Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1247

(03/2016)

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

Seguridad en el ciberespacio – Lucha contra el correo basura

Marco técnico para luchar contra el correo basura en la mensajería móvil

Recomendación UIT-T X.1247

Unión Internacional de Telecomunicaciones

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
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
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/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

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

Recomendación UIT-T X.1247

Marco técnico para luchar contra el correo basura en la mensajería móvil

Resumen

El correo basura en la mensajería móvil ha proliferado extraordinariamente a raíz del rápido desarrollo de los servicios de mensajería móvil. Desgraciadamente, ninguna medida ha demostrado ser realmente eficaz al respecto. Por consiguiente, es necesario establecer un marco práctico para hacer frente al correo basura en la mensajería móvil. En la Recomendación UIT-T X.1247 se proporciona una visión general de los procesos contra el correo basura en la mensajería móvil y se propone un marco técnico para luchar contra el mismo. En dicho marco se especifican las funciones de entidades y los procedimientos de trabajo. En esta Recomendación también se facilitan mecanismos para compartir información sobre la lucha contra el correo basura en la mensajería móvil en un dominio anticorreo basura y entre varios dominios anticorreo basura.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1247	2016-03-23	17	11.1002/1000/12600

Palabras clave

Correo basura en la mensajería móvil, marco técnico, procesos contra el correo basura.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

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 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

Introducción

La mensajería móvil, en particular el servicio de mensajes cortos y el servicio de mensajes multimedios, se desarrolla a un ritmo muy rápido debido a su reducido precio, alta flexibilidad y facilidad de uso. Sin embargo, el correo basura en la mensajería móvil provoca molestias diarias a los usuarios, y tiene muchos efectos negativos.

Es difícil mitigar de forma eficaz el correo basura en la mensajería móvil únicamente mediante una única solución. Si se combinan varias tecnologías contra el correo basura en la mensajería móvil, los efectos de este pueden reducirse sustancialmente. Asimismo, habida cuenta de que el correo basura en la mensajería móvil está presente en todo el mundo, la cooperación entre varios dominios anticorreo basura podría dar lugar a una reducción de costos y a un aumento de la eficiencia. Por consiguiente, es necesario establecer un marco abierto adecuado para varias soluciones que soporte mecanismos de colaboración. Dicho marco es compatible con la mayoría de tecnologías contra el correo basura y no se limita a pormenores técnicos específicos. Los procedimientos relativos al marco requerirán el consentimiento explícito del usuario del dispositivo móvil, y deberán cumplir los reglamentos y la legislación nacionales.

Recomendación UIT-T X.1247

Marco técnico para luchar contra el correo basura en la mensajería móvil

1 Alcance

En la presente Recomendación se proporciona un marco técnico para la lucha contra el correo basura en la mensajería móvil. En dicho marco se especifican las funciones de entidad y los procedimientos de procesado. Los procedimientos incluidos en este marco requieran el consentimiento explícito del usuario del dispositivo móvil y deben ajustarse a los reglamentos y la legislación nacionales. Asimismo, en esta Recomendación se proporcionan mecanismos para compartir información relativa a la lucha frente al correo basura en la mensajería móvil en un dominio anticorreo basura y entre dichos tipos de dominios.

Esta Recomendación es aplicable para el servicio de mensajes cortos (SMS) y el servicio de mensajes multimedios (MMS).

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 correo basura SMS [b-ITU-T X.1242]: Correo basura enviado por SMS.

3.1.2 correo basura [b-ITU-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.

3.1.3 remitente de correo basura [b-ITU-T X.1240]: Entidad o persona que crea y envía spam.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 dominio anticorreo basura: Sistema independiente que incluye una función de gestión anticorreo basura, una función de vigilancia anticorreo basura, una función de procesamiento anticorreo basura y un cliente de mensajería móvil.

NOTA – Las funciones del dominio anticorreo basura están sujetas a la gestión unificada del operador.

3.2.2 entidad de filtrado anticorreo basura: Equipo o sistema que aplica medidas anticorreo basura para filtrar mensajería móvil con arreglo a determinadas reglas de filtrado. Puede bloquear el correo basura, marcar mensajes como sospechosos o enviar mensajes al receptor.

3.2.3 funciones de gestión anticorreo basura: Grupo de funciones utilizadas para administrar y supervisar el dominio anticorreo basura, en particular la comunicación con otros dominios anticorreo basura para compartir información sobre correo basura, generando nuevas reglas de filtrado a partir del análisis de dicho correo basura destinados a las funciones de procesado de correo basura.

3.2.4 funciones de vigilancia de correo basura: Grupo de funciones utilizadas para vigilar y analizar el resultado del filtrado de un dominio de procesado anticorreo basura, incluida la validación del correo basura sospechoso recibido mediante un señuelo, el análisis de los datos de correo basura, la generación de estadísticas sobre correo basura y los resultados del análisis del correo basura.

3.2.5 funciones de procesado de correo basura: Grupo de funciones utilizadas para procesar mensajería móvil con arreglo a reglas y políticas de filtrado. El procesado de mensajes consiste en el bloqueo de correo basura, su envío con una marca especial o el envío de mensajes al receptor.

3.2.6 negativo falso: Correo basura de mensajería móvil procesado erróneamente por el sistema de filtrado.

3.2.7 positivo falso: Mensaje identificado erróneamente como correo basura por el sistema de filtrado.

3.2.8 reglas de filtrado: Conjunto de reglas de algoritmos de protección definidas por la entidad de filtrado anticorreo basura, por ejemplo, listas negras/listas blancas, umbrales de similitud y umbrales estadísticos. Las reglas de filtrado también podrían ser específicas del usuario.

3.2.9 cliente de mensajería móvil: Abonado del servicio de mensajería móvil.

3.2.10 correo basura de mensajería móvil: Comunicaciones electrónicas por servicios de mensajería móvil no solicitadas, habitualmente consistentes en correo basura mediante el servicio de mensajes cortos y el servicio de mensajes multimedios.

3.2.11 correo basura en mensajería multimedios (MMS): Correo basura enviado por el servicio de mensajes multimedios.

3.2.12 servicio de notificación: Servicio que permite realizar y agregar informes sobre correo basura del abonado con el permiso del usuario, con arreglo a los reglamentos y la normativa nacionales.

3.2.13 informe del análisis del correo basura: El resultado analizado representa el rendimiento del sistema de filtrado. Debería incluir, entre otros tipos de análisis, la tasa de filtrado de negativos/positivos falsos, las características del correo basura y las tendencias de éste.

3.2.14 estadísticas sobre correo basura: Los datos agregados sobre correo basura representan el alcance del correo basura en determinadas condiciones restrictivas, por ejemplo, el intervalo temporal en un dominio anticorreo basura. Deberían incluir la cantidad de mensajes de correo basura en los dominios, a la entrada o la salida de los mismos, la proporción de distintos tipos de correo electrónico basura y la lista de remitentes de correo basura, entre otros datos estadísticos sobre correo basura.

3.2.15 correo basura sospechoso: El mensaje móvil no determinado sospechoso de ser correo basura.

3.2.16 informe del usuario: Queja de un abonado que recibe correo basura en su mensajería móvil. Por lo general, el informe puede comprender la hora de recepción del correo basura, el número internacional de abonado móvil de la red digital de servicios integrados internacional / red telefónica pública conmutada (RDSI/RTPC) del remitente y del receptor, etc. Este informe contiene información sobre mensajes marcados incorrectamente como correo basura de mensajería móvil, o los no marcados cuando deberían haberse marcado, por ejemplo, positivos falsos o negativos falsos.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

AMgmt Función de gestión anticorreo basura en la mensajería móvil (*anti-spam mobile messaging management function*)

Amon	Función de vigilancia anticorreo basura en la mensajería móvil (*anti-spam mobile messaging monitoring function*)
AO	Aplicación originada (*application originated*)
APr	Función de procesado anticorreo basura en la mensajería móvil (*anti-spam mobile messaging processing function*)
GGSN	Nodo de soporte de GPRS pasarela (*gateway GPRS supporting node*)
GPRS	Servicio general de radiocomunicaciones por paquetes (*general packet radio service*)
HPLMN	Red móvil terrestre pública de origen (*home public land mobile network*)
HTTP	Protocolo de transferencia de hipertexto (*hypertext transfer protocol*)
ISDN	Red digital de servicios integrados
MAP	Parte aplicación móvil (*mobile application part*)
MMS	Servicio de mensajes multimedios (*multimedia message service*)
MMSC	Centro de servicio de mensajes multimedios (*multimedia message service centre*)
MNO	Operador de red móvil (*mobile network operator*)
MO	Orientado a móvil (*mobile oriented*)
MSC	Centro de conmutación de servicios móviles (*short message service*)
MSISDN	Número internacional RDSI/RTPC de abonado móvil (*mobile subscriber international ISDN/PSTN number*)
MT	Terminado en móvil (*mobile terminated*)
PSTN	Red telefónica pública conmutada *eer*)
SMPP	Mensaje corto entre pares (*short message peer-to-p*
SMS	Servicio de mensajes cortos (*short message service*)
SMSC	Centro de servicio de mensajes cortos (*short message service centre*)
UICC	Tarjeta de circuito integrado universal (*universal integrated circuit card*)
VPLMN	Red móvil terrestre pública visitada (*visited public land mobile network*)
WAP	Protocolo de aplicación inalámbrica (*wireless application protocol*)

5 Convenios

Ninguno.

6 Visión general de la mensajería móvil anticorreo basura

Como se muestra en la Figura 6-1, el correo basura en servicio de mensajes cortos (SMS) puede generarse principalmente de dos formas. La primera de ellas consiste en el envío de mensajes cortos masivos punto a punto mediante herramientas de correo basura utilizadas por los remitentes de dicho correo, con muchas tarjetas de circuito integrado universales. La segunda consiste en la utilización, por parte de los remitentes de correo basura, de los servicios de envío de mensajes masivos ofrecidos por proveedores de servicios a través de las interfaces de pasarela de mensajes cortos del operador. Dado que los operadores no cuentan con mecanismos eficaces de supervisión técnica y de gestión de dicha interfaz de pasarela, esta puede ser utilizada fácilmente por los remitentes de correo basura.

Dependiendo del sentido de reenvío de los mensajes, los remitentes de correo basura pueden utilizar dos procedimientos para generar correo basura en el servicio de mensajes cortos, a saber, el

procedimiento orientado a móvil (MO)/de aplicación originada (AO), o el procedimiento terminado en móvil (MT). Con arreglo al procedimiento MO, el correo basura generado por las herramientas destinadas a tal efecto se envía al centro de servicio de mensajes cortos (SMSC) mediante las entidades conexas de la red del remitente. Con arreglo al procedimiento AO, el mensaje corto enviado como correo basura a través de la pasarela de mensajes cortos del operador se reenvía al SMSC. Posteriormente, el SMSC interroga al centro al Centro de conmutación de servicios móviles (MSC) y le reenvía el mensaje. Por último, el mensaje corto se reenvía al receptor por medio de la red visitada del MSC con arreglo al procedimiento MT.

Con el permiso del abonado y en el marco de la normativa administrativa, los operadores de red móvil (MNO) están facultados para mitigar el correo basura en la mensajería mediante entidades de filtrado. El proceso anticorreo basura deberá regirse minuciosamente por las cláusulas legislativas en vigor para proteger la privacidad de los abonados.

Se acepta habitualmente el despliegue de entidades de filtrado anticorreo basura con arreglo al procedimiento MO/AO, el procedimiento MT, o ambos. En el caso de filtrado de correo basura mediante el procedimiento MO las entidades de filtrado anticorreo basura reciben mensajes cortos del SMSC. Para que el filtrado de correo basura sea eficaz en la red de los receptores, también es necesario que haya comunicación entre el MSC y la entidad de filtrado anticorreo basura.

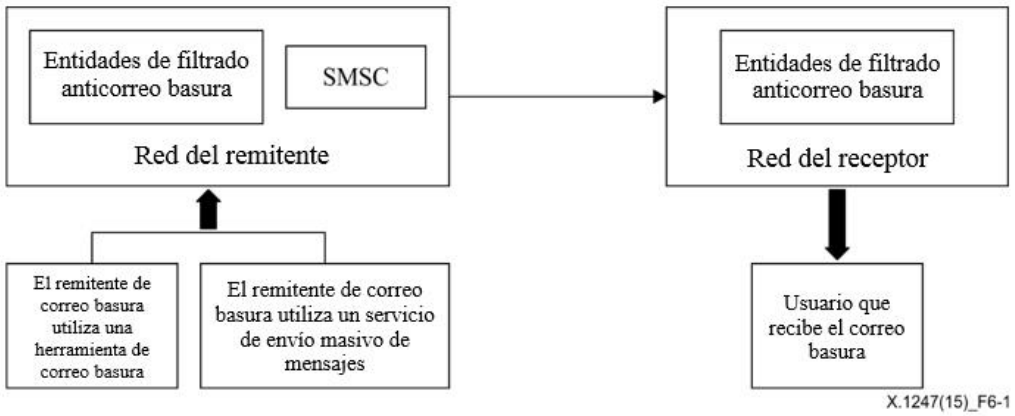

Figura 6-1 – Correo basura por SMS en la red móvil

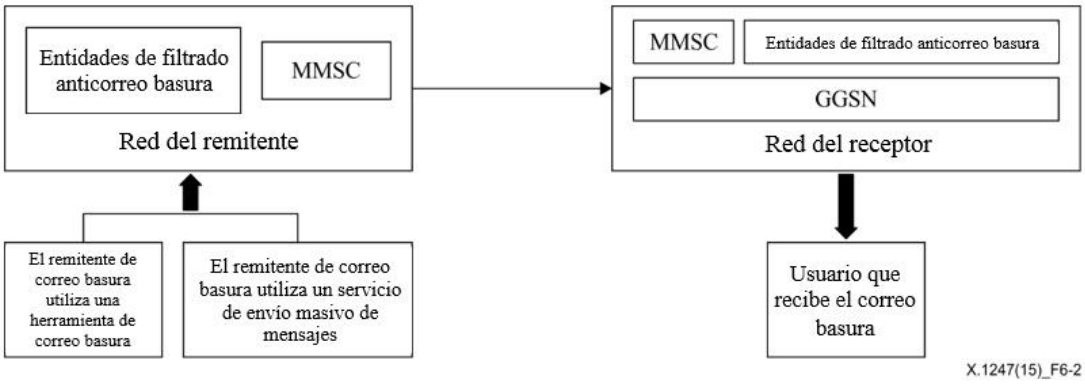

Figura 6-2 – Correo basura por MMS en la red móvil

Como se muestra en la Figura 6-2, el procedimiento de mensajería por el servicio de mensajes multimedios es similar al procedimiento relativo al SMS, salvo en que en lugar del MSC se utiliza el nodo de soporte de GPRS pasarela (GGSN), y en lugar del SMSC se utiliza el Centro de servicio de mensajes multimedios (MMSC). El mensaje MMS se reenvía al MMSC de la red del receptor, y posteriormente el SMSC enviará el mensaje SMS al receptor. El receptor descargará el mensaje MMS

del MMSC. Por esa razón, las entidades antifiltrado MMS pueden desplegarse de manera contigua al MMSC, por lo que es indiferente desplegar dichas entidades en el extremo del remitente o en el del receptor.

7 Estructura de las funciones anticorreo basura en la mensajería móvil

La estructura de las funciones anticorreo basura en la mensajería móvil comprende la función de gestión anticorreo basura en la mensajería móvil (AMgmt), la función de vigilancia anticorreo basura en la mensajería móvil (AMon), la función de procesado anticorreo basura en la mensajería móvil (APr) y los clientes de mensajería móvil. Estas funciones definen el dominio anticorreo basura en la mensajería móvil.

Se recomienda asociar varios dominios anticorreo basura en la mensajería móvil, de forma que se coordinen entre sí con respecto a reglas o políticas definidas en los acuerdos pertinentes.

Estas funciones pueden comunicarse entre sí mediante protocolos de mensajería existentes; sus características se describen a continuación.

7.1 Estructura general

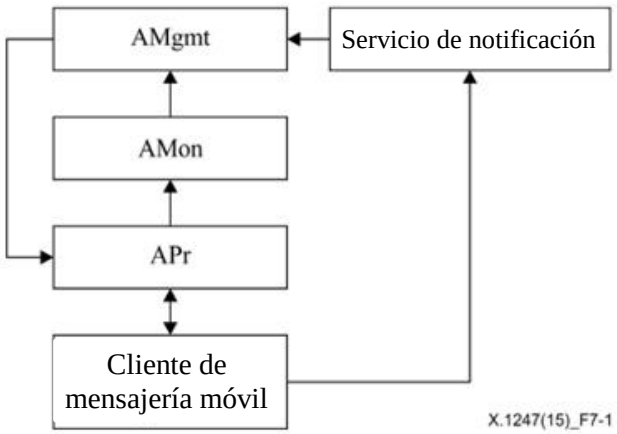

Figura 7-1 – Estructura general

La AMgmt recibe información estadística sobre correo basura de la Amon y actualiza las reglas de filtrado en su dominio. La AMgmt también comparte información sobre correo basura con el servicio de notificación y otras AMgmts.

La Amon recibe correo basura sospechoso por mensajería móvil de la APr, mediante señuelos o plataformas similares, y verifica si se trata de correo basura. La AMon también proporciona el análisis y la información estadística sobre correo basura a la AMgmt tras agregar y analizar los datos relativos a dicho correo basura.

La APr, tras aplicar las reglas a los mensajes móviles, decidirá si los envía marcados como correo basura, o los bloquea con arreglo a las políticas y los resultados de filtrado, a tenor de los permisos del usuario. La APr recibe las reglas de filtrado de la AMgmt y la información del usuario por medio de los clientes de mensajería móvil. Se recomienda desplegar varias plataformas, por ejemplo señuelos en la APr, que permitan acumular el correo basura sospechoso

El cliente de mensajería móvil contribuye al proceso anticorreo basura en la mensajería móvil mediante el envío a la APr de la información de usuario en la que se especifica que el mensaje móvil recibido marcado como correo basura es incorrecto, y el envío del informe sobre correo basura al servicio de notificación.

El servicio de notificación permite recibir y agregar el informe sobre correo basura del abonado con arreglo al permiso, la normativa y la legislación nacional del usuario. También permite compartir datos de notificación de los usuarios entre varios dominios anticorreo basura. El servicio de notificación puede prestarlo, en particular, la administración normativa, una empresa de seguridad o un MNO. Los acuerdos entre dominios permiten a los dominios anticorreo basura en la mensajería móvil compartir información personalizada sobre correo basura.

7.2 Modelo de referencia

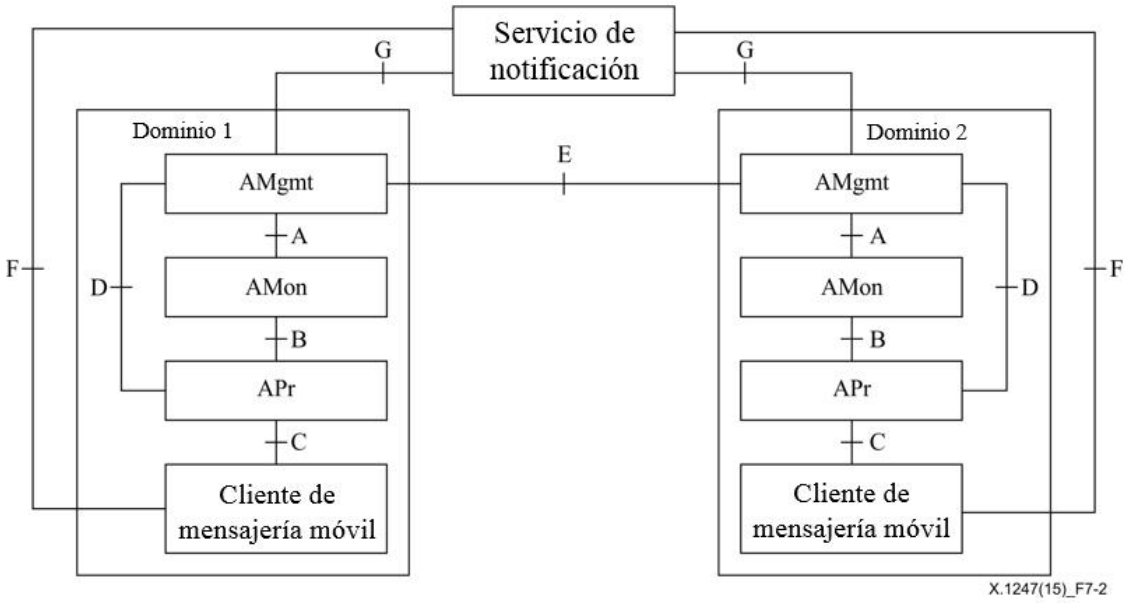

Figura 7-2 – Modelo de referencia

La Interfaz A es una interfaz lógica entre la AMgmt y la AMon. Se utiliza para transmitir los informes analíticos y los datos estadísticos del correo basura.

La Interfaz B es una interfaz lógica entre la AMon y la APr. Se utiliza para transmitir el correo basura sospechoso recibido por el señuelo y la información del usuario en la que se especifica que el mensaje móvil recibido marcado como correo basura es incorrecto, respecto del cliente de mensajería móvil.

La Interfaz C es una interfaz lógica entre la APr y el cliente de mensajería móvil. La utiliza el cliente de mensajería móvil para informar a la APr de la recepción de un mensaje marcado erróneamente como correo basura por el MNO. La Interfaz C también se utiliza para enviar mensajes de la APr al cliente de mensajería móvil. En función del tipo de cliente de mensajería móvil, la Interfaz C deberá soportar diversos protocolos, por ejemplo, la Parte aplicación móvil y el Protocolo de aplicación inalámbrica (MAP/WAP), el Protocolo de transferencia de hipertexto (HTTP) el Mensaje corto entre pares (SMPP).

La Interfaz D es una interfaz lógica entre la AMgmt y la APr. Se utiliza para transmitir las reglas de filtrado.

La Interfaz E es una interfaz lógica entre las AMgmt y otros dominios. Se utiliza para intercambiar datos sobre correo basura entre varios dominios anticorreo basura de mensajería móvil.

La Interfaz F es una interfaz lógica entre el cliente de mensajería móvil y el servicio de notificación. La utiliza el cliente de mensajería móvil para enviar un informe de usuario al servicio de notificación con el consentimiento explícito del usuario. Soporta varios protocolos, entre ellos la Parte aplicación móvil y el Protocolo de aplicación inalámbrica (MAP/WAP), el Protocolo de transferencia de hipertexto (HTTP) el Mensaje corto entre pares (SMPP).

La Interfaz G es una interfaz lógica entre la AMgmt y el servicio de notificación. Se utiliza para la transmisión de informes sobre correo basura del servicio de notificación a la AMgmt.

En este modelo de referencia, las interfaces A a D son interfaces intra-dominio, y las interfaces E a G son interfaces entre dominios.

7.3 Funciones de los componentes

7.3.1 Clientes de mensajería móvil

Las funciones del cliente de mensajería móvil comprenden:

- provisión de mecanismos para ayudar a los usuarios a enviar sus informes al servicio de notificación;
- provisión de mecanismos para ayudar a los usuarios a informar a la APr de mensajes recibidos marcados erróneamente como correo basura;
- filtrado de mensajes con arreglo a reglas específicas de filtrado mediante aplicaciones de seguridad.

7.3.2 APr

Las funciones de la APr comprenden:

- aplicación de las reglas anticorreo basura de la AMgmt y la decisión relativa al envío de mensajes marcados como sospechosos o su bloqueo con arreglo a las políticas y los resultados de filtrado pertinentes;
- recepción de la información de usuario de un cliente de mensajería móvil en la que se reclama que el mensaje móvil recibido marcado como correo basura, en realidad no lo es;
- recepción del correo basura sospechoso por señuelos u otras plataformas similares;
- envío de la información de usuario y del correo basura sospechoso recibido por el señuelo a la AMon.

7.3.3 AMon

Las funciones de la AMon comprenden:

- agregación del correo basura sospechoso que fue recibido por el señuelo de la APr, y del informe de usuario del servicio de notificación;
- validación del correo basura sospechoso de la APr;
- análisis de los datos de correo basura agregados para determinar las características de nuevo correo basura;
- informe de los datos estadísticos y del análisis del correo basura a la AMgmt.

7.3.4 AMgmt

Las funciones de la AMgmt comprenden:

- recepción de los datos estadísticos sobre correo basura y del informe analítico de la AMon;
- análisis de los datos notificados de la AMon para generar reglas de filtrado;
- envío a la APr de las reglas de filtrado que se aplicarán a los clientes de mensajería móvil;
- comunicación con el resto de AMgmt para intercambiar y compartir datos sobre correo basura, entre ellos su cantidad, su origen y sus características, o una nueva lista de remitentes de correo basura;
- recepción de los informes de usuario del servicio de notificación, en particular en relación con el principal remitente de correo basura y las estadísticas y tendencias conexas. La información de usuario puede personalizarse e incluye datos procesados del informe de

usuario, con arreglo al acuerdo con el servicio de notificación en el ámbito permitido por la normativa y la legislación nacional;

- concesión de capacidad para establecer reglas de filtrado específicas para cada usuario al abonado, y envío de dichas reglas a la APr tras verificar su validez.

7.3.5 Servicio de notificación

Las funciones del servicio de notificación comprenden:

- recepción de informes del usuario y comprobación si se trata de correo basura;
- almacenamiento y análisis del correo basura para determinar sus características de forma exclusiva, y no con arreglo a su contenido, a fin de proteger la privacidad;
- provisión de datos de usuario para que el MNO pueda valorar el alcance del correo basura en su red, o del que se transmite hacia o desde las redes de otros operadores, a fin de actuar sobre el mensaje de correo basura únicamente, sin que ello repercuta en los usuarios ni en el contenido.

8 Tecnologías de mensajería móvil anticorreo basura

Las tecnologías presentadas en la presenta cláusula se aplican a la estructura anticorreo electrónico especificadamente anteriormente y deberán utilizarse con precaución a fin de observar las reglamentaciones y legislaciones nacionales en vigor con el permiso del usuario. El objetivo es proteger la privacidad de los abonados.

8.1 Mecanismos de información de usuario

Los mecanismos de información de usuario permiten a los abonados facilitar al sistema de filtrado información sobre sus opiniones sobre el resultado del filtrado del correo basura. Se recomienda utilizar un servicio de notificación e información de usuario para mejorar el resultado del filtrado del MNO.

Un servicio de notificación consiste en un sistema que recibe los informes de los usuarios relativos a la recepción de mensajes de correo basura, puesto en marcha, en particular, por gobiernos u operadores. El servicio de notificación puede ser una línea de atención al cliente, un sitio web o un centro de notificación de mensajes cortos de correo basura, con objeto de que el MNO pueda recibir dichos mensajes y adaptar las reglas de filtrado. Por lo general, el registro del mensaje corto de correo basura notificado deberá incluir el valor de troceo del mensaje de correo basura, la hora de recepción y el MSISDN del remitente, entre otra información. En función de la política de que se trate y si el usuario ha otorgado su consentimiento, el MNO podrá bloquear el mensaje de correo basura y ponerlo en cuarentena a disposición de los receptores, lo que conlleva que esos mensajes puedan enviarse con marca o registrarse en un sitio web específico. Ello permite a los receptores visualizar los "posibles mensajes de correo basura" marcados como correo basura sospechoso, y les brinda la posibilidad de facilitar información si consideran que la decisión sobre un mensaje específico es incorrecta o ha dado lugar a un "positivo falso". No toda la información de usuario es fiable. Los receptores pueden cometer errores o tener otros motivos para notificar mensajes como correo basura. El reconocimiento del correo basura ha de verificarse manualmente antes de usarse para generar datos de exclusividad o reglas de filtrado. Puede implantarse un sistema de calificación de la confianza de un informe para distinguir de forma automática la información correcta frente a la errónea o malintencionada.

8.2 Señuelos

Un señuelo de número telefónico es una cuenta que se crea como "trampa" para detectar, liberar o contrarrestar el uso no autorizado de mensajes móviles. Por lo general, es una cuenta utilizada o creada para que la detecten los remitentes de correo basura, en particular números de teléfono inactivos o no existentes. De este modo, todos los mensajes que sean distintos de los previstos pueden

procesarse como correo basura sospechoso y podría ser pertinente analizar su contenido. Puesto que los números de teléfono pueden reasignarse rápidamente o se teclean erróneamente con frecuencia, los señuelos de número de teléfono recibirán muchos mensajes accidentales que no son correo basura. Será necesario verificar ese correo basura sospechoso para filtrar esos datos no deseados antes de analizar el correo basura sospechoso para generalizar sus características.

La información de usuario puede recibirse con retardo, dado que pueden pasar varios minutos o días antes de que un mensaje no deseado sea notificado por el receptor. Sin embargo, las trampas de señuelos pueden detectar mensajes no deseados tan pronto como se transmiten.

8.3 Método de identificación del MNO

Salvo medidas relativas a la información de usuario y los señuelos, el MNO puede llevar a cabo otras actividades para identificar el correo basura antes de enviarlo a los receptores. Dichos mensajes se bloquearán o enviarán con arreglo a distintas políticas con una marca especial o como sospechosos. Estos métodos de identificación pueden depender de las características del correo basura o de su patrón de envío.

- Lista blanca/lista negra del número internacional de abonado móvil del remitente de la red digital de servicios integrados internacional/red telefónica pública conmutada (RDSI/RTPC) (MSISDN).

  El MSISDN constituye la información fundamental para distinguir un mensaje de un abonado o un remitente de correo basura. Las listas negras/blancas utilizan el MSISDN del remitente para anular o aceptar mensajes. Si bien los operadores móviles pueden bloquear los mensajes de los remitentes de correo basura bien conocidos o reconocidos, los abonados pueden definir sus propias listas negras/blancas para bloquear o aceptar mensajes de remitentes específicos.

- Reconocimiento aproximado

  Con objeto de evitar el filtrado de correo basura, los remitentes de correo basura adoptan medidas de confusión. Por ejemplo, incluyen de forma arbitraria en el texto del mensaje caracteres específicos, por ejemplo "*","^", etc. Sustituyen algunos caracteres por otros similares, por ejemplo, "porno" `puede sustituirse por "p0rno". Las imágenes pueden ampliarse o girarse. La función del reconocimiento aproximado es reconocer esta elusión y filtrarla, siempre y cuando ello esté permitido.

- Frecuencia de envío

  Con objeto de difundir el correo basura rápidamente, los remitentes del mismo pueden enviar mensajes a numerosos receptores en un corto período de tiempo. Los remitentes de correo basura envían sus mensajes a una velocidad mucho mayor que la de un remitente normal, de forma que el intervalo de tiempo entre dos mensajes sea menor. Si la frecuencia de envío de un usuario supera un umbral establecido previamente, se identificará a ese usuario como un remitente de correo basura altamente sospechoso.

- Tasa de envío satisfactorio de mensajes

  Dado que los mensajes de correo basura se envían a receptores desconocidos, el remitente de correo basura escoge a los destinatarios de forma aleatoria. Por consiguiente, es habitual que utilicen números de teléfono no existentes. La tasa de envío satisfactorio de mensajes de correo basura es sustancialmente inferior a la del envío de mensajes móviles.

- Registro de llamadas del remitente

  El registro de llamadas del usuario puede ayudar al operador a analizar el patrón de envío. El registro debe incluir los números de teléfono del remitente y del receptor, así como la hora de envío. Si el mensaje se envía a muchos abonados y obtiene una baja tasa de respuesta, el remitente podrá considerarse un remitente de correo basura sospechoso. Los remitentes de correo basura no utilizan habitualmente otros servicios (por ejemplo, llamadas de voz) del operador, además del servicio de mensajería.

8.4 Mejora adicional

- Configuración de reglas específicas para cada usuario:

  Los mecanismos de configuración de reglas específicas para cada usuario permiten a los receptores definir el tipo de mensajes que el receptor no desea recibir e informar de ello al sistema de filtrado. El filtrado de mensajes con arreglo a determinadas reglas específicas para cada usuario puede llevarse a cabo a través del MNO o mediante un soporte lógico instalado por los receptores.

- Re-encaminamiento a la Red móvil terrestre pública de origen del receptor (HPLMN).

  Los operadores pueden aplicar distintos procesos anticorreo basura para los clientes que se encuentren en una zona de itinerancia fuera de la HPLMN. El proceso de re-encaminamiento de mensajes a la HPLMN es facultativo, por lo que los receptores que se encuentren en una zona de itinerancia podrían recibir mensajes sin que se aplique un filtrado anticorreo basura. En consecuencia, los mensajes enviados a los clientes en zona de itinerancia han de reenviarse a las entidades de filtrado anticorreo basura en la HPLMN, en lugar de basarse en la red visitada. Antes de que los mensajes lleguen a la red móvil terrestre pública visitada (VPLMN), la HPLMN del receptor los deberá recibir y filtrar con arreglo a los procedimientos anticorreo basura pertinentes.

9 Relación entre dominios anticorreo basura

La eficiencia de las medidas anticorreo basura en un dominio anticorreo basura está condicionada desde un punto de vista técnico y económico. Es necesaria la existencia de interconexiones e interfuncionamiento entre MNO, y es muy importante que se establezcan mecanismos de colaboración entre sus dominios anticorreo basura. Dichos mecanismos pueden contribuir a mejorar la eficiencia y mejorar el rendimiento de sus sistemas anticorreo basura.

Existen dos tipos de relaciones entre dominios anticorreo basura, a saber, una relación fiable y una relación no fiable (Figura 9-1). La relación por defecto entre dominios anticorreo basura debe ser una relación no fiable, en virtud de la cual se filtran todos los mensajes de las partes homólogas no fiables. La relación fiable puede establecerse en el marco de acuerdos de cooperación entre dominios anticorreo basura homólogos; en este tipo de relación, los operadores no filtran, si lo desean, los mensajes de las partes homologas fiables con arreglo a sus políticas y reglas de filtrado.

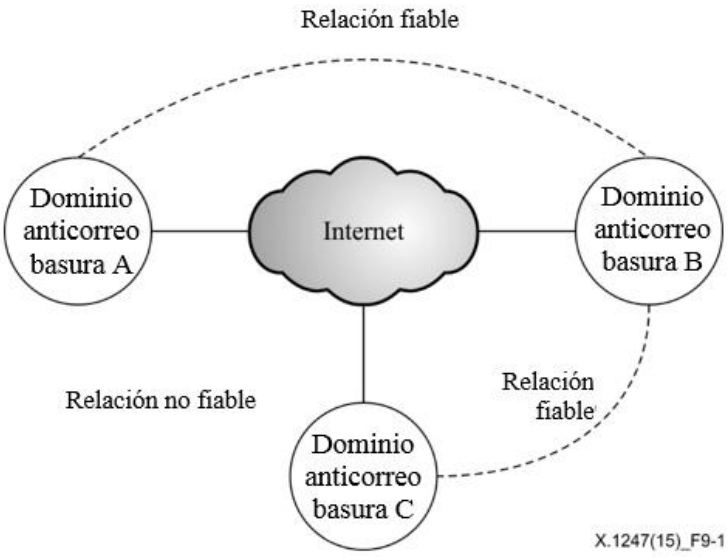

Figura 9-1 – Relaciones fiable y no fiable

La relación fiable no es transitiva. Por ejemplo, si el dominio A tiene una relación fiable con el dominio B y el dominio B tiene una relación fiable con el dominio C, el dominio A no tendrá necesariamente una relación fiable con el dominio C, a menos que hayan negociado y establecido directamente una relación de confianza. La relación de confianza es bidireccional, es decir, las partes fiables se tratan mutuamente por igual.

Una vez que se ha establecido una relación fiable, se recomiendan los siguientes mecanismos de coordinación:

- Compartición de datos sobre correo basura:

  Determinados datos sobre correo basura se comparten mediante la conexión con la AMgmt. La información compartida puede incluir listas negras, palabras clave, informes de quejas y características de nuevos correos basura. El objetivo de esta información se examina durante el proceso de establecimiento de la relación fiable. La compartición de los datos de correo basura requerirá el consentimiento explícito del usuario del dispositivo móvil y deberá ajustarse a las normativas y legislaciones nacionales.

- Autenticación del origen del mensaje:

  Se considerará auténtico el mensaje de una parte homóloga fiable únicamente si se autentica el origen de dicho mensaje.

- Filtrado no necesario:

  Los mensajes de un dominio fiable pueden enviarse directamente al receptor para evitar que se procesen dichos mensajes por duplicado.

- Informe sobre quejas de usuario y correo basura sospechoso:

  Si los informes sobre correo basura y el correo basura sospechoso se reciben en mensajes de partes homólogas fiables, deberán enviarse a las partes homólogas para que mejoren sus reglas de filtrado con arreglo a las normativas y legislaciones nacionales en vigor.

Con objeto de satisfacer todos los mecanismos de coordinación, la APr y la AMon deberán llevar a cabo varios procedimientos para procesar los mensajes móviles. La APr decidirá si filtra el mensaje o no. En función del acuerdo establecido, la AMon reenviará/bloqueará el mensaje o enviará información a las partes homólogas fiables. En las Figuras 9-2 y 9-3 se describen los flujos de funcionamiento de la APr y la AMon.

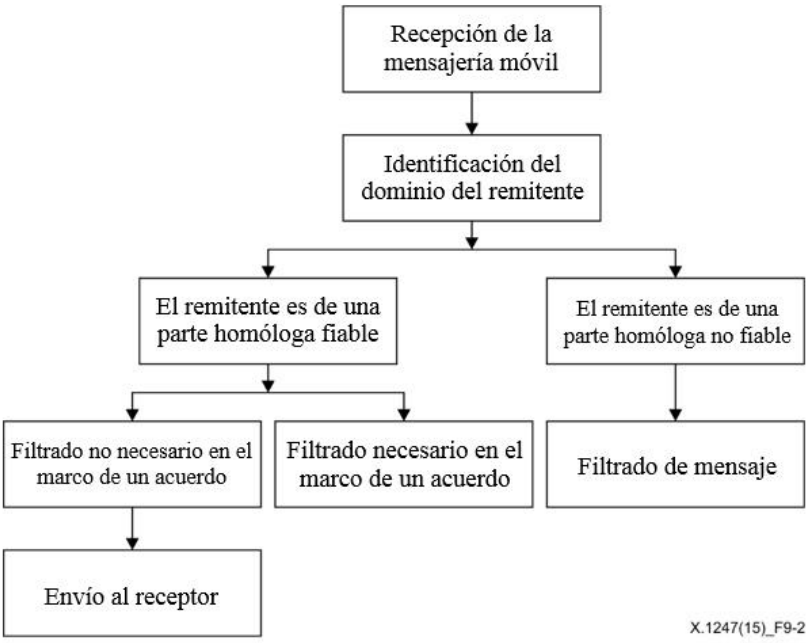

Figura 9-2 – Diagrama de flujo del procesamiento de la mensajería móvil en la APr

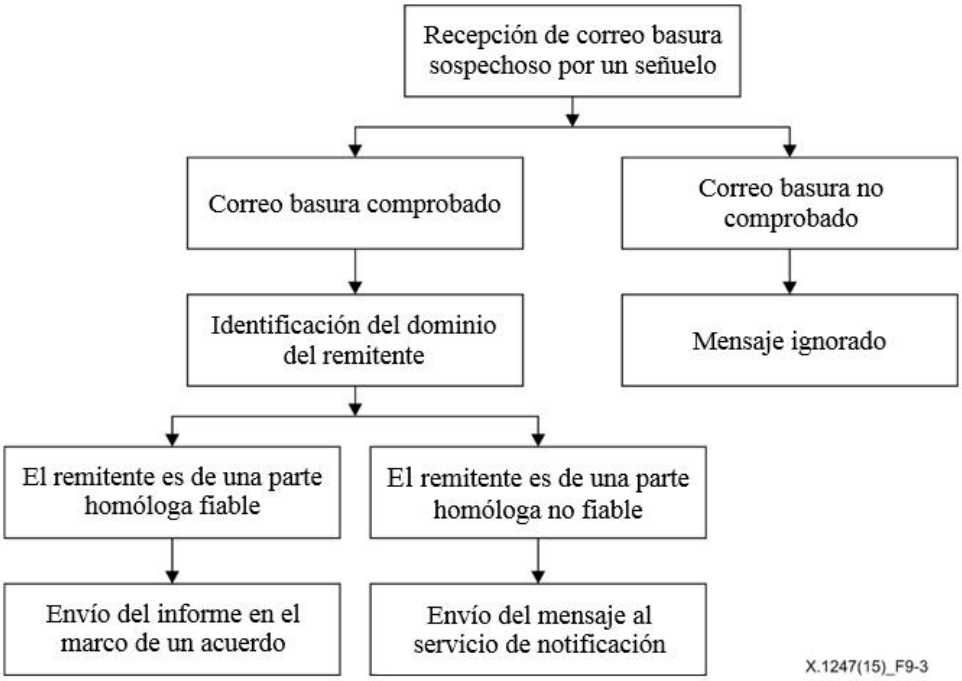

Figura 9-3 – Diagrama de flujo del procesamiento de la mensajería móvil en la Amon

10 Procesado anticorreo basura en la mensajería móvil

En el proceso anticorreo basura en la mensajería móvil hay que introducir un mecanismo adaptativo que se ajuste a los nuevos tipos de correo basura que surgen constantemente y a sus variaciones. Por lo general, el proceso anticorreo basura consiste en los ocho procedimientos que se muestran en la Figura 10-1. Dichos procedimientos constituyen un sistema adaptativo que contribuye a optimizar la eficacia del sistema.

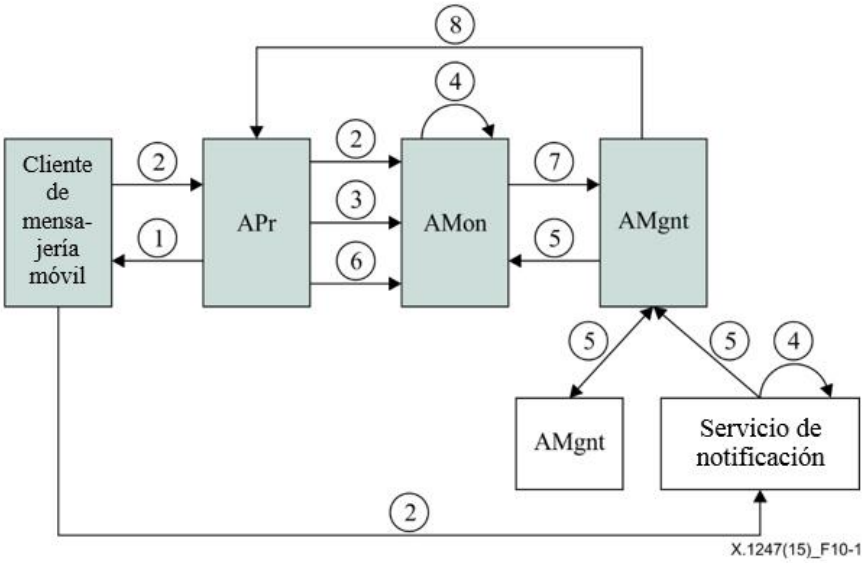

Figura 10-1 – Procedimientos de tratamiento anticorreo basura

Procedimiento 1: Filtrado de mensajes

Sobre la base de políticas y reglas de filtrado pertinentes, la APr filtra o marca específicamente los mensajes de correo basura antes de enviarlos al receptor. Estas reglas de filtrado pueden establecerse en los operadores o mediante la personalización del usuario.

Procedimiento 2: Envío de la información de usuario

El cliente de mensajería móvil envía las quejas del usuario al servicio de notificación para informar del correo basura no filtrado y transmitir la información del usuario a la AMon a fin de marcar los mensajes recibidos erróneamente como correo basura. Ello ayudará a los operadores a mejorar sus reglas de filtrado.

Procedimiento 3: Reenvío de correo basura sospechoso

La APr enviará el correo basura sospechoso acumulado por el señuelo a la AMon para su posterior verificación.

Procedimiento 4: Verificación del correo basura

La AMon verifica el correo basura al tiempo que los servicios de notificación tratan el informe del usuario sobre correo basura. Este procedimiento es complejo y se basa en una intervención manual, conforme a las normativas y legislaciones nacionales en vigor. La verificación del correo basura debe llevarse a cabo de forma exclusiva, sobre la base de datos de troceado, en lugar de usar el contenido de la mensajería. A tal efecto puede utilizarse información adicional, por ejemplo la reputación del remitente de correo basura y del remitente de la información, por lo cual se considera fiable la información del usuario.

Procedimiento 5: Compartición de información

La AMgmt intercambia datos de correo basura con las partes homólogas fiables y recibe datos analíticos personalizados sobre correo basura del servicio de notificación. Con arreglo al consenso de la negociación, los datos pueden incluir información estadística, listas de remitentes de correo basura, quejas y correo basura con nuevas características. Estos datos de correo basura se procesarán pormenorizadamente para garantizar que no se incluye contenido del usuario.

Procedimiento 6: Comprobación de la calidad de funcionamiento del sistema

La AMon también comprobará la calidad de funcionamiento del sistema de filtrado de correo basura. Recibe datos de la APr para generar informes sobre dicha calidad de funcionamiento y analizarlos. Dichos informes pueden incluir datos en tiempo real, la tasa de correo basura o de negativos falsos, etc.

Procedimiento 7: Análisis del correo basura

Los datos de correo basura confirmados por el servicio de notificación, las partes homólogas fiables y la Amon se agregarán y almacenarán teniendo en cuenta las normativas y legislaciones naciones en vigor. La AMon puede analizar periódicamente esos datos para determinar nuevos patrones y características del correo basura. Ello contribuirá a mejorar las reglas de filtrado y la calidad de funcionamiento del sistema. Por último, servirá para generar datos estadísticos y elaborar informes analíticos sobre correo basura que se trasmitirán a la AMgmt.

Procedimiento 8: Ajuste de las medidas de protección

Con arreglo a los datos estadísticos y al informe analítico de la AMon sobre correo basura, la AMgmt evaluará la calidad de funcionamiento del sistema de filtrado del correo basura para introducir posibles mejoras. Sobre la base del resultado de la evaluación, podrán ajustarse las medidas y políticas y modificarse los mecanismos de colaboración con otros dominios. Se adoptarán las medidas pertinentes, entre ellas el establecimiento o la finalización de relaciones fiables y la distribución de nuevas reglas y políticas de filtrado a las APr.

Bibliografía

[b-UIT-T X.1240] Recomendación UIT-T X.1240 (2008), *Tecnologías utilizadas contra el correo basura*.

[b-UIT-T X.1242] Recomendación UIT-T X.1242 (2009), *Sistema de filtrado de correo basura en el servicio de mensajes cortos (SMS) basado en reglas especificadas por el usuario.*

[Informe b-M3AWG] M3AAWG, *Mobile Messaging Best Practices for Service Providers*, actualización de agosto de 2015.
https://www.m3aawg.org/sites/default/files/M3AAWG-Mobile-Messaging-Best-Practices-Service-Providers-2015-08.pdf

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
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	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás 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	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
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, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2020