Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1243

(12/2010)

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

Seguridad en el ciberespacio – Lucha contra el correo basura

Sistema de pasarela interactiva para combatir el correo basura

Recomendación UIT-T X.1243

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
Lucha contra el correo basura	**X.1230–X.1249**
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.1243

Sistema de pasarela interactiva para combatir el correo basura

Resumen

La Recomendación UIT-T X.1243 especifica un sistema de pasarela interactiva para combatir el correo basura, como un medio técnico destinado a luchar contra el correo basura entre dominios. El sistema de pasarela permite notificar el correo basura entre diferentes dominios, e impide que el tráfico no deseado pase de un dominio a otro.

En esta Recomendación se especifica asimismo la arquitectura del sistema de pasarela, se describen las entidades básicas, los protocolos y las funciones del sistema de pasarela, y se proporcionan mecanismos para detectar el correo basura, intercambiar información al respecto y tomar medidas concretas en el sistema de pasarela para combatir ese tipo de correo.

Historia

Edición	Recomendación	Aprobación	Comisión de estudios
1.0	ITU-T X.1243	2010-12-17	17

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/.

ÍNDICE

Recomendación UIT-T X.1243

Sistema de pasarela interactiva para combatir el correo basura

1 Alcance

El sistema de pasarela interactiva para combatir el correo basura es un mecanismo interactivo general diseñado para contrarrestar diversos mensajes no deseados entre dominios, con inclusión del correo electrónico basura, los SMS basura, etc., que permite intercambiar información con esa finalidad e impide enviar y recibir correo indeseable. La presente Recomendación promueve la diversidad de técnicas de filtrado destinadas a combatir el correo basura y tiene flexibilidad para aceptar las técnicas venideras.

Antes de adoptar esta Recomendación debe considerarse el cumplimiento de todas las leyes y reglamentaciones nacionales correspondientes.

2 Referencias

La siguiente Recomendación del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.509] Recomendación UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*.

3 Definiciones

3.1 Términos definidos en otros sitios

En la presente Recomendación se utilizan los siguientes términos definidos en otros sitios:

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 la presente Recomendación se definen los siguientes términos:

3.2.1 sistema de pasarela interactiva para combatir el correo basura (*interactive gateway system for countering spam,* IGCS): Es una entidad responsable de detectar y bloquear el correo

basura, que desempeña un par de funciones: función de pasarela emisora (*sender gateway function,* SGF) y función de pasarela receptora (*receiver gateway function,* RGF). Un IGCS debe trabajar con otros pares para implementar todas las funciones destinadas a luchar contra el correo basura.

3.2.2 base de datos local para combatir el correo basura (*local spam-countering database*): Este término se refiere a una base de datos utilizada para almacenar información sobre el correo basura, listas negras y reglas para combatir el correo basura para las funciones de pasarela del receptor y el emisor.

3.2.3 modalidad (*modality*): Se refiere a la codificación de la información que contiene información discernible por un ser humano.

3.2.4 mensaje multimodal (*multimodal message*): Un mensaje multimodal es un mensaje multimedios que contiene información codificada diferentemente para la interacción por múltiples modalidades.

3.2.5 agente receptor (*receiver agent*): Es un servidor que envía mensajes a receptores de mensajes. En las aplicaciones de correo electrónico, un servidor POP actúa como un agente receptor.

3.2.6 función de pasarela receptora (*receiver gateway function*): Es la función desempeñada por la parte receptora para combatir el correo basura, que detecta y bloquea dicho correo durante el proceso de recepción.

3.2.7 agente emisor (*sender agent*): Un agente emisor es un servidor que envía mensajes a remitentes de mensajes. En las aplicaciones de correo electrónico, un servidor SMPT actúa como un agente emisor.

3.2.8 función de pasarela emisora (*sender gateway function*): Es la función que desempeña la parte emisora para combatir el correo basura, que detecta y bloquea dicho correo durante el proceso de emisión de mensajes.

3.2.9 pares en la lucha contra el correo basura (*spam-countering peer*): Durante el proceso de lucha contra el correo basura, los IGCS trabajan conjuntamente para identificar y bloquear dicho correo, de modo que un IGCS constituye un par con otro.

3.2.10 protocolo de paridad para combatir el correo basura (*spam-countering peering protocol*): Este protocolo se ha definido con el fin de intercambiar mensajes de alerta y listas negras entre pasarelas para combatir el correo basura.

3.2.11 protocolo de notificación de correo basura por el usuario (*user spam report protocol*): Este protocolo se ha definido para que los receptores de mensajes notifiquen la recepción de correo basura a la pasarela.

4 Abreviaturas y acrónimos

Esta Recomendación utiliza las siguientes abreviaturas y acrónimos:

Correo-e Correo electrónico (*electronic mail*)

CSPP Protocolo de paridad para combatir el correo basura (*countering spam peering protocolo*)

FE Entidad funcional (*functional entity*)

IGCS Sistema de pasarela interactiva para combatir el correo basura (*interactive gateway system for countering spam*)

IM Mensaje instantáneo (*instant message*)

IRC Charla interactiva Internet (*Internet relay chat*)

LcsDB Base de datos local para combatir el correo basura (*local countering spam database*)

POP Protocolo de oficina de correos (*post office protocol*)

RA Agente receptor (*receiver agent*)

RBL Lista de agujeros negros en tiempo real (*realtime blackhole list*)

RGF Función de pasarela receptora (*receiver gateway function*)

SA Agente emisor (*sender agent*)

SGF Función de pasarela emisora (*sender gateway function*)

SMPT Protocolo de transferencia de correo simple (*simple mail transfer protocol*)

WPF Filtro de parámetro ponderado (*weighted parameter filter*)

5 Convenios

Bloque funcional: en el contexto del sistema de pasarela interactiva para combatir el correo basura, se define como "bloque funcional" una compilación de funcionalidades, que se representa con el siguiente símbolo:

6 Arquitectura

6.1 Entidades y funciones de lucha contra el correo basura

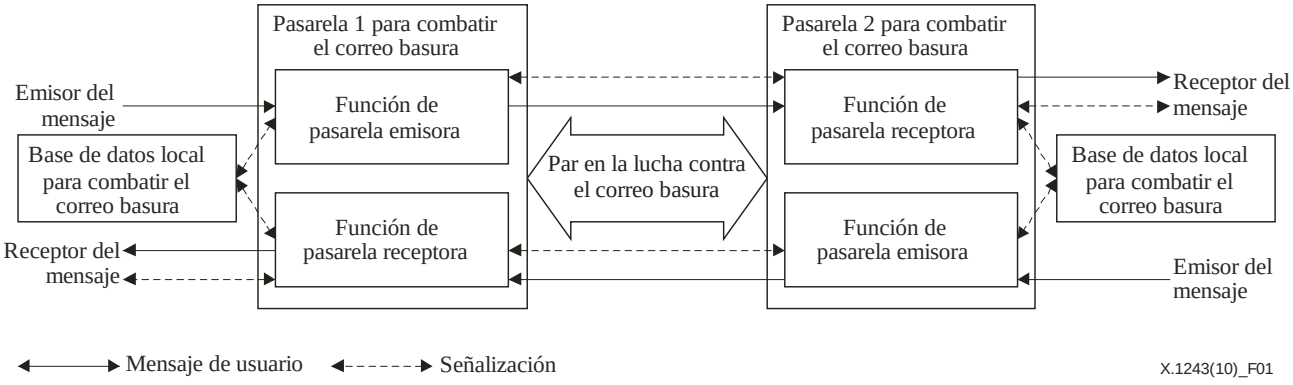

Figura 1 – Arquitectura del sistema de pasarela interactiva para combatir el correo basura

Sistema de pasarela interactiva para combatir el correo basura (IGCS)

Un sistema IGCS está compuesto de una pasarela para combatir el correo basura y una base de datos local para combatir el correo basura. La pasarela tiene dos entidades subfuncionales: SGF y RGF, las cuales actúan como puntos de decisiones y puntos de observancia de políticas. La SGF se utiliza para procesar el correo basura saliente y la RGF se utiliza para procesar el correo basura entrante. La base de datos local para combatir el correo basura (lcsDB) proporciona reglas para identificar al correo basura y tomar medidas para contrarrestarlo. La pasarela local también es responsable de actualizar dichas reglas para la lcsDB.

Las responsabilidades de las RGF y SGF son las siguientes:

- tomar medidas para contrarrestar el correo basura entrante conocido (bloqueo, asilamiento o alerta, etc.);
- detectar nuevo correo basura mediante informes al respecto del receptor y actualizar las reglas para contrarrestarlo a nivel local con destino a la lcsDB;
- notificar a la SGF emisora mediante el envío de una notificación cuando se detecta correo basura.

Una SGF tiene dos responsabilidades:

- tomar medidas para contrarrestar el correo basura saliente conocido (bloqueo, asilamiento o alerta, etc.);
- procesar las notificaciones de correo basura emitidas por la RGF receptora y actualizar las reglas para contrarrestarlo a nivel local con destino a la lcsDB.

Base de datos local para combatir el correo basura (lcsDB)

Una lcsDB se utiliza para almacenar la información destinada a contrarrestar el correo basura. Esa información puede clasificarse a su vez en tres tipos:

- Información para la identificación de correo basura: como la dirección de origen del correo basura y las palabras clave en el campo de sujeto de dicho correo.
- Reglas para combatir el correo basura: como la lista negra y la lista blanca.
- Registro de posible correo basura: ejemplos de correo basura sospechoso que se notifica mediante las RGF y SGF.

6.2 Identificación del correo basura

La RGF o la SGF identifican correo basura conocido gracias a la información de identificación almacenada en la lcsDB. El correo basura se clasificará en varios niveles y se adoptarán las medidas correspondientes.

6.3 Medidas para contrarrestar el correo basura

Una vez identificado el correo basura, la RGF o SGF correspondiente tomará las medidas pertinentes en función del nivel del correo basura identificado. Para contrarrestarlo se pueden tomar, entre otras, las siguientes medidas:

- alerta de correo basura: la RGF/SGF envía una alerta al receptor/emisor del mensaje;
- aislamiento del correo basura: la RGF/SGF aísla al mensaje indeseable y envía periódicamente un resumen de aislamiento al emisor/receptor del mensaje;
- bloqueo del correo basura: la RGF/SGF bloquea el mensaje indeseable.

6.4 Descubrimiento del correo basura

6.4.1 Descubrimiento de correo basura RGF

El receptor puede comunicar las reglas anti correo basura a su RGF en servicio. Las reglas anti correo basura incluyen, entre otras, la lista negra de direcciones de origen/destino y las palabras clave del campo de sujeto del correo electrónico. La RGF actualiza las reglas y la identificación del correo basura en la lcsDB. Cuando llega un mensaje sospechoso, la RGF inicia un proceso de evaluación para juzgar si el mensaje es indeseable de conformidad con las reglas para combatir el correo basura almacenadas en la lcsDB. Si se juzga que el mensaje es indeseable, la RGF tomará las medidas pertinentes.

6.4.2 Descubrimiento de correo basura SGF

El proceso de descubrimiento de correo basura SGF es similar al RGF. La SGF también recibe notificaciones de correo basura de la RGF del receptor, las evalúa y actualiza las reglas de correo basura verificado con destino a su lcsDB local.

6.5 Notificación de correo basura mediante el protocolo de paridad para combatir el correo basura

6.5.1 Descubrimiento del par

Cuando una SA está tratando de enviar un mensaje a una RA, uno de los IGCS inicia el procedimiento de descubrimiento del par, con el fin de encontrar un IGCS par activo en el trayecto de entrega del mensaje. La relación de paridad se establecerá tras un proceso de reconocimiento del par (proceso "handshake").

6.5.2 Notificación de correo basura entre pares

Una vez establecida la relación de paridad, el IGCS puede intercambiar notificaciones de correo basura con su par mediante el protocolo de paridad para combatir el correo basura. Dado que el correo basura es identificado fundamentalmente por el receptor, la RGF del receptor es responsable de identificar dicho correo y proporcionar información al respecto a la SGF del emisor. Una vez que una RGF detecta un mensaje indeseable, lo notificará a la SGF del emisor mediante un proceso de notificación de correo basura. Tras recibir dicha notificación, la SGF debe decidir si lo acepta o no, de conformidad con la política local de lucha contra el correo no deseado.

6.5.3 Aspectos relacionados con la seguridad

En el proceso de notificación de correo basura para la autentificación de pares se recomienda incluir un mecanismo de certificación especificado en la Recomendación [UIT-T X.509]. Se recomienda asimismo que la RGF firme digitalmente el mensaje de notificación, y que sólo se acepte un mensaje de notificación procedente de una RGF de origen fiable.

7 Técnicas de filtrado para combatir el correo basura

7.1 Consideración independiente de la técnica

El sistema IGCS debe admitir las diversas técnicas destinadas a contrarrestar el correo basura y tener flexibilidad para integrar las técnicas de filtrado existentes y futuras. Cada una de las técnicas de filtrado puede implementarse con carácter facultativo. Para detectar eficazmente mensajes indeseables, un IGCS puede admitir varias técnicas de filtrado e integrarlas en un dispositivo de red física. La implementación concreta de las técnicas de filtrado está fuera del alcance de esta Recomendación, en la que sólo se definen interfaces y formatos de datos para cada técnica de filtrado, a efectos de garantizar el interfuncionamiento al intercambiar información contra el correo basura entre los IGCS pares.

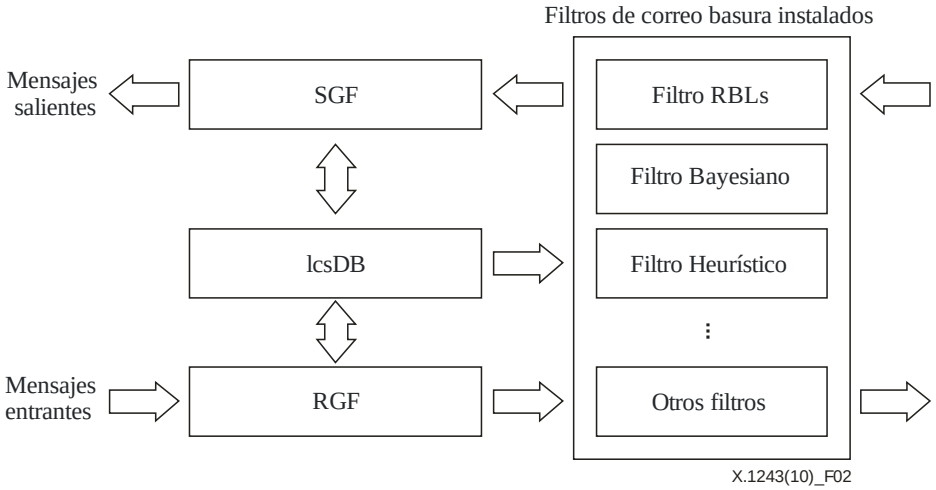

Figura 2 – Un sistema IGCS con múltiples filtros de correo basura

7.2 Técnicas recomendadas para combatir el correo basura

7.2.1 Lista de direcciones

Listas de agujeros negros en tiempo real (RBLs): Varias organizaciones que estudian el correo basura y elaboran sus propias listas de direcciones de origen proporcionan RBLs. Un sistema de lucha contra el correo basura puede inscribirse en la lista y determinar si un correo es o no indeseable cotejándolo con la lista.

Listas negras: Son mecanismos básicos de control de acceso que permiten el acceso a todos salvo a los que figuran en las listas negras. Al igual que las RBL, estas listas se pueden actualizar constantemente, pero el esquema tiene la deficiencia de que muchos mensajes de correo basura no contienen direcciones de origen. Algunos sistemas también permiten a los usuarios mantener listas blancas de remitentes autorizados, pero ese mecanismo puede impedir a los usuarios obtener mensajes normales de fuentes previamente desconocidas.

7.2.2 Filtrado heurístico

Estos filtros están basados en la realización de una prueba para detectar en el mensaje ciertas características típicas del correo basura, como la utilización exclusiva de HTML o el tipo de cliente al que se envía el mensaje. La prueba se pondera mediante un proceso de aprendizaje basado en una serie de mensajes conocidos y una serie de correos electrónicos que se sabe son legítimos.

Estos riesgos comportan el riesgo de que se clasifique como correo basura a un mensaje que utilice las técnicas de un generador de correo indeseable, como por ejemplo mensajes espectaculares en HTML.

Estos filtros pueden detectar una gran proporción de mensaje, y no precisan ser enseñados o configurados. No obstante, dado que realizan un gran número de pruebas, conviene saber que se puede cambiar la configuración con la que se realizan las pruebas y la puntuación utilizada para clasificar los mensajes como correo basura.

7.2.3 Filtrado bayesiano

Conforme a este tipo de filtrado, el motor de lucha contra el correo basura se configura con una serie de correos indeseables conocidos y una serie de mensajes que se sabe son legítimos. Tras ese proceso de aprendizaje se hace una compilación del vocabulario característico de los mensajes de correo basura. Este filtro utilizará las probabilidades bayesianas para calcular si un nuevo mensaje es o no indeseable. Cuando se trata de un filtro grupal, en general se encarga del aprendizaje el administrador del sistema.

Sobre la base del algoritmo de probabilidades bayesianas, este filtro tiene una fuerte tara de cálculo y puede introducir problemas de escalabilidad en los grandes sistemas de lucha contra el correo basura. En un entorno reducido y muy uniforme (por ejemplo una red empresarial o universitaria) ese inconveniente puede resultar aceptable, pero sin duda no lo será para un importante proveedor de servicios y aún menos para un proveedor público.

Aunque el filtro bayesiano se ha utilizado para combatir el correo basura, presenta algunas limitaciones cuando los generadores de correo basura proporcionan información fraudulenta.

7.2.4 Filtrado multimodal

Cuando un sistema IGCS desea realizar filtrado multimodal, las SGF y RGF implementan dicho filtrado, respectivamente, mediante un par de entidades funcionales: la FE de detección de modalidad, la FE de filtrado y otras entidades funcionales necesarias como la FE de procesamiento del mensaje multimodal. Para facilitar el intercambio y almacenamiento de información, se deben definir conjuntos de datos de lucha contra el correo basura multimodal, que la lcsDB almacenará con sus categorías (y temas) de mensajes multimodales y criterios de filtrado adecuados (que provengan de usuarios u operadores, o bien de sistemas IGCS pares).

Si la descripción de los metadatos multimodales está disponible y se considera fidedigna, las aplicaciones multimodales pueden filtrar la información multimodal basada en la descripción en metadatos del contenido multimodal. De otro modo, en el filtrado se considerará preferiblemente toda la información multimodal y las siguientes entidades funcionales realizarán las tareas que se indican a continuación:

- una base de datos o depósito retiene los criterios de filtrado y la categorías de mensajes multimodales adecuados. Dicha base de datos o depósito puede encontrarse en el mismo local/dominio que el agente FE de interfaz DB, el FE de detección de modalidad, el FE de procesamiento multimodal y el agente del usuario multimodal. De otro modo, la base de datos o depósito puede hallarse en otros locales o dominios, diferentes de los del FE;
- un elemento funcional de detección de modalidad inspecciona un mensaje multimodal enviado o recibido para identificar las modalidades contenidas;
- una entidad funcional de agente de interfaz DB trae los criterios de filtrado desde la DB en las categorías de mensaje y las modalidades determinadas;
- una entidad funcional de filtrado filtra el mensaje multimodal sobre la base de los criterios de filtrado. El FE de filtrado puede bloquear total o parcialmente ciertas partes multimodales seleccionadas de un mensaje multimodal procesado.

En la figura 3 se describe la arquitectura general y las entidades funcionales necesarias para el filtrado de los mensajes multimodales. La arquitectura de filtrado abarca al FE de detección de modalidad, el FE de filtrado, el agente FE de interfaz DB y la DB multimodal. Sin embargo, en la figura 3 se muestran otras entidades funcionales que por lo general no realizan ninguna tarea de filtrado multimodal, tales como el FE de procesamiento del mensaje multimodal y el agente de usuario multimodal.

El FE de procesamiento del mensaje multimodal procesa los mensajes multimodales (filtrados), sincroniza los mensajes multimodales recibidos de los agentes de usuario multimodal y multiplexa o envía los mensajes multimodales filtrados hacia los agentes de usuario multimodal. Cada uno de los diversos agentes de usuario multimodal manipula modalidades específicas tales como la entrada y/o salida modal (específica según el dispositivo).

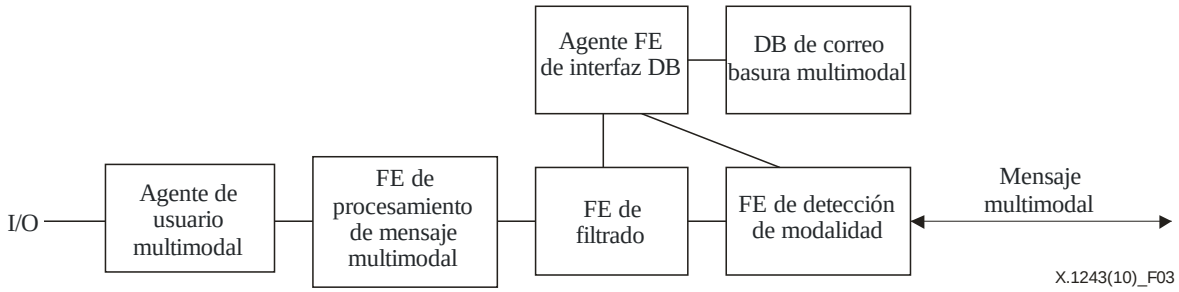

Figura 3 – Arquitectura de filtrado multimodal

En la figura 4 se ilustra la arquitectura genérica de filtrado multimodal, estableciendo una correspondencia entre las entidades funcionales y la función de pasarela receptora (RGF). El procedimiento a seguir cuando las FE reciben un mensaje multimodal puede describirse con los siguientes pasos:

1) La RGF recibe un mensaje multimodal.

2) La FE de detección de modalidad identifica el o los tipos de mensaje y las modalidades contenidas en el mensaje multimodal recibido.

3) La FE de filtrado puede haber sido configurada estáticamente con reglas de filtrado para todos los posibles mensajes multimodales (es decir, independientemente de un determinado mensaje multimodal recibido), o bien dinámicamente, con una regla dependiente del mensaje y/o del modo para cada uno de los mensajes multimodales recibidos.

   a) La FE de detección de modalidad puede transmitir los parámetros del tipo de mensaje y las modalidades identificados al agente de interfaz DB, o bien puede adjuntar los parámetros al mensaje multimodal recibido.

   b) La FE de detección de modalidad retransmite el mensaje multimodal a la FE de filtrado, probablemente anotado con los parámetros del tipo de mensaje y la modalidad.

4) En caso de que la FE de filtrado aún no haya sido configurada con reglas, ésta transmite al agente de interfaz DB los parámetros del tipo de mensaje y las modalidades, a menos que el agente de la interfaz DB haya obtenido esos parámetros directamente de la FE de detección de modalidad.

5) La FE de agente de interfaz DB interroga a la DB multimodal para obtener los criterios del mensaje y las correspondientes modalidades. La FE de agente de interfaz DB compila esos valores en reglas específicas y las transmite a la FE de filtrado.

6) La FE de filtrado aplica las reglas disponibles y realiza el filtrado tras recibir el mensaje multimodal. Dependiendo de las reglas y el entorno de política, se autoriza a pasar al mensaje multimodal, o bien éste se bloquea totalmente, o acaso parcialmente, en caso de que se bloqueen sólo ciertas modalidades dentro del mensaje multimodal.

7) La FE de filtrado pasa el mensaje multimodal filtrado a la FE de procesamiento de mensaje multimodal, posiblemente anotado con algunos resultados del filtrado (por ejemplo, información para el registro o alertas de seguridad).

8) La FE de procesamiento de mensaje multimodal procesa el mensaje multimodal recibido (filtrado). Ésta sincroniza la/s entrada/s de los diversos agentes de usuario multimodal de entrada, envía el mensaje multimodal en sus componentes de modalidad y transmite esas partes específicas de modalidad a los agentes de usuario multimodal de salida.

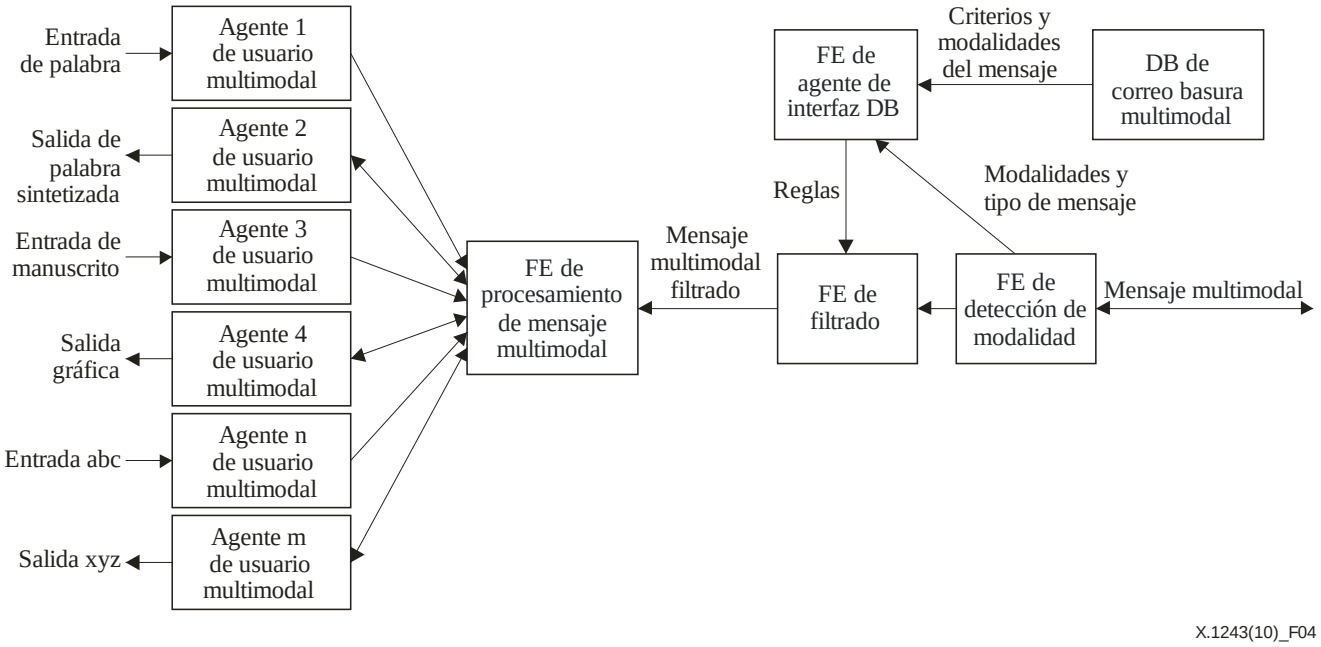

Figura 4 – Filtrado multimodal en una función de pasarela receptora (RGF)

NOTA – En la figura 4 se describen varios agentes de usuario multimodal. La RGF puede no exigir que estén presentes todos los agentes de usuario multimodal indicados.

7.2.5 Filtro amortiguador de correo basura

Este filtro se utiliza para controlar la velocidad de recepción de mensajes. Un parámetro de entrada para este filtro es el coeficiente de amortiguamiento del correo basura, que consiste en una medición de los mensajes sospechosos y el control de las velocidades de recepción de mensajes. Cuando se reciben mensajes muy sospechosos el coeficiente aumenta y el filtro amortiguador del correo basura hace bajar la velocidad de recepción de correos electrónicos sospechosos. Por lo general este parámetro lo genera un sistema externo de lucha contra el correo basura, como una base de datos sobre experiencia o reputación. El filtro amortiguador del correo basura también puede afectar el retardo de respuesta del correo electrónico, el tamaño de la ventana de transporte y el tiempo del ciclo de amortiguamiento, etc.

7.2.6 Filtro de encabezamiento de correo electrónico (*email header filter,* EHF)

Este filtro controla la conversación SMPT y garantiza su observancia de los correspondientes protocolos. Se puede utilizar para identificar la incoherencia de un protocolo o un encabezamiento de correo electrónico falsificado. Con miras a reconstruir las sesiones SMPT y rastrear los estados del protocolo, el EHF puede requerir la desfragmentación de los paquetes, el ensamblado del tren TCP, etc. Este filtro se centra en el análisis a nivel de protocolo y proporciona información adicional para aumentar la precisión general de la identificación del correo basura. Normalmente el EHF está integrado en muchos sistemas comerciales de lucha contra el correo basura, así como en algunos sistemas anti correo indeseable de fuente abierta.

7.2.7 Filtro de parámetro ponderado (*weighted parameter filter,* WPF)

Este filtro se utiliza para detectar el correo basura mediante el análisis de múltiples parámetros, que están basados en información estadística, con inclusión del número de sesiones de correo, el número de servidores de destino, el número de ensayos de correo electrónico, el período de envío de mensajes electrónicos, la velocidad de envío de mensajes electrónicos, la tasa de correos ensayados y correos enviados con éxito, y así sucesivamente. Cada parámetro tiene un umbral configurado y un valor de ponderación configurado. Se necesita además el conjunto de valores ponderados, que pueden estar justificados por varias experimentaciones previas. Para cada correo, se verificarán

todos los parámetros en las reglas. Se añadirán de forma ponderada únicamente los parámetros que pasan el umbral configurado. Si las sumas de los parámetros sobrepasan un umbral predefinido, el WPF podrá hacer una distinción entre el correo electrónico normal y el indeseable.

8 Proceso del protocolo de paridad para combatir el correo basura

8.1 Descubrimiento del par

En el marco del proceso de descubrimiento del par, se establecen relaciones de paridad entre dos IGCS. Este proceso se inicia cuando un IGCS está tratando de descubrir un IGCS válido a lo largo del trayecto de entrega del mensaje. Cuando una RGF detecta un mensaje de correo sospechoso, inicia el proceso de descubrimiento del par.

Se recomienda incluir la siguiente información en el mensaje de descubrimiento del par:

- Lista de direcciones de la RGF/SGF del IGCS inicial: dirección de origen (por ejemplo, par de puertos y dirección IP de origen). Para protegerse contra los fallos de un solo punto, un IGCS puede integrar múltiples RGF y SGF con fines de redundancia. La lista de direcciones puede contener todas las direcciones de la RGF/SGF del IGCS inicial.
- La dirección del IGCS de contraparte: IGCS@{dirección del mandatario de la contraparte}.
- Originador del correo basura: dirección del remitente del correo basura.
- Tipo de correo basura que es motivo de sospecha: WELL_KNOWN, USER_REPORTED u OTHER.
- Correo basura sospechoso adjunto: el correo basura que es motivo de sospecha figura adjunto.

Cuando se envía un mensaje de descubrimiento de par, el IGCS inicial activará un temporizador. Si tras un plazo de expiración configurado no se recibe ningún mensaje de respuesta, se considerará que el IGCS ha fallado en su intento de descubrir un IGCS par. La respuesta al mensaje de descubrimiento del par puede contener la siguiente información:

- Lista de direcciones de la RGF/SGF del IGCS que responde.
- Confirmación del correo basura que dio lugar a la sospecha: confirmar si el IGCS que responde ha considerado correo basura al mensaje sospechoso.

8.2 Establecimiento de la paridad

Si el IGCS inicial recibe una respuesta al mensaje de descubrimiento del par antes de que expire el plazo, puede comenzar a establecer la relación de paridad. Dicho proceso constará de dos acciones principales:

- El IGCS actualiza la lista de direcciones: añade a la lista par la lista de direcciones del IGCS de contraparte.
- Designa la lista de filtros para combatir el correo basura recomendados: filtros de lucha contra el correo basura recomendados en cada IGCS.

8.3 Intercambio de mensajes para combatir el correo basura

Tras el proceso de establecimiento de la paridad, el IGCS inicia el intercambio de mensajes para contrarrestar el correo basura. Durante este proceso los dos IGCS pares intercambian la información de los filtros comunes recomendados para combatir el correo basura. En consecuencia, cada IGCS actualiza su lcsDB con el mensaje intercambiado.

8.4 Disolución de la paridad

Si no se detecta ningún correo basura durante cierto periodo de tiempo, un IGCS puede poner término a la relación de paridad mediante el envío de un mensaje de disolución de paridad. Al recibir ese mensaje, el IGCS suprimirá o reutilizará la información de paridad conexa, según la política en vigor.

9 Modelos de implementación de sistemas de pasarelas para combatir el correo basura

9.1 Modelo integrado

9.1.1 Descripción del modelo

Conforme a este modelo, el IGCS está integrado con un sistema de mensajes que consta de un RA y un SA. Cada sistema tiene una pasarela (una RGF y una SGF) y una lcsDB. En el sistema del correo electrónico, por ejemplo, el RA puede ser un servidor POP3 y el SA puede ser un servidor SMTP. Una RGF/SGF puede implementarse como un servidor integrado que presta tanto servicios POP3 como SMTP. También se necesita una lcsDB para que un sistema de correo electrónico proporcione reglas de lucha contra el correo basura. En la figura 5 se ilustra un modelo integrado.

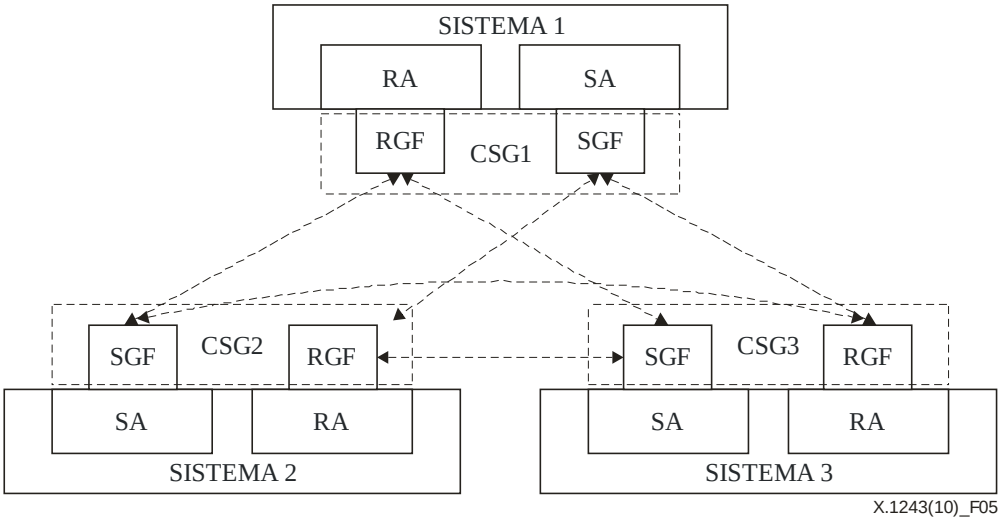

Figura 5 – Modelo integrado de IGCS

9.1.2 Modo de utilización

Un modelo integrado es un modelo adecuado de cliente/servidor, a tenor del cual el servidor es responsable de enviar y recibir numerosos mensajes de clientes. En este caso, el servidor actúa como un punto de decisión y un punto de observancia de política para actividades tendientes a combatir el correo basura.

9.2 Modelo basado en el dominio

9.2.1 Descripción del modelo

Conforme a este modelo, el IGCS actúa como un mandatario de entrega de mensaje en un dominio que puede tener múltiples SA y RA para satisfacer los requisitos de equilibrio de carga. La SGF/RGF puede tener numerosas instancias distribuidas en un dominio, cada una de las cuales está a cargo de varios SA/RA en un dominio y es responsable de contrarrestar los mensajes de correo basura tanto en el dominio local como entre dominios.

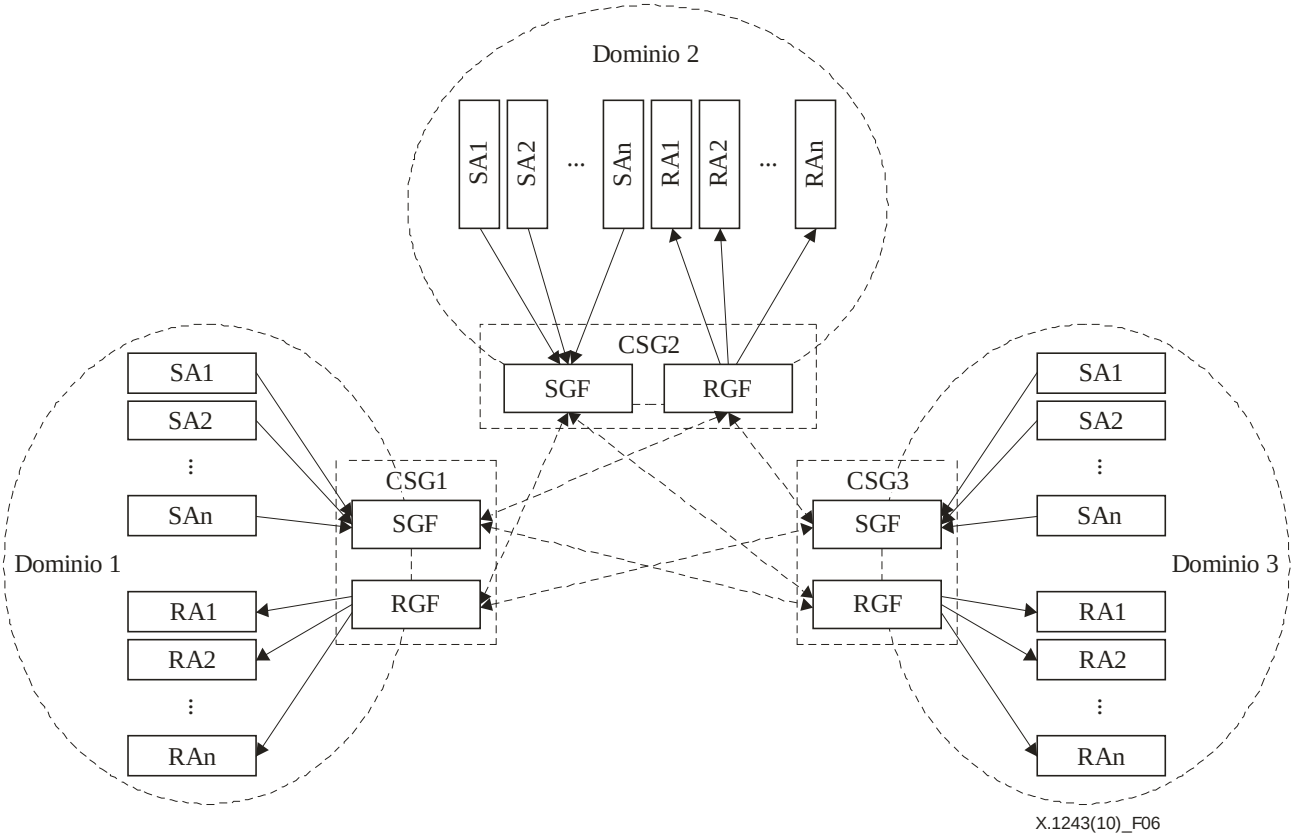

Figura 6 – Modelo basado en el dominio

9.2.2 Modo de utilización

Este modelo puede utilizarse para combatir el correo basura sobre la base del dominio, y es especialmente adecuado para los sistemas de comunicaciones de par a par, como son muchas aplicaciones IM populares: IRC y otras. En el caso de un modelo de par a par, el propio sistema del lado del usuario actúa al mismo tiempo como RA y SA. Con un modelo IGCS integrado resultaría muy difícil gestionar un gran número de RA y SA del lado del usuario, pero con un modelo basado en el dominio esta dificultad se puede superar de una manera distribuida.

9.3 Modelo de despliegue con desvío

9.3.1 Descripción del modelo

En la red inalámbrica, el IGCS también se puede desplegar con un punto de acceso inalámbrico que desvía todos los mensajes en su dirección. El IGCS juzga a los mensajes entrantes sobre la base de las reglas almacenadas en la lcsDB e inyecta los mensajes normales en la red inalámbrica.

9.3.2 Modos de utilización

Este modelo de despliegue con desvío se puede utilizar en la red inalámbrica, y permite filtrar y excluir el correo basura antes de que ingrese en la red inalámbrica, de modo que evita el coste innecesario que implica cursar el tráfico de correo basura.

Apéndice I

Ejemplo de definición de mensaje

(Este apéndice no forma parte integrante de la Recomendación)

A continuación figura un ejemplo de mensajes SCPP definidos en el lenguaje ASN.1, verificados por el compilador ASN.1.

```
SCPP-MESSAGES {itu-t(0) recommendation(0) x(24) igscs(1243)
asn1-module(0) scpp-messages(1)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

-- SCPP Message body definition
SCPP-PDU ::= SEQUENCE {
     sourceAddress        IGCS-Address,
     destAddress          IGCS-Address,
     igcs-message-body    CHOICE {
               peerDiscovery   PeerDiscoveryDEF,
               peerSetup       PeerSetupDEF,
               dataExchange    DataExchangeDEF,
               peerKeepAlive   PeerKeepAliveDEF,
               peerRelease     PeerReleaseDEF},
     nonStandardData      OCTET STRING OPTIONAL,
     ...
}

-- PeerDiscovery Message definition
PeerDiscoveryDEF::=SEQUENCE {
     setupRequest    BOOLEAN,
     igcsSignature   IGCS-Signature
}

-- PeerSetup Message definition
PeerSetupDEF::=SEQUENCE {
     setupResponse        BOOLEAN,
     sgfList              SEQUENCE OF IGCS-Address,
     rgfList              SEQUENCE OF IGCS-Address,
     supportedFilters     SupportedSpamFilters,
     igcsSignature        IGCS-Signature
}

-- Countering Spam Data Exchange Message definition
DataExchangeDEF::=SEQUENCE {
     csData               SET OF SpamFilterData,
     ...
}

-- Peer Keep Alive Message definition
PeerKeepAliveDEF::=SEQUENCE {
     sgfUpdates      GF-Updates,
     rgfUpdates      GF-Updates,
     filtersUpdates  SupportedSpamFilters
}
-- Peer Release Message definition
PeerReleaseDEF::=SEQUENCE {
     peerRelease     ENUMERATED{request(0), confirm(1)},
     nonStandardData OCTET STRING OPTIONAL,
     ...
}

-- IGCS supported addresses, include IGCS,SGF,RGF address definition
-- Support IP address, Email ID and other types of address
IGCS-Address::=CHOICE{
     ipAddress
```

```
     SEQUENCE { ip OCTET STRING(SIZE(4)),
                port INTEGER(0..65535) },
                ip6Address
                SEQUENCE { ip OCTET STRING(SIZE(16)),
                           port INTEGER(0..65535) },

     emailAddress         IA5String(SIZE(1..512)),
     nonStandardAddress   OCTET STRING,
     ...
}

-- Signature data for authentication
IGCS-Signature::=SEQUENCE {
     igcsID          INTEGER(0..65535),
     signatureData   OCTET STRING,
     ...
}

-- RGF/SGF status update information
GF-Updates::=SEQUENCE {
     gateType        ENUMERATED {sgf(0),rgf(1)},
     gateAdd         IGCS-Address,
     gateRemove      IGCS-Address
}

-- IGCS Supported Spam filters and related data

SupportedSpamFilters::= SEQUENCE {
     supportedFilter SEQUENCE OF SpamFilters

}

SpamFilters::=SEQUENCE{
     filterID        INTEGER(0..128),
     filterName      IA5String(SIZE(1..512))
}

SpamFilterData::=SEQUENCE {
     filterID        INTEGER(0..128),
     filterData      OCTET STRING,
     ...
}

END
```

Bibliografía

[b-UIT-T X.680] Recomendación UIT-T X.680 (2008) | ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

[b-UIT-T X.681] Recomendación UIT-T X.681 (2008) | ISO/IEC 8824-2:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification.*

[b-UIT-T X.682] Recomendación UIT-T X.682 (2008) | ISO/IEC 8824-3:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*

[b-UIT-T X.683] Recomendación UIT-T X.683 (2008) | ISO/IEC 8824-4:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*

[b-UIT-T X.1231] Recomendación UIT-T X.1231 (2008), *Technical strategies for countering spam.*

[b-UIT-T X.1240] Recomendación UIT-T X.1240 (2008), *Technologies involved in countering e-mail spam.*

[b-UIT-T X.1241] Recomendación UIT-T X.1241(2008), *Technical framework for countering e-mail spam.*

[b-IETF RFC 1869] IETF RFC 1869 (1995), *SMTP Service Extensions*.

[b-IETF RFC 1939] IETF RFC 1939 (1996), *Post Office Protocol – Version 3*.

[b-IETF RFC 2060] IETF RFC 2060 (1996), *Internet Message Access Protocol – Version 4rev1*.

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*.

[b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)*.

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*.

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format*.

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions.*

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
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
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

Impreso en Suiza
Ginebra, 2011