguridad de las TIC CCN-STIC 140

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



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– MODO PASARELA	4
2.2.2. CASO DE USO 2 – MODO TRANSPARENTE	4
2.2.3. CASO DE USO 3 – INCLUIDO EN EL SERVIDOR DE CORREO.....	5
2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN	5
2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO	6
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	10
4.3 AUDITORÍA	11
4.4 CANALES SEGUROS	12
4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES	12
4.6 CAPACIDADES ANTI-EXPLOTACIÓN.....	13
4.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES	13
4.8 CRIPTOGRAFÍA.....	13
4.9 PROTECCIÓN DE CORREO ELECTRÓNICO.....	13
4.10 NOTAS DE APLICACIÓN GENERAL	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 Protección de correo electrónico 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 para los que sea de aplicación el **Esquema Nacional de Seguridad (ENS), para 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 **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.

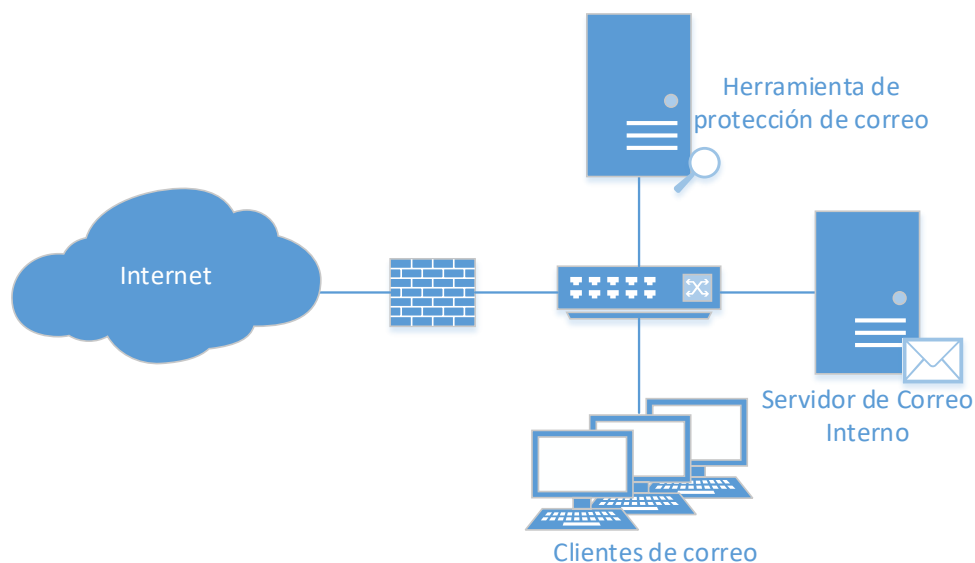


Figura 1 – Ejemplo de Caso de Uso: Modo Pasarela

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.

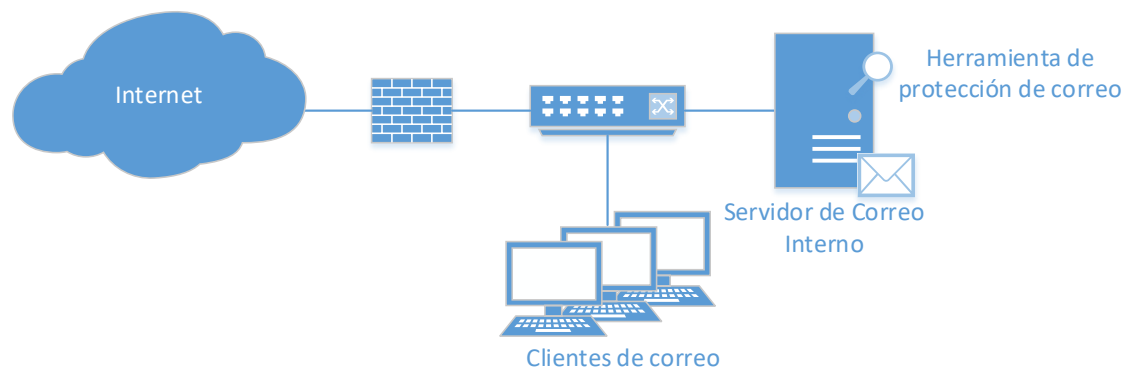


Figura 3 – Ejemplo de Caso de Uso: Herramienta de protección de correo en el servidor de correo

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

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 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 *Protección de correo electrónico* 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

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 CERTIFICACIÓN LINCE

14. 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)¹ que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.
15. El alcance de la evaluación deberá incluir el módulo de evaluación básico de 25 días de esfuerzo y el Módulo de Evaluación Criptográfica (MEC). El Módulo de Revisión de Código Fuente (MCF) será opcional.
16. En caso de estimarse que el esfuerzo de evaluación de los requisitos incluidos en el apartado 4 excede de los días de esfuerzo determinados dentro de la metodología LINCE, se contempla la posibilidad de realizar una Evaluación STIC Complementaria que incluya las pruebas que no han podido ser encajadas en el mencionado periodo.

¹ 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

17. Los recursos que deben protegerse mediante el uso de estos productos son:

- **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

18. 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.SPM. Contenido externo potencialmente dañino.** Un atacante consigue introducir en la red interna, contenido potencialmente dañino a través del correo electrónico.

3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD

19. 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.SPM
ADM.1	X									
ADM2	X									
ADM.3	X									
IAU.1	X							X		
IAU.2									X	
IAU.3									X	
IAU.4	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.SPM
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					
AUD.4					X					
AUD.5					X					
EXP.3						X				
PSC.1							X			
CIF.1		X	X							
COR.1										X
COR.2										X
COR.3										X
COR.4										X
COR.5										X
COR.6										X

4. REQUISITOS DE SEGURIDAD

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.
21. 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

22. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
23. **ADM.1** El TOE debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.
24. **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].
25. **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

26. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

27. **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*].
28. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
29. **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.

30. **IAU.4** El TOE debe [selección: *bloquear; cerrar*] la sesión de un usuario después de [asignación: *tiempo de inactividad*] de inactividad.

4.3 AUDITORÍA

31. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
32. **AUD.1** El TOE 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*].
33. **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.
34. **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*]

35. **AUD.4** El TOE debe ser capaz de almacenar en sí mismo la información de auditoría generada y [**selección:** transmitir la información de auditoría generada a una entidad externa utilizando un canal seguro COM.1; no transmitir la información de auditoría generada].
36. **AUD.5** El TOE deberá [**selección:** sobrescribir los registros siguiendo el criterio de mayor antigüedad; enviar a una entidad externa y eliminar; otra opción validada por el CPSTIC] en el caso de que el espacio para almacenamiento de los registros alcance su límite.

4.4 CANALES SEGUROS

37. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
38. **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*].
39. **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.
40. **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*].

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

41. **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].
42. **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.
43. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.
44. **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).

45. **ACT.5** En el caso de que el TOE sea una *aplicación software*, este no descargará ni modificará su propio código binario.

4.6 CAPACIDADES ANTI-EXPLOTACIÓN

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*].

4.7 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**.

4.8 CRIPTOGRAFÍA

48. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
49. **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.

4.9 PROTECCIÓN DE CORREO ELECTRÓNICO

50. **COR.1**. El TOE debe proporcionar una política de correo electrónico que permita analizar todos los correos entrantes y salientes.
51. **COR.2**. El TOE debe analizar un correo completo (cabecera y cuerpo) y sus adjuntos.
52. **COR.3**. El TOE aplicará como técnicas de análisis de protección de correo, al menos, un análisis heurístico y firmas de correo no deseado conocidos.
53. **COR.4**. El TOE permitirá configurar reglas para detectar patrones de texto dentro del cuerpo o de la cabecera del mensaje.
54. **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.
55. **COR.6**. El TOE permitirá usar listas blancas y negras para descartar o permitir correos electrónicos, basadas en direcciones de correo, nombres de dominio o direcciones IP.

4.10 NOTAS DE APLICACIÓN GENERAL

56. 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***.
57. 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	<i>Common Criteria</i>
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
EAL	<i>Evaluation Assurance Level</i>
ENS	Esquema Nacional de Seguridad
NIAP	<i>National Information Assurance Partnership</i>
RFS	Requisitos Fundamentales de Seguridad
SFR	<i>Security Functional Requirements</i>
TOE	<i>Target of Evaluation</i>

