Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1234

(01/2022)

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

Seguridad en el ciberespacio – Lucha contra el correo basura

Directrices para la lucha contra el correo basura en el servicio de mensajería multimedios

Recomendación UIT-T X.1234

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 (1)	
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 (1)	X.1140–X.1149
Seguridad de las aplicaciones	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 (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1319
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Correo certificado	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350–X.1369
Seguridad en los sistemas de transporte inteligente (STI)	X.1370–X.1399
Seguridad de tecnología de libro mayor distribuido (DLT)	X.1400–X.1429
Seguridad de las aplicaciones (2)	X.1450–X.1459
Seguridad de la web (2)	X.1470–X.1489
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
Ciberdefensa	X.1590–X.1599
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
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
Protección de los datos	X.1770–X.1789
SEGURIDAD DE IMT-2020	X.1800–X.1819

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

Recomendación UIT-T X.1234

Directrices para la lucha contra el correo basura en el servicio de mensajería multimedios

Resumen

En la Recomendación UIT-T X.1234 se describen directrices para la lucha contra el correo basura en el servicio de mensajería multimedios (MMS). Se analizan los casos típicos, las características y los métodos de reconocimiento del correo basura MMS, y se ofrece un marco técnico, flujos de trabajo y algunas tecnologías clave para el reconocimiento del correo basura MMS con el fin de ayudar a los proveedores y a los usuarios del servicio MMS a luchar contra el correo basura.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1234	07-01-2022	17	11.1002/1000/14796

Palabras clave

Correo basura del servicio de mensajería multimedios, marco técnico, servicio de mensajería multimedios.

* 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, https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11830&lang=es.

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 la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

El servicio de mensajería multimedios (MMS) es una forma normalizada de enviar mensajes que incluyen contenido multimedios a un teléfono móvil, o desde él, por una red celular. Los usuarios y los proveedores pueden referirse a esos mensajes como una foto, un vídeo, sonido y animación, etc. Con el desarrollo de las tecnologías de telecomunicaciones y la popularidad de los teléfonos inteligentes, el MMS se han convertido en una vía popular de enviar mensajes, especialmente entre la gente joven y las empresas de los medios de comunicación, que los utilizan comercialmente como método para entregar noticias y contenidos de entretenimiento. El MMS ofrece un contacto social práctico y mensajes vistosos, pero también se convierten en una vía por la que los emisores de correo basura envían sus mensajes basura MMS. Este correo basura MMS, que incluye anuncios no deseados, información fraudulenta y virus, se está convirtiendo en un problema generalizado que provoca pérdidas económicas significativas a los operadores de telecomunicaciones, los proveedores de servicio y los usuarios.

Por lo tanto, luchar de manera eficaz contra los mensajes basura del servicio MMS se ha convertido en un aspecto importante de la lucha contra las tecnologías del correo basura.

Recomendación UIT-T X.1234

Directrices para la lucha contra el correo basura en el servicio de mensajería multimedios

1 Alcance

En esta Recomendación se propone un marco técnico para la lucha contra el correo basura MMS con el fin de conseguir gestionar y controlar los mensajes basura MMS. En este marco técnico se especifican componentes funcionales, flujos de trabajo y algunas tecnologías clave para el reconocimiento del correo basura MMS. Además, en esta Recomendación, se incluyen escenarios típicos de correo basura MMS, con un análisis de los diferentes tipos y las características generales de dicho correo basura.

Conviene señalar que todas las operaciones descritas en esta Recomendación necesitan la autorización de los usuarios y las reglamentaciones administrativas. Todos los procesos deberán regirse minuciosamente según la legislación aplicable para evitar la violación de la privacidad de los usuarios.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

[UIT-T X.1231] Recomendación UIT-T X.1231(2008), *Estrategias técnicas de lucha contra el correo basura.*

[UIT-T X.1247] Recomendación UIT-T X.1247 (2016), UIT-T X.1247, *Marco técnico para luchar contra el correo basura en la mensajería móvil*.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 servicio de mensajería multimedios (MMS) [UIT-T X.1231]: El servicio de mensajería multimedios es un tipo de servicio de mensajería posterior al servicio de mensajes cortos (SMS) mediante el cual se pueden transferir diversos mensajes multimedios que contienen texto, gráficos, audio, vídeo, etc., a través de redes móviles, inalámbricas o fijas.

3.1.2 correo basura en el servicio de mensajería multimedios (MMS) [UIT-T X.1247]: Correo basura enviado mediante el MMS.

3.1.3 emisor de correo basura (correo basura) [UIT-T X.1231]: Entidad o persona que crea y envía correo basura.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se define el término siguiente:

3.2.1 funciones de identificación del correo basura MMS (MMSSIF): Sistema contra el correo basura MMS que es independiente de un Centro de servicio de mensajes multimedios (MMSC), que incluye los siguientes componentes funcionales: función de monitorización, función de adquisición de datos, función de preprocesamiento, función de reconocimiento, función de verificación, función de eliminación y función de gestión del sistema.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

ASR	Reconocimiento automático de la voz (*automatic speech recognition*)
MMS	Servicio de mensajes multimedios (*multimedia message service*)
MMSC	Centro de servicio de mensajes multimedios (*multimedia message service centre*)
MMSSIF	Función de identificación del correo basura en el servicio de mensajería multimedios (*multimedia messaging service correo basura identification function*)
SMS	Servicio de mensajes cortos (*short message service*)
UICC	Tarjeta de circuito integrado universal (*universal integrated circuit card*)
URL	Localizador uniforme de recursos (*uniform resource location*)

5 Convenios

En la presente Recomendación se utilizan los siguientes convenios:

La expresión "**se recomienda**" indica que se trata de un requisito recomendado pero que no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

La expresión "**se tiene la opción de**" u "**opcionalmente**" indica que el requisito se permite, sin que ello signifique que se recomiende.

En el cuerpo de la presente Recomndación, ocasionalmente puede aparece la palabra "**puede**", en cuyo caso deben interpretarse como "**es capaz de**".

6 Visión general

El servicio de mensajería multimedios (MMS) es un tipo de servicio de mensajería posterior al servicio de mensajes cortos (SMS) mediante el cual se pueden transferir diversos mensajes multimedios que incluyen texto, voz y vídeo a través de redes móviles o redes IP. Con el rápido desarrollo de las tecnologías de telecomunicaciones y la creciente popularidad de los teléfonos inteligentes, los MMS ofrecen un contacto social cómodo y mensajes vistosos, y es un medio importante de enviar mensajes, especialmente entre la gente joven y las empresas de los medios de comunicación, que los utilizan comercialmente como método para entregar noticias y contenido de entretenimiento.

Sin embargo, también es posible para los emisores de correo basura enviar mensajes basura MMS. El correo basura MMS, que incluye información no solicitada como anuncios, mensajes fraudulentos, virus y otros tipos de mensajes no deseados, se han convertido en un problema generalizado y provoca cuantiosas pérdidas económicas a operadores de telecomunicaciones, proveedores de servicio y usuarios. En consecuencia, luchar de manera eficaz técnicamente y contra los mensajes basura MMS es un reto en el ámbito de la lucha contra el correo basura.

7 Casos y características del correo basura MMS

Como se muestra en la Figura 7-1, el tratamiento de los MMS se compone de tres etapas fundamentales: (1) el emisor prepara el MMS y se lo envía al MMSC al que pertenece su tarjeta universal de circuito integrado (UICC); (2) el MMSC recibe el contenido del MMS enviado por el emisor y decide si enviar este MMS al siguiente Centro MMS o directamente al receptor; (3) el receptor recibe el MMS desde el MMSC que puede ser diferente del MMSC que el emisor utilizó.

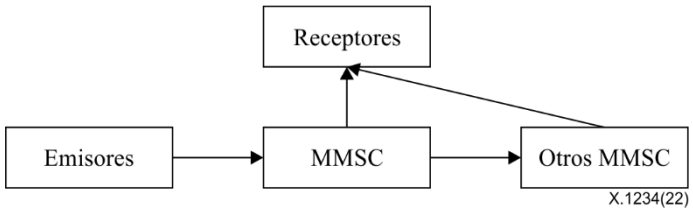


Figura 7-1 – Procedimiento de los MMS

Los emisores de correo basura utilizarán el procedimiento anterior para enviar correo basura a los usuarios, que son molestos y pueden provocar pérdidas a los usuarios. El contenido del correo basura pueden incluir, entre otros, publicidad o un fraude. A continuación, se describen algunos casos de correo basura MMS:

1) Correo basura de fraude: es un mensaje basura MMS que utiliza argumentos para convencer a los receptores de que crean que pueden obtener algún beneficio o de que algo es verdad. Si el receptor responde como indica el mensaje, se le cobrará algo o se le suscribirá a un servicio de valor añadido de la empresa del fraude para que realice pagos.
2) Correo basura de troyanos: algunos correos basura MMS contienen un archivo de medios con un troyano que, si se encuentra en un teléfono celular que es vulnerable y el usuario del teléfono abre el archivo de medios, consigue la autorización de administrador de máximo nivel del sistema del teléfono y puede robar toda la información confidencial que contiene, sin que el receptor tenga conciencia de que eso ha ocurrido.
3) Correo basura de virus: el correo basura MMS puede contener algún tipo de archivo de instalación de virus que tiene apariencia de archivo normal. Una vez que el receptor abre el archivo y se ha realizado la instalación, el virus empieza a destruir el sistema del teléfono de muchas maneras posibles, normalmente con un borrado rápido o una desagregación.
4) Publicidad no deseada: el correo basura MMS de publicidad incluye normalmente diferentes tipos de publicidad sobre cuestiones como préstamos, venta de casas, formación, entre otros. Este mensaje basura se envía al receptor sin su autorización o suscripción. Algunos son típicamente engañosos y pueden incluir un enlace de publicidad en el gráfico o vídeo del MMS, y si el receptor pulsa en el gráfico o en el vídeo, se redirigirá el navegador web a la página de la publicidad.

8 Directrices sobre el marco técnico

8.1 Estructura general

Como se muestra en la Figura 8-1, un emisor envía un mensaje MMS al MMSC y el receptor descarga el mensaje MMS desde el MMSC, por tanto, el MMSC almacena todos los mensajes MMS. Por esa razón, se recomienda que la función de identificación del correo basura MMS (MMSSIF) se despliegue al lado del MMSC.

Es difícil que cualquier tecnología contra el correo basura garantice un 100% de efectividad, y la MMSSIF también necesita una configuración y una gestión manual fuera de línea, en consecuencia, se recomienda que los operadores de servicio la instalen como que se muestra en la Figura 8-1.

Por otro lado, se recomienda que el proceso de funcionamiento del MMSC original debe modificarse para que el MMSC envíe el mensaje MMS a la MMSSIF, en vez de enviarlo directamente al receptor o al siguiente MMSC. La MMSSIF decide si el mensaje es correo basura o no, y luego envía las correspondientes sugerencias al MMSC. De acuerdo con las sugerencias, el MMSC decidirá si sigue enviando el mensaje MMS al receptor o al siguiente MMSC.

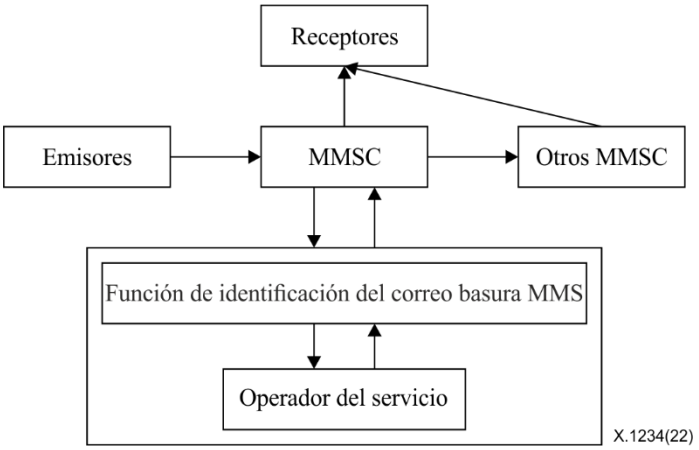


Figura 8-1 – Estructura general para la lucha contra el correo basura MMS

8.2 Estructura de referencia de la MMSSIF

La estructura de referencia de la MMSSIF incluye básicamente siete módulos que corresponden con diferentes funciones: monitorización, adquisición de datos, preprocesamiento, reconocimiento, verificación, eliminación y gestión del sistema. Se recomienda asociar diferentes módulos de forma que se coordinen entre sí de acuerdo con reglas o políticas definidas en los acuerdos pertinentes.

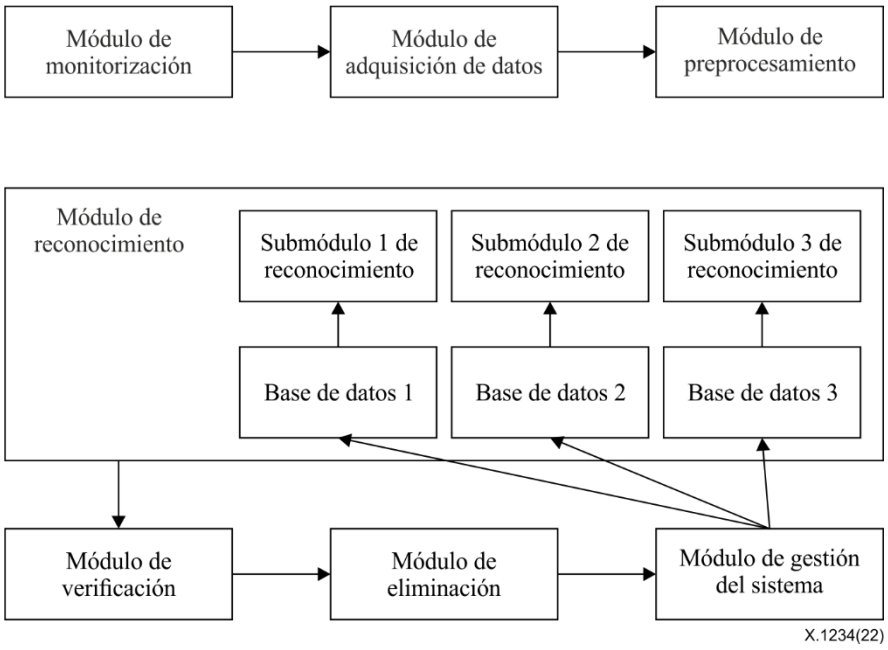


Figura 8-2 – Estructura de referencia de la MMSSIF

En la Figura 8-2, el módulo de monitorización recibe un MMS desde el MMSC y extrae el encabezamiento de dicho MMS que incluye el asunto, el número de teléfono del emisor, el número de adjuntos, los URL de dichos adjuntos, entre otros.

El módulo de adquisición de datos recibe los mensajes del encabezamiento del MMS desde el módulo de monitorización y descarga todos los adjuntos desde las URL.

El módulo de preprocesamiento recibe todos los mensajes de este MMS desde el módulo de adquisición de datos, incluidos el encabezamiento y todos los adjuntos, y normaliza los mensajes de acuerdo con las reglas. Los mensajes pueden ser de encabezamiento o del cuerpo del MMS, y estos mensajes pueden ser de tipo texto, imagen, vídeo, audio, etc. En consecuencia, se recomienda que las reglas sean reglas compuestas del tipo "fuente + tipo de mensaje + mensaje".

El módulo de reconocimiento recibe el mensaje normalizado desde el módulo de preprocesamiento y analiza si dicho MMS es un correo basura mediante diferentes tecnologías como listas negras, reconocimiento de texto, reconocimiento de imágenes, reconocimiento de vídeos, entre otros.

El módulo de verificación recibe los resultados posibles del módulo de reconocimiento y efectúa un análisis posterior como verificaciones manuales con el fin de reducir las posibilidades de falsas alarmas.

El módulo de eliminación recibe el resultado del reconocimiento desde el módulo de verificación, se deshace del MMS considerado correo basura, por ejemplo, bloqueándolo y enviando un mensaje de alerta al emisor del mismo. También envía el MMS original, el registro de eliminaciones y el número de teléfono del emisor al módulo de gestión del sistema.

El módulo de gestión del sistema recibe los registros del módulo de eliminación y guarda el registro de operaciones y el registro del sistema. También envía el número de teléfono del emisor del correo basura, palabras clave e imágenes a las diferentes bases de datos del módulo de reconocimiento con el fin de actualizar dichas bases de datos.

8.3 Componentes funcionales de la MMSSIF

8.3.1 Módulo de monitorización

Las funciones del módulo de monitorización incluyen:

- Monitorizar el envío de un nuevo MMS por el MMSC.
- Recibir el flujo de datos completo del MMS.
- Analizar el flujo de datos y extraer el encabezamiento del MMS.
- Enviar el asunto, el número de teléfono del emisor, el número de adjuntos, los URL de dichos adjuntos y el cuerpo del MMS al módulo de adquisición de datos.

8.3.2 Módulo de adquisición de datos

Las funciones del módulo de adquisición de datos incluyen:

- Recibir los mensajes del módulo de monitorización y extraer los URL de los adjuntos.
- Descargar todos los adjuntos.
- Enviar todos los mensajes del MMS al módulo de preprocesamiento, con el encabezamiento y el cuerpo del MMS, que incluye todos los adjuntos.

8.3.3 Módulo de preprocesamiento

Las funciones del módulo de preprocesamiento incluyen:

- Recibir todos los mensajes desde el módulo de adquisición de datos.
- Controlar todos los adjuntos y analizar si son texto, imágenes, audios o vídeos, pues según el protocolo de transporte actual de los MMS, sólo se permite incluir texto, imágenes, audios o vídeos en un MMS.
- Clasificar los mensajes según los diferentes tipos y normalizar los mensajes de acuerdo con reglas, del tipo de las reglas compuestas "fuente + tipo de mensaje + mensaje".

- Enviar el MMS original, todos los mensajes normalizados y el número de teléfono del emisor al módulo de reconocimiento.

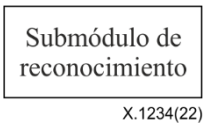
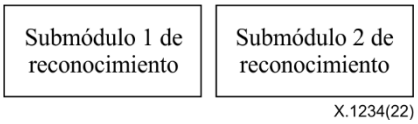
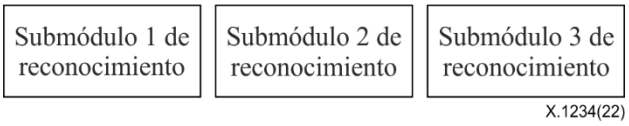
8.3.4 Módulo de reconocimiento

Las funciones del módulo de reconocimiento incluyen:

- analizar si el MMS es un mensaje de correo basura;
- enviar el resultado del reconocimiento al módulo de verificación.

Existen básicamente tres tipos de tecnologías de reconocimiento de acuerdo con las diferentes partes de un MMS. El primer tipo se basa en el número de teléfono, como son las listas negras o las listas blancas. El segundo tipo se basa en el texto, como es el reconocimiento de texto. El último tipo se basa en los adjuntos, como son el reconocimiento de imágenes, el reconocimiento de vídeo, etc. De acuerdo con los requisitos específicos y las características del proveedor del servicio, el módulo de reconocimiento puede incluir diferentes submódulos en función del tipo de tecnología.

Cuadro 8-1 – Modelo de configuración del módulo de reconocimiento

Modelo	Descripción
Modelo 0	 El modelo 0 sólo contiene un submódulo, y tiene un tipo de tecnología de reconocimiento.
Modelo 1	 El modelo 1 está formado por el submódulo 1 y el submódulo 2 configurados conjuntamente. El submódulo 1 y el submódulo 2 son de dos de los tres tipos de tecnologías.
Modelo 2	 El modelo 2 está formado por el submódulo 1, el submódulo 2 y el submódulo 3 configurados conjuntamente.

En el Modelo 1 y el Modelo 2 pueden existir diferentes maneras de calcular el resultado del reconocimiento. Por ejemplo, en el Modelo 1, el submódulo 1 de reconocimiento puede realizar el reconocimiento de texto y el submódulo 2 de reconocimiento puede realizar el reconocimiento de imágenes. El submódulo 1 de reconocimiento reconoce el MMS como correo basura, pero el submódulo 2 no reconoce ese mismo MMS como correo basura. Es necesaria, por tanto, una estrategia general en el módulo de reconocimiento para reconocer o no dicho MMS como correo basura. Se recomienda configurar la estrategia de acuerdo con las necesidades y la situación reales.

8.3.5 Módulo de verificación

Las funciones del módulo de verificación incluyen:

- recibir los posibles resultados del módulo de reconocimiento;
- realizar análisis posteriores, como verificaciones manuales.

8.3.6 Módulo de eliminación

Las funciones del módulo de eliminación de datos incluyen:

- recibir los resultados del módulo de verificación;
- deshacerse del MMS de acuerdo con los resultados del reconocimiento que es capaz de decidir si el MMS es correo basura;
- enviar el resultado de las eliminaciones al módulo de gestión del sistema si se reconoce el MMS como correo basura;
- enviar el MMS original al MMSC si no se reconoce el MMS como correo basura.

8.3.7 Módulo de gestión del sistema

Las funciones del módulo de gestión del sistema incluyen:

- guardar el registro de operaciones y el registro del sistema;
- actualizar las bases de datos;
- recibir las respuestas de los usuarios.

8.4 Modelo de referencia

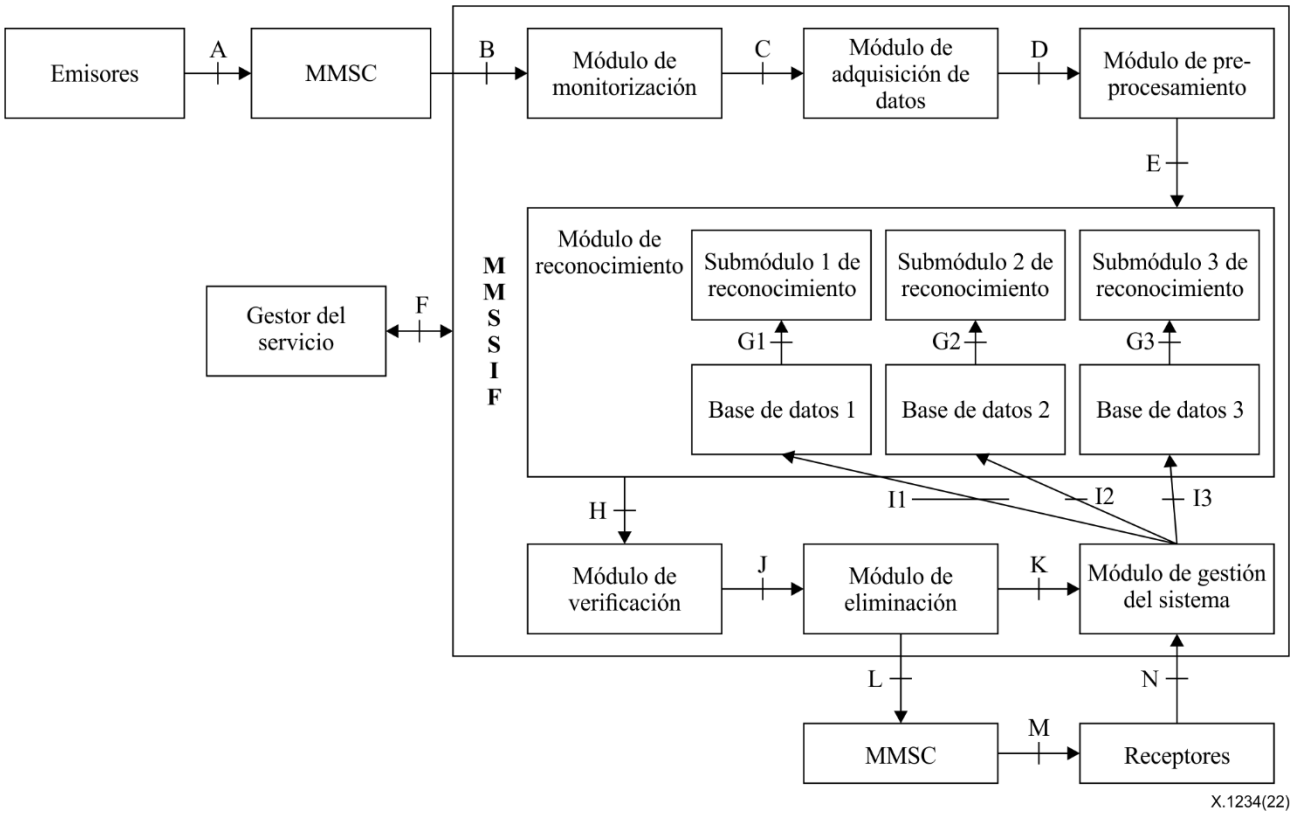


Figura 8-3 – Modelo de referencia para la lucha contra el correo basura MMS

La interfaz A está entre los emisores y el MMSC. La interfaz A se utiliza para transmitir un MMS al MMSC. Esto ya se implementó cuando el proveedor de servicios empezó a ofrecer el servicio MMS a los usuarios. No es necesario cambiarla en este modelo.

La interfaz B está entre el MMSC y el módulo de monitorización. La interfaz B es una nueva interfaz y se utiliza para transmitir un MMS al módulo de monitorización en vez de reenviarlos directamente al receptor o al siguiente MMSC.

La interfaz C está entre el módulo de monitorización y el módulo de adquisición de datos. La interfaz C se utiliza para transmitir el encabezamiento del MMS, el número de teléfono del usuario, los URL, etc., que se analizan en el módulo de monitorización.

La interfaz D está entre el módulo de adquisición de datos y el módulo de preprocesamiento. La interfaz D se utiliza para transmitir todos los mensajes, que incluyen el encabezamiento y el cuerpo del MMS, el asunto, todos los adjuntos, etc.

La interfaz E está entre el módulo de preprocesamiento y el módulo de reconocimiento. La interfaz E se utiliza para transmitir los mensajes normalizados, como "fuente + tipo de mensaje + mensaje". La interfaz E debe soportar FTP y HTTP.

La interfaz F está entre el operador del servicio y la MMSSIF. La Interfaz F se utiliza para transmitir las reglas de configuración y los datos estadísticos del correo basura.

La interfaz G está entre la base de datos y el submódulo. La interfaz G no es una interfaz específica. Representa un tipo de interfaces que está entre las diferentes bases de datos y los submódulos de reconocimiento correspondientes. La interfaz G se utiliza para transmitir los números, textos, imágenes, etc. sospechosos, que se controlan con la base de datos para reconocer el correo basura.

La interfaz H está entre el módulo de reconocimiento y el módulo de verificación. La interfaz H se utiliza para transmitir los resultados probables y el MMS original.

La interfaz I está entre la gestión del sistema y la base de datos. La interfaz I no es una interfaz específica, como en el caso de la interfaz G, representa un tipo de interfaces que está entre las diferentes bases de datos y la gestión del sistema.

La interfaz J está entre el módulo de verificación y el módulo de eliminación. La interfaz J se utiliza para transmitir el resultado del reconocimiento y el MMS original.

La interfaz K está entre el módulo de eliminación y la gestión del sistema. La interfaz K se utiliza para transmitir el número de teléfono del emisor, el resultado del reconocimiento, la eliminación realizada y el MMS original

La interfaz L está entre el módulo de eliminación y el MMSC. La interfaz K se utiliza para transmitir el MMS original que no se reconoce como correo basura.

La interfaz M está entre el MMSC y los receptores. La interfaz M se utiliza para transmitir los MMS a los receptores. Esto se ha implementado desde que el proveedor de servicios comenzó a ofrecer el servicio MMS a los usuarios y no es necesario cambiarla en este modelo.

La interfaz N está entre los receptores y la gestión del sistema. La interfaz N se utiliza para transmitir las respuestas de los usuarios.

9 Procedimientos de trabajo

La Figura 9-1 muestra que la lucha contra el correo basura MMS se basa en doce procedimientos. Dichos procedimientos constituyen un sistema adaptativo que contribuye a optimizar la eficacia del sistema.

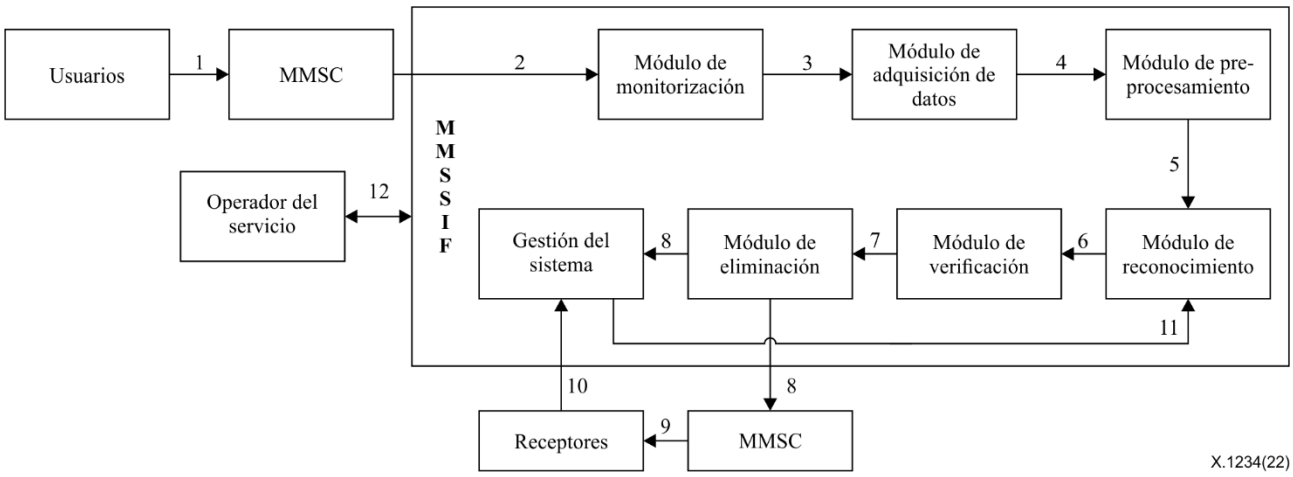


Figure 9-1 – Procedimientos de procesamiento en la lucha contra el correo basura MMS

Procedimiento 1: Envío del MMS al MMSC

El emisor prepara el contenido de un MMS, el número de teléfono del receptor y envía el MMS al MMSC.

Procedimiento 2: Reenvío del MMS al módulo de monitorización

El MMSC recibe el mensaje MMS desde el MMSC y lo reenvía directamente al módulo de monitorización.

Procedimiento 3: Extracción del encabezamiento del MMS

El módulo de monitorización supervisará en todo momento si se recibe un nuevo envío de MMS desde el MMSC. Una vez que se recibe un nuevo MMS, recibirá el flujo de datos completo del MMS, lo analizará y extraerá el encabezamiento del MMS, incluido el asunto, el número de teléfono del emisor, el número de adjuntos y los URL de esos adjuntos. El módulo de monitorización enviará entonces todos los mensajes al módulo de adquisición de datos.

Procedimiento 4: Descarga de todos los adjuntos

El módulo de adquisición de datos recibirá los mensajes del módulo de monitorización, identificará los URL y con ellos descargará los adjuntos. Después de obtener todos los mensajes del MMS, el módulo de adquisición de datos lo enviará al módulo de preprocesamiento.

Procedimiento 5: Normalización de los mensajes del MMS

El módulo de preprocesamiento controlará todos los adjuntos y analizará si contienen texto, imágenes, audios o vídeos tras recibir los mensajes desde el módulo de adquisición de datos. Si todos los mensajes son legales, el módulo de preprocesamiento clasificará los mensajes según los diferentes tipos y normalizará los mensajes de acuerdo con reglas. Posteriormente, enviará el MMS original, todos los mensajes normalizados y el número de teléfono del emisor al módulo de reconocimiento.

Procedimiento 6: Análisis del MMS

El módulo de reconocimiento analizará si el MMS es o no es correo basura, en función de diferentes tecnologías, que están instaladas en el sistema real. El módulo de reconocimiento enviará entonces el resultado del reconocimiento al módulo de verificación. Salvo para algunas tecnologías específicas, el módulo de reconocimiento necesita alguna estrategia general para conseguir el resultado probable final.

Procedimiento 7: Análisis suplementario

El módulo de verificación realizará análisis suplementarios después de recibir los posibles resultados del módulo de reconocimiento y enviará el resultado del reconocimiento al módulo de eliminación.

Procedimiento 8: Eliminación del MMS

El módulo de eliminación actuará sobre el MMS de acuerdo con los resultados del reconocimiento. Si se ha reconocido el MMS como correo basura, el módulo de eliminación actuará sobre el MMS según el conjunto de reglas, por ejemplo, con el bloqueo del MMS, el envío de un mensaje de alerta al emisor del correo basura, etc. También envía el MMS original, el registro de eliminación y el número de teléfono del emisor al módulo de gestión del sistema. El receptor no recibirá ese MMS. Si no se ha reconocido el MMS como correo basura, el módulo de eliminación enviará el MMS original al MMSC.

Procedimiento 9: Envío del MMS al receptor

El MMSC enviará el MMS al receptor. Algunas veces, enviará el MMS a otro MMSC que, a su vez, lo enviará al receptor. Este procedimiento es el mismo que antes cuando no existe una función MMSSIF.

Procedimiento 10: Respuestas de los receptores

Los receptores son las posibles víctimas del correo basura, pueden por tanto enviar respuestas e información voluntariamente al módulo de gestión del servicio. La participación de los receptores contribuirá a combatir los mensajes basura de manera eficaz y eficiente. Por consiguiente, se recomienda que el módulo de gestión del sistema utilice las respuestas de los receptores cuando se desarrollen soluciones o estrategias para la luchar contra el correo basura.

Procedimiento 11: Actualización de las bases de datos

El módulo de gestión del sistema almacenará el registro de operaciones, el registro del sistema y los MMS originales. Actualizará las bases de datos también, en función de las nuevas muestras, números de teléfono, palabras clave, etc.

Procedimiento 12: Ajuste de las medidas de protección

Con arreglo a los datos estadísticos y al informe analítico de la MMSSIF sobre el correo basura, un operador del servicio evaluará la calidad de funcionamiento del MMSSIF para introducir posibles mejoras. Sobre la base del resultado de la evaluación, el operador del servicio podrá ajustar las medidas y las estrategias y podrá modificar los mecanismos de colaboración en el módulo de reconocimiento.

10 Directrices sobre las tecnologías fundamentales

Un MMS pueden transmitir diferentes tipos de mensajes incluidas imágenes, texto, vídeo, audio, etc. En consecuencia, las tecnologías clave de reconocimiento en la lucha contra los mensajes basura MMS incluyen sobre todo reconocimiento de imágenes, reconocimiento de texto, reconocimiento de vídeo y reconocimiento de audio.

10.1 Listas para filtrado del correo basura

Las listas para filtrado del correo basura incluyen listas negras, listas blancas y listas de ambigüedades. El proveedor de servicio debe configurar el MMSSIF para almacenar las actividades sospechosas u, opcionalmente, configurarlo de manera automática (por ejemplo, bloquear los MMS sospechosos, permitir los MMS normales) para las listas negras y las listas blancas. El proveedor de servicio debe mantener también las listas para que la MMSSIF esté disponible y funcione establemente. Cuando se detectan anomalías para un número de teléfono que no está incluido en las listas, el número de teléfono debe pasar un proceso de revisión manual para una evaluación completa.

10.2 Reconocimiento de imágenes

En primer lugar, el módulo de reconocimiento de imágenes, extrae una característica relativa a la representación de la imagen y crea una base de datos con los valores propios de las imágenes. La detección de los mensajes basura se transforma entonces en un problema de clasificación binaria de las características, y puede resolverse mediante la aplicación del aprendizaje automático convencional. O, de manera más sencilla, si el valor propio de la imagen de un mensaje MMS concuerda con alguno de la base de datos, el mensaje se reconoce como correo basura. Este método depende de la calidad de la base de datos de valores propios de imágenes.

10.3 Reconocimiento de texto

El reconocimiento de texto utiliza principalmente el reconocimiento de palabras clave y el reconocimiento semántico. El reconocimiento de palabras clave establece primero una base de datos de palabras clave. Cuando el texto de un mensaje MMS contiene cualquier palabra clave contenida en la base de datos de palabras clave, se reconoce dicho mensaje como correo basura; además, el reconocimiento de texto puede elaborar modelos lógicos booleanos y el modelo de espacio vectorial, que, con entrenamiento, permite obtener el modelo de reconocimiento que puede mejorar la precisión del reconocimiento de texto. Este método depende de la calidad de la base de datos de palabras clave.

En ocasiones, los emisores de correos basura son muy creativos a la hora de evitar la detección. Por ejemplo, pueden falsificar mensajes electrónicos normales y aleatorizar el contenido para evitar que los filtros de correo basura detecten palabras clave. En consecuencia, sobre la base del reconocimiento de palabras clave, resulta muy eficaz y eficiente utilizar el reconocimiento semántico para conseguir un reconocimiento secundario (por ejemplo, un enfoque de procesamiento del lenguaje natural basado en el reconocimiento semántico mediante una lógica borrosa), que puede reducir mucho la proporción de falsos positivos.

10.4 Reconocimiento de vídeo

En general, el reconocimiento de vídeo crea primero una base de datos de muestras, y luego compara el vídeo de un mensaje MMS con cada una de las muestras de vídeo para analizar si el vídeo es correo basura. También puede identificarlo extrayendo tramas clave del vídeo. Las principales operaciones son las siguientes: descodificación del vídeo, procesamiento del mismo como un conjunto de imágenes, tomar muestras de las imágenes, identificación de las imágenes muestreadas en base a la tecnología de reconocimiento de imágenes, y finalmente, obtener el resultado del reconocimiento del vídeo utilizando el conjunto de resultados del análisis de las imágenes muestreadas.

10.5 Reconocimiento de audio

El reconocimiento de audio puede llevarse a cabo en combinación con la tecnología de reconocimiento automático de la voz (ASR). El objetivo de la tecnología ASR es que se pueda "dictar" a las computadoras mediante la voz hablada, en continuo o con enunciados de palabras o frases clave por parte de diferentes personas, para que puedan convertir la "voz" en "texto". Además, con el fin de identificar datos de audios similares o iguales, se extraen las características espectrales, y se calcula una huella corta y sólida del audio. En consecuencia, el ASR es capaz de "reconocer" algunas palabras clave de un audio, lo que puede determinar que un audio es correo basura.

10.6 Respuesta de los usuarios

La respuesta de los usuarios finales, las orientaciones para la implementación asociadas y otras informaciones indicadas en la cláusula 8.5 de [UIT-T X.1231] y en el Anexo A a [UIT-T X.1247] son aplicables.

Algunos usuarios finales borrarán directamente los mensajes basura MMS cuando los reciban, y unos pocos usuarios finales informarán del correo basura MMS a través del canal oficial de respuesta a disposición del cliente. La eficacia de este método depende del interés y de la iniciativa de los usuarios finales. La participación de los usuarios contribuirá de forma eficaz a combatir el correo basura MMS.

Bibliografía

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

[b-UIT-T X.1241] Recomendación UIT-T X.1241 (2008), *Marco técnico 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.*

[b-UIT-T X.1245] Recomendación UIT-T X.1245 (2010), *Marco de aplicaciones multimedios IP para la lucha contra el correo basura.*

[b-UIT-T X.1246] Recomendación UIT-T X.1246 (2015), *Tecnologías implicadas en la lucha contra el correo basura de voz en las organizaciones de telecomunicaciones.*

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, 2022