

Unión Internacional de Telecomunicaciones

**UIT-T**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

**X.1245**

(12/2010)

SERIE X: REDES DE DATOS, COMUNICACIONES DE  
SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Lucha contra el correo  
basura

---

**Marco para la lucha contra el correo basura en  
aplicaciones multimedios IP**

Recomendación UIT-T X.1245

RECOMENDACIONES UIT-T DE LA SERIE X  
**REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD**

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
<b>Lucha contra el correo basura</b>	<b>X.1230–X.1249</b>
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de eurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589

Para más información, véase la Lista de Recomendaciones del UIT-T.

## Recomendación UIT-T X.1245

### Marco para la lucha contra el correo basura en aplicaciones multimedios IP

#### Resumen

La Recomendación UIT-T X.1245 contiene el marco general para combatir el correo basura en las aplicaciones multimedios IP tales como la telefonía IP, la mensajería instantánea, las conferencias multimedios, etc. Dicho marco consta de cuatro funciones de lucha contra el correo basura, a saber, funciones medulares de lucha contra el correo basura (*core anti-spam functions*, CASF), funciones de lucha contra el correo basura en el lado receptor (*recipient-side anti-spam functions*, RASF), funciones de lucha contra el correo basura en el lado emisor (*sender-side anti-spam functions*, SASF), y funciones receptoras de correo basura (*spam recipient functions*, SRF). En esta Recomendación se describen las funcionalidades y las interfaces de cada función para combatir el correo basura en multimedios IP.

#### Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1245	2010-12-17	17

#### Palabras clave

Correo basura, correo basura en multimedios IP, funciones de lucha contra el correo basura.

## PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

## NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

## PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT [ha recibido/no ha recibido] notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección <http://www.itu.int/ITU-T/ipr/>.

© UIT 2011

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

## ÍNDICE

	<b>Página</b>
1 Alcance .....	1
2 Referencias .....	1
3 Definiciones.....	1
3.1    Términos definidos en otros sitios.....	1
3.2    Términos definidos en esta Recomendación .....	1
4 Abreviaturas y acrónimos .....	2
5 Convenios .....	3
6 Métodos técnicos para combatir el correo basura en multimedios IP .....	4
6.1    Método de análisis de la fuente .....	5
6.2    Método de análisis de las características .....	5
6.3    Método de análisis del contenido .....	7
7 Marco para la lucha contra el correo basura en multimedios IP.....	7
7.1    Generador de correo basura.....	8
7.2    Funciones SAS .....	8
7.3    Funciones RAS .....	12
7.4    Funciones CAS.....	14
7.5    Funciones SR.....	18
7.6    Puntos de referencia en el marco.....	21
Apéndice I – Lucha contra el correo basura creando numerosas dificultades para su transmisión.....	22
Apéndice II – Consideraciones relativas a la seguridad y de orden práctico para utilizar el marco .....	23
II.1    Consideraciones relativas a la seguridad.....	23
II.2    Consideraciones de orden práctico.....	24
Bibliografía .....	26



## Recomendación UIT-T X.1245

### Marco para la lucha contra el correo basura en aplicaciones multimedios IP

#### 1 Alcance

La presente Recomendación contiene el marco general para combatir el correo basura en las aplicaciones multimedios IP. Dicho marco puede aplicarse a las aplicaciones multimedios IP tales como la telefonía IP, la mensajería instantánea, las conferencias multimedios, etc., y consta de cuatro funciones de lucha contra el correo basura, a saber, funciones medulares contra el correo basura (*core anti-spam functions*, CASF), funciones de lucha contra el correo basura en el lado receptor (*recipient-side anti-spam functions*, RASF), funciones de lucha contra el correo basura en el lado emisor (*sender-side anti-spam functions*, SASF), y funciones receptoras de correo basura (*spam recipient functions*, SRF). En esta Recomendación se describen las funcionalidades y las interfaces de cada función para combatir el correo basura en multimedios IP. Los medios técnicos para la implementación del marco están fuera del alcance de esta Recomendación.

Antes de adoptar los métodos de lucha contra el correo basura descritos en esta Recomendación debe considerarse la observancia de todas las leyes y reglamentaciones correspondientes.

#### 2 Referencias

Ninguna.

#### 3 Definiciones

##### 3.1 Términos definidos en otros sitios

Esta Recomendación utiliza los siguientes términos definidos en otros textos:

**3.1.1 correo basura (*spam*)** [b-UIT-T X.1240]: El significado de "correo basura" varía según la percepción que se tiene en cada país de la privacidad y de lo que constituye correo basura, visto desde una óptica tecnológica, económica, social y práctica. De hecho, su significado evoluciona y se amplía a medida que se desarrollan nuevas tecnologías y se presentan más posibilidades de utilización indebida de las comunicaciones electrónicas. Si bien no existe una definición universalmente aceptada del correo basura, este término se utiliza comúnmente para describir aquellas comunicaciones electrónicas masivas y no solicitadas, transmitidas a través del correo electrónico o la mensajería móvil, destinadas a promocionar la venta de productos o servicios comerciales.

**3.1.2 generador de correo basura (*spammer*)** [b-UIT-T X.1240]: Entidad o individuo que crea y envía correo basura.

##### 3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

**3.2.1 función de lucha contra el correo basura (*anti-spam function*, ASF):** Función lógica de lucha contra el correo basura en aplicaciones multimedios IP. Las ASF pueden estar ubicadas en elementos de red tales como el servidor apoderado, el servidor de aplicaciones, etc.

**3.2.2 lista negra (*blacklist*):** Lista identificativa de personas o fuentes vinculadas a servicios de comunicación, cuando a las identificaciones de la lista se les deniega el acceso a determinados recursos de comunicación.

**3.2.3 ASF medular (core ASF, CASF):** Una instancia de ASF que identifica y bloquea el correo basura en multimedios IP. Tiene asimismo la capacidad de administrar políticas contra el correo basura y controlar las RASF y SASF.

**3.2.4 correo basura en multimedios IP (IP multimedia spam):** Mensajes o comunicaciones no solicitados a través de aplicaciones de multimedios IP que normalmente tienen las características especiales del correo basura, tales como la transmisión a granel. Distinto del correo basura tradicional por correo electrónico, el correo basura en multimedios IP indica tráfico indeseable en métodos de comunicación por IP, tal como mensajería instantánea o transmisión de voz por IP.

**3.2.5 ASF en el lado receptor (recipient-side ASF, RASF):** Una instancia de ASF que identifica y bloquea el correo basura en multimedios IP enviado a receptores a través de la frontera de la red interna. La RASF puede estar ubicada en los elementos de red en los cuales se envían como último salto solicitudes de comunicación entrante.

**3.2.6 ASF en el lado emisor (sender-side ASF, SASF):** Una instancia de ASF que identifica y bloquea el correo basura en multimedios IP enviado por los generadores de correo basura a la frontera de la red interna. La RASF puede estar ubicada en los elementos de red en los cuales se envían como último salto solicitudes de comunicación saliente.

**3.2.7 receptor de correo basura (spam recipient):** Entidad o persona que recibe correo basura.

**3.2.8 función receptora de correo basura (spam recipient function, SRF):** Una ASF cuya función es identificar y bloquear el correo basura multimedios IP que le llega a los receptores de dicho correo. La SRF puede estar ubicada en el terminal o la red residencial de los receptores de correo basura.

**3.2.9 lista blanca (whitelist):** Lista identificativa de personas o fuentes vinculadas a servicios de comunicaciones, cuando las identificaciones de la lista son conocidas, fiables o explícitamente autorizadas.

## 4 Abreviaturas y acrónimos

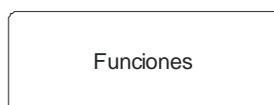
En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

ARS	Sistema de respuesta automatizado ( <i>automated response system</i> )
ASF	Funciones de lucha contra el correo basura ( <i>anti-spam functions</i> )
CA	Autoridad de certificación ( <i>certification authority</i> )
CAS	Lucha medular contra el correo basura ( <i>core anti-spam</i> )
CASF	Funciones de lucha medular contra el correo basura ( <i>core anti-spam functions</i> )
CRL	Lista de revocaciones de certificados ( <i>certificate revocation list</i> )
DAC	Control de acceso discrecional ( <i>discretionary access control</i> )
HBAC	Control de acceso basado en la historia ( <i>history-based access control</i> )
IM	Mensajería instantánea ( <i>instant messaging</i> )
IP	Protocolo Internet ( <i>Internet protocol</i> )
IPSec	Seguridad del protocolo Internet ( <i>Internet protocol security</i> )
L2TP	Protocolo de tunelización de la capa 2 ( <i>layer 2 tunneling protocol</i> )
MAC	Control de acceso obligatorio ( <i>mandatory access control</i> )
MTA	Agente de transferencia de mensajes ( <i>mail transfer agent</i> )

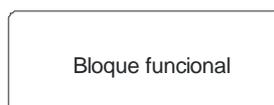
NDAC	Control de acceso no discrecional ( <i>non-discretionary access control</i> )
OTP	Contraseña para una sola vez ( <i>one time password</i> )
PBAC	Control de acceso basado en la finalidad ( <i>purpose-based access control</i> )
PKI	Infraestructura de clave pública ( <i>public key infrastructure</i> )
RAS	Lucha contra el correo basura en el lado receptor ( <i>recipient-side anti-spam</i> )
RASF	Funciones de lucha contra el correo basura en el lado receptor ( <i>recipient-side anti-spam functions</i> )
RBAC	Control de acceso basado en las funciones ( <i>role-based access control</i> )
RuBAC	Control de acceso basado en la reglas ( <i>rule-based access control</i> )
SAS	Lucha contra el correo basura en el lado emisor ( <i>sender-side anti-spam</i> )
SASF	Funciones de lucha contra el correo basura en el lado emisor ( <i>sender-side anti-spam functions</i> )
SPF	Convenio de remitentes ( <i>sender policy framework</i> )
SR	Receptor de correo basura ( <i>spam recipient</i> )
SRF	Funciones de receptor de correo basura ( <i>spam recipient functions</i> )
SSL	Capa de zócalo segura ( <i>secure socket layer</i> )
TCAC	Control de acceso con limitaciones temporales ( <i>temporal constraints access control</i> )
TTP	Tercera parte fiable ( <i>trusted third party</i> )
TTS	Síntesis de la voz a partir del texto ( <i>text to speech</i> )
VoIP	Protocolo de transmisión de la voz por Internet ( <i>voice over Internet protocol</i> )
VPN	Red privada virtual ( <i>virtual private network</i> )

## 5 Convenios

**Funciones:** En el marco de la lucha contra el correo basura multimedios IP, se entiende por "funciones" una compilación de funcionalidades, que se representa con el siguiente símbolo:



**Bloque funcional:** En el marco de la lucha contra el correo basura multimedios IP, se entiende por "bloque funcional" un grupo de funcionalidades que no se ha seguido subdividiendo hasta el nivel de detalle descrito en esta Recomendación, y se representa con el siguiente símbolo:

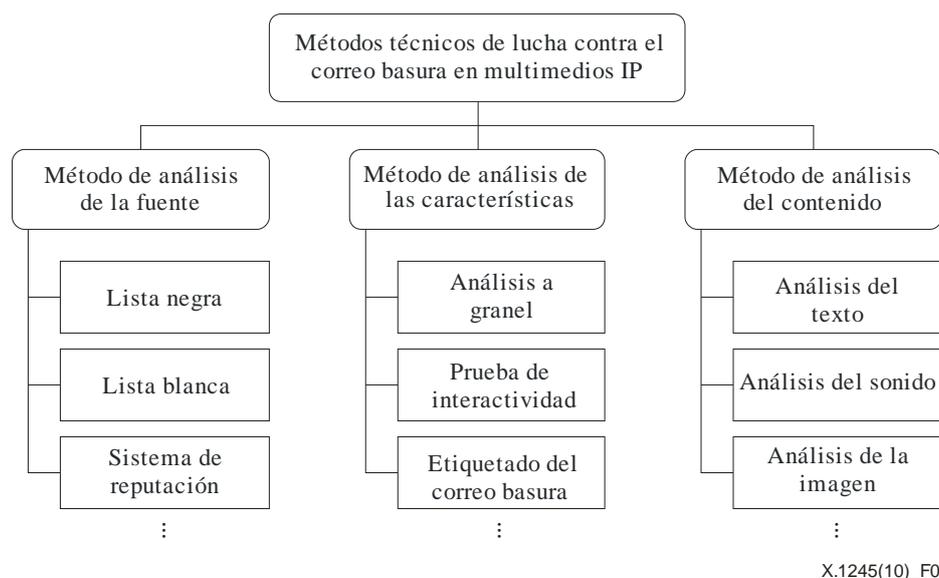


## 6 Métodos técnicos para combatir el correo basura en multimedios IP

El correo basura en multimedios IP puede definirse como la transmisión de mensajes o comunicaciones no solicitados a través de aplicaciones multimedios IP. La diferencia entre el correo basura en multimedios IP y el correo basura electrónico tradicional es que el primero indica correo indeseable en métodos de comunicaciones basados en IP, como la transmisión de voz por IP, la mensajería instantánea, etc. Por lo general el correo basura en multimedios IP tiene ciertas características especiales que lo distinguen de las aplicaciones multimedios IP normales, las cuales pueden utilizarse para desempeñar funciones de lucha como la identificación y el filtrado del correo basura, implementando esas funciones en los elementos de red IP adecuados. Los métodos técnicos para luchar contra el correo basura en multimedios IP pueden clasificarse en las tres categorías siguientes:

- lucha contra el correo basura en multimedios IP mediante análisis de la fuente de las aplicaciones multimedios IP;
- lucha contra el correo basura en multimedios IP mediante análisis de las características de las aplicaciones multimedios IP;
- lucha contra el correo basura en multimedios IP mediante análisis del contenido de las aplicaciones multimedios IP.

En la figura 1 se ilustran estos tres métodos técnicos y se brindan ejemplos de técnicas de lucha contra el correo basura.



**Figura 1 – Métodos técnicos de lucha contra el correo basura en multimedios IP**

Muchas de las técnicas indicadas en la figura 1 ya han sido aplicadas para combatir el correo electrónico basura y también se pueden aplicar al correo basura en multimedios IP. Las técnicas de lucha contra el correo basura en multimedios IP no están limitadas a esos ejemplos.

En una red IP, las funciones de lucha contra el correo basura deben interactuar entre sí para poder utilizar dichas técnicas. En los párrafos siguientes se describen las funciones e interfaces de las entidades de lucha contra el correo basura necesarias para aplicar esos métodos. La utilización de una sola técnica podría no bastar para combatir eficazmente el correo basura en multimedios IP. En tal caso, será preciso aplicar simultáneamente más de una técnica en la red IP para filtrar dicho correo con mayor eficacia.

## **6.1 Método de análisis de la fuente**

Es posible determinar si una aplicación multimedios IP procedente de cierta fuente es o no correo basura mediante el análisis de la información sobre la fuente de dicha aplicación, como por ejemplo la información sobre la reputación o la historia de la fuente en materia de correo basura. Se pueden utilizar como identificadores de la fuente la dirección IP, el nombre de dominio, el número de teléfono y el identificador de usuario.

Cabe citar como ejemplos de técnicas de lucha contra el correo basura basadas en la fuente a las listas blanca y negra, el sistema de reputación, etc., que han sido utilizadas de manera generalizada para el correo electrónico basura y también se pueden aplicar al correo basura en multimedios IP. En [b-UIT-T X.1244] se describe la aplicabilidad de esas técnicas al correo basura en multimedios IP. No obstante, los métodos de análisis de la fuente pueden padecer de ciertas deficiencias que reducen la eficacia de las técnicas; por ejemplo los generadores de correo basura pueden intentar la usurpación de remitente o lograr abrir muchas cuentas de servicio. Así pues, para que las técnicas de lucha contra el correo basura en multimedios IP sean más eficaces, deben tomarse las siguientes medidas:

- sólida autenticación de las fuentes de las aplicaciones multimedios IP;
- gestión eficaz de la política de identificación de correo basura y de la información conexas.

En primer lugar, para que el filtrado del correo basura sea eficaz, es necesario que la información de la fuente de las aplicaciones multimedios IP sea muy fiable, pues los generadores de correo indeseable pueden intentar una desviación para eludir esas técnicas, creando un gran número de cuentas de servicio o mediante la usurpación de la identidad del remitente para encubrir el hecho de que el emisor es un generador de correo indeseable. Por consiguiente, la firme autenticación de las fuentes de la aplicación multimedios IP puede ayudar a conferirle una elevada fiabilidad a la información sobre la fuente.

Según se indicó anteriormente, la información sobre filtrado de correo basura (es decir, lista blanca, lista negra, etc.), así como las fuentes de las aplicaciones multimedios IP, se utilizan para identificar el correo basura. Por lo tanto, la información sobre el filtrado y los criterios para la identificación del correo indeseable deben administrarse con eficacia.

Esta técnica presenta la ventaja de que permite bloquear el correo basura antes de que éste llegue al receptor. Además, suponiendo que se satisfagan las consideraciones anteriores, es posible contrarrestar eficazmente el correo indeseable con un esfuerzo relativamente reducido en comparación con otras técnicas similares, como el análisis del contenido o de las características.

## **6.2 Método de análisis de las características**

### **6.2.1 Métodos de lucha contra el correo basura basados en el análisis de las características**

El correo basura multimedios IP posee varias características especiales que permiten distinguirlo del normal. Por ejemplo, éste a veces se envía a granel, es decir en grandes cantidades, y tiene una interactividad limitada en comparación con las aplicaciones multimedios IP normales. Cuando una aplicación multimedios IP tiene una o más de esas características, se puede filtrar y excluir como correo basura. A continuación se indican algunas de esas características, aunque la lista no es exhaustiva:

- Transmisión a granel

A veces el correo basura multimedios IP se envía a granel, pues normalmente los generadores de ese correo tratan de enviarlo a un gran número de receptores por vez, con miras a minimizar los costes. Cuando se envía desde una fuente a múltiples destinos una gran cantidad de aplicaciones multimedios IP en un breve período de tiempo, cabe sospechar que se trata de correo basura.

#### – Interactividad limitada

En muchos casos el correo basura multimedios IP sólo tiene una interactividad limitada, dado que los generadores de este correo tienden a enviarlo utilizando máquinas, en vez de personas, para reducir los costos. Cuando se trata, por ejemplo, de un correo basura de mensajería instantánea o de conversación, los generadores pueden no responder, dado que el mensaje indeseable ha sido enviado por máquinas. El correo indeseable VoIP, que es una forma de telecomercialización, también puede tener una interactividad limitada cuando se envía utilizando ARS. Así pues, es posible identificar al correo basura comprobando si el emisor de la aplicación proporciona interactividad o no lo hace. Las técnicas de lucha contra el correo basura más comunes basadas en este método en un sistema de correo-e son la prueba Turing y el listado gris ("*greylisting*"), que ponen a prueba la interactividad del remitente y el MTA respectivamente.

### **6.2.2 Uso de la información del protocolo para combatir el correo basura**

Para identificar el correo basura con el método de análisis de las características, resulta más eficaz usar la información del protocolo que la información sobre el contenido. La parte de protocolo de una aplicación multimedios IP puede utilizarse para identificar el correo indeseable mediante el análisis de la fuente de una aplicación multimedios IP. La identificación del correo basura utilizando la información de protocolo antes de que el contenido de las aplicaciones multimedios basadas en IP se entreguen al receptor requiere menos esfuerzo y es más eficaz en comparación con otras técnicas para contrarrestar el correo basura que se sirven de la información del contenido. Los resultados que figuran a continuación hacen más viable esta conclusión.

#### – Información sobre suministro de aplicación

La parte de protocolo de las aplicaciones multimedios IP contiene información relacionada con el suministro de aplicaciones multimedios IP, como por ejemplo fuente, destino, tiempo de entrega, protocolo de entrega utilizado, etc. Algunas de estas partes de protocolo pueden utilizarse para identificar el correo basura.

#### – Sincronización del análisis

La información de protocolo para la iniciación del servicio se proporciona antes que el contenido de las aplicaciones multimedios IP. En el servicio VoIP, por ejemplo, el proceso de señalización durante el cual se utiliza la información de protocolo es ejecutado antes de iniciar la sesión de llamada. Por lo tanto, es posible identificar el correo basura antes de que éste llegue al receptor, gracias al análisis de la información de protocolo.

#### – Encriptación

En general los mensajes de protocolo se envían sin encriptación, aunque el contenido de las aplicaciones multimedios IP puede entregarse con encriptación. Cuando los paquetes IP están encriptados resulta muy difícil o imposible decriptarlos. Por lo tanto, puede ser más fácil analizar la parte de protocolo que la parte de contenido de las aplicaciones multimedios IP.

#### – Tipo de medio

La parte de protocolo de las aplicaciones multimedios IP utiliza únicamente un tipo de medio, aunque a veces la parte de contenido se encuentra en forma de multimedios difíciles de analizar.

#### – Trayecto de entrega

Los mensajes de protocolo para la iniciación de la sesión o el servicio pasan a través del equipo de red; por ejemplo el servidor de aplicación para la mensajería instantánea y los servidores apoderados para las comunicaciones VoIP, que pueden obtener información de aprovisionamiento de las aplicaciones multimedios IP a partir de los mensajes de protocolo. Por otro lado, los mensajes de contenido pueden ir directamente del emisor al receptor sin pasar a través de esos equipos de red. En este último caso, puede resultar difícil analizar el contenido de las aplicaciones multimedios IP.

### **6.3 Método de análisis del contenido**

Conforme a este método, el resultado del análisis del contenido de las aplicaciones multimedios IP se utiliza para identificar el correo basura. Este método ha sido utilizado ampliamente para contrarrestar el correo electrónico basura. El análisis del contenido de las aplicaciones multimedios IP puede ser mucho más difícil que el de los mensajes electrónicos, dado que las primeras pueden ser aplicaciones en tiempo real y/o utilizar multimedios, mientras que los últimos generalmente están basados en textos y no son en tiempo real. Las consideraciones que figuran a continuación facilitan la lucha eficaz contra el correo basura en multimedios IP aplicando el método de análisis del contenido.

#### – Duración temporal del análisis del contenido

El contenido debe analizarse dentro de un lapso de tiempo razonable para que los usuarios de aplicaciones multimedios IP puedan identificar el correo basura. Cuando se trata de aplicaciones multimedios IP en tiempo real, puede resultar imposible realizar el análisis del de contenido antes de iniciar la aplicación.

#### – Exactitud del análisis del contenido

Para identificar efectivamente el correo basura, el resultado del análisis de contenido de las aplicaciones multimedios IP debe tener cierto nivel de calidad. En este sentido, será útil emplear tecnologías avanzadas de reconocimiento de sonido e imagen, dado que el análisis del contenido de los multimedios puede resultar muy difícil en comparación con el análisis de textos.

#### – Encriptación del contenido

Cuando los paquetes están encriptados, el análisis del contenido de las aplicaciones multimedios IP puede resultar muy difícil o imposible de decriptar.

#### – Trayecto de entrega del contenido

El contenido de las aplicaciones multimedios IP se analiza cuando pasa a través de ciertos equipos de red tales como un servidor de aplicación o un servidor de medios que posee la función de análisis de contenido.

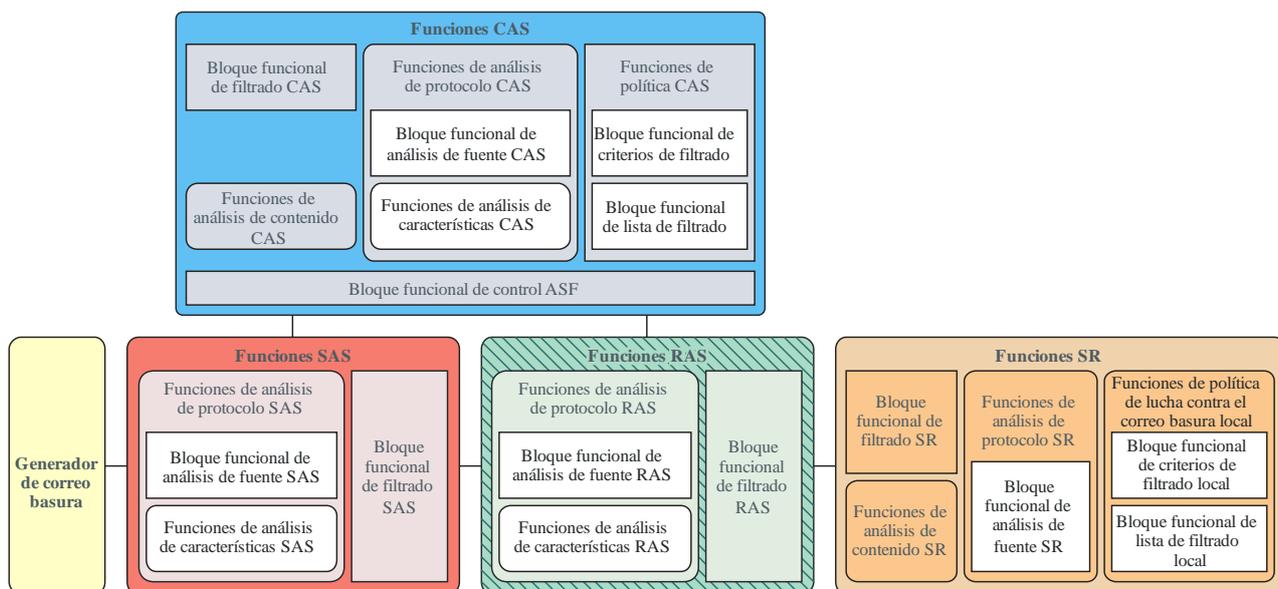
En muchos casos las aplicaciones multimedios IP podrían no satisfacer los criterios requeridos. Cuando se trata de aplicaciones multimedios IP en tiempo real, como el VoIP, parecería imposible detectar y filtrar el correo basura mediante análisis del contenido dentro de un plazo de tiempo tolerable para los usuarios del servicio, dado que sólo se puede analizar el contenido después de haber establecido la sesión de comunicación entre la parte llamante y la parte llamada. Por otro lado, cuando se trata de aplicaciones multimedios IP que no son en tiempo real, como los mensajes vocales registrados, podría haber tiempo suficiente para analizar el contenido. No obstante, podría resultar difícil obtener con dicho análisis suficiente información como para identificar al correo basura, a causa del carácter prematuro de las tecnologías de reconocimiento de voz e imagen o la insuficiente cantidad de contenido. Cuando se analiza el contenido de aplicaciones multimedios IP basadas en textos, tales como los servicios IM y los servicios de mensajes de textos, la identificación del correo basura también puede resultar difícil si el contenido está encriptado o ha pasado directamente entre usuarios del servicio sin pasar a través de los equipos de red adecuados para proceder al análisis del contenido.

## **7 Marco para la lucha contra el correo basura en multimedios IP**

Las entidades de red IP que desempeñan funciones de lucha contra el correo basura deben interactuar entre sí para combatir dicho correo en multimedios IP. En este párrafo se describen las funciones e interacciones que deben realizar las entidades de lucha contra el correo indeseable para implementar los métodos pertinentes. La aplicación de uno solo de esos métodos podría no bastar,

de modo que tal vez sea preciso aplicar más de una técnica simultáneamente en la red IP para un filtrado más eficaz.

En este párrafo se describe el marco para combatir el correo basura en multimedios IP, y ha sido diseñado de modo que pueda ampliarse para abarcar diversos medios técnicos de lucha contra el correo basura en varias aplicaciones y redes. La finalidad de dicho marco es proteger a los usuarios y las redes contra el correo indeseable en multimedios IP. Dado que el correo basura puede aparecer en cualquier lado, a lo largo de la red debe haber mecanismos de detección y filtrado para diversos tipos de correo basura.



X.1245(10)\_F02

**Figura 2– Marco para la lucha contra el correo basura en multimedios IP**

El marco para la lucha contra el correo basura en multimedios IP consta de cinco elementos, tal como se ilustra en la figura 2. En los párrafos que figuran a continuación se describen las funciones e interfaces de cada elemento.

### 7.1 Generador de correo basura

El generador de correo basura crea y propaga dicho correo a lo largo de la red. Es su originador y no implementa las funciones de lucha contra el correo basura.

### 7.2 Funciones SAS

Las SASF (funciones de lucha contra el correo basura en el lado emisor) son un grupo de funciones destinadas a identificar y bloquear el correo basura en multimedios IP. Las SASF pueden implementarse en elementos de red tales como el servidor apoderado, donde se envían como último salto las solicitudes de comunicación salientes de los generadores de correo indeseable. Las SASF interactúan con las CASF (funciones medulares de lucha contra el correo basura). Resulta más eficaz bloquear el correo indeseable del lado de la fuente antes de que éste se propague a lo largo de la red, aunque las SASF podrían desempeñar un papel menos activo que otros componentes en el entorno de comunicaciones real.

Las SASF están compuestas de las funciones de análisis del protocolo SAS y del bloque funcional de filtrado SAS para controlar el filtrado del correo basura. En los párrafos siguientes se describen diversas técnicas que puede adoptar la SASF para contrarrestar el correo indeseable en multimedios IP.

### 7.2.1 Bloque funcional de filtrado SAS

El bloque funcional de filtrado SAS determina si la aplicación multimedia IP analizada es o no correo basura, sobre la base del resultado del análisis de las funciones de análisis de protocolo SAS y la política de lucha contra el correo basura. Por lo tanto, este bloque interactúa con la CASF y otras funciones o bloques funcionales en las SASF.

### 7.2.2 Funciones de análisis de protocolo SAS

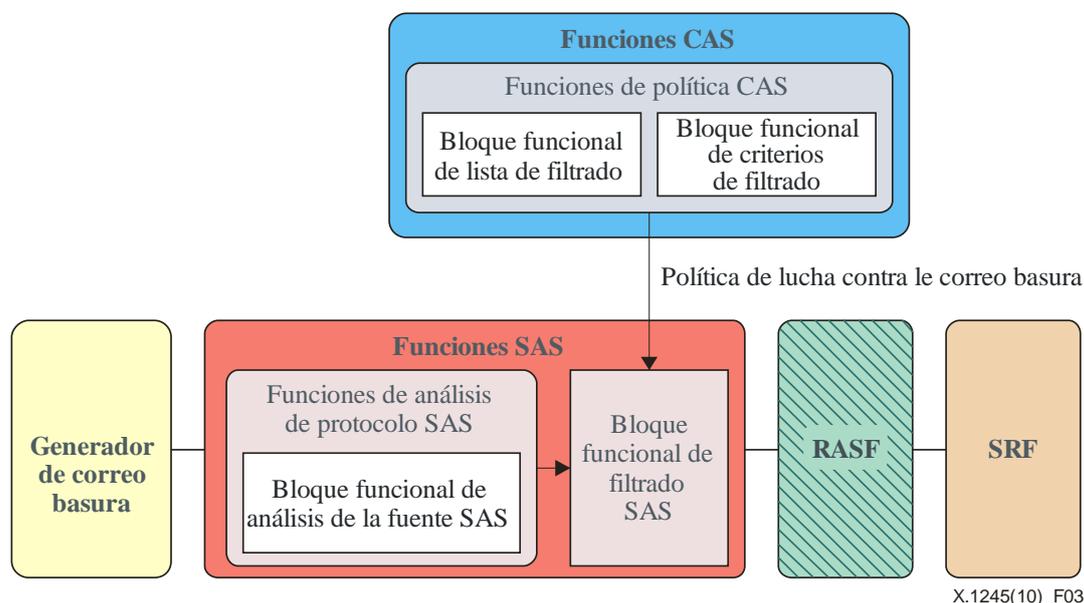
Las funciones de análisis de protocolo SAS analizan la información de protocolo de las aplicaciones multimedia IP recibidas. Están compuestas del bloque funcional de análisis de fuente SAS y de las funciones de análisis de las características SAS, que analizan la información de la fuente y las características de las aplicaciones multimedia IP recibidas, respectivamente.

#### i) Bloque funcional de análisis de la fuente SAS

Las SASF pueden hacer una distinción entre el correo basura en multimedia IP y las aplicaciones multimedia IP normales sobre la base de la información de la fuente de las aplicaciones multimedia IP. Las SASF tienen dos aspectos relacionados con las aplicaciones multimedia IP: uno es el filtrado de la fuente con la política para combatir el correo basura y el otro es la autenticación del remitente.

#### – Política para combatir el correo basura

Las SASF pueden identificar y filtrar el correo basura utilizando la dirección de la fuente del paquete de datos multimedia IP. El filtrado no sólo se efectúa con la dirección de la fuente, sino también con otra información de protocolo disponible. En la figura 3 se ilustran las funciones de lucha contra el correo basura y las interacciones entre las funciones destinadas a combatir el correo indeseable en multimedia IP mediante el análisis de la fuente en la SASF.

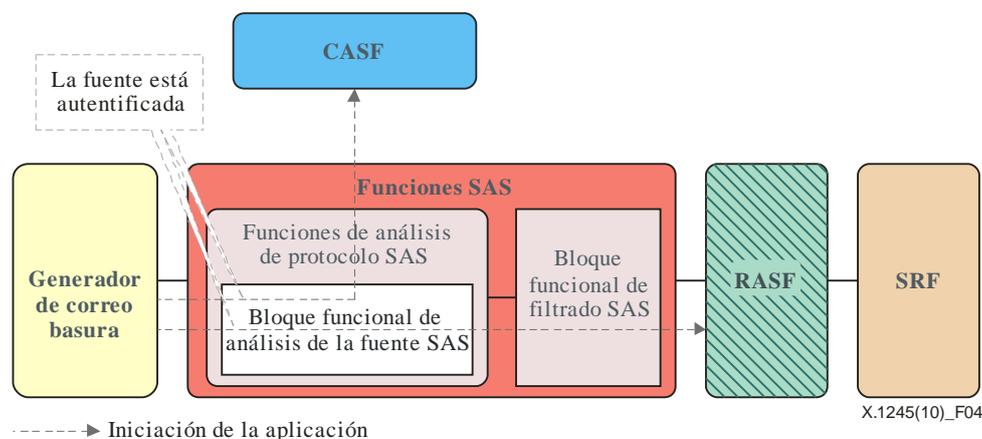


**Figura 3 – Lucha contra el correo basura en multimedia IP mediante el análisis de la fuente en las SASF**

El bloque funcional de filtrado SAS puede obtener la política de lucha contra el correo basura de las funciones de política CAS. El bloque funcional de filtrado SAS filtra el paquete IP enviado por el generador cuando dicho paquete es identificado como correo indeseable sobre la base del resultado del análisis.

– Autenticación del remitente

La SASF tiene la información de autenticación de los remitentes y puede proporcionar autenticación de usuario para el tráfico originado. Cuando sea necesario, las SASF pueden impedir que entidades no autorizadas utilicen las aplicaciones multimedios IP.



**Figura 4 – Autenticación de la fuente por las SASF**

En la figura 4 se ilustra el esquema de la autenticación de la fuente por la SASF. La capacidad de análisis de la fuente de la SASF tiene una funcionalidad de autenticación que puede autenticar el tráfico del generador de correo basura antes de que éste sea enviado a la CASF o la RASF (funciones de lucha contra el correo basura en el lado receptor). En caso necesario, la SASF puede descartar el tráfico que no pasó la autenticación y enviar a otras ASF únicamente el tráfico autenticado. El rechazo del tráfico no autorizado puede resultar útil para frustrar a los generadores de correo basura que intentan usurpar identidades.

– Procedimiento de filtrado

El procedimiento a tenor del cual la SAFS filtra el correo basura en multimedios IP mediante el análisis de la fuente puede describirse como sigue:

- 1) Entrega de la política de lucha contra el correo basura: La SASF recibe de la CASF la política de lucha contra el correo basura, que se le puede entregar como una notificación o bajo la forma de una solicitud/respuesta.
- 2) Recepción de aplicaciones multimedios IP: La SASF recibe una iniciación de aplicaciones multimedios IP.
- 3) Autenticación de la fuente: La SASF autentifica la fuente de las aplicaciones. Si el proceso de autenticación falla, la SASF rechaza la solicitud de autenticación del generador de correo basura.
- 4) Identificación y filtrado del correo basura: La SASF toma una decisión sobre la aplicación multimedios IP recibida sobre la base de la política de lucha contra el correo basura recibida de la CASF y la fuente de la solicitud. La SASF puede rechazar o ignorar el tráfico que haya sido determinado como correo basura en multimedios IP.

ii) Funciones de análisis de características SAS

La SASF puede identificar al correo basura utilizando las características de las aplicaciones, como por ejemplo el carácter a granel. La SASF puede utilizar un umbral para determinar el volumen, y entre sus funciones de análisis de características puede contar con varios bloques funcionales de análisis de características específicas. La funcionalidad y la interfaz de cada bloque funcional es un medio técnico específico para combatir el correo basura en multimedios IP; su estudio está fuera del

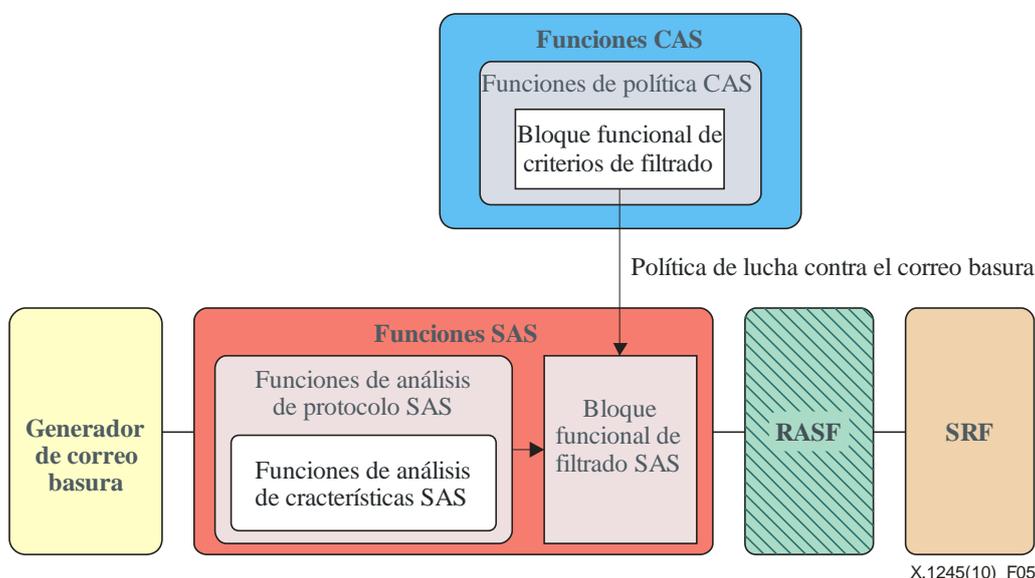
alcance de esta Recomendación. A continuación figuran algunos ejemplos de las características que puede distinguir la SASF para aplicar el método de lucha contra el correo indeseable.

- Transmisión a granel

Las funciones de análisis de características SAS pueden tener capacidad para analizar la cantidad de solicitudes de servicio desde una sola fuente y analizar la tasa de solicitud de servicio. El bloque funcional de filtrado SAS identifica el correo basura en multimedios IP sobre la base del resultado del análisis de las funciones de análisis de características SAS y la política de lucha contra el correo indeseable recibida del bloque funcional de los criterios de filtrado CAS.

- Interactividad limitada

La SASF puede tener capacidad de someter a prueba la interactividad del generador de correo basura, aunque por lo general la CASF se encarga de probar la interactividad de la fuente de las aplicaciones multimedios IP. Los generadores de correo indeseable tienden a emplear máquinas, que cuestan relativamente menos que los recursos humanos, para iniciar dichas aplicaciones. Por consiguiente, verificar si hay interactividad es una manera de detectar el correo indeseable en multimedios IP.



**Figura 5 – Lucha contra el correo basura en multimedios IP mediante el análisis de las características en la SASF**

El procedimiento mediante el cual la SASF filtra el correo basura en multimedios IP mediante un análisis de las características es el siguiente:

- 1) Entrega de la política de lucha contra el correo basura: El bloque funcional de filtrado SAS recibe de la CASF la política de lucha contra el correo basura tras el análisis de las características, ya sea en forma de una notificación o en forma de solicitud/respuesta.
- 2) Recepción de las aplicaciones multimedios IP: La SASF recibe una iniciación de aplicaciones multimedios IP.
- 3) Análisis de características: Las funciones de análisis de características de la SAS extraen las características relacionadas con el correo basura de las aplicaciones multimedios IP recibidas.
- 4) Procesamiento de los resultados: Los resultados del análisis de las características se envían desde las funciones de análisis de características SAS hasta el bloque funcional de filtrado SAS.

- 5) Filtrado del correo basura: El bloque funcional de filtrado SAS procesa el correo basura de conformidad con la política de lucha contra el mismo. Si el resultado del análisis es correo basura, la SASF puede rechazar o ignorar el tráfico determinado indeseable.

La política de gestión del correo basura en multimedios IP depende de los proveedores y los usuarios del servicio, las aplicaciones multimedios IP, la reglamentación nacional, etc. Así pues, la SASF y la RASF deben interactuar con la CASF para obtener información sobre la política de lucha contra el correo basura sobre la base de las características de una aplicación multimedios IP.

### **7.3 Funciones RAS**

La RASF es un grupo de funciones cuyo objetivo es identificar y bloquear el correo basura en multimedios IP que se quiere enviar al receptor. La RASF puede implementarse en elementos de red tales como el servidor apoderado cuando las solicitudes de comunicación entrante se envían como último salto a los receptores de correo basura. La RASF interactúa con la CASF para ejecutar las funciones de lucha contra el correo indeseable.

La CASF y la RASF pueden implementarse en los mismos equipos de red, que abarcan al mismo tiempo a los generadores y a los receptores del correo indeseable. Sin embargo, las funciones para combatir el correo basura ejecutadas en los equipos son diferentes según el flujo de tráfico. En otras palabras, las funciones de los equipos funcionan como SASF cuando el tráfico procede de usuarios de aplicaciones multimedios IP que abarca el equipo, y como RASF cuando el tráfico se retransmite a dichos usuarios de aplicaciones multimedios IP.

La RASF está compuesta de las funciones de análisis de protocolo RAS y el bloque funcional de filtrado RAS que controla el filtrado.

Aunque es técnicamente posible que la SASF o la RASF analicen el contenido del tráfico cursado para contrarrestar el correo basura, en esta Recomendación, no se consideran las funciones de análisis de contenido pues ello exigiría restricciones de procesamiento adicionales en dichas funciones. Cuando una aplicación multimedios IP no pasa a través de la CASF, la RASF puede entregar la aplicación a la CASF y pedirle que analice el contenido de la misma con el fin de identificar al correo basura.

En los párrafos que figuran a continuación se describen varias técnicas que puede adoptar la RASF para contrarrestar el correo indeseable en aplicaciones multimedios IP.

#### **7.3.1 Bloque funcional de filtrado RAS**

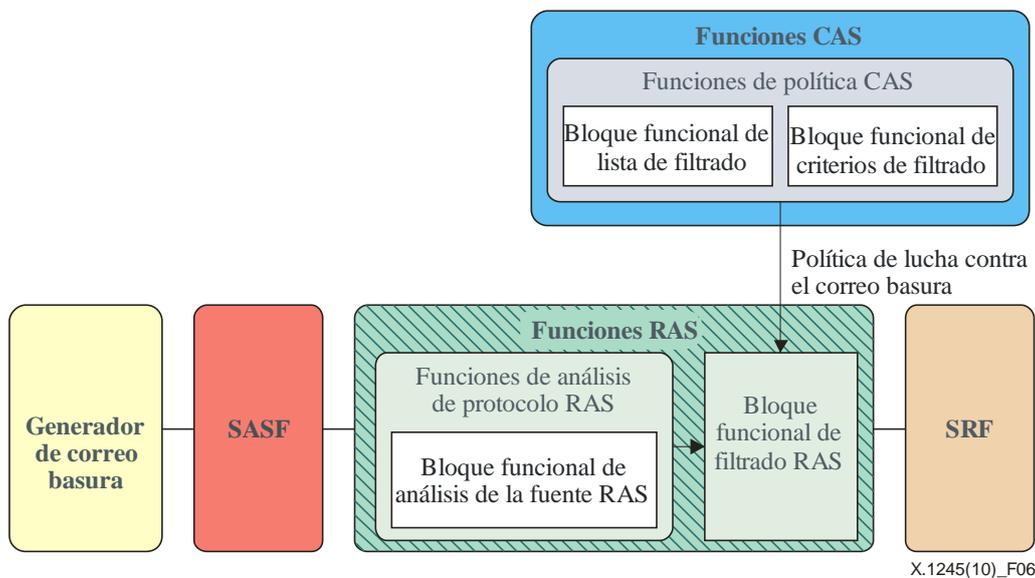
El bloque funcional de filtrado RAS determina si la aplicación multimedios IP analizada es o no indeseable sobre la base del resultado del análisis y la política de lucha contra el correo basura. Por lo tanto, interactúa con la CASF y otras funciones o bloques funcionales de lucha contra el correo basura en la RASF.

#### **7.3.2 Funciones de análisis de protocolo RAS**

Las funciones de análisis de protocolo RAS analizan la información de protocolo de las aplicaciones multimedios IP recibidas. Están compuestas del bloque funcional de análisis de la fuente RAS y de las funciones de análisis de las características RAS, que analizan la información de la fuente y las características de las aplicaciones multimedios IP recibidas, respectivamente.

##### **i) Bloque funcional de análisis de la fuente RAS**

La RASF puede hacer una distinción entre el correo basura y el normal en las aplicaciones multimedios IP, sobre la base de la información de la fuente de dichas aplicaciones. Para identificar el correo indeseable, la RASF caracteriza la política de lucha contra el correo basura en relación con la fuente proporcionada por la CASF, como por ejemplo lista negra, lista blanca, puntuación de reputación, etc. En la figura 6 se ilustran las funciones e interacciones de las funciones para combatir el correo basura en multimedios IP mediante un análisis de la fuente.



**Figura 6 – Lucha contra el correo basura en multimedios IP mediante el análisis de la fuente**

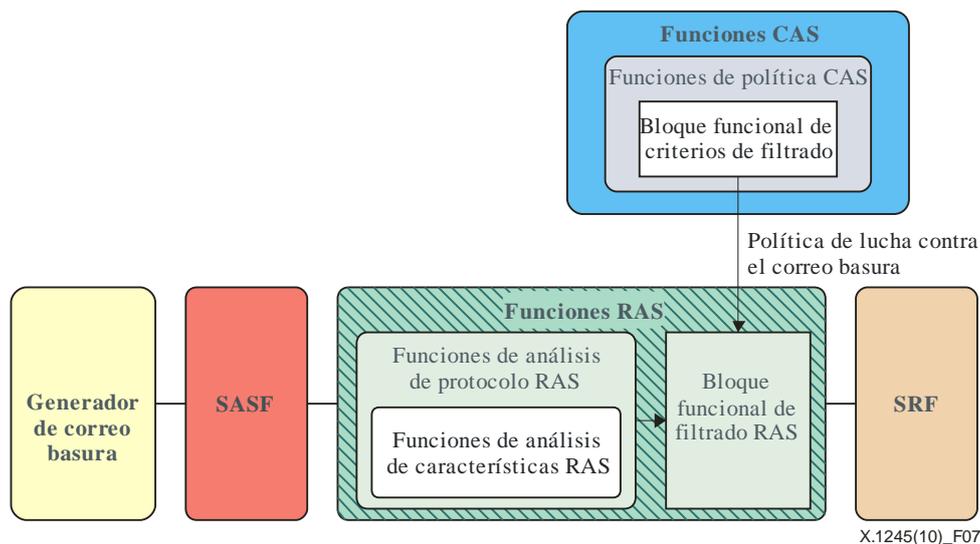
La RASF determina si una aplicación multimedios IP es o no indeseable sobre la base de la información de la fuente de dicha aplicación y la trata de conformidad con el resultado. Dado que para aplicar con eficacia la técnica de combate basada en la fuente se requiere una información de la fuente muy fiable, se supone que la aplicación multimedios IP que la RASF recibe de la SASF es fidedigna, es decir, autenticada. La RASF identifica el correo basura multimedios IP de conformidad con los criterios o la lista de filtrado proporcionados por la CASF. La CASF mantiene los criterios y la lista de filtrado para ayudar a la RASF y a la SASF o facilitarse a sí misma la identificación del correo indeseable. A continuación se describen los procesos de identificación y filtrado del correo basura en la RASF utilizando el método de análisis de la fuente:

- 1) Entrega de la política de lucha contra el correo basura de la CASF: La RASF recibe de la CASF la política de lucha contra el correo basura, ya sea en forma de una notificación o en forma de solicitud/respuesta.
- 2) Recepción de las aplicaciones multimedios IP: La RASF recibe una aplicación multimedios IP y verifica la fuente de dicha aplicación.
- 3) Identificación y filtrado del correo basura: La RASF toma una decisión respecto de la aplicación multimedios IP recibida sobre la base de la información de la fuente y la política de gestión del correo basura recibida en una fase previa. La RASF puede rechazar o ignorar el tráfico que ha sido determinado como indeseable a tenor de la política de lucha contra el correo basura del proveedor de servicio o usuario del servicio.

Cuando la RASF identifica el correo basura sobre la base de las listas negra o blanca, se puede utilizar la lista de filtrado de la CASF. Cuando la RASF identifica al correo basura sobre la base de la puntuación de reputación, se pueden utilizar criterios de filtrado tales como el umbral de puntuación de reputación, a tenor de la cual se determina que la aplicación multimedios IP es indeseable.

#### ii) Funciones de análisis de características RAS

La RASF puede identificar al correo basura utilizando la aplicación multimedios IP para verificar si tiene o no características indeseables. Las funciones de análisis de las características RAS pueden incluir varios bloques funcionales de análisis de características específicas. Los medios técnicos para combatir el correo basura en multimedios IP están fuera de alcance de esta Recomendación.



**Figura 7 – Lucha contra el correo basura en multimedios IP mediante el análisis de las características**

En la figura 7 se ilustran las funciones e interacciones entre las funciones para combatir el correo basura en multimedios IP mediante el análisis de las características en la RASF. El procedimiento a tenor del cual la RASF identifica el correo indeseable mediante el análisis de las características es el siguiente:

- 1) Transferencia de la política de lucha contra el correo basura: El bloque funcional de filtrado RAS recibe de la CASF la política de lucha contra el correo basura tras el análisis de las características, ya sea en forma de una notificación o en forma de solicitud/respuesta.
- 2) Recepción de las aplicaciones multimedios IP: La SASF recibe una iniciación de aplicaciones multimedios IP.
- 3) Análisis de características: Las funciones de análisis de características de la RAS extraen las características relacionadas con el correo basura de las aplicaciones multimedios IP recibidas.
- 4) Procesamiento de los resultados: Las funciones de análisis de las características RAS proporcionan el resultado del análisis al bloque funcional de filtrado SAS.
- 5) Filtrado del correo basura: El bloque funcional de filtrado RAS procesa el correo basura de conformidad con la política de lucha contra el mismo. Si el resultado del análisis es correo basura, la RASF puede rechazar o ignorar el tráfico determinado indeseable.

## 7.4 Funciones CAS

La CASF tiene capacidades para gestionar las políticas de lucha contra el correo basura y controlar a la RASF y la SASF. Tiene asimismo capacidades para analizar la fuente o las características de las aplicaciones multimedios IP con miras a identificar y filtrar el correo indeseable cuando hay un trayecto de paquetes IP entre los generadores y los receptores de dicho correo al proporcionar aplicaciones multimedios IP de conformidad con el tipo de aplicación. La CASF tiene funciones de análisis de protocolo y de contenido CAS, bloques funcionales de filtrado CAS, funciones de política de lucha contra el correo basura y bloques funcionales de control ASF. En este párrafo se describen las funcionalidades e interacciones de cada entidad en la CASF con miras a contrarrestar el correo basura en multimedios IP.

### 7.4.1 Bloque funcional de filtrado CAS

El bloque funcional de filtrado CAS determina si la aplicación multimedios IP analizada es o no indeseable sobre la base del resultado del análisis y la política de lucha contra el correo basura. Por

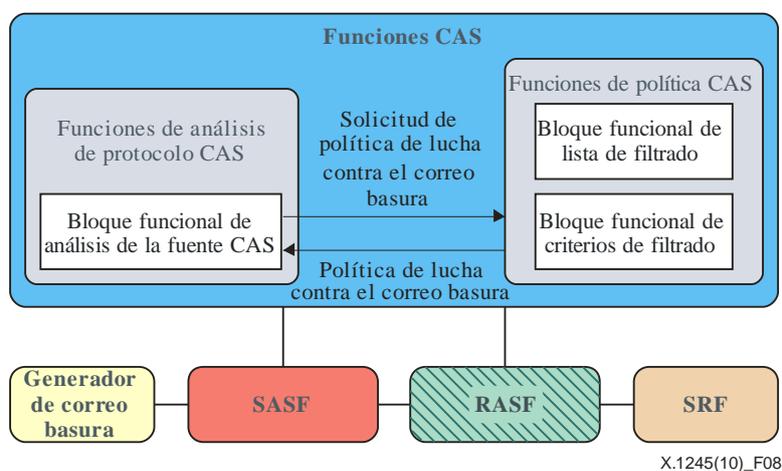
lo tanto, interactúa con otras funciones o bloques funcionales de lucha contra el correo basura en la CASF.

#### 7.4.2 Funciones de análisis de protocolo CAS

Las funciones de análisis de protocolo CAS analizan la información de protocolo de las aplicaciones multimedios IP recibidas. Están compuestas del bloque funcional de análisis de la fuente CAS y de las funciones de análisis de las características CAS, que analizan la información de la fuente y las características de las aplicaciones multimedios IP recibidas, respectivamente.

##### i) Bloque funcional de análisis de la fuente CAS

Cuando se proporciona una aplicación multimedios IP bajo el control del componente de red en el cual reside la CASF, por ejemplo la inscripción de un usuario en un servicio de mensajería instantánea, o en un servicio VoIP bajo el control de los servidores de la aplicación, la CASF puede ser una posible entidad funcional para identificar al correo basura mediante el análisis de la fuente. En la figura 8 se ilustran las funciones e interacciones entre las funciones para combatir el correo basura en multimedios IP mediante un análisis de la fuente en la CASF.



**Figura 8 – Lucha contra el correo basura en multimedios IP mediante el análisis de la fuente**

A continuación se describe un posible procedimiento para luchar contra el correo basura en multimedios IP basado en la información de la fuente de una aplicación en la CASF:

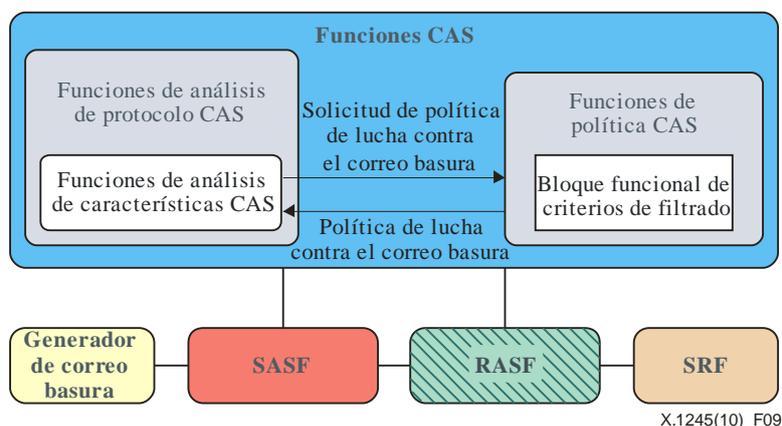
- 1) Autenticación: Un usuario desea usar una aplicación multimedios IP (por ejemplo, el servicio de mensajería instantánea) y dicho usuario es autenticado por un componente de red tal como un servidor de aplicación que tiene la CASF.
- 2) Recepción de aplicaciones multimedios IP: El usuario envía a la CASF una solicitud de entrega de mensaje IP, y el bloque funcional de análisis de la fuente CAS verifica la fuente del usuario.
- 3) Obtención de la política de lucha contra el correo basura: El bloque funcional de análisis de la fuente CAS solicita la política de lucha contra el correo basura y la recibe de las funciones de política CAS.
- 4) Identificación y filtrado del correo basura: La CASF toma una decisión respecto de la aplicación multimedios IP recibida sobre la base de la información de la fuente y la política de lucha contra el correo indeseable recibida en las etapas anteriores. La CASF puede rechazar o ignorar el tráfico determinado como indeseable en multimedios IP y en ese caso se trata adecuadamente de conformidad con la política de lucha contra el correo basura del proveedor del servicio o del usuario del servicio.

## ii) Funciones de análisis de las características CAS

La CASF puede ser un punto de análisis de las características para combatir el correo indeseable cuando se proporciona una aplicación bajo el control de una entidad de la red de la CASF. La CASF analiza una aplicación multimedios IP para determinar si ésta posee o no las características de indeseable y utiliza los criterios de filtrado de la política de lucha contra el correo basura para determinar si es o no indeseable. En la figura 9 se ilustra la arquitectura general y las interfaces aplicando el método de análisis de las características para combatir el correo basura multimedios IP en la CASF.

Las funciones de política CASF tienen el bloque funcional de criterios de filtrado con los criterios de filtrado necesarios para identificar el correo basura en multimedios IP y proporcionan a la SASF o la RASF dichos criterios para ayudarlas en la identificación. Por ejemplo, cuando las funciones de análisis de las características CAS tratan de identificar correo indeseable en una aplicación multimedios IP que se transmite a granel, el bloque funcional de criterios de filtrado CASF puede proporcionar los criterios de cantidad que permiten identificar como indeseable una aplicación por su nivel de cantidad.

En la figura 9 se ilustran las funciones e interacciones entre las funciones de lucha contra el correo basura en multimedios IP mediante el análisis de las características en la CASF.



**Figura 9 – Lucha contra el correo basura en multimedios IP mediante el análisis de las características**

A continuación se describen los procedimientos de análisis de las características para combatir el correo basura en multimedios IP en la CASF.

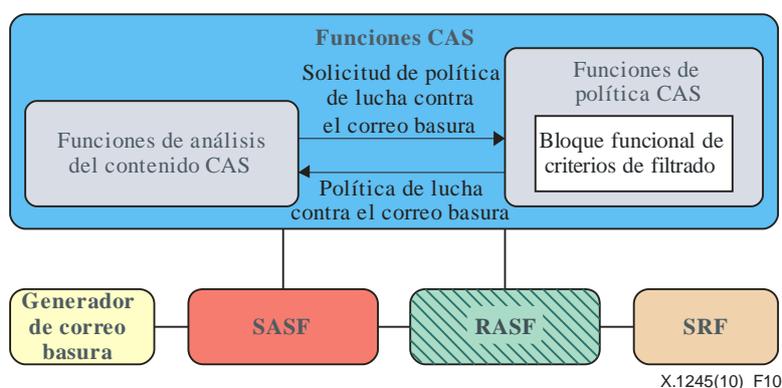
- 1) **Análisis de las características del correo basura:** Cuando se intenta conectar una aplicación multimedios IP bajo el control de una entidad de red a la que pertenece la CASF, esta última analiza si aquélla posee o no características de indeseable, como por ejemplo transmisión a granel, interactividad limitada, etc.
- 2) **Obtención de la política de lucha contra el correo basura:** Las funciones de análisis de las características CAS solicitan a las funciones de política CAS la política de lucha contra el correo basura relacionada con el análisis de las características para filtrar dicho correo. El bloque de política de lucha contra el correo basura envía la información solicitada a las funciones de análisis de características CAS.
- 3) **Identificación y filtrado del correo basura:** Las funciones de análisis de las características CAS determinan si la aplicación multimedios IP es o no indeseable sobre la base del resultado del análisis de las funciones de análisis de las características y la política de lucha contra el correo basura recibida.

### 7.4.3 Funciones de análisis del contenido CAS

La CASF tiene las funciones de análisis del contenido CAS. Estas funciones analizan el contenido de una aplicación multimedia IP para identificar al correo basura cuando dicha aplicación se transmite al receptor por conducto de un equipo de red en el cual reside la CASF, como un servidor de aplicación o un servidor de medios.

Cuando el correo basura se identifica utilizando la información de protocolo de las aplicaciones multimedia IP, como por ejemplo la información de la fuente o las características de correo basura, se pueden encargar de ese análisis las CASF, las SASF o las RASF. Por otro lado, cuando el correo basura se identifica utilizando el análisis del contenido, la CASF, por donde pasa el contenido de aplicaciones multimedia IP, es un punto de entidad funcional razonable para el análisis del contenido cuando se emplean técnicas basadas en el contenido para combatir el correo basura en multimedia IP.

En la figura 10 se ilustran las funciones e interacciones entre las funciones de lucha contra el correo basura en multimedia IP mediante el análisis del contenido en la CASF.



**Figura 10 – Lucha contra el correo basura en multimedia IP mediante el análisis del contenido**

A continuación se describen los procedimientos de análisis de contenido para contrarrestar el correo basura multimedia IP en la CASF.

- 1) Recepción de aplicaciones multimedia IP: El contenido de la aplicación llega a la CASF.
- 2) Análisis del contenido: Las funciones de análisis CAS analizan el contenido de la aplicación IP.
- 3) Obtención de la política de lucha contra el correo basura: La CASF solicita la política de lucha contra el correo basura a las funciones de política CAS y la recibe del bloque funcional de criterios de filtrado.
- 4) Identificación y filtrado del correo basura: La CASF decide si la aplicación multimedia IP es o no indeseable sobre la base del resultado del análisis y de la política de lucha contra el correo basura.

Según se indicó en el párrafo 6, la aplicabilidad del método de análisis del contenido puede verse limitada por las características de la aplicación multimedia IP; por ejemplo si se trata de una aplicación en tiempo real o no, si es o no multimedia, si su contenido está encriptado o no.

### 7.4.4 Funciones de política CAS

Las funciones de política CAS mantienen las políticas de lucha contra el correo basura en multimedia IP y están compuestas del bloque funcional de criterios de filtrado y el bloque funcional de lista de filtrado.

i) **Bloque funcional de criterios de filtrado**

El bloque funcional de criterios de filtrado mantiene los criterios de filtrado para la identificación del correo basura en multimedios IP. Dependiendo de las técnicas utilizadas para combatir el correo basura, hay diversos tipos de criterios de filtrado. Cuando se trata del análisis de transmisiones a granel, por ejemplo, un criterio puede ser la cuantía umbral de aplicaciones multimedios IP que se envía al mismo tiempo desde una fuente. Los mecanismos de creación y gestión de criterios de filtrado están fuera del alcance de la presente Recomendación.

ii) **Bloque funcional de lista de filtrado**

El bloque funcional de lista de filtrado gestiona la lista de filtrado para la identificación del correo basura en multimedios IP sobre la base del análisis de la fuente. Dependiendo de las técnicas aplicadas para combatir el correo basura, puede haber diversos tipos de listas de filtrado, como por ejemplo lista negra, lista blanca, y puntuación de reputación. La lista de filtrado puede ser una lista pública para muchos usuarios de servicio idénticos o una lista personal que se administra de forma individual, o bien una combinación de ambas. Los mecanismos de creación y gestión de listas de filtrado están fuera del alcance de esta Recomendación.

#### **7.4.5 Bloque funcional de control ASF**

El bloque funcional de control ASF interactúa con la SASF y la RASF para ayudarlas a identificar y filtrar el correo basura, y les transmite las políticas de lucha contra dicho correo desde las funciones de política CAS.

### **7.5 Funciones SR**

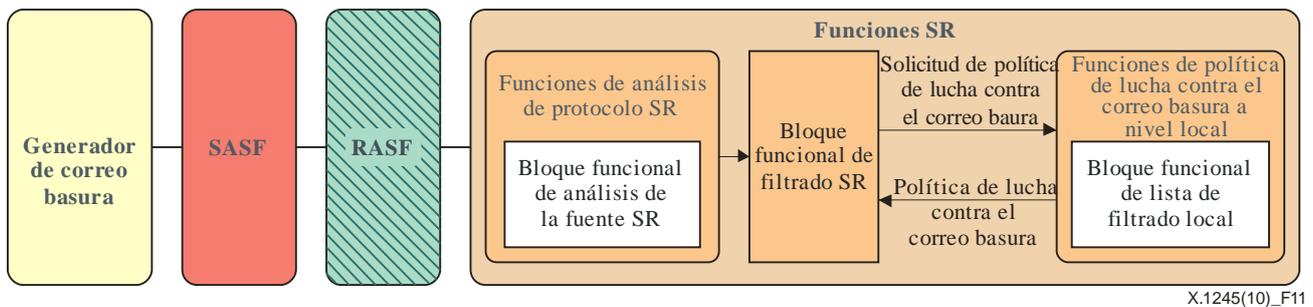
El receptor del correo basura es el punto final del correo indeseable en multimedios IP. Si no se establece ningún mecanismo para contrarrestar el correo basura, éste puede afectar y perjudicar a los usuarios.

El receptor de correo basura tiene funciones SR ("*spam recipient*" – receptor de correo basura) para protegerse a sí mismo contra el correo basura en multimedios IP. Los usuarios pueden establecer la política de lucha contra el correo basura o recibirla de los proveedores de servicio para filtrar el correo indeseable en multimedios IP. Las funciones SR están compuestas de funciones de análisis de protocolo SR, funciones de análisis de contenido SR, bloques funcionales de filtrado SR y funciones de política de lucha contra el correo basura a nivel local. En este párrafo se describen las funcionalidades e interacciones de cada función de lucha contra el correo basura que puede adoptar el receptor para combatir dicho correo.

#### **7.5.1 Funciones de análisis de protocolo SR**

Las funciones de análisis de protocolo SR tienen el bloque funcional de análisis de la fuente SR que permite identificar el correo basura sobre la base de la información del remitente. Aunque es posible filtrar el correo basura en la CASF, la SASF y la RASF, en caso de conexión directa a las aplicaciones multimedios IP se pueden utilizar las funciones y la política de lucha contra el correo basura de la SRF para combatir dicho correo.

El receptor del correo basura puede definir la lista y los criterios de filtrado local, o puede recibir dicha lista de otras funciones de lucha contra el correo basura tales como la CASF. Los mecanismos específicos para definir la política de lucha contra el correo basura están fuera del alcance de esta Recomendación. En la figura 11 se ilustran las funciones e interacciones entre las funciones de lucha contra el correo basura en multimedios IP mediante el análisis de la fuente en la SRF.



**Figura 11 – Lucha contra el correo basura en multimedios IP mediante el análisis de la fuente en el receptor de dicho correo**

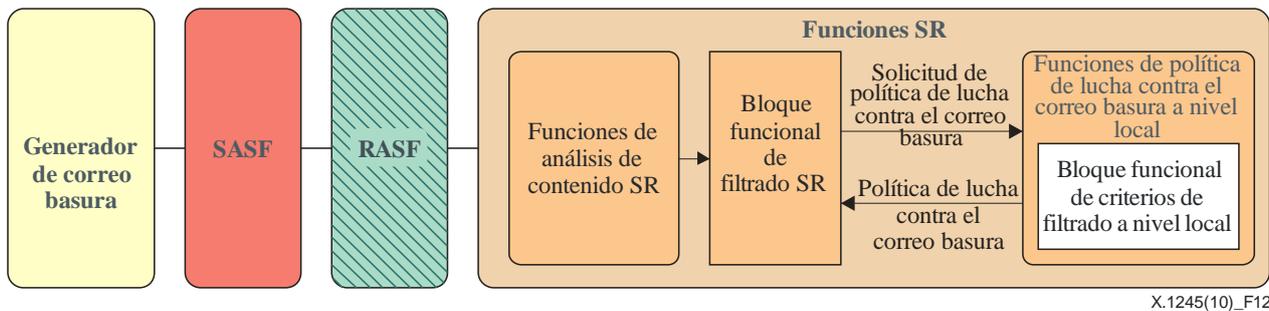
A continuación se describe un posible procedimiento para combatir el correo basura basado en la información de la fuente de la aplicación multimedios IP en el receptor de dicho correo.

- 1) Recepción de aplicaciones multimedios IP: El SRF recibe una iniciación de aplicaciones multimedios IP y verifica la fuente de dicha aplicación.
- 2) Obtención de la política de lucha contra el correo basura: Las funciones de análisis de protocolo SR solicitan la política de lucha contra el correo basura y la reciben de las funciones de política de lucha contra el correo basura a nivel local.
- 3) Identificación y filtrado del correo basura: El bloque funcional de filtrado SR toma una decisión respecto de la aplicación multimedios IP recibida, sobre la base de la política de lucha contra el correo indeseable y el resultado del análisis de la fuente. El receptor del correo basura puede rechazar o ignorar el tráfico determinado como indeseable en multimedios IP.

Desde el punto de vista técnico, las funciones de receptor pueden identificar el correo basura mediante el análisis de las características, pero las funciones de análisis de protocolo SR no tienen el bloque funcional de análisis de características dado que es arriesgado depender del receptor del correo basura para llevar a cabo las funciones complejas de lucha contra dicho correo, como en el método de análisis de las características, porque las funciones de análisis del protocolo SR se encuentran bajo el control de un grupo de usuarios muy variable.

### 7.5.2 Funciones de análisis del contenido SR

El receptor del correo basura puede contrarrestar dicho correo mediante el análisis del contenido. Éste puede mantener su propio mecanismo específico de análisis del contenido, o bien recibirlo de los proveedores de servicio. La política de lucha contra el correo basura basada en el análisis del contenido está ubicada en las funciones de política de lucha contra el correo basura a nivel local, como parte del bloque funcional de los criterios de filtrado a nivel local. En la figura 12 se ilustran las funciones e interacciones entre las funciones de lucha contra el correo basura en multimedios IP mediante el análisis del contenido en la SRF.



**Figura 12 – Lucha contra el correo basura en multimedios IP mediante análisis del contenido en el receptor de dicho correo**

A continuación figura el procedimiento mediante el cual el receptor del correo basura en multimedios IP filtra dicho correo mediante un análisis del contenido.

- 1) Recepción de aplicaciones multimedios IP: El SRF recibe una iniciación de aplicaciones multimedios IP. Las funciones de análisis de contenido SR realizan el análisis del contenido para identificar al correo basura.
- 2) Obtención de la política de lucha contra el correo basura: El resultado del análisis del contenido se envía al bloque funcional de filtrado SR. Este último solicita la política de lucha contra el correo basura a las funciones de política de lucha contra el correo basura a nivel local y recibe dicha política.
- 3) Identificación y filtrado del correo basura: El bloque funcional de filtrado SR toma una decisión respecto de la aplicación multimedios IP recibida, sobre la base de la política de lucha contra el correo indeseable y el resultado del análisis del contenido. El receptor de correo basura puede rechazar o ignorar el tráfico determinado como indeseable en multimedios IP.

### 7.5.3 Bloque funcional de filtrado SR

El bloque funcional de filtrado SR determina si la aplicación multimedios IP analizada es o no indeseable sobre la base del resultado del análisis y de la política de lucha contra el correo basura. Por lo tanto, éste interactúa con otras funciones o bloques funcionales de lucha contra el correo basura en la SRF.

### 7.5.4 Funciones de política de lucha contra el correo basura a nivel local

Las mantienen las políticas específicas del usuario para combatir dicho correo en multimedios IP. Estas funciones están compuestas del bloque funcional de criterios de filtrado local y del bloque funcional de lista de filtrado local.

#### i) Bloque funcional de criterios de filtrado local

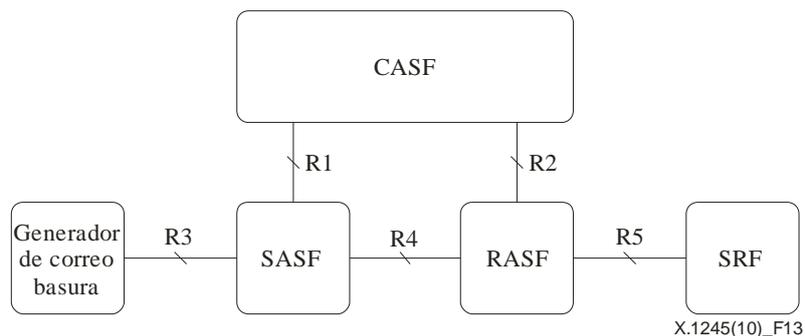
El bloque funcional de criterios de filtrado local mantiene las políticas específicas del usuario para identificar el correo basura en multimedios IP. Los tipos de criterios de filtrado dependen de las funciones de lucha contra el correo basura que soporta la SRF.

#### ii) Bloque funcional de lista de filtrado local

El bloque funcional de lista de filtrado local administra la lista de filtrado específica del usuario para identificar el correo basura en multimedios IP mediante un análisis de la fuente. Los tipos de listas dependen de las funcionalidades de análisis de la fuente que soporta la SRF.

## 7.6 Puntos de referencia en el marco

En este párrafo se definen los puntos de referencia entre diversos elementos del marco. En la figura 13 se identifican los puntos de referencia en el marco.



**Figura 13 – Puntos de referencia en el marco de lucha contra el correo basura**

### 7.6.1 Punto de referencia R1

El punto de referencia R1 está ubicado entre la CASF y la SASF, y se utiliza para obtener la política de filtrado de la CASF a la SASF. La CASF controla a la SASF a través de R1.

### 7.6.2 Punto de referencia R2

El punto de referencia R2 está ubicado entre la CASF y la RASF, y se utiliza para obtener la política de filtrado de la CASF a la RASF. La CASF controla la RASF a través de R1.

### 7.6.3 Punto de referencia R3

El R3 está ubicado entre los generadores de correo basura y la SASF, y se utiliza en el protocolo de aplicación de multimedia IP y/o en la transmisión de tráfico de datos.

### 7.6.4 Punto de referencia R4

El R4 está ubicado entre la SASF y la RASF, y se utiliza en el protocolo de aplicación de multimedia IP y/o en la transmisión de tráfico de datos.

### 7.6.5 Punto de referencia R5

El R5 está ubicado entre la RASF y los receptores de correo basura, y se utiliza en el protocolo de aplicación de multimedia IP y/o en la transmisión de tráfico de datos.

## Apéndice I

### **Lucha contra el correo basura creando numerosas dificultades para su transmisión**

(Este apéndice no es parte integrante de la presente Recomendación)

La creación de abundantes dificultades con el fin de impedir la transmisión de correo basura puede ser una de las técnicas para combatirlo. Sin embargo, este método es diferente de los otros, que identifican y filtran directamente el correo basura. Creando dificultades para transmitir correo basura se ayuda a reducir su volumen de una manera indirecta, pero este método requiere tiempo y esfuerzo y es además muy costoso. Una forma de disminuir la cantidad de correo basura en multimedios IP es aumentar las dificultades que tengan los generadores del correo basura para generar dicho correo, incrementando el coste y los esfuerzos para crear y transmitir el citado correo. Para los generadores de correo basura, el costo está formado por la tasa de reglamentación, con inclusión de la cuantía de la multa prevista por el correo basura ilegal, el coste que entraña la utilización de las aplicaciones multimedios IP que se paga al proveedor de servicio o de red y una tasa de transmisión del correo basura, como el permanecer en línea para pasar las pruebas de interactividad, etc. Para aumentar esas dificultades se pueden aplicar los siguientes métodos:

- Dificultar el acceso a las direcciones IP: Multiplicar los esfuerzos necesarios para recopilar información sobre las víctimas del correo basura, como por ejemplo sus direcciones IP y sus cuentas de servicio de aplicación multimedios IP e incrementar las dificultades para que los generadores de correo basura puedan enviar este correo a los multimedios IP.
- Sistema de pago: La imposición de una tasa al correo basura en multimedios IP puede resultar útil para reducir su volumen. No obstante, la adopción de un sistema de pago por posible correo basura, por ejemplo mensajes IP a granel, no es una cuestión de carácter técnico.
- Prueba de interactividad: Si se somete al generador de correo basura a una prueba de interactividad se puede aumentar el coste de transmisión de dicho correo. No obstante, esto puede tener el efecto secundario de molestar a los usuarios de aplicaciones multimedios IP normales.

Estos ejemplos de cómo luchar contra el correo basura aumentando las dificultades de transmisión de dicho correo no son exhaustivos.

En la prueba de interactividad, la CASF puede asumir la función de ensayador. Cuando se aplica el método de prevención de transmisiones a granel, la CASF, SASF o RASF pueden detectar la abundancia de mensajes, es decir una determinada cuantía, y bloquear las aplicaciones multimedios IP que tengan ese nivel. Con el fin de aumentar las dificultades, también es posible imponer un precio a los mensajes o comunicaciones a granel bajo el control de la CASF.

En ocasiones la SASF o la RASF pueden analizar la información de protocolo, pero en general no es necesario tomar medidas adicionales para aumentar las dificultades de transmisión de correo basura como el control de las transmisiones a granel, la gestión de pagos o las pruebas de interactividad. En resumen, se espera que la SASF o la RASF tomen alguna medida para ayudar a la CASF a combatir el correo basura, y que esta última asuma el papel principal en lo tocante a aumentar las dificultades para transmitir dicho correo.

## Apéndice II

### Consideraciones relativas a la seguridad y de orden práctico para utilizar el marco

(Este apéndice no es una parte integrante de la presente Recomendación)

#### II.1 Consideraciones relativas a la seguridad

A continuación figuran consideraciones relativas a la seguridad con miras a combatir el correo basura en multimedios IP.

##### – Autenticación

La autenticación es el proceso a tenor del cual una entidad, ya sea el receptor del correo basura o la CASF, confirma su identidad mediante la presentación de credenciales que solamente el usuario real está en condiciones de presentar.

Es necesario proceder a la autenticación del usuario para identificar al emisor de un mensaje de aplicaciones multimedios IP que ayuda a bloquear y excluir muchos tipos de ataques de suplantación de identidad con fines de correo basura. Si no se autentifica adecuadamente al usuario no se podrá rastrear a los generadores de correo basura, ya que éstos podrían falsificar su dirección IP mediante ataques de suplantación de identidades.

La autenticación se puede realizar de diversas maneras. Hay algunos métodos de autenticación que son fáciles de implementar, como la autenticación con contraseña, pero que en general son precarios y primitivos. Existen otros métodos, como los de capa de zócalo segura (SSL), IPsec, secure shell o Kerberos, cuya implementación y mantenimiento pueden ser más complejos y exigir más tiempo, pero garantizan una autenticación sólida y fiable.

Otras tecnologías incipientes, como los métodos de firma criptográfica, pueden ser una mejor solución. Sin embargo, el método de autenticación del remitente más disponible y adoptado de forma más generalizada sigue siendo el convenio de remitentes (SPF), claves de dominio.

##### – Control de acceso

El control del acceso es un medio de aplicar y hacer cumplir las políticas de autorización. El control de acceso autoriza o prohíbe al usuario la realización de una acción en el receptor del correo basura y la ASF, según lo estipulado en la política de seguridad.

Normalmente el control de acceso se aplica después de haber establecido la autenticación, y por lo general se clasifica en control de acceso discrecional (DAC) y control de acceso no discrecional (NDAC). Conforme al DAC, el propietario del objeto especifica quién tiene acceso al objeto o especifica las políticas. Todas las políticas de control de acceso distintas del DAC son consideradas NDAC. Con arreglo al NDAC, las políticas son normas que no están especificadas a discreción del usuario. Cabe citar como ejemplos de NDAC las siguientes políticas: control de acceso obligatorio (MAC), control de acceso basado en la función (RBAC), control de acceso basado en la finalidad (PBAC), control de acceso basado en la historia (HBAC), control de acceso con limitaciones temporales (TCAC) y control de acceso basado en las reglas (RuBAC).

##### – Confidencialidad

La confidencialidad se refiere a los mecanismos que garantizan que sólo los usuarios autorizados tienen acceso a unas comunicaciones seguras. Hay dos mecanismos fundamentales para proporcionar confidencialidad a la información transmitida electrónicamente: encriptación o transmisión por una infraestructura segura, por ejemplo a través de una red privada virtual (VPN) u otro enlace encriptado.

El IPSec es el protocolo utilizado en la mayoría de las VPN para establecer una conexión segura por Internet. Se trata de una norma ampliamente aceptada para una transmisión segura y es flexible y menos oneroso que algunos otros métodos de encriptación. El IPSec garantiza una encriptación sólida, integridad y autenticación, y le resulta particularmente útil a las organizaciones que necesitan transferir datos con seguridad a través de Internet.

El protocolo de tunelización de capa 2 (L2TP) se utiliza para soportar a las VPN; éste encapsula un protocolo de capa de red determinado dentro del protocolo punto a punto (PPP) para proteger criptográficamente las tramas PPP y encapsular los datos dentro de un protocolo de tunelización.

#### – Integridad de los datos

Por integridad se entiende el hecho de que la información permanece inalterada mientras se desplaza entre el receptor y el generador del correo basura. Sin una protección adecuada, los generadores podrían alterar o mezclar desordenadamente el contenido de los mensajes multimedios IP.

Al utilizar las compilaciones de mensajes generadas por una función de troceado criptográfico, el administrador de un sistema puede detectar cambios no autorizados en los mensajes. Las funciones de troceado también pueden combinarse con otros métodos criptográficos normalizados para verificar la fuente de los datos. Cuando se combinan algoritmos de troceado con encriptación, se produce un compendio de mensaje especial que identifica la fuente de los datos.

Cuando se utilizan firmas digitales para favorecer la integridad de los datos, puede ser necesario disponer de una infraestructura de clave pública (PKI) para gestionar las claves de encriptación. La PKI hace un seguimiento de la asignación y revocación de claves de encriptación públicas para los usuarios y las organizaciones.

Otra posibilidad además de las firmas digitales y las PKI es la criptografía secreta, que se utiliza para proporcionar integridad a los datos. Una aplicación de clave secreta es más sencilla, por cuanto se utiliza una sola clave y ésta debe obrar en poder tanto del remitente como del receptor para que puedan funcionar la encriptación y la decriptación. Si bien estos sistemas de clave secreta se utilizan ampliamente, éstos plantean las dificultades inherentes a la distribución de claves secretas de una manera segura.

#### – No denegación

La no denegación es el mecanismo a tenor del cual el emisor de un mensaje u originador de una transacción no puede negar posteriormente que esa transacción tuvo lugar.

La no denegación se logra mediante la ratificación de un documento jurídico y de los siguientes mecanismos de seguridad y procesos fiables para la gestión del servidor: SSL, símbolo OTP de impugnación/respuesta, troceado seguro y registro de auditoría.

Una práctica habitual para implementar la no denegación es sacar provecho de las firmas digitales, que pueden considerarse como una de las mejores alternativas para sustituir a las firmas tradicionales en el procesamiento electrónico de datos. Para implementar las firmas digitales es preciso contar con una tercera parte fiable (TTP) o una PKI. Estos últimos pueden soportar al menos una autoridad de certificación (CA) para expedir certificados digitales y listas de revocación de certificados (CRL) con miras a hacer una comparación con los certificados revocados.

## **II.2 Consideraciones de orden práctico**

Uno de los principales objetivos del marco es garantizar que se mantienen a un nivel mínimo los efectos negativos en la actividad económica. Debe dejarse en claro que la observancia de las medidas de lucha contra el correo basura puede tener resultados positivos en los particulares y las empresas, mediante el cumplimiento de los requisitos de la empresa.

Las consideraciones prácticas que figuran a continuación están basadas en las operaciones de procesamiento, y su finalidad es proporcionar orientación para implementar el sistema de lucha contra el correo basura y ofrecer a los posibles proveedores información de alto nivel:

- Proporcionar gran precisión y buen rendimiento.
- Poder desplegarse en el perímetro de Internet.
- Integrarse con los sistemas populares de aplicaciones multimedios IP.
- Funcionar en la plataforma de elección del servidor del cliente: UNIX, Windows, etc.
- Filtrar el correo basura en multimedios IP tanto entrante como saliente.
- Tener flexibilidad para estar en armonía con las políticas y preferencias de la organización.
- Ofrecer la capacidad de que el usuario establezca filtros individuales o específicos.
- Permitir a los usuarios finales administrar sus propias carpetas de correo basura en aplicaciones multimedios IP y fijar preferencias sencillas.
- Ofrecer la capacidad de gestionar la funcionalidad de la lista blanca y la lista negra.
- Brindar la posibilidad de filtrar el contenido, incluida la capacidad de incorporar filtrado de contenido en el lado del servidor, con capas de administración hasta el nivel del usuario.

## **Bibliografía**

- [b-ITU-T X.1240] Recomendación UIT-T X.1240 (2008), *Tecnologías utilizadas contra el correo basura.*
- [b-ITU-T X.1244] Recomendación UIT-T X.1244 (2008), *Características generales de la lucha contra el correo basura (spam) en aplicaciones multimedios basadas en IP.*



## SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
<b>Serie X</b>	<b>Redes de datos, comunicaciones de sistemas abiertos y seguridad</b>
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación