



PSTmail

# Declaración de seguridad (Versión pública)

Revisión 1.2

**Copyright © 2010-2011 Autek Ingeniería. Todos los derechos reservados.**

*Ninguna parte de este documento podrá ser reproducida, total o parcialmente, incluso para uso personal, por cualquier medio y bajo cualquier forma, ya fuere permanente o transitoria. Tampoco están permitidos la traducción, adaptación, arreglo o cualquier otra transformación, modificación y/o manipulación de todo o parte del documento, la transferencia de cualquier forma o por cualquier medio electrónico, mecánico, fotocopia, grabación o cualquier otro sin el permiso previo por escrito de Autek Ingeniería, S.L.*

*Los autores del presente documento han sido muy rigurosos en la preparación del mismo pero no podemos ofrecer ninguna garantía ni asumir responsabilidad alguna por errores, omisiones o daños producidos por la utilización de la información aquí contenida.*

# Índice

1. Introducción .....	1
1.1. Referencia Declaración de Seguridad .....	1
1.2. Resumen del TOE .....	1
1.2.1. Uso del TOE .....	1
1.2.2. Tipo de TOE .....	1
1.3. Descripción del TOE .....	3
1.3.1. Alcance físico .....	3
1.3.2. Alcance lógico .....	3
1.3.3. Descripción general del sistema .....	3
1.3.4. Entrada de correo .....	4
1.3.5. Salida de correo .....	5
1.3.6. Administración .....	6
1.3.7. Auditoría .....	6
1.3.8. Configuración segura del TOE .....	7
2. Declaraciones de conformidad .....	9
2.1. Conformidad con respecto a la norma CC .....	9
2.2. Conformidad de otros PP .....	9
3. Definición del problema de seguridad .....	11
3.1. Activos del TOE .....	11
3.1.1. Flujo de información .....	11
3.2. Amenazas .....	11
3.2.1. Flujo de información .....	11
3.3. Hipótesis .....	11
3.3.1. Entorno de uso .....	11
3.4. Políticas organizativas .....	12
3.4.1. Criterios de diseño .....	12
4. Objetivos de seguridad .....	15
4.1. Objetivos de seguridad para el TOE .....	15
4.2. Objetivos de seguridad para el entorno operacional .....	16
4.3. Justificación de los objetivos de seguridad .....	17
5. Requisitos de seguridad del TOE .....	19
5.1. Requisitos funcionales de seguridad .....	19
5.1.1. Roles y control de acceso .....	19
5.1.2. Flujo de información .....	22
5.1.3. Auditoría .....	28
5.2. Requisitos de garantía de seguridad .....	33
5.2.1. ADV_ARC.1 Security architecture description .....	33
5.2.2. ADV_FSP.4 Complete functional specification .....	34
5.2.3. ADV_IMP.1 Implementation representation of the TSF .....	34
5.2.4. ADV_TDS.3 Basic modular design .....	35
5.2.5. AGD_OPE.1 Operational user guidance .....	36
5.2.6. AGD_PRE.1 Preparative procedures .....	37
5.2.7. ALC_CMC.4 Production support, acceptance procedures and automation .....	38
5.2.8. ALC_CMS.4 Problem tracking CM coverage .....	39
5.2.9. ALC_DEL.1 Delivery procedures .....	40

---

5.2.10. ALC_DVS.1 Identification of security measures .....	40
5.2.11. ALC_FLR.1 Basic flaw remediation .....	40
5.2.12. ALC_LCD.1 Developer defined life-cycle model .....	41
5.2.13. ALC_TAT.1 Well-defined development tools .....	41
5.2.14. ASE_INT.1 ST introduction .....	42
5.2.15. ASE_CCL.1 Conformance claims .....	43
5.2.16. ASE_SPD.1 Security problem definition .....	44
5.2.17. ASE_OBJ.2 Security objectives .....	45
5.2.18. ASE_ECD.1 Extended components definition .....	46
5.2.19. ASE_REQ.2 Derived security requirements .....	46
5.2.20. ASE_TSS.1 TOE summary specification .....	47
5.2.21. ATE_COV.2 Analysis of coverage .....	48
5.2.22. ATE_DPT.1 Testing: basic design .....	48
5.2.23. ATE_FUN.1 Functional testing .....	49
5.2.24. ATE_IND.2 Independent testing - sample .....	49
5.2.25. AVA_VAN.3 Focused vulnerability analysis .....	50
5.3. Justificación de los requisitos de seguridad .....	50
5.3.1. Justificación de dependencias no satisfechas .....	50
5.3.2. Justificación de requisitos de seguridad funcionales .....	51
5.3.3. Justificación de requisitos de seguridad de garantía .....	51
6. Especificación resumida del TOE .....	53
6.1. FMT_SMR.2 Restrictions on security roles .....	53
6.1.1. Roles de administración .....	53
6.2. FMT_SMF.1 Specification of Management Functions .....	53
6.3. FIA_UID.2 User identification before any action .....	54
6.4. FIA_UAU.2 User authentication before any action .....	54
6.5. FMT_MSA.1 / IFF Management of security attributes .....	54
6.6. FMT_MSA.1 / ACC Management of security attributes .....	54
6.7. FMT_MSA.3 / IFF Static attribute initialization .....	55
6.7.1. Política y filtros de entrada y salida .....	55
6.8. FMT_MSA.3 / ACC Static attribute initialization .....	55
6.8.1. Política de acceso y roles .....	55
6.9. FDP_ACF.1 Security attribute based access control .....	55
6.10. FDP_ACC.2 Complete access control .....	55
6.11. FDP_IFC.2 / ENT Complete information flow control .....	56
6.12. FDP_IFF.1 / ENT Simple security attributes .....	56
6.13. FDP_IFC.2 / SAL Complete information flow control .....	56
6.14. FDP_IFF.1 / SAL Simple security attributes .....	57
6.15. FAU_GEN.1 Audit data generation .....	57
6.15.1. Eventos del sistema .....	57
6.15.2. Registros de transferencias .....	57
6.16. FAU_SAR.1 Audit review .....	58
6.17. FAU_SAR.2 Restricted audit review .....	58

---

---

## Lista de ilustraciones

1. Entorno de PSTmail .....	2
2. Componentes de PSTmail .....	4
3. Entrada de correo .....	5
4. Salida de correo .....	6
5. Administración .....	6
6. Auditoría .....	7



## Lista de tablas

1. Objetivos de seguridad para el TOE .....	17
2. Objetivos de seguridad para el entorno operacional .....	17
3. Asignación de funcionalidad a roles de administración .....	21
4. Justificación de los requisitos de seguridad .....	50

---



# 1. Introducción

## 1.1. Referencia Declaración de Seguridad

1       **Título:** Declaración de seguridad de PSTmail

2       **Versión de la declaración de seguridad:** 1.2

3       **Autor:** Autek Ingeniería, S.L.

4       **Fecha de publicación:** 12 de julio de 2011

5       **Nombre producto:** PSTmail

6       **Versión producto:** 3.0.5

## 1.2. Resumen del TOE

### 1.2.1. Uso del TOE

7       PSTmail es un sistema que permite el intercambio de correo electrónico entre dos redes TCP/IP con diferentes grados de clasificación o políticas de seguridad lo que impediría su conexión por cualquier otro medio. Las dos redes no son equivalentes: una se considera que tiene un grado de clasificación o un nivel de seguridad mayor. PSTmail garantiza la imposibilidad de cualquier tipo de tráfico entre las dos redes excepto el correo transmitido por el propio sistema.

8       El sistema se administra exclusivamente desde la red más segura.

9       Los protocolos de correo soportados son los estándar de Internet: POP3 e IMAP4 para la recepción y SMTP para el envío. La pasarela no sustituye a los servidores de correo electrónico de las dos redes sino que los usa como elementos intermedios para el envío y recepción de mensajes.

10      El correo entra a la red segura de manera transparente para los usuarios, aunque se le pueden aplicar políticas de filtrado, desvíos condicionales y se puede redirigir a varias cuentas internas.

11      La salida de correo de la red segura requiere la autorización mediante firma electrónica de cada uno de los mensajes.

### 1.2.2. Tipo de TOE

12      PSTmail es una pasarela de correo electrónico, software que permite el intercambio de correo electrónico entre dos redes separadas conforme a unas políticas configurables de flujo de mensajes.

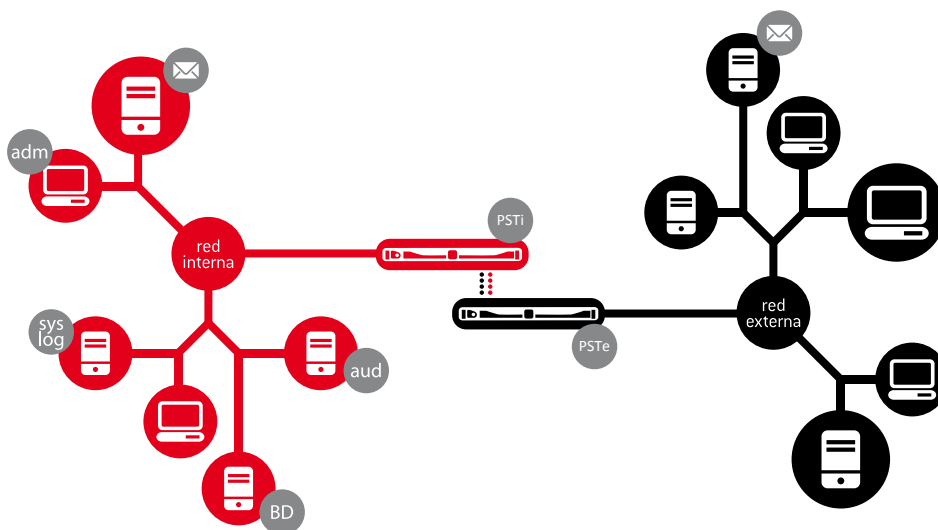
13      Un elemento PSTmail lo constituyen dos equipos que se denominan 'unidades'. Cada uno de ellos se conecta a una de las redes y se denomina PSTi al de la Red Interna y PSTe al de la Externa. Se trata de equipos dedicados, es decir, no se ejecuta en ellos ninguna aplicación software aparte de las propias de PSTmail.

---

- 14 El TOE está compuesto por los componentes software específicos que se ejecutan en las unidades y por el servicio de registro de transferencias ‘PSTaud’.
- 15 PSTmail requiere de un entorno físico de uso seguro.

### 1.2.2.1. Hardware y software requerido

- 16 La parte central del TOE se ejecuta en dos servidores específicos suministrados por el fabricante que ejecutan Windows Embedded Standard. Se soporta la serie S2 de dichos servidores que incluye en las unidades internas un dispositivo de transferencia pasivo.
- 17 Para instalación y ejecución del servicio de registro de transferencias PSTaud es necesario un PC estándar con un procesador de 1GHz o superior y mínimo 1GB de memoria ejecutando el Sistema Operativo Windows XP SP3 o superior.
- 18 El entorno donde se ejecuta PSTmail debe incluir:
- Para la instalación y ejecución de la aplicación de administración PSTadm es necesario un PC estándar con un procesador de 1GHz o superior y mínimo 1GB de memoria ejecutando el Sistema Operativo Windows XP SP3 o superior.
  - Infraestructura de clave pública
  - Servidor(es) de syslog (Red Interna)
  - Servidor de base de datos para el registro de transferencias accesible mediante ODBC (Red Interna)
  - Servidores de correo electrónico
  - Clientes de correo electrónico con soporte S/MIME (Red Interna)



**Ilustración 1. Entorno de PSTmail**

## 1.3. Descripción del TOE

### 1.3.1. Alcance físico

- 19 El TOE está compuesto por los componentes software específicos desarrollados por Autek Ingeniería que se ejecutan en las unidades PSTmail y por el servicio de registro de transferencias 'PSTaud'.
- 20 También forman parte del TOE las siguientes guías:
- 21 [IG] Manual de instalación y puesta en servicio. Ref 0521-14
- 22 [OG] Manual de operación. Ref. 0521-15

### 1.3.2. Alcance lógico

- 23 La funcionalidad del TOE es la siguiente:
- Entrada de correo
  - Salida de correo
  - Administración (Funcionalidad de administración implementada en las unidades PSTmail)
  - Auditoría

### 1.3.3. Descripción general del sistema

- 24 El componente fundamental de PSTmail lo constituyen dos equipos que se denominarán 'unidades'. Cada uno de ellos se conecta a una de las redes y se denomina PSTi al de la red interna y PSTe al de la externa. Se trata de equipos dedicados, es decir, no se ejecuta en ellos ninguna aplicación software aparte de las propias de PSTmail. Se suministran con todo el software necesario instalado.

- **Elemento PSTmail**

Cada pareja de unidades PSTi y PSTe, forma un elemento. El elemento incluye también el dispositivo hardware necesario para la comunicación entre las unidades.

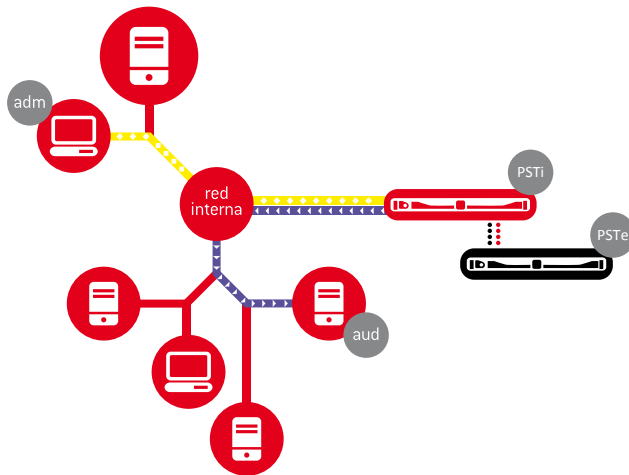
Existen dos posibles configuraciones: estándar –formada por un elemento– y alta disponibilidad –formada por dos elementos en un esquema de redundancia activo-pasivo–.

- 25 Adicionalmente el sistema está formado por los siguientes componentes software que se ejecutarán en puestos de propósito general o servidores situados en la red interna:
- **PSTadm** - Aplicación de administración
-

La administración del sistema completo se realiza desde un puesto de la red interna. La unidad situada en la red externa (PSTe) no necesita ser administrada.

- **PSTaud** - Servicio de recepción de registros de auditoría

Los datos de actividad (datos de los mensajes transferidos por la pasarela) se registran en una base de datos ajena a PSTmail. La misión de PSTaud es insertar los datos que recibe de la unidad interna, en una base de datos.



## Ilustración 2. Componentes de PSTmail

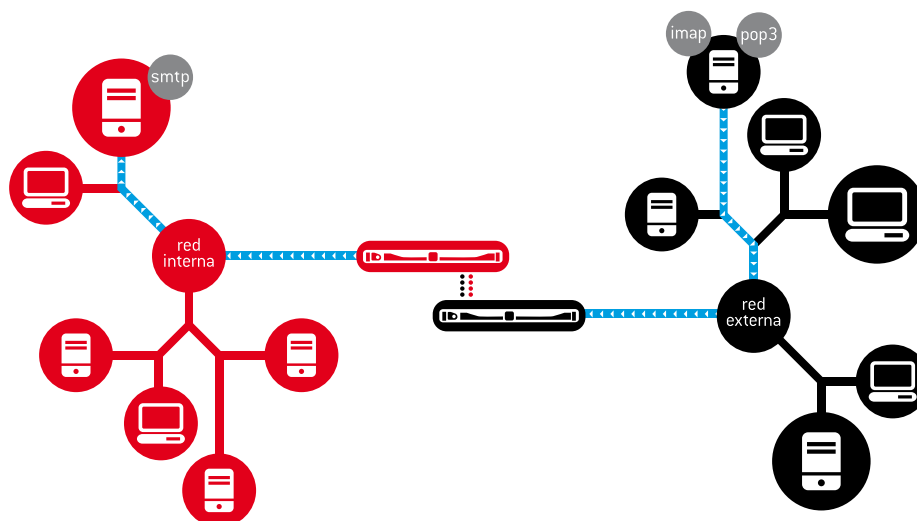
### 1.3.4. Entrada de correo

- 26 La pasarela gestiona de forma transparente los mensajes de entrada: Consulta periódicamente los buzones de la red externa que se configuren, introduce a la red interna los mensajes que encuentre y los envía a las cuentas de destino en la red interna que se establezcan por configuración.

- Canal de entrada de correo

Se denomina así a la correspondencia entre un buzón de la red externa y uno o más buzones de la red interna. El caso más sencillo es que cada usuario tenga una cuenta en cada una de las redes y la correspondencia sea 1 a 1.

Existe además una serie de parámetros que se pueden especificar de manera individual para cada canal, como por ejemplo un filtro de rechazo de mensajes y desvíos condicionales.



**Ilustración 3. Entrada de correo**

### 1.3.5. Salida de correo

27 Todo mensaje de salida necesita ser autorizado mediante firma digital. PSTi funciona como un servidor de correo en la red interna y verifica la firma digital de cada mensaje, antes de enviarlo a sus destinatarios en la red externa.

28 Además, elimina toda información de la red interna que pudieran contener las cabeceras del mensaje y permite realizar un filtrado básico por formato de los mensajes.

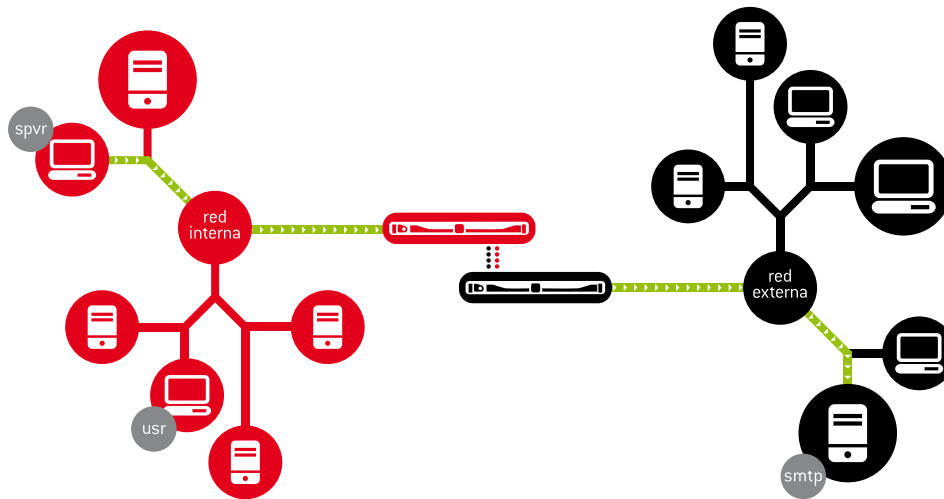
- Supervisor

Se denomina supervisores a los usuarios de la red interna con potestad para autorizar los envíos.

- Canal de salida de correo

Un canal se caracteriza por la dirección de remite en la red externa. A cada canal se le asigna por configuración un supervisor (o más de uno).

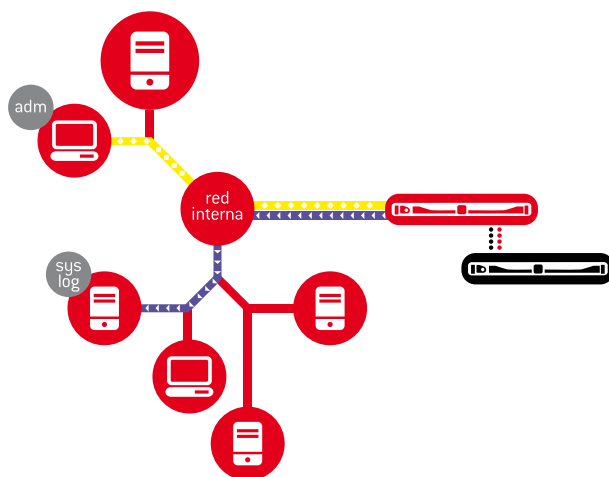
Para cada canal se pueden configurar individualmente, las características de filtrado y otros parámetros como la notificación de los envíos.



**Ilustración 4. Salida de correo**

### 1.3.6. Administración

- 29 La administración local sólo se realiza con el sistema detenido, sobre las unidades internas, para establecer una serie de parámetros de configuración iniciales que raramente es necesario modificar.
- 30 La administración remota se realiza desde un puesto de la Red Interna, mediante la aplicación PSTadm que no forma parte del TOE. PSTadm se conecta mediante SSL a la unidad interna PSTi. Adicionalmente, la pasarela envía eventos de sistema mediante el protocolo 'syslog' a servidores situados en la Red Interna.
- 31 Existen 4 roles diferenciados de administración con sus correspondientes permisos. A un administrador se le pueden asignar los roles que se desee.

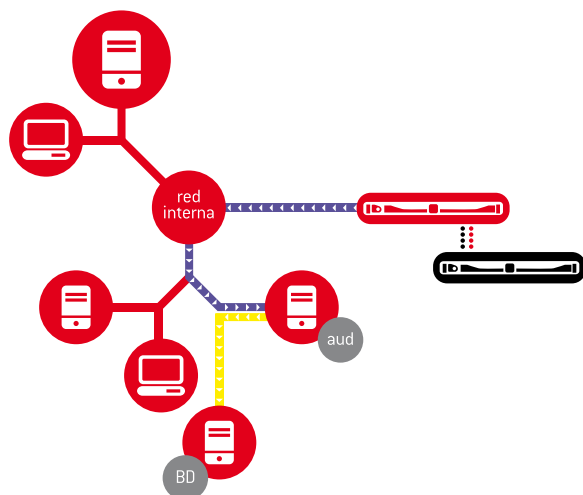


**Ilustración 5. Administración**

### 1.3.7. Auditoría

- 32 Auditoría es el registro de información de las transferencias realizadas por el sistema (Ej. mensajes enviados a sus destinatarios en la red interna).

- 33 El componente software PSTaud, instalado en un equipo de la red interna, se encarga de insertar estos registros en una base de datos ajena al sistema.
- 34 PSTi se conecta de manera automática a PSTaud mediante SSL.
- 35 Para cada servicio (entrada y salida de correo) se puede configurar si se enviará información de auditoría o no y el nivel de detalle.



**Ilustración 6. Auditoría**

### 1.3.8. Configuración segura del TOE

#### 1.3.8.1. Filtro de rechazo

- 36 Las siguientes condiciones de filtrado configurables, se refieren exclusivamente a los nombres de los ficheros adjuntos declarados en la forma prevista en los estándares MIME:
- Permitir ficheros con más de una extensión
  - Permitir ficheros sin extensión
  - Restringir extensiones
- 37 **El filtrado no hace ninguna comprobación sobre el contenido de los ficheros a la hora de aplicar estas condiciones. Existen por lo tanto innumerables posibilidades de falsificar los nombres de los ficheros. Se debe tener esto en cuenta y utilizar algún producto de control de contenidos si lo que se quiere es evitar que transmitan cierto tipo de ficheros.**
- 38 Asimismo, si un mensaje no incluye el nombre del fichero, no será posible aplicar sobre el mismo filtros de rechazo sobre las extensiones.

#### 1.3.8.2. Filtro de selección

- 39 Para poder utilizar este filtro de entrada de correo de modo eficaz, se debe configurar un filtro de rechazo que sólo admita formato MIME estándar.

- 40 Además, se debe tener en cuenta que, cuando se aplica un filtro de selección, se utiliza el servidor SMTP interno configurado para el canal. Esto podría resultar poco intuitivo por ejemplo en el caso de que se configurara el mismo filtro de selección sobre canales con distintos servidores internos SMTP.

### **Coherencia de los destinos**

- 41 La pasarela no hace ningún tipo de comprobación sobre los destinos de los canales ni de los filtros de selección. Es responsabilidad del administrador comprobar que las cuentas de destino de los desvíos son las deseadas.

#### **1.3.8.3. Orden de aplicación de los filtros en la entrada de correo**

- 42 La ejecución de los filtros se realiza sólo una vez, primero el filtrado de rechazo y después el filtrado de selección. El filtrado de rechazo se define y aplica sobre un canal, es decir sobre el correo que se recibe en una dirección externa.

#### **1.3.8.4. Responsabilidad de la salida de correo**

- 43 Un canal de salida se corresponde a una dirección de correo electrónico en la red externa. Los supervisores asignados a un canal son los únicos responsables de lo que se envía por ese canal. En la red externa no existe visibilidad de usuarios, ni supervisores de la red interna. El supervisor puede enviar lo que quiera, ya que tiene autoridad organizativa para ello. Esto incluye la posibilidad de realizar modificaciones en los mensajes de los usuarios que recibe para su autorización.
-

## **2. Declaraciones de conformidad**

### **2.1. Conformidad con respecto a la norma CC**

- 44 Esta declaración de seguridad cumple con los requisitos de la norma CC v. 3.1, rel 3, ISO/IEC 15408:2009, partes 2 y 3, y define un nivel de garantía de evaluación EAL4, incrementado hasta ALC\_FLR.1.
- 45 Documentación de referencia:  
*FS PSTmail: Especificación funcional*

### **2.2. Conformidad de otros PP**

- 46 Esta declaración de seguridad se ha desarrollado atendiendo al problema específico de seguridad del sistema PSTmail, y no declara cumplimiento de perfil de protección alguno.
-



---

## 3. Definición del problema de seguridad

### 3.1. Activos del TOE

47 Se declaran como activos a proteger por el TOE los siguientes:

#### 3.1.1. Flujo de información

- **A1.IFF-ENT;** Flujo de información de entrada. No debe ser posible la entrada de información de la Red Externa a la Interna excepto la que transmita la propia pasarela por correo electrónico conforme a la correspondiente política y reglas de filtrado de rechazo de entrada de correo. El destino final de los mensajes introducidos en la Red Interna deben ser las cuentas de correo especificadas en la correspondiente definición de canales y reglas de desvío.
- **A2.IFF-SAL;** Flujo de información de salida. No debe ser posible la salida de información de la Red Interna excepto la que transmita la propia pasarela por correo electrónico conforme a la correspondiente política y reglas de autorización y filtrado de rechazo de salida de correo. El destino final de los mensajes autorizados en la Red Externa debe ser el envío a través de los servidores configurados a los destinatarios especificados en el mensaje original.

## 3.2. Amenazas

### 3.2.1. Flujo de información

- **T1.IFF-ENT;** Un atacante en la Red Interna recibe en su buzón, de manera no autorizada, mensajes destinados a otros usuarios.
- **T2.IFF-SAL;** Un atacante en la Red Interna envía un mensaje no autorizado a través de la pasarela.
- **T3.IFF-EXT1;** Un atacante en la Red Externa consigue introducir información en la Red Interna, a través del hardware de la pasarela pero, por un cauce distinto del correo electrónico de entrada.
- **T4.IFF-EXT2;** Un atacante en la Red Externa consigue obtener información de la Red Interna por cualquier medio distinto de la salida autorizada de correo.

## 3.3. Hipótesis

### 3.3.1. Entorno de uso

- **AS1;** Nadie tiene acceso al hardware de ninguna de las dos unidades (salvo los administradores locales). Se supone que las maneras obvias de circunvalar el sistema (como por ejemplo conectar ambas unidades directamente mediante un cable de red) quedan descartadas por medidas físicas u organizativas del entorno de explotación.
-

- **AS2;** La Red Interna es una red aislada y totalmente asegurada y confiable. La Red Externa es una red físicamente controlada (no se pueden conectar nuevas máquinas a la red) y con medidas de seguridad (cortafuegos en sus conexiones a otras redes, máquinas en la red securizadas y con las últimas actualizaciones y parches de seguridad, etc.) pero que sí está conectada mediante TCP/IP a otras redes.
- **AS3;** La plataforma (entorno del TOE) estará diseñada de tal modo y configurada de manera segura, de manera que no existan caminos de ataque a través de dicha plataforma.

## 3.4. Políticas organizativas

### 3.4.1. Criterios de diseño

- **P1.SEP;** Las dos redes deben permanecer separadas. No debe ser posible el establecimiento de conexiones TCP/IP entre las dos redes.
  - **P2.SAL;** Los mensajes de correo electrónico salientes (es decir, los dirigidos desde la Red Interna hacia la Red Externa) deben ser autorizados mediante firma electrónica.
  - **P3.CRYPT;** La información (de configuración y la procesada por el sistema) que se guarde en disco en las unidades (PSTi, PSTe) debe estar cifrada, *al igual que las comunicaciones para administración remota y envío de datos de auditoría.*
  - **P4.ROLES;** PSTmail deberá implementar los siguiente roles, con las capacidades indicadas:
    1. **Administrador raíz:**
      1. Establece los CN de los certificados que se consideran válidos para la administración de la pasarela y sus permisos.
    2. **Administrador de Seguridad:**
      1. Establece la configuración de monitorización: parámetros que afectan a los eventos del sistema y al registro de transferencias.
      2. Puede obtener una copia de los ficheros de registro de eventos de seguridad (que se almacenan localmente en la Unidad Interna de la pasarela).
    3. **Administrador de Servicios:**
      1. Establece toda la configuración de los servicios (entrada y salida de correo).
      2. Puede arrancar y parar los servicios de entrada y salida de correo.
-

3. Puede obtener una copia de los ficheros de registro de eventos de funcionamiento (que se almacenan localmente en la Unidad Interna de la pasarela).
4. **Administrador de Monitorización:**
  1. Supervisa el estado de funcionamiento de la pasarela.
  2. Puede reiniciar las estadísticas de los servicios (entrada y salida de correo).
5. **Administrador Local:**
  1. Establece la configuración local de las unidades internas.

Estos roles y sus capacidades se implementarán mediante las funcionalidades de autenticación que permitan establecer las políticas y funciones de control de acceso que regulen el ejercicio autorizado de las capacidades indicadas.

- **P5.AUDITORIA;** PSTmail implementará un mecanismo de registro de su actividad.
-



---

## 4. Objetivos de seguridad

### 4.1. Objetivos de seguridad para el TOE

- **O1.FLUJO;** PSTmail implementará la siguiente política de flujo de información:
    1. No debe ser posible la salida de información de la Red Interna excepto la que transmita la propia pasarela por correo electrónico tras comprobar que está debidamente autorizada (mediante firma electrónica).
    2. No debe ser posible la entrada de información de la Red Externa a la Interna excepto la que transmita la propia pasarela por correo electrónico y conforme a la definición de canales y reglas de desvío.
  - **O2.ROLES;** PSTmail deberá implementar los siguiente roles, con las capacidades indicadas:
    1. **Administrador raíz:**
      1. Establece los CN de los certificados que se consideran válidos para la administración de la pasarela y sus permisos.
    2. **Administrador de Seguridad:**
      1. Establece la configuración de monitorización: parámetros que afectan a los eventos del sistema y al registro de transferencias.
      2. Puede obtener una copia de los ficheros de registro de eventos de seguridad (que se almacenan localmente en la Unidad Interna de la pasarela).
    3. **Administrador de Servicios:**
      1. Establece toda la configuración de los servicios (entrada y salida de correo).
      2. Puede arrancar y parar los servicios de entrada y salida de correo.
      3. Puede obtener una copia de los ficheros de registro de eventos de funcionamiento (que se almacenan localmente en la Unidad Interna de la pasarela).
    4. **Administrador de Monitorización:**
      1. Supervisa el estado de funcionamiento de la pasarela.
      2. Puede reiniciar las estadísticas de los servicios (entrada y salida de correo).
-

## 5. Administrador Local:

1. Establece la configuración local de las unidades internas.

Estos roles y sus capacidades se implementarán mediante las funcionalidades de autenticación que permitan establecer las políticas y funciones de control de acceso que regulen el ejercicio autorizado de las capacidades indicadas.

- **O3.AUDITORIA**; PSTmail implementará un mecanismo de registro de su actividad.

## 4.2. Objetivos de seguridad para el entorno operacional

- **O.ENV.AS1**; Nadie tendrá acceso al hardware de ninguna de las dos unidades (salvo el administrador Local). Se supone que las maneras obvias de circunvalar el sistema (como por ejemplo conectar ambas unidades directamente mediante un cable de red) quedan descartadas por medidas físicas u organizativas del entorno de explotación.
  - **O.ENV.AS2**; La Red Interna es una red aislada y totalmente asegurada y confiable. La Red Externa es una red físicamente controlada (no se pueden conectar nuevas máquinas a la red) y con medidas de seguridad (cortafuegos en sus conexiones a otras redes, IDS, máquinas en la red securizadas y con las últimas actualizaciones y parches de seguridad, etc.) pero que sí está conectada mediante TCP/IP a otras redes no seguras.
  - **O.ENV.AS3**; La plataforma (entorno del TOE) estará diseñada de tal modo y configurada de manera segura, de manera que no existan caminos de ataque a través de dicha plataforma.
  - **O.ENV.AS4**; Las operaciones criptográficas utilizan la criptografía de Windows para lo siguiente:
    - Cifrado de disco de las unidades internas (PSTi). El cifrado en las unidades internas se realiza con una clave que se guarda en un dispositivo externo y se recupera en cada arranque para descifrar.
    - Cifrado de disco de las unidades externas (PSTe). El cifrado en las unidades Externas se realiza con una clave de sesión lo que garantiza que no haya persistencia entre sesiones.
    - Verificación de firma de los mensajes de salida
    - Establecimiento de conexiones TLS de administración y envío de datos de auditoría
  - **O.ENV.AS5**; Separación de redes. La arquitectura hardware debe ser tal que exista un host distinto en cada una de las redes. La comunicación entre ambos hosts debe realizarse mediante un dispositivo pasivo de intercambio de información.
-

### 4.3. Justificación de los objetivos de seguridad

	O1.FLUJO	O2.ROLES	O3.AUDITORIA
P2.SAL	X		
P4.ROLES		X	
P5.AUDITORIA			X
T1.IFF-ENT	X		
T2.IFF-SAL	X		
T3.IFF-EXT1	X		
T4.IFF-EXT2	X		

**Tabla 1. Objetivos de seguridad para el TOE**

- 48 El objetivo de control de flujo (O1.FLUJO) mitiga las amenazas T1.IFFENT, T1.IFF-SAL, T1.IFF-EXT1, T1.IFF-EXT2 y hace que se cumpla la política P2.SAL.
- 49 El objetivo de roles y capacidades (O2.ROLES) hace que se cumpla la política P4.ROLES, excepto en el caso del Administrador Local (ver más adelante).
- 50 El objetivo (O3.AUDITORIA) hace que se cumpla la política P5.AUDITORIA.

	O.ENV.AS1	O.ENV.AS2	O.ENV.AS3	O.ENV.AS4	O.ENV.AS5
P1.SEP					X
P2.SAL				X	
P3.CRYPT				X	
AS1	X				
AS2		X			
AS3			X		

**Tabla 2. Objetivos de seguridad para el entorno operacional**

- 51 El objetivo del entorno O.ENV.AS1, hace que se cumpla directamente la suposición de entorno AS1.
- 52 El objetivo del entorno O.ENV.AS2, hace que se cumpla directamente la suposición de entorno AS2.
- 53 El objetivo del entorno O.ENV.AS3, hace que se cumpla directamente la suposición de entorno AS3.
- 54 El objetivo del entorno O.ENV.AS4, hace que se cumplan las políticas:
- P2.SAL para la verificación de las firmas
  - P3.CRYPT en el cifrado de los datos que se escriben en disco en ambas unidades

- 55 El objetivo del entorno O.ENV.AS5 hace que se cumpla la política de separación de redes P1.SEP.
-

---

## 5. Requisitos de seguridad del TOE

### 5.1. Requisitos funcionales de seguridad

#### 5.1.1. Roles y control de acceso

##### 5.1.1.1. FMT\_SMR.2 Restrictions on security roles

###### 5.1.1.1.1. FMT\_SMR.2.1

56 The TSF shall maintain the roles: [assignment: *Administrador Raíz, Administrador de Seguridad, Administrador de Servicios, Administrador de Monitorización, Administrador Local* ].

###### 5.1.1.1.2. FMT\_SMR.2.2

57 The TSF shall be able to associate users with roles.

###### 5.1.1.1.3. FMT\_SMR.2.3

58 The TSF shall ensure that the conditions [assignment: *Pueden existir hasta cinco Administradores Raíz, que sólo se pueden dar de alta en la unidad interna en conexión local. Este perfil es el único que puede dar de alta nuevos administradores y asignarles roles. No existen restricciones en cuanto a los roles que se le pueden asignar a un administrador en particular.* ] are satisfied.

##### 5.1.1.2. FMT\_SMF.1 Specification of Management Functions

59 The TSF shall be capable of performing the following management functions: [assignment: *Administrador Raíz, Administrador de Seguridad, Administrador de Servicios, Administrador de Monitorización: las reflejadas en la Tabla 3; Administrador Local: Establecimiento de la configuración estática en la unidad interna PSTi (parámetros de red de ambas unidades, certificados de las entidades emisoras raíces de confianza, clave privada y certificado para la pasarela, CN de los administradores raíz – identificación de administradores raíz)* ].

##### 5.1.1.3. FIA\_UID.2 User identification before any action

###### 5.1.1.3.1. FIA\_UID.2.1

60 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

##### 5.1.1.4. FIA\_UAU.2 User authentication before any action

###### 5.1.1.4.1. FIA\_UAU.2.1

61 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

---

- 62 **Nota:** El administrador Local solo se autentica con una contraseña que el mismo suministra la primera vez que accede a la interfaz local de configuración. Las medidas organizativas del entorno deben impedir el acceso físico a otras personas que no ostenten este rol.

### **5.1.1.5. FMT\_MSA.1/ IFF Management of security attributes**

#### **5.1.1.5.1. FMT\_MSA.1.1**

- 63 The TSF shall enforce the [assignment: *“política y filtros de entrada y salida de mensajes”*] to restrict the ability to [selection: *change\_default, query, modify, delete*] the security attributes [assignment: *de la sección 5.1.2.1 para la entrada y de la sección 5.1.2.2 para la salida*] to [assignment: *Administrador de Servicios*]

### **5.1.1.6. FMT\_MSA.1 / ACC Management of security attributes**

#### **5.1.1.6.1. FMT\_MSA.1.1**

- 64 The TSF shall enforce the [assignment: *“política de acceso y roles”*] to restrict the ability to [selection: *change\_default, query, modify, delete*] the security attributes [assignment: *roles de los usuarios*] to [assignment: *Administrador Raíz (CU6 de Tabla 3)*].

### **5.1.1.7. FMT\_MSA.3 / IFF Static attribute initialisation**

#### **5.1.1.7.1. FMT\_MSA.3.1**

- 65 The TSF shall enforce the [assignment: *“política y filtros de entrada de mensajes”, “política y filtros de salida de mensajes”*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

#### **5.1.1.7.2. FMT\_MSA.3.2**

- 66 The TSF shall allow the [assignment: *Administrador de Servicios*] to specify alternative initial values to override the default values when an object or information is created.

### **5.1.1.8. FMT\_MSA.3 / ACC Static attribute initialisation**

#### **5.1.1.8.1. FMT\_MSA.3.1**

- 67 The TSF shall enforce the [assignment: *“política de acceso y roles”*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

#### **5.1.1.8.2. FMT\_MSA.3.2**

- 68 The TSF shall allow the [assignment: *Administrador raíz*] to specify alternative initial values to override the default values when an object or information is created.
-

### 5.1.1.9. FDP\_ACF.1 Security attribute based access control

#### 5.1.1.9.1. FDP\_ACF.1.1

69 The TSF shall enforce the [assignment: *“política de acceso y roles”*] to objects based on the following: [assignment:

- *Sujetos: los usuarios del TOE, atributo su role*
- *Objetos: las funcionalidades del TOE referidas en la Tabla 3, atributo el identificador de funcionalidad].*

#### 5.1.1.9.2. FDP\_ACF.1.2

70 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *el control de acceso arbitrará el ejercicio de las capacidades del TOE conforme a los roles asociados al usuario, según se indica en la definición de roles.* ].

#### 5.1.1.9.3. FDP\_ACF.1.3

71 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *None.*].

		<b>Administra- dor Raíz</b>	<b>Administra- dor de Servi- cios</b>	<b>Administra- dor de Seguri- dad</b>	<b>Administra- dor de Monito- rización</b>
CU2	Monitorización del funcionamiento				X
CU3	Arranque y parada de servicios		X		
CU4	Edición configuración de servicios		X		
CU5	Edición configuración de monitorización			X	
CU6	Edición de permisos de administración	X			
CU7	Obtención de ficheros de eventos de funcionamiento		X		
CU8	Obtención de ficheros de eventos de seguridad			X	

		Administra- dor Raíz	Administra- dor de Servi- cios	Administra- dor de Seguri- dad	Administra- dor de Monito- rización
CU9	Reinicio de esta- dísticas				X

**Tabla 3. Asignación de funcionalidad a roles de administración**

#### 5.1.1.9.4. FDP\_ACF.1.4

72 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *None*].

#### 5.1.1.10. FDP\_ACC.2 Complete access control

##### 5.1.1.10.1. FDP\_ACC.2.1

73 The TSF shall enforce the [assignment: *“política de acceso y roles”*] on [assignment: *usuarios del TOE y funcionalidades del TOE referidas en la Tabla 3*] and all operations among subjects and objects covered by the SFP.

##### 5.1.1.10.2. FDP\_ACC.2.2

74 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

### 5.1.2. Flujo de información

#### 5.1.2.1. Flujo de entrada

75 El control del flujo de entrada de mensajes de correo electrónico se realiza mediante la definición de 'canales de entrada'. Para que la pasarela procese los mensajes recibidos en una cuenta de correo de la Red Externa, es necesario definir un canal asociado a dicha cuenta. La pasarela soporta hasta 5000 canales de entrada. El permiso necesario para establecer la configuración de canales de entrada, que por tanto tiene control total sobre el flujo de mensajes de entrada, es el de 'Administrador de Servicios'.

76 La definición de un canal establece el tratamiento que PSTmail da a los mensajes recibidos en una cuenta externa. Por claridad expositiva, se presenta un 'Flujo básico' que constituye la esencia de un canal y los elementos opcionales 'Filtrado' y 'Desvío' que pueden no estar presentes.

- Flujo básico de un canal
- Filtrado (opcional)
- Selección (opcional)

##### 5.1.2.1.1. Flujo básico de un canal

77 La definición del flujo básico de un canal determina lo siguiente:

- Cuenta de correo externa
- Servidor de correo externo y todos los elementos de configuración necesarios para acceder a la cuenta de correo (POP o IMAP) en la Red Externa.
- Direcciones de destino en la Red Interna

De 1 a 20 direcciones de correo alojadas en un servidor de la Red Interna, a las que se moverán los mensajes presentes en la cuenta externa.

#### **5.1.2.1.2. Filtrado**

- 78 Se puede definir opcionalmente filtrado para un canal. El filtrado permite establecer una serie de condiciones sobre el formato y contenido de los mensajes, de manera que si no se cumple alguna condición, el mensaje se rechaza.
- 79 Acciones alternativas sobre los mensajes que no pasen el filtro (rechazados):
- Borrado
  - Envío a cuenta configurable de la Red Externa
- 80 Condiciones de filtrado:
- Permitir o denegar (uno de los dos) una lista de extensiones
  - Permitir adjuntos sin extensión
  - Permitir adjuntos con más de una extensión
  - Tamaño máximo de un adjunto permitido
  - Tamaño máximo del mensaje permitido
  - Máximo número de destinatarios permitido
  - Máximo número de adjuntos permitido
  - Máximo nivel de anidamiento permitido
  - Exigir cumplimiento formato estándar

#### **5.1.2.1.3. Selección**

- 81 Se pueden establecer el número de condiciones de selección que se desee. Se aplican después del filtrado. Cada condición de selección está formada por una dirección de destino en la Red Interna y una condición booleana sobre una serie de propiedades del mensaje. La primera condición de selección que se verifique determina la dirección de destino del mensaje en la Red Interna.
- 82 Propiedades del mensaje que se pueden usar en la expresión lógica
-

- Tipo/Subtipo MIME del mensaje
- Tipo/Subtipo MIME de adjuntos
- Nombre de los adjuntos
- Extensión de los adjuntos
- Contenido del asunto
- Remitente
- Dominio del remitente

### 5.1.2.2. Flujo de salida

83 El control del flujo de salida de mensajes de correo electrónico se realiza mediante la definición de 'canales de salida'. Para poder utilizar una dirección de la Red Externa como remite, es necesario definir un canal de salida asociado a dicha dirección de correo electrónico. La pasarela soporta hasta 5000 canales de salida. El permiso necesario para establecer la configuración de canales de salida, que por tanto tiene control total sobre el flujo de mensajes de salida, es el de 'Administrador de Servicios'.

84 La pasarela realiza las siguientes operaciones sobre un mensaje que se pretende enviar por un determinado canal:

- Comprobación de autorización
- Limpieza de información de la Red Interna
- Filtrado (opcional)

#### 5.1.2.2.1. Autorización

85 Todo mensaje de salida debe ser autorizado mediante firma digital por un supervisor. Los supervisores tienen que estar dados de alta en la configuración de la pasarela. Cada canal de salida tiene que tener asociados uno o más supervisores. La pasarela sólo aceptará enviar por un determinado canal, mensajes autorizados por un supervisor asociado al canal.

86 Las condiciones de autorización que debe cumplir un mensaje para que la pasarela lo envíe a sus destinatarios en la Red Externa son las siguientes:

- El mensaje debe estar correctamente firmado
  - El certificado de la clave con la que se firma el mensaje debe estar en el mensaje y haber sido emitido por una CA configurada en la pasarela
  - El CN del certificado que firma el mensaje debe estar configurado para el canal por el que se pretende enviar
-

### 5.1.2.2.2. Limpieza de información de la Red Interna

87 Se eliminan de los mensajes todos los campos de encabezamiento que no aparecen en la siguiente lista. Además, de los campos que se respetan se eliminan las direcciones de correo electrónico que pertenecen a dominios internos. Los dominios considerados internos se especifican por configuración.

- Bcc:
- Cc:
- Comments:
- Content-Description:
- Content-Transfer-Encoding:
- Content-Type:
- Date:
- Disposition-Notification-To:
- From:
- In-Reply-To:
- Keywords:
- MIME-Version:
- Organization:
- Priority:
- References:
- Reply-To:
- Subject:
- To:

### 5.1.2.2.3. Filtrado

88 Se puede definir opcionalmente filtrado para un canal. Si se define, los mensajes que no cumplan alguna condición serán rechazados.

89 Condiciones de filtrado

- Permitir o denegar (uno de los dos) una lista de extensiones
  - Permitir adjuntos sin extensión
-

- Permitir adjuntos con más de una extensión
- Tamaño máximo de un adjunto permitido
- Tamaño máximo del mensaje permitido
- Máximo número de destinatarios permitido
- Máximo número de adjuntos permitido
- Máximo nivel de anidamiento permitido

### 5.1.2.3. FDP\_IFC.2 / ENT Complete information flow control

#### 5.1.2.3.1. FDP\_IFC.2.1

90 The TSF shall enforce the [assignment: *“política y filtros de entrada de mensajes”*] on [assignment: ] on [assignment:

- *Información: mensajes de correo (según la Sección 5.1.2.1, “Flujo de entrada”).*
- *Sujetos: entidades origen en la Red Externa y destino en la Red Interna de la información.]*

and all operations that cause that information to flow to and from subjects covered by the SFP.

#### 5.1.2.3.2. FDP\_IFC.2.2

91 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

### 5.1.2.4. FDP\_IFF.1 / ENT Simple security attributes

#### 5.1.2.4.1. FDP\_IFF.1.1

92 The TSF shall enforce the [assignment: *“política y filtros de entrada de mensajes”*] based on the following types of subject and information security attributes: [assignment:

- *Información: mensajes de correo, atributos requeridos por las reglas y políticas de filtrado de la Sección 5.1.2.1, “Flujo de entrada” ]*.
- *Sujetos: entidades origen en la Red Externa y destino en la Red Interna de la información.]*

#### 5.1.2.4.2. FDP\_IFF.1.2

93 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:[assignment: *para*

*la entrada de mensajes de correo, el cumplimiento de la política y filtro indicados en la sección 5.1.2.1.].*

#### **5.1.2.4.3. FDP\_IFF.1.3**

94 The TSF shall enforce the [assignment: *las reglas indicadas en la sección 5.1.2.1 no asociadas al role o identidad del destinatario, sino asociadas al contenido del mensaje.*].

#### **5.1.2.4.4. FDP\_IFF.1.4**

95 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *None* ].

#### **5.1.2.4.5. FDP\_IFF.1.5**

96 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *None*].

### **5.1.2.5. FDP\_IFC.2 / SAL Complete information flow control**

#### **5.1.2.5.1. FDP\_IFC.2.1**

97 The TSF shall enforce the [assignment: *“política y filtros de salida de mensajes”*] on [assignment:

- *Información: mensajes de correo, (según la Sección 5.1.2.2, “Flujo de salida”).*
- *Sujetos: entidades origen en la Red Interna y destino en la Red Externa de la información. ]*

and all operations that cause that information to flow to and from subjects covered by the SFP.

#### **5.1.2.5.2. FDP\_IFC.2.2**

98 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

### **5.1.2.6. FDP\_IFF.1 / SAL Simple security attributes**

#### **5.1.2.6.1. FDP\_IFF.1.1**

99 The TSF shall enforce the [assignment: *“política y filtros de salida de mensajes”*] based on the following types of subject and information security attributes: [assignment:

- *Información: mensajes de correo, atributos requeridos por las reglas y políticas de filtrado indicados en la Sección 5.1.2.1, “Flujo de entrada”. ]*
  - *Sujetos: entidades origen en la Red Interna y destino en la Red Externa de la información.]*
-

#### 5.1.2.6.2. FDP\_IFF.1.2

100 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *para la salida de mensajes de correo, el cumplimiento de la política y filtro indicados en la sección 5.1.2.2.* ].

#### 5.1.2.6.3. FDP\_IFF.1.3

101 The TSF shall enforce the [assignment: *las reglas indicadas en la sección 5.1.2.2 no asociadas al role o identidad del remitente, sino asociadas al contenido del mensaje.* ].

#### 5.1.2.6.4. FDP\_IFF.1.4

102 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *None*].

#### 5.1.2.6.5. FDP\_IFF.1.5

103 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *None*].

### 5.1.3. Auditoría

#### 5.1.3.1. FAU\_GEN.1 Audit data generation

##### 5.1.3.1.1. FAU\_GEN.1.1

104 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the [selection: *not specified*] level of audit; and
- [assignment: *Los siguientes eventos:*]

#### **Eventos de funcionamiento**

AuditServerConnect

AuditServerConnectFail

AuditServerDisconnect

AuditServerCommandFailed

AuditServerUnavailable

ChannelWarning

ChannelError

---

---

ChannelOk  
ChannelRequestAcceptance  
ChannelRequestRejection  
ChannelDebug  
GlobalFailure  
GlobalSystemStartup  
GlobalSystemShutdown  
GlobalLinkUp  
GlobalLinkDown  
GlobalLinkFailure  
GlobalAuditFailure  
GlobalPrimaryConnect  
GlobalPrimaryConnectFail  
GlobalPrimaryDisconnect  
GlobalSecondaryConnect  
GlobalSecondaryDisconnect  
GlobalPrimaryEnabled  
GlobalPrimaryDisabled  
GlobalSecondaryEnabled  
GlobalSecondaryStandBy  
GlobalDebug  
ServiceStart  
ServiceStop  
ServiceFailure

**Eventos de seguridad**

AdminConnect  
AdminDisconnect

---

AdminConnectRejection  
 AdminWriteCommand  
 AuditServerConnectinSecFail  
 ChannelRequestSecRejection  
 ServiceRequestRejection

### **Transferencias de entrada de correo**

SendingTransfer	Envío de un mensaje a las cuentas de destino en la Red Interna.
RejectionTransfer	Rechazo de un mensaje.
SelectionTransfer	Envío de un mensaje a las cuentas de desvío por filtrado de selección.
DeletionTransfer	Borrado de un mensaje de la cuenta de la Red Externa.

### **Transferencias de salida de correo**

OmTransfer	Envío satisfactorio de un mensaje de salida a través de la pasarela
OmFailedTransfer	Fallo en el envío de un mensaje de salida a través de la pasarela

#### **5.1.3.1.2. FAU\_GEN.1.2**

105 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: ]

### **Eventos de funcionamiento y seguridad**

Severidad	Informational (6), Notice (5), Warning (4), Error (3) y Critical (2)
Información específica del evento	Depende del evento
Hostname	Dirección IP de la unidad interna de la pasarela que envía el evento
Tag	Identificador de la pasarela

## Transferencias de entrada de correo

ChannelId	Identificador del canal
TransferId	Identificador de la transferencia
CycleStartTime	Fecha y hora de inicio del ciclo de correo

Opcionalmente si se configura el registro de información adicional:

From	Remitente del mensaje
To	Destinatario principal (To:) del mensaje
Cc	Destinatario copia (Cc:) del mensaje
MimeType	Tipo MIME
Attachment info	Para cada adjunto: Nombre y extensión, tamaño, tipo y subtipo MIME, número de extensiones.
IsStandard	Tiene formato estándar
Nesting	Nivel de anidamiento
Subject	Asunto
SizeKB	Tamaño en KB
ToNumber	Número de destinatarios principales (To:)
CcNumber	Número de destinatarios copia (Cc:)
AttachmentNumber	Número de ficheros adjuntos

## Transferencias de salida de correo

ChannelId	Identificador del canal
TransferId	Identificador de la transferencia
AcceptanceTime	Fecha y hora de aceptación del mensaje
SigningAuthority	Dirección de correo interna del supervisor que autoriza la transferencia
OriginatingUser	Dirección de correo interna del usuario que originó el mensaje
ExternalRcptTo	Dirección de correo externa de destino del mensaje

---

FailReason (sólo en caso de fallo)	Motivo del fallo en el envío
AdditionalInfo (sólo en caso de fallo)	Información adicional
Opcionalmente si se configura el registro de información adicional:	
From	Remitente del mensaje
To	Destinatario principal (To:) del mensaje
Cc	Destinatario copia (Cc:) del mensaje
MimeType	Tipo MIME
Attachment info	Para cada adjunto: Nombre y extensión, tamaño, tipo y subtipo MIME, número de extensiones.
IsStandard	Tiene formato estándar
Nesting	Nivel de anidamiento
Subject	Asunto
SizeKB	Tamaño en KB
ToNumber	Número de destinatarios principales (To:)
CcNumber	Número de destinatarios copia (Cc:)
AttachmentNumber	Número de ficheros adjuntos

### 5.1.3.2. FAU\_SAR.1 Audit review

#### 5.1.3.2.1. FAU\_SAR.1.1

106 The TSF shall provide [assignment: *Administrador de Seguridad / de Servicios*] with the capability to read [assignment: *los eventos del sistema de seguridad / funcionamiento*] from the audit records.

#### 5.1.3.2.2. FAU\_SAR.1.2

107 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

### 5.1.3.3. FAU\_SAR.2 Restricted audit review

#### 5.1.3.3.1. FAU\_SAR.1.2 Restricted audit review

108 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

## 5.2. Requisitos de garantía de seguridad

109 El desarrollo y evaluación del TOE se realizará conforme al siguiente nivel de garantía:

- EAL4
- ALC\_FLR.1

### 5.2.1. ADV\_ARC.1 Security architecture description

Developer action elements:

#### 5.2.1.1. ADV\_ARC.1.1D

110 **The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.**

#### 5.2.1.2. ADV\_ARC.1.2D

111 **The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.**

#### 5.2.1.3. ADV\_ARC.1.3D

112 **The developer shall provide a security architecture description of the TSF.**

Content and presentation of evidence elements:

#### 5.2.1.4. ADV\_ARC.1.1C

113 **The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.**

#### 5.2.1.5. ADV\_ARC.1.2C

114 **The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.**

#### 5.2.1.6. ADV\_ARC.1.3C

115 **The security architecture description shall describe how the TSF initialisation process is secure.**

#### 5.2.1.7. ADV\_ARC.1.4C

116 **The security architecture description shall demonstrate that the TSF protects itself from tampering.**

---

### **5.2.1.8. ADV\_ARC.1.5C**

- 117      **The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.**

## **5.2.2. ADV\_FSP.4 Complete functional specification**

Developer action elements:

### **5.2.2.1. ADV\_FSP.4.1D**

- 118      **The developer shall provide a functional specification.**

### **5.2.2.2. ADV\_FSP.4.2D**

- 119      **The developer shall provide a tracing from the functional specification to the SFRs.**

### **5.2.2.3. ADV\_FSP.4.1C**

- 120      **The functional specification shall completely represent the TSF.**

### **5.2.2.4. ADV\_FSP.4.2C**

- 121      **The functional specification shall describe the purpose and method of use for all TSFI.**

### **5.2.2.5. ADV\_FSP.4.3C**

- 122      **The functional specification shall identify and describe all parameters associated with each TSFI.**

### **5.2.2.6. ADV\_FSP.4.4C**

- 123      **The functional specification shall describe all actions associated with each TSFI.**

### **5.2.2.7. ADV\_FSP.4.5C**

- 124      **The functional specification shall describe all direct error messages that may result from an invocation of each TSFI.**

### **5.2.2.8. ADV\_FSP.4.6C**

- 125      **The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.**

## **5.2.3. ADV\_IMP.1 Implementation representation of the TSF**

Developer action elements:

---

### **5.2.3.1. ADV\_IMP.1.1D**

126      **The developer shall make available the implementation representation for the entire TSF.**

### **5.2.3.2. ADV\_IMP.1.2D**

127      **The developer shall provide a mapping between the TOE design description and the sample of the implementation representation.**

Content and presentation of evidence elements:

### **5.2.3.3. ADV\_IMP.1.1C**

128      **The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.**

### **5.2.3.4. ADV\_IMP.1.2C**

129      **The implementation representation shall be in the form used by the development personnel.**

### **5.2.3.5. ADV\_IMP.1.3C**

130      **The mapping between the TOE design description and the sample of the implementation representation shall demonstrate their correspondence.**

## **5.2.4. ADV\_TDS.3 Basic modular design**

Developer action elements:

### **5.2.4.1. ADV\_TDS.3.1D**

131      **The developer shall provide the design of the TOE.**

### **5.2.4.2. ADV\_TDS.3.2D**

132      **The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.**

Content and presentation of evidence elements:

### **5.2.4.3. ADV\_TDS.3.1C**

133      **The design shall describe the structure of the TOE in terms of subsystems.**

### **5.2.4.4. ADV\_TDS.3.2C**

134      **The design shall describe the TSF in terms of modules.**

---

**5.2.4.5. ADV\_TDS.3.3C**

135 The design shall identify all subsystems of the TSF.

**5.2.4.6. ADV\_TDS.3.4C**

136 The design shall provide a description of each subsystem of the TSF.

**5.2.4.7. ADV\_TDS.3.5C**

137 The design shall provide a description of the interactions among all subsystems of the TSF.

**5.2.4.8. ADV\_TDS.3.6C**

138 The design shall provide a mapping from the subsystems of the TSF to the modules of the TSF.

**5.2.4.9. ADV\_TDS.3.7C**

139 The design shall describe each SFR-enforcing module in terms of its purpose and relationship with other modules.

**5.2.4.10. ADV\_TDS.3.8C**

140 The design shall describe each SFR-enforcing module in terms of its SFR-related interfaces, return values from those interfaces, interaction with other modules and called SFR-related interfaces to other SFR-enforcing modules.

**5.2.4.11. ADV\_TDS.3.9C**

141 The design shall describe each SFR-supporting or SFR-non-interfering module in terms of its purpose and interaction with other modules.

**5.2.4.12. ADV\_TDS.3.10C**

142 The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

**5.2.5. AGD\_OPE.1 Operational user guidance**

Developer action elements:

**5.2.5.1. AGD\_OPE.1.1D**

143 The developer shall provide operational user guidance.

Content and presentation of evidence elements:

---

### **5.2.5.2. AGD\_OPE.1.1C**

- 144      **The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.**

### **5.2.5.3. AGD\_OPE.1.2C**

- 145      **The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.**

### **5.2.5.4. AGD\_OPE.1.3C**

- 146      **The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.**

### **5.2.5.5. AGD\_OPE.1.4C**

- 147      **The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.**

### **5.2.5.6. AGD\_OPE.1.5C**

- 148      **The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.**

### **5.2.5.7. AGD\_OPE.1.6C**

- 149      **The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.**

### **5.2.5.8. AGD\_OPE.1.7C**

- 150      **The operational user guidance shall be clear and reasonable.**

## **5.2.6. AGD\_PRE.1 Preparative procedures**

Developer action elements:

### **5.2.6.1. AGD\_PRE.1.1D**

- 151      **The developer shall provide the TOE including its preparative procedures.**

Content and presentation of evidence elements:

---

**5.2.6.2. AGD\_PRE.1.1C**

152 The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

**5.2.6.3. AGD\_PRE.1.2C**

153 The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

**5.2.7. ALC\_CMC.4 Production support, acceptance procedures and automation**

Developer action elements:

**5.2.7.1. ALC\_CMC.4.1D**

154 The developer shall provide the TOE and a reference for the TOE.

**5.2.7.2. ALC\_CMC.4.2D**

155 The developer shall provide the CM documentation.

**5.2.7.3. ALC\_CMC.4.3D**

156 The developer shall use a CM system.

Content and presentation of evidence elements:

**5.2.7.4. ALC\_CMC.4.1C**

157 The TOE shall be labelled with its unique reference.

**5.2.7.5. ALC\_CMC.4.2C**

158 The CM documentation shall describe the method used to uniquely identify the configuration items.

**5.2.7.6. ALC\_CMC.4.3C**

159 The CM system shall uniquely identify all configuration items.

**5.2.7.7. ALC\_CMC.4.4C**

160 The CM system shall provide automated measures such that only authorised changes are made to the configuration items.

---

**5.2.7.8. ALC\_CMC.4.5C**

161 The CM system shall support the production of the TOE by automated means.

**5.2.7.9. ALC\_CMC.4.6C**

162 The CM documentation shall include a CM plan.

**5.2.7.10. ALC\_CMC.4.7C**

163 The CM plan shall describe how the CM system is used for the development of the TOE.

**5.2.7.11. ALC\_CMC.4.8C**

164 The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

**5.2.7.12. ALC\_CMC.4.9C**

165 The evidence shall demonstrate that all configuration items are being maintained under the CM system.

**5.2.7.13. ALC\_CMC.4.10C**

166 The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

**5.2.8. ALC\_CMS.4 Problem tracking CM coverage**

Developer action elements:

**5.2.8.1. ALC\_CMS.4.1D**

167 The developer shall provide a configuration list for the TOE.

Content and presentation of evidence elements:

**5.2.8.2. ALC\_CMS.4.1C**

168 The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

**5.2.8.3. ALC\_CMS.4.2C**

169 The configuration list shall uniquely identify the configuration items.

**5.2.8.4. ALC\_CMS.4.3C**

170 For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

---

## **5.2.9. ALC\_DEL.1 Delivery procedures**

Developer action elements:

### **5.2.9.1. ALC\_DEL.1.1D**

171      **The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.**

### **5.2.9.2. ALC\_DEL.1.2D**

172      **The developer shall use the delivery procedures.**

Content and presentation of evidence elements:

### **5.2.9.3. ALC\_DEL.1.1C**

173      **The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.**

## **5.2.10. ALC\_DVS.1 Identification of security measures**

Developer action elements:

### **5.2.10.1. ALC\_DVS.1.1D**

174      **The developer shall produce and provide development security documentation.**

Content and presentation of evidence elements:

### **5.2.10.2. ALC\_DVS.1.1C**

175      **The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.**

## **5.2.11. ALC\_FLR.1 Basic flaw remediation**

Developer action elements:

### **5.2.11.1. ALC\_FLR.1.1D**

176      **The developer shall document and provide flaw remediation procedures addressed to TOE developers.**

Content and presentation of evidence elements:

### **5.2.11.2. ALC\_FLR.1.1C**

177      **The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.**

---

### **5.2.11.3. ALC\_FLR.1.2C**

- 178      **The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.**

### **5.2.11.4. ALC\_FLR.1.3C**

- 179      **The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.**

### **5.2.11.5. ALC\_FLR.1.4C**

- 180      **The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.**

## **5.2.12. ALC\_LCD.1 Developer defined life-cycle model**

Developer action elements:

### **5.2.12.1. ALC\_LCD.1.1D**

- 181      **The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.**

### **5.2.12.2. ALC\_LCD.1.2D**

- 182      **The developer shall provide life-cycle definition documentation.**

Content and presentation of evidence elements:

### **5.2.12.3. ALC\_LCD.1.1C**

- 183      **The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.**

### **5.2.12.4. ALC\_LCD.1.2C**

- 184      **The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.**

## **5.2.13. ALC\_TAT.1 Well-defined development tools**

Developer action elements:

### **5.2.13.1. ALC\_TAT.1.1D**

- 185      **The developer shall provide the documentation identifying each development tool being used for the TOE.**
-

### **5.2.13.2. ALC\_TAT.1.2D**

186      **The developer shall document and provide the selected implementationdependent options of each development tool.**

Content and presentation of evidence elements:

### **5.2.13.3. ALC\_TAT.1.1C**

187      **Each development tool used for implementation shall be well-defined.**

### **5.2.13.4. ALC\_TAT.1.2C**

188      **The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.**

### **5.2.13.5. ALC\_TAT.1.3C**

189      **The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.**

## **5.2.14. ASE\_INT.1 ST introduction**

Developer action elements:

### **5.2.14.1. ASE\_INT.1.1D**

190      **The developer shall provide an ST introduction.**

Content and presentation of evidence elements:

### **5.2.14.2. ASE\_INT.1.1C**

191      **The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.**

### **5.2.14.3. ASE\_INT.1.2C**

192      **The ST reference shall uniquely identify the ST.**

### **5.2.14.4. ASE\_INT.1.3C**

193      **The TOE reference shall identify the TOE.**

### **5.2.14.5. ASE\_INT.1.4C**

194      **The TOE overview shall summarise the usage and major security features of the TOE.**

---

**5.2.14.6. ASE\_INT.1.5C**

195 The TOE overview shall identify the TOE type.

**5.2.14.7. ASE\_INT.1.6C**

196 The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

**5.2.14.8. ASE\_INT.1.7C**

197 The TOE description shall describe the physical scope of the TOE.

**5.2.14.9. ASE\_INT.1.8C**

198 The TOE description shall describe the logical scope of the TOE.

**5.2.15. ASE\_CCL.1 Conformance claims**

Developer action elements:

**5.2.15.1. ASE\_CCL.1.1D**

199 The developer shall provide a conformance claim.

**5.2.15.2. ASE\_CCL.1.2D**

200 The developer shall provide a conformance claim rationale.

Content and presentation of evidence elements:

**5.2.15.3. ASE\_CCL.1.1C**

201 The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

**5.2.15.4. ASE\_CCL.1.2C**

202 The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

**5.2.15.5. ASE\_CCL.1.3C**

203 The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

**5.2.15.6. ASE\_CCL.1.4C**

204 The CC conformance claim shall be consistent with the extended components definition.

---

**5.2.15.7. ASE\_CCL.1.5C**

205      **The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.**

**5.2.15.8. ASE\_CCL.1.6C**

206      **The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.**

**5.2.15.9. ASE\_CCL.1.7C**

207      **The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.**

**5.2.15.10. ASE\_CCL.1.8C**

208      **The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.**

**5.2.15.11. ASE\_CCL.1.9C**

209      **The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.**

**5.2.15.12. ASE\_CCL.1.10C**

210      **The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.**

**5.2.16. ASE\_SPD.1 Security problem definition**

Developer action elements:

**5.2.16.1. ASE\_APD.1.1D**

211      **The developer shall provide a security problem definition.**

Content and presentation of evidence elements:

**5.2.16.2. ASE\_SPD.1.1C**

212      **The security problem definition shall describe the threats.**

**5.2.16.3. ASE\_SPD.1.2C**

213      **All threats shall be described in terms of a threat agent, an asset, and an adverse action.**

---

**5.2.16.4. ASE\_SPD.1.3C**

214 The security problem definition shall describe the OSPs.

**5.2.16.5. ASE\_SPD.1.4C**

215 The security problem definition shall describe the assumptions about the operational environment of the TOE.

**5.2.17. ASE\_OBJ.2 Security objectives**

Developer action elements:

**5.2.17.1. ASE\_OBJ.2.1D**

216 The developer shall provide a statement of security objectives.

**5.2.17.2. ASE\_OBJ.2.2D**

217 The developer shall provide a security objectives rationale.

Content and presentation of evidence elements:

**5.2.17.3. ASE\_OBJ.2.1C**

218 The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

**5.2.17.4. ASE\_OBJ.2.2C**

219 The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

**5.2.17.5. ASE\_OBJ.2.3C**

220 The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

**5.2.17.6. ASE\_OBJ.2.4C**

221 The security objectives rationale shall demonstrate that the security objectives counter all threats.

**5.2.17.7. ASE\_OBJ.2.5C**

222 The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

---

### **5.2.17.8. ASE\_OBJ.2.6C**

- 223      **The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.**

### **5.2.18. ASE\_ECD.1 Extended components definition**

Developer action elements:

#### **5.2.18.1. ASE\_ECD.1.1D**

- 224      **The developer shall provide a statement of security requirements.**

#### **5.2.18.2. ASE\_ECD.1.2D**

- 225      **The developer shall provide an extended components definition.**

Content and presentation of evidence elements:

#### **5.2.18.3. ASE\_ECD.1.1C**

- 226      **The statement of security requirements shall identify all extended security requirements.**

#### **5.2.18.4. ASE\_ECD.1.2C**

- 227      **The extended components definition shall define an extended component for each extended security requirement.**

#### **5.2.18.5. ASE\_ECD.1.3C**

- 228      **The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.**

#### **5.2.18.6. ASE\_ECD.1.4C**

- 229      **The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.**

#### **5.2.18.7. ASE\_ECD.1.5C**

- 230      **The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.**

### **5.2.19. ASE\_REQ.2 Derived security requirements**

Developer action elements:

#### **5.2.19.1. ASE\_REQ.2.1D**

- 231      **The developer shall provide a statement of security requirements.**
-

**5.2.19.2. ASE\_REQ.2.2D**

232 The developer shall provide a security requirements rationale.

Content and presentation of evidence elements:

**5.2.19.3. ASE\_REQ.2.1C**

233 The statement of security requirements shall describe the SFRs and the SARs.

**5.2.19.4. ASE\_REQ.2.2C**

234 All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

**5.2.19.5. ASE\_REQ.2.3C**

235 The statement of security requirements shall identify all operations on the security requirements.

**5.2.19.6. ASE\_REQ.2.4C**

236 All operations shall be performed correctly.

**5.2.19.7. ASE\_REQ.2.5C**

237 Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

**5.2.19.8. ASE\_REQ.2.6C**

238 The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

**5.2.19.9. ASE\_REQ.2.7C**

239 The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

**5.2.19.10. ASE\_REQ.2.8C**

240 The security requirements rationale shall explain why the SARs were chosen.

**5.2.19.11. ASE\_REQ.2.9C**

241 The statement of security requirements shall be internally consistent.

**5.2.20. ASE\_TSS.1 TOE summary specification**

Developer action elements:

---

### **5.2.20.1. ASE\_TSS.1.1D**

242      **The developer shall provide a TOE summary specification.**

Content and presentation of evidence elements:

### **5.2.20.2. ASE\_TSS.1.1C**

243      **The TOE summary specification shall describe how the TOE meets each SFR.**

## **5.2.21. ATE\_COV.2 Analysis of coverage**

Developer action elements:

### **5.2.21.1. ATE\_COV.2.1D**

244      **The developer shall provide an analysis of the test coverage.**

Content and presentation of evidence elements:

### **5.2.21.2. ATE\_COV.2.1C**

245      **The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.**

### **5.2.21.3. ATE\_COV.2.2C**

246      **The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.**

## **5.2.22. ATE\_DPT.1 Testing: basic design**

Developer action elements:

### **5.2.22.1. ATE\_DPT.1.1D**

247      **The developer shall provide the analysis of the depth of testing.**

Content and presentation of evidence elements:

### **5.2.22.2. ATE\_DPT.1.1C**

248      **The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.**

### **5.2.22.3. ATE\_DPT.1.2C**

249      **The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.**

---

### **5.2.23. ATE\_FUN.1 Functional testing**

Developer action elements:

#### **5.2.23.1. ATE\_FUN.1.1D**

250      **The developer shall test the TSF and document the results.**

#### **5.2.23.2. ATE\_FUN.1.2D**

251      **The developer shall provide test documentation.**

Content and presentation of evidence elements:

#### **5.2.23.3. ATE\_FUN.1.1C**

252      **The test documentation shall consist of test plans, expected test results and actual test results.**

#### **5.2.23.4. ATE\_FUN.1.2C**

253      **The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.**

#### **5.2.23.5. ATE\_FUN.1.3C**

254      **The expected test results shall show the anticipated outputs from a successful execution of the tests.**

#### **5.2.23.6. ATE\_FUN.1.4C**

255      **The actual test results shall be consistent with the expected test results.**

### **5.2.24. ATE\_IND.2 Independent testing - sample**

Developer action elements:

#### **5.2.24.1. ATE\_IND.2.1D**

256      **The developer shall provide the TOE for testing.**

Content and presentation of evidence elements:

#### **5.2.24.2. ATE\_IND.2.1C**

257      **The TOE shall be suitable for testing.**

#### **5.2.24.3. ATE\_IND.2.2C**

258      **The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.**

---

### 5.2.25. AVA\_VAN.3 Focused vulnerability analysis

Developer action elements:

#### 5.2.25.1. AVA\_VAN.3.1D

259 The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

#### 5.2.25.2. AVA\_VAN.3.1C

260 The TOE shall be suitable for testing.

## 5.3. Justificación de los requisitos de seguridad

	O1.FLUJO	O2.ROLES	O3.AUDITORIA
FMT_SMF.1 FDP_IFC.2 / ENT FDP_IFF.1 / ENT FDP_IFC.2 / SAL FDP_IFF.1 / SAL FMT_MSA.1 / IFF FMT_MSA.3 / IFF	X		
FMT_SMR.2 FMT_SMF.1 FDP_ACF.1 FDP_ACC.2 FMT_MSA.1 / ACC FMR_MSA.3 / ACC FIA_UID.2 FIA_UAU.2		X	
FAU_GEN.1 FAU_SAR.1 FAU_SAR.2 FMT_SMF.1			X

**Tabla 4. Justificación de los requisitos de seguridad**

### 5.3.1. Justificación de dependencias no satisfechas

261 FPT\_STM.1 no se satisface porque el TOE toma la fuente de tiempo del reloj del sistema.

### 5.3.2. Justificación de requisitos de seguridad funcionales

- 262 El objetivo O1.FLUJO se cumple porque existe una política de control de flujo completo (FDP\_IFC.2 / ENT para la entrada y FDP\_IFC.2 / SAL para la salida) con los atributos de seguridad expresados en FDP\_IFF.1 / ENT para la entrada y FDP\_IFF.1 / SAL para la salida y gestionándose dichos atributos de seguridad de acuerdo con FMT\_MSA.1 / IFF y FMT\_MSA.3 / IFF. La gestión de los atributos correspondientes se realiza con FMT\_SMF.1.
- 263 El objetivo O2.ROLES se cumple mediante los roles especificados en FMT\_SMR.2. Las funciones de cada rol se especifican en FMT\_SMF.1. La identificación y autenticación de usuarios antes de cualquier acción están cubiertas en FIA\_UID.2 y FIA\_UAU.2. Los atributos de seguridad se gestionan de acuerdo con FMT\_MSA.1 / ACC y FMT\_MSA.3 / ACC. El control acceso basado en atributos de seguridad y el control completo los imponen FDP\_ACF.1 y FDP\_ACC.2.
- 264 El objetivo O3.AUDITORIA se satisface mediante las funciones FAU\_GEN.1, FAU\_SAR.1 y FAU\_SAR.2. La auditoría es configurable conforme a FMT\_SMF.1

### 5.3.3. Justificación de requisitos de seguridad de garantía

- 265 La garantía de seguridad deseada para el TOE es la proporcionada por el nivel de evaluación EAL4 + ALC\_FLR.1.
- 266 Se ha elegido EAL4 para que el usuario final obtenga la máxima confianza en el producto desarrollado en base a métodos de ingeniería sistemáticos y buenas prácticas de desarrollo, siendo capaz el producto de resistir a ataques con potencial de ataque “Enhanced Basic”.



---

## 6. Especificación resumida del TOE

### 6.1. FMT\_SMR.2 Restrictions on security roles

#### 6.1.1. Roles de administración

267 Se mantienen los siguientes 5 roles para usuarios administradores:

- Administrador Raíz
- Administrador de Seguridad
- Administrador de Servicios
- Administrador de Monitorización
- Administrador Local

268 La asociación del rol de administrador Local a un usuario se realiza mediante medidas organizativas de limitación de acceso físico a las unidades de PSTmail. La primera vez que se accede a la interfaz local de las unidades internas se establece una contraseña que es necesario suministrar en posteriores accesos.

269 La asociación de roles a usuarios se realiza en base al CN (Common Name) de un certificado del usuario emitido por una CA (Certification Authority) preconfigurada (inicialización estática) en PSTmail.

270 La asignación a usuarios del rol “Administrador Raíz” se realiza exclusivamente de manera local (inicialización estática) y está limitado a 5 usuarios.

271 La asignación a usuarios de los roles “Administrador de Seguridad”, “Administrador de Servicios” y “Administrador de Monitorización” se realiza de manera remota (desde la Red Interna) por un administrador Raíz. No existe ninguna restricción en cuanto a los roles que se le pueden asignar a un usuario.

### 6.2. FMT\_SMF.1 Specification of Management Functions

272 En la Tabla 3 se especifican las funciones de cada uno de los roles Administrador Raíz, Administrador de Seguridad, Administrador de Servicios, Administrador de Monitorización.

273 El Administrador Local establece la configuración estática en la unidad interna PSTi. La configuración estática tiene los siguientes atributos:

- Parámetros de red de ambas unidades
  - Certificados de las entidades emisoras raíces de confianza
  - Clave privada y certificado para la pasarela
-

- CN de los administradores Raíz

### **6.3. FIA\_UID.2 User identification before any action**

- 274 Los administradores, excepto los locales, acceden a la funcionalidad de seguridad mediante funciones de admAPI. Para acceder a cualquier función de admAPI, es necesario establecer previamente una conexión SSL con PSTi. Se utiliza el CN del certificado enviado en la conexión SSL para identificar al administrador.
- 275 Los administradores Locales se identifican mediante una contraseña. El administrador Local solo se autentica con una contraseña que el mismo suministra la primera vez que accede a la interfaz local de configuración. La identificación es implícita al acceder a dicho interface.

### **6.4. FIA\_UAU.2 User authentication before any action**

- 276 Los administradores, excepto los locales, acceden a la funcionalidad de seguridad mediante funciones de admAPI. Para acceder a cualquier función de admAPI, es necesario establecer previamente una conexión SSL con PSTi. Se utiliza el CN del certificado enviado en la conexión SSL para autenticar al administrador.
- 277 El certificado debe estar firmado por una CA dada de alta en la configuración estática de PSTi.
- 278 Los administradores Locales se autentican mediante una contraseña.

### **6.5. FMT\_MSA.1 / IFF Management of security attributes**

- 279 La política y filtros de entrada y salida, se establecen mediante comandos de admAPI. Para acceder a cualquier función de admAPI, es necesario establecer previamente una conexión SSL con PSTi. Se utiliza el CN del certificado enviado en la conexión SSL para autenticar al administrador.
- 280 Para acceder a estos comandos es necesario el rol de “Administrador de Servicios”.
- 281 En la entrada de correo los atributos que se gestionan son los descritos en la sección 5.1.2.1 Flujo de entrada.
- 282 En la salida de correo los atributos que se gestionan son los descritos en la sección 5.1.2.2 Flujo de salida.

### **6.6. FMT\_MSA.1 / ACC Management of security attributes**

- 283 El administrador Local establece mediante la interfaz local de configuración, en la configuración estática, el CN de los administradores Raíz. El acceso físico a la interfaz local de configuración se limita mediante políticas organizativas del entorno.
-

- 284 La política de acceso y roles se establece mediante un comando de admAPI. Para acceder a cualquier función de admAPI, es necesario establecer previamente una conexión SSL con PSTi. Se utiliza el CN del certificado enviado en la conexión SSL para autenticar al administrador.
- 285 Para acceder a este comando es necesario el rol de “administrador Raíz”.
- 286 El comando permite establecer la lista de administradores autorizados y la lista de IPs desde las que se permite administrar el sistema. Cada uno de los administradores se identifica por el CN y los permisos posibles son: ‘administrador de Monitorización’, ‘administrador de Servicios’ y ‘administrador de Seguridad’. El permiso de ‘administrador Raíz’ sólo se puede modificar localmente.

287

## **6.7. FMT\_MSA.3 / IFF Static attribute initialization**

### **6.7.1. Política y filtros de entrada y salida**

- 288 La inicialización proporciona una configuración sin canales ni ningún elemento otro elemento de configuración (incluidos usuarios y supervisores). Esto impide cualquier flujo tanto de entrada como de salida, si no se establece explícitamente por un administrador de Servicios (ver FMT\_MSA.1.IFF).

## **6.8. FMT\_MSA.3 / ACC Static attribute initialization**

### **6.8.1. Política de acceso y roles**

- 289 La inicialización proporciona una configuración en la que ningún usuario tiene asignado ningún rol de administración excepto los administradores Raíz que sólo se pueden establecer mediante la inicialización estática. Esto garantiza que no exista inicialmente ningún administrador con rol “administrador de Seguridad”, “administrador de Servicios” ni “administrador de Monitorización” configurado. Todos los administradores de estos tipos, deben ser dados de alta mediante admAPI (ver FMT\_MSA.1.ACC).

## **6.9. FDP\_ACF.1 Security attribute based access control**

- 290 Los administradores acceden a la funcionalidad de seguridad mediante funciones de admAPI. Para acceder a cualquier función de admAPI, es necesario establecer previamente una conexión SSL con PSTi. Se utiliza el CN del certificado enviado en la conexión SSL para autenticar al administrador. Al invocarse cualquier función se comprueba que el administrador que ha establecido la conexión tiene el permiso necesario para ejecutar el comando. Cada comando tiene un único permiso requerido (ver tabla de comandos en FDP\_ACF.1.3). En caso afirmativo se permite ejecutar el comando y en caso negativo se interrumpe la conexión SSL.

## **6.10. FDP\_ACC.2 Complete access control**

- 291 Ver Sección 6.9, “FDP\_ACF.1 Security attribute based access control”.
-

## 6.11. FDP\_IFC.2 / ENT Complete information flow control

- 292 El servicio de entrada de correo de PSTmail transmite exclusivamente un mensaje de la Red Externa a la Red Interna si se cumplen las siguientes condiciones:
- El mensaje se encuentra en un buzón de la Red Externa para el que existe un canal de entrada definido en la configuración de canales de entrada.
  - El canal al que corresponde el mensaje se encuentra activo.
  - El mensaje cumple las condiciones de filtrado establecidas para el canal.
- 293 La configuración de los canales de entrada incluye la definición de los elementos mencionados: buzones de la Red Externa que se consultarán, estado (activo – no activo) de los canales, condiciones de filtrado que se aplican a cada canal. Esto se describe en detalle en la sección 5.1.2.1 Flujo de entrada.
- 294 La configuración de los canales se establece mediante comandos de admAPI. Para acceder a estos comandos es necesario el rol de “Administrador de Servicios”.

## 6.12. FDP\_IFF.1 / ENT Simple security attributes

- 295 Ver Sección 6.11, “FDP\_IFC.2 / ENT Complete information flow control”.

## 6.13. FDP\_IFC.2 / SAL Complete information flow control

- 296 El servicio de salida de correo de PSTmail transmite exclusivamente un mensaje de la Red Interna a la Red Externa si se cumplen las siguientes condiciones:
- El canal por el que se pretende enviar el mensaje se encuentra activo.
  - El mensaje está correctamente firmado.
  - La firma se ha realizado con un certificado emitido por una CA de confianza.
  - El supervisor, identificado por el CN del certificado, que lo autoriza se encuentra entre los configurados para autorizar la salida por ese canal.
  - El mensaje cumple las condiciones de filtrado establecidas para el canal.
- 297 La configuración de los canales de salida incluye los supervisores que pueden autorizar el envío de mensajes por ese canal, las condiciones de filtrado y el estado (activo o no) del canal. Esta configuración se describe en detalle en la sección 5.1.2.2 Flujo de salida
- 298 Dicha configuración se establece mediante comandos de admAPI. Para acceder a estos comandos es necesario el rol de “Administrador de Servicios”.
-

- 299 La selección del canal de salida para cada mensaje se realiza del siguiente modo:
- Si el campo de encabezamiento ‘Reply-to:’ está presente, se comprueba si su valor coincide con el remite externo de algún canal configurado y en caso afirmativo se selecciona este.
  - Si no está presente se utiliza el remite externo por defecto del usuario (o supervisor) originario del mensaje.

## 6.14. FDP\_ IFF.1 / SAL Simple security attributes

- 300 Ver Sección 6.13, “FDP\_ IFC.2 / SAL Complete information flow control”.

## 6.15. FAU\_ GEN.1 Audit data generation

- 301 PSTmail genera dos tipos distintos de datos de auditoría:
- Eventos de sistema
  - Registros de transferencias

### 6.15.1. Eventos del sistema

- 302 Los eventos de sistema se envían por “syslog” y además se guardan en ficheros que se rotan (con tamaño y número de ficheros configurables). Los eventos de sistema están divididos en dos grupos: seguridad y funcionamiento. Los parámetros de configuración (servidor al que se envían, niveles de severidad mínimos y parámetros de rotación de ficheros) son independientes para ambos tipos. El Administrador de Seguridad exclusivamente es el que puede establecer estos parámetros.
- 303 Los ficheros en los que se guardan no se pueden borrar, pero sí se pueden consultar remotamente mediante comandos de admAPI. Es necesario el rol de “Administrador de Seguridad” para tener acceso a los ficheros correspondientes a los de seguridad y el rol de “Administrador de Servicios” para tener acceso a los ficheros correspondientes a los de funcionamiento.
- 304 En todos los eventos de este tipo se registra la siguiente información: fecha y hora del evento, tipo de evento, identidad del sujeto (en los casos en que aplique) y otra información relevante como el nivel de severidad.
- 305 Los eventos que señalizan el inicio y final de las funciones de auditoría son GlobalSystemStartUp y GlobalSystemShutdown respectivamente.

### 6.15.2. Registros de transferencias

- 306 Los datos de cada transferencia de entrada o salida de correo se registran en una base de datos ajena al sistema mediante PSTaud. La configuración para el acceso a PSTaud se configura con el rol de “Administrador de Seguridad”.
-

- 307 La activación o no del registro de transferencias es un parámetro de la configuración general de cada servicio. Para establecer este parámetro es necesario el rol de “Administrador de Servicios”.
- 308 En todos los eventos de este tipo se registra la siguiente información: fecha y hora de la transferencia, tipo de transferencia (entrada o salida de correo), identidad del canal, origen y destino del mensaje y otra información relevante como tamaño del mensaje transferido, etc.

## **6.16. FAU\_SAR.1 Audit review**

- 309 Este requisito sólo lo implementa el TOE para los eventos del sistema.
- 310 Es necesario el rol de “Administrador de Seguridad” para tener acceso a los ficheros correspondientes a los eventos de sistema de seguridad.
- 311 Es necesario el rol de “Administrador de Servicios” para tener acceso a los ficheros correspondientes a los eventos de sistema de funcionamiento.
- 312 El formato de los ficheros de eventos de sistema es texto plano con una línea para cada evento en formato ‘syslog’.

## **6.17. FAU\_SAR.2 Restricted audit review**

- 313 Este requisito sólo lo implementa el TOE para los eventos del sistema.
- 314 Para tener acceso a los ficheros se utilizan comandos de admAPI. Para acceder a cualquier comando de admAPI, es necesario establecer previamente una conexión SSL con PSTi. Se utiliza el CN del certificado enviado en la conexión SSL para autenticar al administrador.
-