Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2770

(11/2012)

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

Redes de la próxima generación – Seguridad

Requisitos para la inspección detallada de paquetes en las redes de la próxima generación

Recomendación UIT-T Y.2770

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
Televisión IP sobre redes de próxima generación	Y.1900–Y.1999
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación	Y.2250–Y.2299
	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Redes basadas en paquetes	Y.2600–Y.2699
Seguridad	**Y.2700–Y.2799**
Movilidad generalizada	Y.2800–Y.2899
Entorno abierto con calidad de operador	Y.2900–Y.2999
REDES FUTURAS	Y.3000–Y.3499
COMPUTACIÓN EN LA NUBE	Y.3500–Y.3999

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

Recomendación UIT-T Y.2770

Requisitos para la inspección detallada de paquetes en las redes de la próxima generación

Resumen

En esta Recomendación se especifican los requisitos para la inspección detallada de paquetes (IDP) en las redes de la próxima generación (NGN). Se especifican principalmente los requisitos para las entidades que efectúan la inspección detallada de paquetes (IDP) en las NGN, en particular aspectos tales como la identificación de aplicación, la identificación de flujo, tipos de tráfico inspeccionado, la gestión de firmas, la presentación de informes al sistema de gestión de red (NMS) y la interacción con la entidad funcional de decisión política. Aunque orientados a las NGN, los requisitos pueden ser aplicables a otros tipos de redes.

Historia

Edición	Recomendación	Aprobación	Comisión de estudios	ID único*
1.0	ITU-T Y.2770	2012-11-20	13	11.1002/1000/11566-en

* 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 base de esta Recomendación es el protocolo de gestión CPE WAN (CWMP) del Foro de la Banda Ancha, comúnmente denominado TR-069.

Este protocolo está previsto para la comunicación entre un CPE y un servidor de autoconfiguración (ACS). El protocolo de gestión CPE WAN define un mecanismo que comprende la autoconfiguración segura de un CPE, además de otras funciones de gestión del CPE en un marco común.

TR-069 especifica los requisitos genéricos del protocolo de gestión y los métodos que pueden aplicarse a cualquier CPE TR-069. En otros Informes técnicos (TR) del Foro de la Banda Ancha se especifican los objetos gestionados, o modelos de datos, de cada tipo de dispositivo o servicio específico.

Este protocolo puede emplearse para gestionar diversos tipos de CPE, incluidos los encaminadores autónomos y los dispositivos de cliente LAN. El protocolo es independiente del medio de acceso concreto utilizado por el proveedor de servicios, aunque depende de que el dispositivo haya establecido previamente una conexión en la capa IP.

Recomendación UIT-T Y.2770

Requisitos para la inspección detallada de paquetes en las redes de la próxima generación

1 Alcance

En esta Recomendación se especifican los requisitos para las entidades de inspección detallada de paquetes (IDP) en las redes de la próxima generación (NGN), en particular, aspectos tales como la identificación de aplicación, la identificación de flujo, los tipos de tráfico inspeccionado, la gestión de firmas, la presentación de informes al sistema de gestión de red (NMS) y la interacción con la entidad funcional de decisión política.

En esta Recomendación también se indican los requisitos para la IDP de tráfico en formatos de codificación no nativos (por ejemplo, tráfico encriptado, datos comprimidos e información transcodificada).

Toda función IDP puede describirse generalmente mediante el concepto de reglas políticas (véase la cláusula 1.2).

Los ingenieros y usuarios de las técnicas descritas deberán cumplir la legislación, los reglamentos y las políticas nacionales y regionales aplicables. El mecanismo descrito en la presente Recomendación quizá no sea aplicable a la correspondencia internacional a los efectos de garantizar los requisitos jurídicos nacionales en materia de secreto y soberanía que se imponen a las telecomunicaciones y a la Constitución y el Convenio de la UIT.

La Recomendación no aborda el efecto específico de aplicar una funcionalidad IDP distribuida. Los requisitos se refieren principalmente a los aspectos funcionales de la IDP, aunque también se contemplan aspectos físicos. En cuanto a la relación entre los aspectos funcionales y físicos, en esta Recomendación trata exclusivamente de la correspondencia 1 a 1 y no la correspondencia N a 1 entre una DPI-FE y una DPI-PE. Es decir, los requisitos no se refieren a las DPI-PE distribuidas.

1.1 Ámbito de aplicación

La presente Recomendación se aplica a los casos que se indican en la Figura 1-1:

		Tipo de red por paquetes	
		NGN	no NGN
Tecnología de transporte por paquetes	IP	Aplicable	Posiblemente aplicable
	no IP	Posiblemente aplicable	Posiblemente aplicable

Y.2770(12)_F1-1

Figura 1-1 – Ámbito de aplicación de esta Recomendación

El concepto de "no IP" se refiere a las pilas de protocolo para los tipos de transporte de paquetes sin ninguna capa de protocolo IP ([IETF RFC 791] e [IETF RFC 2460]).

Si bien la presente Recomendación trata principalmente de los requisitos de IDP para las NGN, dichos requisitos también podrían aplicarse a otros tipos de redes. Dicha aplicación será objeto de un estudio ulterior.

1.2 Reglas políticas

En esta Recomendación se emplea un mismo formato genérico de alto nivel para todas las reglas políticas. Este formato se aplica a las reglas IDP como se indica en la Figura 1-2. El formato consta de tres bloques básicos:

i) identificador/nombre de la regla (se indica la posición o el orden, ya que pueden haber varias reglas);

ii) firma/condiciones de IDP;

iii) acciones.

Existe una relación lógica entre las acciones y las condiciones. Véase la cláusula 3.1.2.

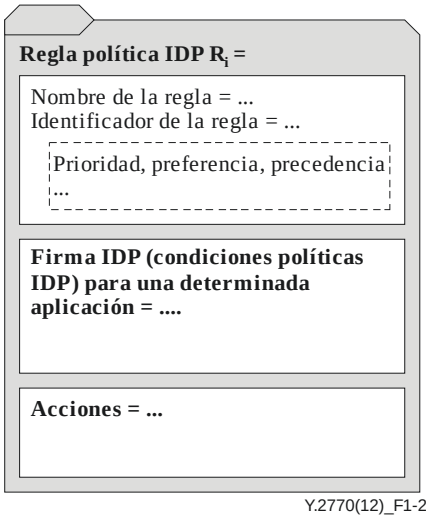


Figura 1-2 – Formato genérico de las reglas políticas IDP

Obsérvese que en la presente Recomendación se contemplan los aspectos siguientes:

- la especificación de requisitos relacionados con la firma IDP (es decir, las firmas IDP se utilizan para la identificación de la aplicación y del flujo);
- la especificación de requisitos relativos a la identificación y denominación de reglas políticas IDP; y
- la identificación de posibles casos que conllevan acciones de política, es decir posibles actividades que se han de realizar tras la evaluación de firmas IDP.

En cambio, en la presente Recomendación no se contemplan los siguientes aspectos:

- la especificación de requisitos relacionados con acciones relativas a la modificación de paquetes inspeccionados;
- la especificación de relaciones explícitas entre acciones y condiciones (véase la Nota);
- la especificación de reglas políticas IDP exhaustivas;
- la especificación de un lenguaje para firmas IDP; y
- las especificaciones de condiciones de política de IDP concretas (tales como funciones estadísticas o funcionales).

NOTA – Por ejemplo, puede especificarse la acción de descartar un paquete y la condición de buscar la firma de un paquete, pero *no* habrá ninguna especificación que relacione una acción concreta en respuesta a una condición real.

2 Referencias

Las siguientes Recomendaciones 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.

[ITU-T E.107] Recomendación UIT-T E.107 (2007), *Servicio de telecomunicaciones de emergencia (ETS) y marco de interconexión para implementaciones nacionales del ETS*.

[ITU-T X.200] Recomendación UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico*.

[ITU-T X.731] Recomendación UIT-T X.731 (1992) | ISO/CEI 10164-2:1992, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de gestión de estados*.

[ITU-T Y.1221] Recomendación UIT-T Y.1221 (2010), *Control de tráfico y control de congestión en las redes basadas en el protocolo Internet*.

[ITU-T Y.2111] Recomendación UIT-T Y.2111 (2008), *Funciones de control de recursos y admisión en las redes de próxima generación*.

[ITU-T Y.2205] Recomendación UIT-T Y. 2205 (2011), *Redes de la próxima generación – Telecomunicaciones de emergencia – Consideraciones técnicas*.

[ITU-T Y.2701] Recomendación UIT-T Y.2701 (2007), *Requisitos de seguridad para las redes de la próxima generación, versión 1*.

[ITU-T Y.2704] Recomendación UIT-T Y.2704 (2010), *Mecanismos y procedimientos de seguridad en las redes de próxima generación*.

[IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.

[IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6), Specification*.

[IETF RFC 5101] IETF RFC 5101 (2008), *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*.

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 filtro (*filter*) [b-IETF RFC 3198]: Conjunto de términos y/o criterios utilizados para distinguir y categorizar. Para ello se emplea la concordancia de uno o varios campos de datos de la carga útil y/o del encabezamiento del tráfico. Los "Filtros" se suelen manipular y se utilizan en la política y explotación de redes. Por ejemplo, en los filtros de paquetes se especifican los criterios de concordancia con un patrón (por ejemplo, criterios IP o 802) para distinguir diferentes clases de tráfico.

NOTA – En la presente Recomendación, el término "encabezamiento de tráfico" equivale a "encabezamiento de paquetes".

3.1.2 regla de filtro/política (*filter/policy rule*) [b-IETF RFC 3198]: Componente básico de un sistema basado en políticas. Relaciona un conjunto de acciones con un conjunto de condiciones, de modo que se evalúan las condiciones para determinar qué acciones deben realizarse.

NOTA – En la presente Recomendación, una regla de filtro es una regla política específica destinada a separar tráfico, por ejemplo, en las categorías principales de "aceptado" y "no aceptado".

3.1.3 flujo (*flow*) [IETF RFC 5101]: Conjunto de paquetes IP que pasan por un punto de observación en la red durante un cierto intervalo de tiempo. Todos los paquetes que pertenecen a un determinado flujo tienen ciertas propiedades comunes. Cada propiedad se define como el resultado de aplicar una función a los valores de:

1) Uno o varios campos de encabezamiento del paquete (por ejemplo, dirección IP de destino), campos de encabezamiento de transporte (por ejemplo, número de puerto de destino), o campos de encabezamiento de aplicación (por ejemplo, campos del encabezamiento RTP [b-IETF RFC 3550]).
2) Una o varias características del paquete propiamente dicho (por ejemplo, el número de etiquetas MPLS, etc.).
3) Uno o varios campos obtenidos al procesar el paquete (por ejemplo, la dirección IP del próximo tramo, la interfaz de salida).

Un paquete pertenece a un flujo determinado si satisface completamente todas las propiedades definidas de dicho flujo.

Esta definición comprende desde un flujo que contiene todos los paquetes observados en una interfaz de red hasta un flujo que consiste en sólo un paquete en una interfaz de red o un flujo que consta de un solo paquete entre dos aplicaciones. Quedan comprendidos los paquetes seleccionados mediante un mecanismo de muestreo.

NOTA – La lista numerada anterior indica las propiedades del flujo en las categoría de 1) "Información de control de protocolo (PCI) de paquetes", 2) "propiedades de la Unidad de datos de protocolo (PDU) de los paquetes" y 3) "Información local de renvío de paquetes".

3.1.4 política (*policy*) [b-IETF RFC 3198]: Conjunto de reglas para administrar, gestionar y controlar el acceso a recursos de red.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 aplicación (*application*): puede referirse a lo siguiente:

- *un tipo de protocolo de aplicación* (por ejemplo, los protocolos de aplicación IP de vídeo UIT-T H.264 o protocolo de inicio de sesión (SIP);
- *una instancia del usuario del servicio* (por ejemplo, VoIP, VoLTE, VoIMS, VoNGN, y VoP2P) de un tipo de aplicación, por ejemplo, "aplicación de voz por paquetes";
- *una "aplicación específica del proveedor"* de voz por paquetes, (por ejemplo, VoIP de proveedor 3GPP, VoIP de Skype);
- una aplicación integrada en otra aplicación (por ejemplo, el contenido de aplicación en un elemento de SIP o un mensaje HTTP).

Cada aplicación se identifica mediante un identificador en concreto (por ejemplo, un campo de bits, un patrón, una firma o una expresión ordinaria como "condiciones a nivel de aplicación", véase también la cláusula 3.2.2), que es una característica común a todos los niveles de aplicaciones antes enumerados.

3.2.2 descriptor de la aplicación (también denominado condiciones a nivel de aplicación) (*application-descriptor*): Conjunto de condiciones normativas que identifican la aplicación (conforme a la cláusula 3.2.1).

En esta Recomendación se considera el descriptor de aplicaciones como un objeto en general, que es sinónimo de condiciones a nivel de aplicación. No se tiene en cuenta su estructura detallada, por ejemplo la sintaxis, la codificación y el tipo de datos.

3.2.3 etiqueta de la aplicación (*application tag*): Nombre único de una aplicación que se utiliza para indicar la semántica de la aplicación y que se suele utilizar en informes.

La Figura 3-1 resume la relación entre la etiqueta y el descriptor de la aplicación.

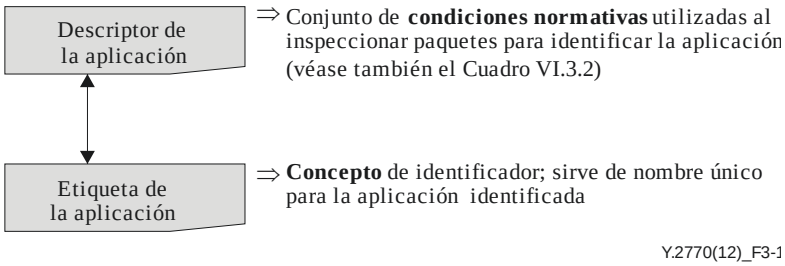


Figura 3-1 – Relación entre la etiqueta y el descriptor de la aplicación

3.2.4 IDP bidireccional (*bidirectional DPI*): IDP que comprende condiciones de política que conciernen a los dos sentidos del tráfico.

NOTA – Hay al menos una condición simple por cada sentido de tráfico en el caso de IDP bidireccional.

3.2.5 inspección detallada de paquetes (IDP) (*deep packet inspection*): Análisis, con arreglo a la arquitectura de protocolo por capas OSI-BRM [ITU-T X.200], de:

- las propiedades de la carga útil y/o los paquetes (véase la lista de posibles propiedades en la cláusula 3.2.11 para información de encabezamiento más profunda que las capas de protocolo 2, 3 ó 4 (L2/L3/L4)); y
- otras propiedades de los paquetes;

con el fin de identificar inequívocamente la aplicación.

NOTA – El resultado de la función IDP, junto con otra información adicional como la relativa al flujo, se suele utilizar en funciones ulteriores, tales como las de notificación o acciones sobre los paquetes.

3.2.6 motor IDP (*DPI engine*): **s**ubcomponente y parte central de la entidad funcional IDP que realiza todas las funciones de procesamiento de paquetes (por ejemplo, identificación de paquetes y otras funciones de procesamiento de paquetes de la Figura 6-1).

3.2.7 entidad IDP (*DPI entity*): por entidad IDP se entiende la entidad funcional IDP o la entidad física IDP.

3.2.8 entidad funcional IDP (*DPI functional entity*) (DPI-FE): entidad funcional que realiza la inspección detallada de paquetes.

3.2.9 entidad física IDP (*DPI physical entity*) (DPI-PE): materialización de una entidad funcional IDP.

3.2.10 política IDP (*DPI policy*): política definida, por ejemplo en [b-IETF RFC 3198] (véase la cláusula 3.1.4), que se aplica en una entidad IDP.

3.2.11 condición de política IDP (también denominada firma IDP) (*DPI policy condition*): representación del estado y/o prerrequisitos necesarios que identifican una aplicación y definen si deben realizarse las acciones de una regla política. El conjunto de condiciones de política IDP relacionadas con una regla política especifica cuando ésta es aplicable (véase también [b-IETF RFC 3198]).

Las condiciones de política IDP deben contener condiciones a nivel de aplicación y quizá otras opciones tales como condiciones de estado y/o condiciones a nivel de flujo:

1) Condición de estado (facultativo):
   a) grado de condiciones de servicio en la red (por ejemplo, congestión experimentada en trayectos de paquetes); o
   b) situación del elemento de red (por ejemplo, condición de sobrecarga local de DPI-FE).
2) Descriptor del flujo/condiciones a nivel de flujo (facultativo):
   a) contenido del paquete (campos de encabezamiento);
   b) características del paquete (por ejemplo, número# de etiquetas MPLS);
   c) tratamiento del paquete (por ejemplo, interfaz de salida del DPI-FE).
3) Descriptor de la aplicación/condiciones a nivel de aplicación:
   a) contenido del paquete (campos del encabezamiento de la aplicación y carga útil de la aplicación).

NOTA – La condición está relacionada con la "condición simple" en las descripciones formales de las condiciones a nivel de flujo y a nivel de aplicación.

3.2.12 entidad funcional de decisión política IDP (DPI-PDFE) (*DPI policy decision functional entity*): La función remota respecto de la DPI-FE que decide las reglas basadas en la firma que se aplicarán en la DPI-FE. Algunas funciones de control y/o gestión no tienen por qué ser remota respecto de la DPI-FE.

3.2.13 regla política IDP (*DPI policy rule*): regla política pertinente a la IDP (véase también la cláusula 3.1.2). En esta Recomendación, se hace referencia a la regla política IDP simplemente como una regla.

3.2.14 firma IDP (*DPI signature*): sinónimo de condiciones de política IDP (véase la cláusula 3.2.11).

3.2.15 biblioteca de firmas IDP (*DPI signature library*): base de datos que consta de un conjunto de firmas IDP. También se denomina biblioteca de protocolo IDP, porque las firmas puede utilizarse normalmente para la identificación del protocolo.

3.2.16 descriptor del flujo (también denominado condiciones a nivel de flujo) (*flow descriptor*): Conjunto de condiciones de reglas que se utiliza para identificar un determinado tipo de flujo (con arreglo a la cláusula 3.1.3) en el tráfico inspeccionado.

NOTA 1 – Esta definición de descriptor del flujo amplía la definición que Figura en [b-ITU-T Y.2121] con elementos adicionales, como se describe en la cláusula 3.

NOTA 2 – En el Anexo A se realiza un examen normativo del descriptor del flujo con mayor detalle.

3.2.17 identificador de flujo IPFIX (*IPFIX flow ID*): Conjunto de valores de las claves de flujo IPFIX, que se utilizan junto con el descriptor del flujo para identificar un determinado flujo.

3.2.18 clave de flujo IPFIX (*IPFIX flow key*): Cada elemento de información del descriptor del flujo que se utiliza en los procesos de identificación de flujo basados en IPFIX (con arreglo a [IETF RFC 5101]).

NOTA – La definición de clave del flujo IPFIX es coherente desde el punto de vista semántico con la definición de clave del flujo especificada en IPFIX [IETF RFC 5101]. La única diferencia entre los dos términos radica en que la definición en este documento se limita al descriptor del flujo.

3.2.19 inspección de encabezamiento L3,4 ($L_{3,4}$HI) (***L3,4 header inspection***): Procesamiento de reglas políticas con condiciones de política que sólo implica a elementos de información de control del protocolo (PCI) de la capa de red y/ la capa de transporte.

3.2.20 inspección de encabezamiento L4+ (L_{4+}HI) (***L4+header inspection***): Procesamiento de reglas políticas con condiciones de política que sólo implica elementos PCI situados por encima de la capa de transporte.

3.2.21 inspección de carga útil L4 (L_4PI) (***L4 payload inspection***): Procesamiento de reglas políticas con condiciones de política en el que sólo interviene la carga útil de transporte que, en el caso de protocolos de aplicación particulares (por ejemplo, SIP) pueden ser los "datos de la aplicación".

NOTA – L_4PI está relacionada con la unión de condiciones de política L_4+HI y L_7PI.

3.2.22 inspección de carga útil L7 (L_7PI) (***L7 payload inspection***): procesamiento de reglas políticas con condiciones de política basadas en los datos de la aplicación.

3.2.23 carga útil (*payload*): unidad de datos precedida por los elementos del encabezamiento en un paquete, excluyendo los elementos opcionales situados al final del paquete (por ejemplo, elementos de relleno, de cola o de suma de verificación).

NOTA 1 – Por consiguiente, el concepto de carga útil es sinónimo de la unidad de datos del servicio (SDU) en OSI-BRM [ITU-T X.200], paquete es sinónimo de unidad de datos de protocolo (PDU), y la información de control del protocolo (PCI) comprende todos los elementos del encabezamiento y de cola del paquete. En resumen, "PDU = PCI + SDU".

NOTA 2 – El concepto de carga útil es específico de la capa de protocolo del caso (es decir, Lx-Payload se refiere a la carga útil en la capa de protocolo x). Lo mismo en el caso de *Lx-SDU*, *Lx-PDU* y *Lx-PCI*.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siglas y los acrónimos siguientes:

AH Encabezamiento de autentificación (*authentication header*)

BRM Modelo de referencia básico (*basic reference model*)

DCCP Protocolo de control de congestión de datagrama (*datagram congestion control protocol*)

IDP Inspección detallada de paquetes (*deep packet inspection*)

DPI-FE Entidad funcional IDP (*DPI functional entity*)

DPI-PDFE Entidad funcional de decisión política IDP (*DPI policy decision functional entity*)

DPI-PE Entidad física IDP (*DPI physical entity*)

DPI-PIB Base de información de política IDP (*DPI policy information base*)

ESP Carga útil de seguridad de encapsulado (*encapsulating security payload*)

ET Telecomunicaciones de emergencia (*emergency telecommunications*)

FPA Análisis exhaustivo de la carga útil (*full payload area analysis*)

FSL Lenguaje de especificación de filtros (*filter specification language*)

HTTP Protocolo de transferencia de hipertexto (*hypertext transfer protocol*)

IANA Organismo de asignación de números de Internet (*Internet assigned numbers authority*)

IE Elementos de información (*information elements*)

IP Protocolo Internet (*Internet protocol*)

IPFIX Exportación de información de flujo IP (*IP flow information export*)

IS En servicio (*in-service*)

L-PDF PDF local (*local PDF*)

MPLS Conmutación por etiquetas multiprotocolo (*multi protocol label switching*)

NGN Red de la próxima generación (*next generation network*)

NMS Sistema de gestión de red (*network management system*)

OGP Protocolo de juegos abierto (*open game protocol*)

OoS Fuera del servicio (*out-of-service*)

OSI-BRM Interconexión de sistemas abiertos – modelo de referencia básico (*open systems interconnection – basic reference model*)

P2P Punto a punto (*peer to peer*)

PCC Control de políticas y tarificación (*policy and charging control*)

PCI Información de control del protocolo (*protocol control information*)

PDF Función de decisión política (*policy decision function*)

PDU Unidad de datos del protocolo (*protocol data unit*)

PEL Lenguaje de expresión de políticas (*policy expression language*)

PFF Función de renvío de paquetes (*packet forwarding function*)

PIB Base de información de políticas (*policy information base*)

PPA Análisis predeterminado de la carga útil (*payload area analysis*)

PSAMP Muestreo de paquetes (*packet sampling*)

PSL Lenguaje de especificación de políticas (*policy specification language*)

RACF Funciones de control de admisión y de recursos (*resource and admission control functions*)

RACS Subsistema de control de admisión y de recursos (*resource and admission control subsystem*)

R-PDF PDF distante (*remote PDF*) (es decir, PDF situada a distancia desde la perspectiva del nodo IDP)

RTP Protocolo de transporte en tiempo real (*real-time transport protocol*)

SA Asociación de seguridad (*security association*) (*IPsec*)

SCTP Protocolo de transmisión de control de trenes (*stream control transmission protocol*)

SDU Unidad de datos de servicio (*service data unit*)

SigComp Comprensión de señalización (*signaling compression*)

SIP Protocolo de inicio de sesión (*session initiation protocol*)

SPI Índice de parámetro de seguridad (*security parameter index*) (*IPsec*)

TCP Protocolo de control de transmisión (*transmission control protocol*)

TISPAN Servicios y protocolos convergentes de telecomunicaciones e Internet para la interconexión avanzada (*telecommunication and Internet converged services and protocols for advanced networking*)

UDP Protocolo de datagramas de usuario (*user datagram protocol*)

5 Convenios

Este documento contiene una lista de elementos en el formato ***R-x/y***, siendo *x* el número de cláusula e *y* un número dentro de dicha cláusula. En estos elementos se utilizan las siguientes expresiones con el significado que se indica a continuación:

La expresión "**se requiere**" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con este documento.

La expresión "**se prohíbe**" indica que el requisito está terminantemente prohibido y no se permite excepción alguna si se pretende declarar la conformidad con este documento.

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

La expresión "**se tiene la opción de**" indica que el requisito se permite, sin que ello signifique que se recomienda. No se pretende implicar que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

En el cuerpo de la presente Recomendación y en sus anexos aparecen algunas veces verbos que expresan obligación, prohibición, recomendación y posibilidad, en cuyo caso deben interpretarse en dicho sentido. Cuando estas expresiones o términos aparecen en apéndices o en partes incluidas explícitamente a título informativo no deben interpretarse en su sentido normativo.

6 Requisitos de la entidad funcional IDP

6.1 Identificación de flujos y aplicaciones

R-6.1/1: Se requiere que la entidad funcional IDP realice la identificación de la aplicación.

R-6.1/2: Se requiere que la entidad funcional IDP admita diversos tipos de reglas políticas IDP.

R-6.1/3: Se requiere que la DPI-FE identifique la aplicación inspeccionando la carga útil de la misma.

R-6.1/4: Se requiere que las condiciones a nivel de aplicación IDP (y las condiciones a nivel de flujo facultativas) permitan identificar la aplicación a partir del tráfico unidireccional (IDP unidireccional) para todas las aplicaciones unidireccionales y bidireccionales a condición de que una dirección del tráfico permita la identificación inequívoca.

R-6.1/5: Se tiene la opción de que las condiciones a nivel de aplicación IDP (y las condiciones a nivel de flujo facultativas) permitan la identificación de la aplicación a partir del tráfico bidireccional (IDP bidireccional).

R-6.1/6: Se recomienda que los elementos de información utilizados en las condiciones a nivel de flujo cumplan lo estipulado en [b-IETF RFC 5102]**,** registrado por la IANA [b-IETF IANA IPFIX]. En tales casos se recomienda que los elementos de información incluyan elementos de información IPFIX relacionados con las capas de enlace (L2), de red (L3) y de transporte (L4) del protocolo, en consonancia con la arquitectura estratificada básica del protocolo del IETF.

NOTA – El registro IANA para elementos de información IPFIX se podría ampliar para incluir elementos adicionales (por el IETF). El actual registro IANA (a finales del año 2011) carece de elementos de información para protocolos L4 distintos de UDP y TCP (por ejemplo, para SCTP y DCCP).

R-6.1/7: Se tiene la opción de que los elementos de información sean distintos de los relacionados con L2, L3 o L4 fuera del registro IPFIX (denominados elementos de información específicos de la empresa en el protocolo IPFIX [IETF RFC5101]).

6.2 Gestión de firmas IDP

En esta cláusula se definen los requisitos relativos a las operaciones en la biblioteca de firmas IDP. Estas operaciones puede iniciarlas localmente la DPI-FE, o una entidad de red remota (véase la

Figura 6-1). Todos los tipos posibles de entidades de red remotas pueden considerarse una abstracción de la entidad funcional de decisión política IDP que decide las reglas basadas en la firma que se aplicarán en la DPI-FE.

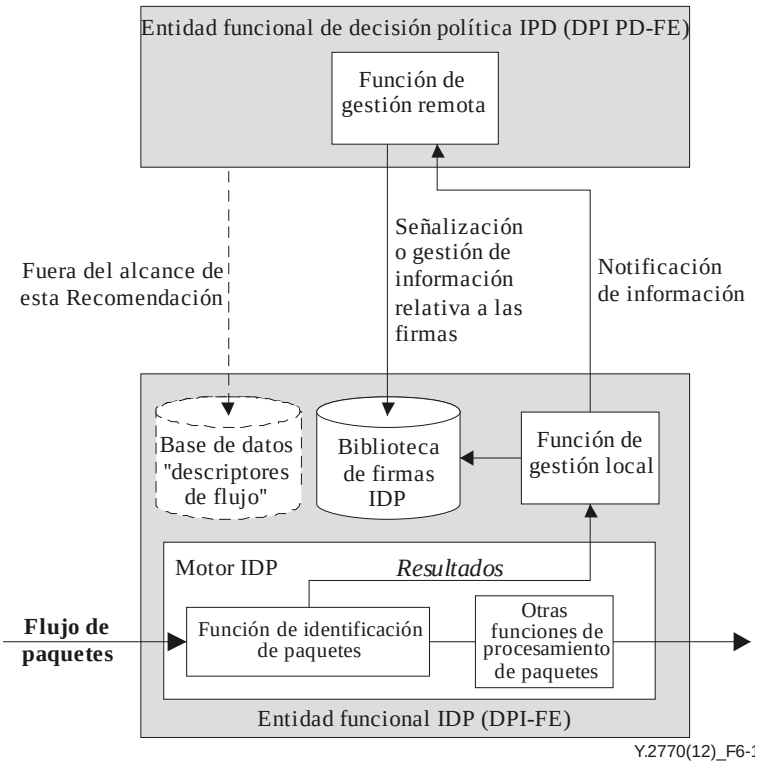


Figura 6-1 – Gestión de firmas IDP en el contexto de un ejemplo de arquitectura de entidad funcional IDP (véase también la Figura 8-2 en relación con las interfaces internas)

La entidad funcional de decisión política IDP guardará relación con la RACF (en el caso de una NGN con RACF), pero su especificación queda fuera del alcance de la presente Recomendación. Se incluye en la Figura 6.1 porque contiene las funciones de gestión remota para la DPI-FE.

6.2.1 Requisitos generales de la firma

R-6.2.1/1: Se requiere que las firmas IDP estén almacenadas en la *biblioteca de firmas IDP,* que es una subentidad de la DPI-FE.

NOTA – La razón de esta biblioteca de firmas IDP local es que la función de identificación de paquetes necesita acceso inmediato al contenido de la base de datos.

La firma IDP puede utilizarse para:

- la identificación aproximada (por ejemplo, basada en el análisis funcional, heurística, etc.); y
- la identificación exacta (es decir, reglas de concordancia exacta).

El lenguaje (formal o funcional) utilizado para especificar las reglas políticas IDP en esta biblioteca, y las reglas de concordancia, quedan fuera del alcance de la presente Recomendación. En esta Recomendación sólo se especifica la existencia de la biblioteca de firmas IDP, se define la firma IDP y se especifican las funciones de gestión de la biblioteca.

R-6.2.1/2: Se requiere que la biblioteca de firmas IDP esté protegida y sea invisible para usuarios no autorizados.

6.2.2 Gestión de la biblioteca de firmas IDP

En esta cláusula se definen los requisitos para la gestión de la biblioteca de firmas IDP.

6.2.2.1 Adición de nuevas firmas

R-6.2.2.1/1: Se requiere que se puedan añadir nuevas firmas IDP a la biblioteca de firmas.

6.2.2.2 Operaciones sobre las firmas existentes

R-6.2.2.2/1: Se requiere que se puedan modificar (actualizar) las firmas existentes en la biblioteca de firmas IDP.

R-6.2.2.2/2: Se requiere que se puedan habilitar y deshabilitar firmas IDP específicas en la biblioteca de firmas IDP.

R-6.2.2.2/3: Se requiere que se puedan suprimir (borrar) firmas IDP específicas de la biblioteca de firmas IDP.

6.2.2.3 Formato de las reglas que se intercambian a través de la interfaz externa

R-6.2.2.3/1: Se tiene la opción de que la firma IDP para la identificación de la aplicación que se intercambia a través de interfaces externas (es decir, *e1* y *e2* en la Figura 8-1) pueda tener cualquier formato de regla (véase también la cláusula 1.2).

6.2.3 Ubicación de la función de gestión

R-6.2.3/1: Se requiere que las acciones de gestión de firmas IDP especificadas en la cláusula 6.2.2 las efectúe localmente la entidad funcional IDP o a distancia o ambas (véase la Figura 6-1).

6.2.4 Inicio de acciones de gestión

R-6.2.4/1: Se requiere poder emplear el modo 'a discreción' (*push*) para las operaciones relacionadas con firmas IDP, cuando las operaciones se inician a distancia (por ejemplo, las inicia la DPI-PDFE en la Figura 6-1).

R-6.2.4/2: Se requiere poder emplear el modo 'por solicitud' (*pull*) para las operaciones relacionadas con firmas IDP, cuando las operaciones las inicia localmente la DPI-FE. El concepto de 'por solicitud' significa que la función de gestión local DPI-FE solicita a la DPI-PDFE que realice una acción de gestión sobre una firma nueva o existente.

La forma en que la DPI-FE formula la solicitud queda fuera del alcance de la presente Recomendación.

6.3 Aspectos relativos a la inspección del tráfico

Esta cláusula versa sobre los aspectos relativos a los tipos de tráfico a los que puede aplicarse la IDP.

6.3.1 Aspectos relativos a la identificación de flujos

R-6.3.1/1: Se requiere que la entidad funcional IDP admita la identificación de aplicaciones, sin tener que efectuar una inspección a nivel de flujo.

R-6.3.1/2: Se tiene la opción de que toda IDP sea independiente del flujo inicialmente, es decir, que la regla política IDP suministrada a la DPI-FE no contenga un descriptor del flujo. Ahora bien, la regla podrá solicitar que se recabe información de interés sobre el flujo.

R-6.3.1/3: Se requiere que esta solicitud proporcione una clave de flujo IPFIX y tenga la opción de completar la información que falte sobre el flujo.

R-6.3.1/4: La entidad funcional IDP tiene la opción de solicitar el reconocimiento completo del identificador de flujo IPFIX basado en una determinada clave de flujo IPFIX y la inspección de varios paquetes posteriores.

R-6.3.1/5: Se tiene la opción de que la notificación de un identificador de flujo IPFIX completo o incompleto por parte de la DPI-FE a una entidad de red remota sea condicional (es decir, en función del evento, de un temporizador, etc.).

6.3.2 Aspectos de la IDP que conoce o desconoce la pila de protocolo

La función de identificación IDP (en una DPI-FE) es responsable de identificar la aplicación y de comparar y buscar operaciones, en función de la firma IDP, con respecto al paquete entrante (PDU). Existen dos opciones: la DPI-FE conoce la estructura interna de la PDU (es decir, "*DPI-FE conoce la pila del protocolo*") o no conoce dicha estructura ("*DPI-FE desconoce la pila del protocolo*").

Las dos opciones permiten obtener el mismo resultado de la identificación y pueden ser funcionalmente equivalentes. La principal diferencia radica en que la lógica de identificación que conoce la pila del protocolo puede ser más eficiente.

Resulta útil distinguir entre los siguientes dos tipos de análisis relativos a la eficiencia operativa (es decir, identificación de la aplicación e identificación opcional del flujo):

a) Análisis predeterminado de la carga útil (PPA): cuando los paquetes (flujo) se corresponden a una aplicación conocida que tiene una estructura de carga útil claramente definida, la DPI-FE puede inspeccionar la ubicación predeterminada de la carga útil (es decir, modo de inspección de paquetes que conoce la pila del protocolo).

b) Análisis exhaustivo de la carga útil (FPA): Cuando los paquetes (flujo) no se corresponden con una aplicación conocida o la estructura de la carga útil de la aplicación no está claramente definida o se desconoce, la DPI-FE inspecciona "toda la carga útil" (es decir, modo de inspección de paquetes que desconoce la pila del protocolo).

La PPA y FPA pueden aplicarse al mismo flujo de tráfico.

R-6.3.2/1: Se recomienda que la DPI-FE admita la identificación de la aplicación que conoce la pila del protocolo.

R-6.3.2/2: se recomienda que la DPI-FE admita la identificación de la aplicación que desconoce la pila de protocolo.

R-6.3.2/3: Se requiere que la DPI-FE identifique aplicaciones que se ejecutan en la parte superior de la pila del protocolo IPv4 e IPv6 y que tenga la opción de identificar aplicaciones que se ejecutan en otras pilas de protocolo subyacentes.

R-6.3.2/4: Se recomienda que la DPI-FE identifique aplicaciones en el tráfico anidado, por ejemplo tráfico encapsulado o por túneles.

6.3.3 Aspectos relativos a las acciones de regla política IDP

6.3.3.1 Antecedentes

Las acciones de política IDP pueden realizarse a distintos niveles jerárquicos, por ejemplo, en la DPI-FE, en PDF locales y remotas, y pueden incluir, por ejemplo, lo siguiente:

1) Acciones a nivel de trayecto de paquetes (por la DPI-FE):
    a) Aceptación y renvío del paquete a la función de retransmisión de paquetes (PFF) (acción condicional en el modo *IDP en el trayecto* solamente).
    b) Descarte del paquete (con o sin indicarlo).
    c) Redireccionamiento del paquete hacia otras interfaces de salida.
    d) Duplicación/copia exacta del paquete hacia otras interfaces de salida.
    e) Clasificación del tráfico, mediciones locales y notificación de datos medidos.
    f) Establecimiento de prioridades, bloqueo, conformación y planificación de paquetes individuales.

2) Acciones a nivel de nodo (con la intervención de la *función de decisión política local* (L-PDF)):

   a) Creación dinámica de nuevas reglas políticas IDP y/o modificación de las existentes (almacenadas en la base de información de política IDP (DPI-PIB)).

   b) Generación de registros/rastros de datos y notificación a la gestión de políticas (véase la cláusula 2.11.2 in [b-IETF RFC 3871]).

   c) Detección y notificación de aplicaciones no identificables.

   d) Notificación de sistemas de detección de intrusión (por ejemplo, informando de muestras de tráfico o paquetes sospechosos).

3) Acciones a nivel de red (por medio de la *función de decisión política remota* (R-PDF)):

   a) Gestión de recursos, control de admisión y filtrado de alto nivel (a nivel de subsistemas de red, como se especifica para RACF en [ITU-T Y.2111], ETSI TISPAN RACS [b-ETSI ES 282 003] y 3GPP PCC [b-ETSI TS 123 203]).

   b) Tasación del contenido en función de los tipos de aplicaciones del abonado (por ejemplo, IETF RADIUS o Diameter).

En la Figura 6.2 se explica el principio de estructuración anterior mediante un formato de regla política genérico pormenorizado (a diferencia del presentado en la cláusula 1.2):

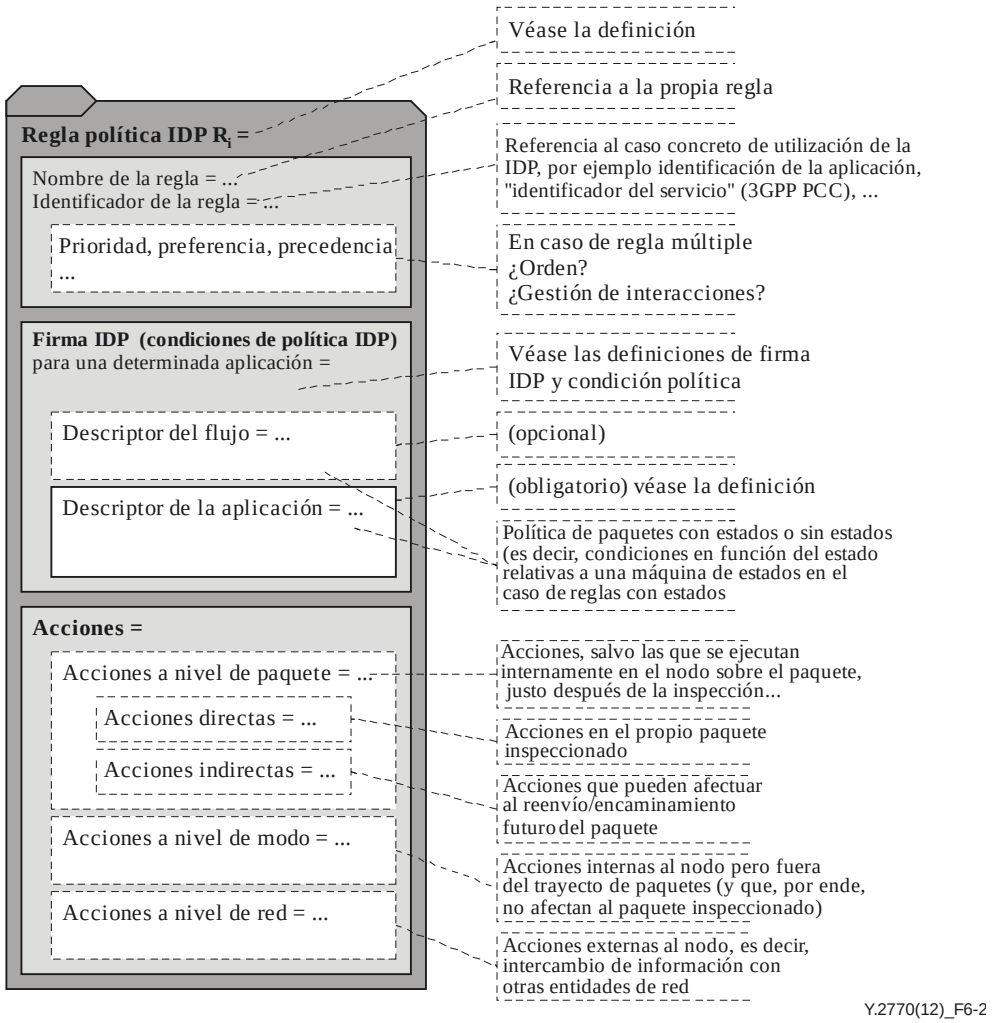


Figura 6-2 – Ejemplo de formato pormenorizado de regla política (en comparación con la Figura 1-2)

La relación entre las acciones específicas y las condiciones queda fuera del alcance de la presente Recomendación.

6.3.3.2 Requisitos

R-6.3.3.2/1: Una vez que la DPI-FE ha identificado la aplicación, tiene la opción de extraer información específica de la aplicación.

Por ejemplo, una URL en HTTP, un formato de medios ("tipo de códec") en el protocolo de transporte en tiempo real (RTP), o un identificador de sesión RTP (por ejemplo, SSRC para el extremo de origen RTP).

R-6.3.3.2/2: La DPI-FE tiene la opción de colaborar con una función de cómputo de flujo, por ejemplo el proceso de cómputo IPFIX [IETF RFC 5101] y con algunas capacidades de filtrado, tales como [b-IETF RFC 5476].

NOTA – Es proceso de cómputo suele rellenar los siguientes campos de información IPFIX (utilizados como claves de flujo): sourceIPv6Address y destinationIPv6Address, sourceIPv4Address y destinationIPv4Address, protocolIdentifier, sourceTransportPort, destinationTransportPort, etc. Ahora bien, corresponde a la DPI-FE rellenar la etiqueta de la aplicación y completar el identificador del flujo IPFIX (a partir de la clave de flujo IPFIX determinada, véase también la Figura A.1).

6.4 Capacidad de notificación

Se refiere a la notificación (por ejemplo, cuando la DPI-FE detecta un determinado evento) a otra entidad funcional, que por lo general estará ubicada en un elemento de red distante (del plano de usuario, de control o de gestión). La DPI-FE puede ofrecer múltiples interfaces de notificación para "diferentes tipos de eventos".

6.4.1 Notificación al sistema de gestión de red (NMS)

6.4.1.1 Interfaz y protocolo para la notificación

R-6.4.1.1/1: Se recomienda que el protocolo *export* cumpla las especificaciones IPFIX [IETF RFC 5101], y tenga la opción de cumplir las extensiones IPFIX.

R-6.4.1.1/2: El protocolo *export* tiene la opción de cumplir la especificación IPFIX [b-IETF RFC 5103] en el caso de flujos bidireccionales.

R-6.4.1.1/3: Se recomienda que los protocolos *export* basados en IPFIX utilicen la interfaz externa e2 (véase la Figura 8.1).

6.4.1.2 Información notificada

R-6.4.1.2/1: Se requiere que la DPI-FE notifique al plano de gestión IDP los resultados de la inspección (por ejemplo la etiqueta de la aplicación y posibles elementos de información específicos de la aplicación) junto con la información específica del flujo. Tiene la opción de exportar los valores clave de flujo actualizados localmente (incluidos los campos característicos de la función de cómputo de flujo) a un función de decisión política (por ejemplo, la PD-FE definida en [ITU-T Y.2111]).

R-6.4.1.2/2: Se recomienda reutilizar los elementos de información IPFIX ([b-IETF IANA IPFIX]), que fueron inicialmente especificados en el modelo de información IPFIX [b-IETF RFC 5102].

La información específica del flujo se especifica en el modelo de información IPFIX [b-IETF RFC 5102], por ejemplo:

1) Información específica de la aplicación:
   - etiqueta de la aplicación; y
   - campos extraídos, por ejemplo el formato de medios RTP y RTP SSRC.

2) Campos del encabezamiento L3/L4 correspondientes a direcciones IP, puertos L4 (por ejemplo, TCP o UDP, Nota 1), y tipo de protocolo;

3) Información de calidad de funcionamiento (como métrica, estadística) cómputo de bits, cómputo de paquetes, y tamaño máximo del paquete (Nota 2);

4) Información de tiempo: tiempo de inicio del flujo, tiempo de fin del flujo;

5) Información relativa a los paquetes: próximo tramo y tamaño del paquete (Nota 3);

NOTA 1 – Algunos elementos de información enumerados (aún) no forman parte del registro IPFIX de la entidad de asignación de números Internet (IANA), pero son válidos en el contexto de la presente Recomendación.

NOTA 2 – La información específica del flujo puede generarse por muestreo de paquetes (PSAMP), pero al exportar tales resultados al NMS, se recomienda añadir la información específica de la aplicación.

NOTA 3 – Quizá se hayan de registrar nuevos elementos de información en la IPFIX IANA, con arreglo a la sección 7 "consideraciones de la IANA" de la [b-IETF RFC 5102].

6.4.2 Notificación de una aplicación nueva, desconocida o incorrecta

6.4.2.1 Características de este tráfico

Las diferencias entre estos tipos de aplicación son sutiles. Pueden caracterizarse por las siguientes propiedades específicas, que resultan en diferentes condiciones de nivel de aplicación para su detección:

– Nueva aplicación: por ejemplo, una nueva versión de una aplicación, una nueva versión de un elemento de información específico de la aplicación (por ejemplo, una nueva versión de juego dentro del protocolo de juegos abierto (OGP)), o una nueva versión del protocolo; cabe destacar que el concepto de 'nuevo' se refiere al punto de vista del servicio IDP (que puede basarse en un historial de los servicios IDP anteriores).

– Aplicación desconocida: por ejemplo, un tipo de paquete desconocido, un protocolo desconocido, o una "aplicación" desconocida.

– Aplicación incorrecta: por ejemplo, una gramática del protocolo incorrecta (Nota), etc.

NOTA – Una sintaxis del protocolo incorrecta puede explotarse para realizar un ataque contra la seguridad. Los protocolos afectados suelen ser los que terminan en el equipo del usuario (como los protocolos de señalización).

6.4.2.2 Requisitos de notificación

R-6.4.2.2/1: La DPI-FE tiene la opción de admitir la notificación de aplicaciones nuevas, desconocidas o incorrectas tras inspeccionar el tráfico.

6.4.3 Notificación de tráfico anómalo

R-6.4.3/1: La DPI-FE tiene la opción de proporcionar una capacidad de notificación de *tráfico anómalo* una vez detectado.

El *tráfico anómalo* se define como el tráfico que no se corresponde con las clases del tráfico normal. La clase de tráfico normal es un conjunto de tráfico que corresponde con las propiedades estadísticas existentes de aplicaciones bien definidas, tales como el tiempo de llegada de paquetes, el orden de llegada, el tamaño de la PDU de una capa de protocolo específica, el tamaño de la carga útil, o el volumen de tráfico (en una determinada capa de protocolo).

6.4.4 Notificación de eventos relacionados con la DPI-PE

En esta cláusula se describen los eventos relacionados con el estado operativo de la entidad IDP y los requisitos de notificación correspondientes.

6.4.4.1 Eventos de averías relacionadas funcionamiento incorrecto de la DPI-PE

La forma más sencilla de representar el estado de la DPI-PE es mediante dos estados: "en servicio" (IS) y "fuera de servicio" (OoS).

R-6.4.4.1/1: Se recomienda que la gestión IDP se base en la versión actual (por ejemplo, [ITU-T X.731] y [b-IETF RFC 4268]) y se recomienda que como mínimo admita los estados de gestión IS y OoS.

R-6.4.4.1/2: Siempre que no exista una arquitectura redundante, toda avería de la DPI-PE tiene la opción de desencadenar una transición del estado IS al OoS. Se recomienda que se notifiquen tales eventos.

6.4.4.2 Eventos relacionados con la gestión de averías de la DPI-PE

La DPI-PE dispone de interfaces de red para el tráfico entrante y saliente. Pueden producirse averías en estas interfaces.

R-6.4.4.2/1: Se recomienda que la DPI-PE disponga de una función de notificación de alarmas como la definida en [b-ITU-T X.734].

6.4.4.3 Eventos relacionados con el registro de la entidad funcional IDP

R-6.4.4.3/1: La entidad funcional IDP tiene la opción de admitir una capacidad de registro (*logging*) del sistema con arreglo, por ejemplo, a *Syslog* [b-IETF RFC 5424]. En tal caso, la entidad funcional IDP es un punto de origen de *mensajes Syslog*.

Cabe señalar que en caso de que el flujo de paquetes inspeccionado transporte tráfico de registro, la entidad funcional IDP no es un punto de origen ni un punto de terminación de mensajes de registro. Es decir, la clave de búsqueda para este flujo de paquetes puede basarse en un *descriptor de la aplicación* (relacionado con la capa de *aplicación syslog*) y un *descriptor del flujo* IPFIX (relacionado con el modo de *transporte syslog* seleccionado). Para mayor información, véanse [b-IETF RFC 5424] y [b-IETF RFC 5426].

6.4.4.4 Eventos relacionados con el estado de la carga y el consumo de recursos de la entidad física IDP

La DPI-PE dispone de recursos limitados para el procesamiento IDP. Los recursos concretos dependen de la implementación y quedan fuera del alcance de la presente Recomendación.

R-6.4.4.4/1: Se recomienda que la entidad física IDP notifique al plano de gestión el nivel de carga de los componentes de recursos IDP.

Por ejemplo, en redes con tráfico de telecomunicaciones de emergencia (véase la cláusula 7.1.1), el proceso IDP debe ser capaz de retransmitir el tráfico ET a través de nodos de red congestionados; por consiguiente, conviene que el sistema de gestión de red conozca el nivel de carga.

6.5 Interacción con la función de decisión política

R-6.5/1: La DPI-FE tiene la opción de actuar como una parte de la entidad funcional de aplicación e política definida en [ITU-T Y.2111] y proporcionar la función de transporte correspondiente.

R-6.5/2: Se tiene la opción de que la interfaz entre la DPI-FE y la RACF sea la Rw, definida en [ITU-T Y.2111].

R-6.5/3: Se tiene la opción de intercambiar la información entre DPI-FE y la RACF PD-FE a través de las interfaces RACI *existentes* (por ejemplo, la interfaz *Rw*) o *nuevas*, dependiendo del caso específico de utilización de la IDP.

NOTA – En este caso, es preciso modificar la RACF para que incluya información IDP (por ejemplo, una firma de protocolo en una regla política IDP); la RACF definida en [ITU-T Y.2111] admite reglas políticas

basadas principalmente en la identificación del flujo. El punto de referencia RACF específico dependerá del caso concreto de utilización de la IDP.

6.6 Control del tráfico

Se pueden deducir los siguientes requisitos de alto nivel:

R-6.6/1: La entidad funcional IDP tiene la opción de intervenir en situaciones de red a los efectos de control del tráfico (por ejemplo, las funciones de control del tráfico definidas en [ITU-T Y.1221]). Se recomienda que la DPI-FE admita capacidades de control de tráfico.

R-6.6/2: La DPI-FE tiene la opción de efectuar nativamente el control de tráfico. No obstante, la descripción detallada de los requisitos funcionales para el control del tráfico queda fuera del alcance de la presente Recomendación.

R-6.6/3: La DPI-FE tiene la opción de interaccionar con funciones externas de control del tráfico. Los correspondientes requisitos funcionales quedan fuera del alcance de la presente Recomendación.

6.7 Identificación de sesiones

En esta sesión se utilizan muchos términos relacionados con la *sesión*. La DPI-FE puede identificar inequívocamente todo el tráfico de una sesión, por cuanto el "*descriptor de sesión*" es igual al descriptor del flujo y/o de la aplicación o a un subconjunto del mismo.

6.7.1 Requisitos para la identificación de sesión

R-6.7.1/1: Se requiere que la DPI-FE sea capaz de realizar un análisis funcional de la sesión (por ejemplo, sesión RTP, sesión HTTP, sesión IM, sesión VoIP SIP).

R-6.7.1/2: Se requiere que la DPI-FE sea capaz de conocer el estado de la sesión.

6.7.2 Acciones IDP "a nivel de sesión"

R-6.7.2/1: La DPI-FE tiene la opción de extraer o generar datos de medición a nivel de sesión (por ejemplo, para supervisar la métrica de la calidad de funcionamiento relativa a la calidad percibida por el abonado.

6.8 Inspección de tráfico encriptado

Existe una opinión generalizada de que las firmas IDP sólo pueden aplicarse al tráfico no encriptado. Sin embargo, las firmas IDP pueden aplicarse al tráfico encriptado en función de:

- El nivel de encriptación (véase la cláusula 6.8.1).
- La disponibilidad local de la clave de desencriptación (véase la cláusula 6.8.2).
- Las condiciones de inspección basadas en la información encriptada (véase la cláusula 6.8.3).

6.8.1 Grado de encriptación

Todo "paquete" en calidad de unidad de datos de protocolo (PDU) consta de información de control de protocolo (PCI) y unidades de datos de servicio (SDU) en diversas capas de protocolo. En el trayecto de comunicación inspeccionado, la encriptación puede aplicarse:

- a toda la pila del protocolo o sólo a una parte de la misma (Nota 1); y
- dentro de la capa del protocolo, a la PDU de la capa x (Lx) (es decir, a toda la Lx-PDU) o sólo parcialmente (por ejemplo, solo a la parte Lx-PCI o Lx-SDU).

NOTA 1 – Ejemplo: el servicio de paquetes RTP por IP puede proporcionar encriptado a:

a) la capa de red (por ejemplo, por medio del modo de transporte IPsec o de túnel IPsec);

b) la capa de transporte (por ejemplo, mediante DTLS); y/o

c) la capa de aplicación (por ejemplo, a través de SRTP).

La IDP puede realizarse en cualquier parte no encriptada del paquete.

R-6.8.1/1: Conocimiento del tráfico encriptado (desde la perspectiva de la firma IDP): se tiene la opción de efectuar la IDP en todos los elementos de información no encriptados del tráfico inspeccionado, dependiendo del grado de encriptación (Nota 2).

NOTA 2 – Ejemplo: el flujo de paquetes SRTP por IP aún puede inspeccionarse en caso de firmas IDP, en función de los elementos de información acerca de RTP PCI ("encabezamiento RTP"), UDP PCI ("encabezamiento UDP"), IP PCI ("encabezamiento IP"), etc., si sólo está encriptada la RTP SDU (que contiene los datos de la aplicación IP).

R-6.8.1/2: Desconocimiento del tráfico encriptado (desde la perspectiva de la firma IDP): la IDP tiene la opción de realizar una IDP parcial (porque algunas partes de las firmas IDP podrían estar relacionadas con elementos de información de paquetes no encriptados).

Esta "IDP parcial" del tráfico encriptado puede dar lugar a "servicios IDP limitados", aunque puede que sean suficientes para determinados casos de utilización (por ejemplo, si basta con una identificación "de granularidad gruesa" de la aplicación o el protocolo).

6.8.2 Disponibilidad de clave de desencriptación

R-6.8.2/1: Se tiene la opción de aplicar la IDP en caso de disponibilidad local de la clave o claves de encriptación utilizadas. Así, toda IDP conllevará la desencriptación inicial del paquete inspeccionado (o de una copia local del mismo).

6.8.3 Condiciones para inspecciones basadas en información encriptada

R-6.8.3/1: Se tiene la opción de aplicar la IDP al tráfico encriptado, en el caso de condiciones de política aplicables para inspecciones basadas en información encriptada (Nota).

NOTA – Ejemplo: puede obtenerse un patrón de bits (que identifique inequívocamente a un determinado flujo de paquetes) mediante la observación (inspección) de tráfico parcialmente encriptado (véase la cláusula 6.8.1). El diagrama de bits, como parte de las ulteriores firmas IDP, ya estará disponible en la codificación encriptada.

6.8.4 Requisitos de IDP específicos de IPsec

Los requisitos estipulados en las cláusulas 6.8.1 a 6.8.4 son igualmente válidos para los paquetes encriptados con IPsec. Esta Recomendación se centra en los aspectos de identificación de flujo del tráfico encriptado IPsec. Los aspectos relativos a la identificación de la aplicación serán objeto de un estudio ulterior.

6.8.4.1 Requisitos generales

R-6.8.4.1/1: La DPI-FE tiene la opción de admitir, como mínimo, la *identificación de flujo* para el tráfico encriptado IPsec. El correspondiente descriptor del flujo de n tuplas tiene la opción de limitarse exclusivamente a los elementos básicos de L2 y L3.

R-6.8.4.1/2: El flujo también tiene la opción de corresponder al tráfico de una misma *asociación de seguridad* (SA) IPsec o a varias SA.

R-6.8.4.1/3: La identificación de flujo basada en SA implica que se tiene la opción de que el *índice de parámetro de seguridad* (SPI) IPsec de 32 bits forme parte del descriptor del flujo.

6.8.4.2 Modo túnel y de transporte IPsec

Pueden utilizarse los protocolos IPsec (AH y ESP, véase *infra*) para proteger la carga útil IP (es decir, el modo túnel) o los protocolos de capa superior de una carga útil IP (es decir, modo transporte).

R-6.8.4.2/1: La DPI-FE tiene la opción de detectar tráfico encriptado IPsec en el modo túnel.

R-6.8.4.2/2: La DPI-FE tiene la opción de detectar tráfico encriptado IPsec en el modo transporte.

6.8.4.3 Tráfico con AH protegido IPsec

El *encabezamiento de autentificación* (AH) proporciona integridad en los datos, autentificación del origen de los datos y servicios antirespuesta optativos limitados.

R-6.8.4.3/1: La DPI-FE tiene la opción de detectar tráfico con AH protegido basado en el correspondiente número de protocolo IP.

6.8.4.4 Tráfico con ESP protegido IPsec

El *encapsulado de carga útil de seguridad* (ESP) proporciona confidencialidad adicional.

R-6.8.4.4/1: La DPI-FE tiene la opción de detectar tráfico con ESP protegido basado en el correspondiente número de protocolo IP.

6.9 Inspección de tráfico comprimido

La finalidad de la compresión es reducir el volumen de tráfico. Por ejemplo:

- la compresión "ZIP" [b-IETF RFC 1950] reduce el tamaño del fichero (pertinente para los flujos FTP por TCP/IP);
- la compresión "SigComp" [b-IETF RFC 3320] reduce el tamaño de los mensajes SIP (atañe a los flujos SIP por L4/IP).

6.9.1 Conocimiento del método de compresión

R-6.9.1/1: Se tiene la posibilidad de realizar la IDP cuando se disponga de información local relativa al tipo de compresión aplicado (por ejemplo, si el nodo IDP es consciente de que el trayecto de señalización SIP inspeccionado está codificado con arreglo a la cláusula 8 de [b-ETSI TS 124 229]). La aplicación de cualquier IDP implicará la descompresión inicial del paquete inspeccionado (o de una copia local del mismo).

R-6.9.1/2: Se tiene la opción de realizar la IDP cuando sea posible obtener el tipo de compresión aplicada inspeccionando el flujo de tráfico (por ejemplo, se tiene la posibilidad de obtener el método de compresión zip concreto a partir de los elementos de información del encabezamiento del fichero).

6.10 Detección de tráfico anómalo

6.10.1 Requisitos para detectar el tráfico anómalo

R-6.10.1/1: Se requiere que la DPI-FE pueda detectar el tráfico anómalo. Concretamente, se requiere que las firmas IDP permitan caracterizar el tráfico normal y el anómalo (por ejemplo, mediante una lista negra o blanca).

NOTA – Aspectos relativos a la regla política de IDP: Esta capacidad podría implicar la verificación de muchas métricas en relación con las características del tráfico y/o de los paquetes, así como la posibilidad de mantener un árbol de decisiones para llegar a una conclusión definitiva acerca de las clases de tráfico, normal o anómalo.

7 Requisitos funcionales desde el punto de vista de la red

7.1 Requisitos generales

7.1.1 Telecomunicaciones de emergencia

El diseño general, la implementación, el despliegue y la utilización de funciones IDP tienen que contar con medidas adecuadas para impedir los efectos negativos sobre la calidad de funcionamiento y la seguridad de las telecomunicaciones de emergencia (TE). Por TE

[ITU-T Y.2205] se entiende cualquier servicios de emergencia que requiere trato preferente respecto de otros servicios (por ejemplo, prioridad sobre los servicios ordinarios). Como ejemplos cabe citar los servicios de emergencia autorizados por el gobierno, tales como, el servicio de telecomunicaciones de emergencia [ITU-T E.107] y los servicios de seguridad pública.

La presente Recomendación se basa en la utilización de una etiqueta de la aplicación para identificar la semántica de las diferentes aplicaciones, por ejemplo el tipo de protocolo de aplicación (por ejemplo, vídeo UIT-T H.264 video o SIP como ejemplo de protocolo de aplicación IP) de manera genérica. Se utilizan los mismos tipos de aplicación (por ejemplo, SIP) para servicios ordinarios y de TE. Ahora, en esta Recomendación no se especifica ninguna etiqueta única para identificar los servicios de aplicaciones de TE, por lo que será necesario tomar las debidas precauciones para no afectar negativamente a dichos servicios.

R-7.1/1: Se requiere no interferir con el tratamiento prioritario del tráfico correspondiente a los servicios de aplicaciones TE respecto a los servicios ordinarios.

R-7.1/2: Se requiere que el diseño general, la implementación, el despliegue y la utilización de funciones IDP incluyan medidas adecuadas para no afectar negativamente a la calidad de funcionamiento de los servicios de aplicaciones TE (por ejemplo, introducción de retardos innecesarios).

R-7.1/3: Se requiere que el diseño general, la implementación, el despliegue y la utilización de funciones IDP incluyan medidas adecuadas para impedir que se ponga en peligro la seguridad y la integridad, confidencialidad o disponibilidad de las comunicaciones/sesiones de TE.

NOTA – En la presente Recomendación no se estipula cómo deben cumplirse estos requisitos. Para ello puede recurrirse a capacidades funcionales, mediciones operativas o una combinación de ambas.

7.2 Plano de datos, plano de control y plano de gestión en el nodo IDP

7.2.1 Planos de tráfico y tipos de tráfico desde la perspectiva del nodo IDP

De acuerdo con el modelo de red del plano de usuario, control y gestión (véase [b-ITU-T Y.2011]), el nodo IDP se encarga del trayecto de datos y del trayecto de decisión local (véase la Figura 7-1). El trayecto de datos puede funcionar en modo unidireccional o bidireccional.

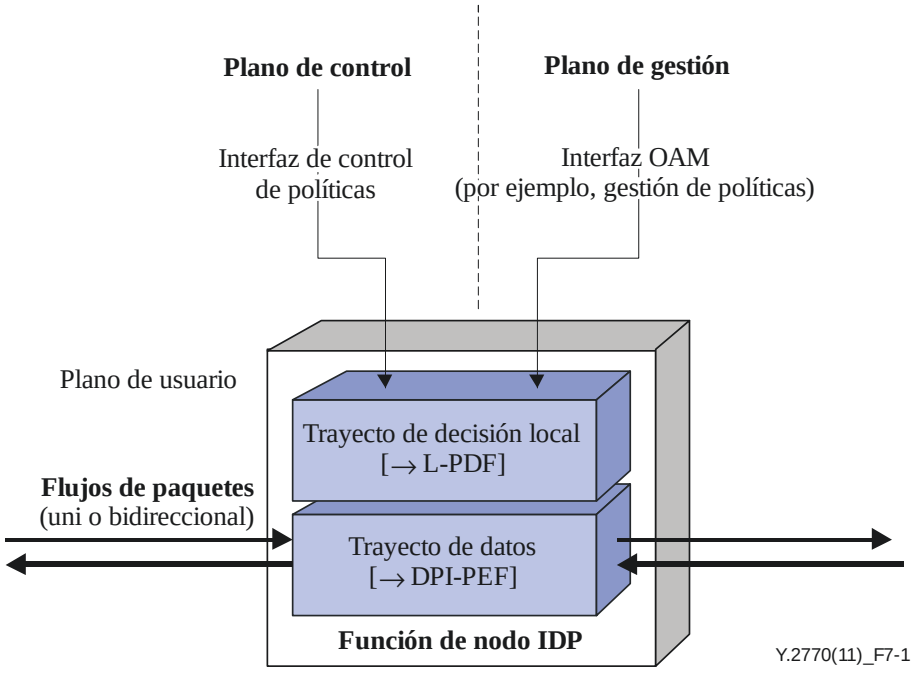


Figura 7-1 – Planos de tráfico externo e interno de un nodo IDP

NOTA 1 – Los flujos de paquetes se encaminan/conmutan a lo largo de trayectos de paquetes, que a menudo se llaman *trayectos de datos* en redes IP (véase por ejemplo [b-IETF RFC 4778]); por consiguiente el término *plano de datos* es sinónimo de *plano de usuario*.

NOTA 2 – El trayecto de datos IP también se denomina trayecto de medios IP (*o trayecto portador*) en el caso de tráfico de datos de aplicación IP, o *trayecto de señalización* IP en el caso de tráfico de control de aplicaciones IP [b-ITU-T X.1141].

R-7.2.1/1: Se requiere que el nodo IDP disponga de una interfaz con el plano de gestión para la gestión de políticas y tenga la opción de disponer de una interfaz del plano de control para el control de políticas.

La entidad de *trayecto de decisión local* proporciona capacidades de gestión y control internas del nodo.

R-7.2.1/2: Se requiere que el nodo IDP reconozca dos tipos de paquetes (véase la Figura 7-2):

a) paquetes de datos, que pertenecen a clientes y transportan tráfico del cliente (denominado "tráfico A TRAVÉS DE", véase [b-IETF opsec]); y

b) paquetes de control y gestión, que pertenecen al proveedor de red y están relacionados con las operaciones de red (denominado "tráfico HACIA"; véase [b-IETF opsec]).

Los dos tipos de paquetes atraviesan un "conducto común" (o están "en la banda") o atraviesan canales diferentes que separan lógicamente datos de los paquetes de control "fuera de banda" (en la cláusula 2.2 de [b-IETF RFC 4778] se da un ejemplo de tráfico de gestión).

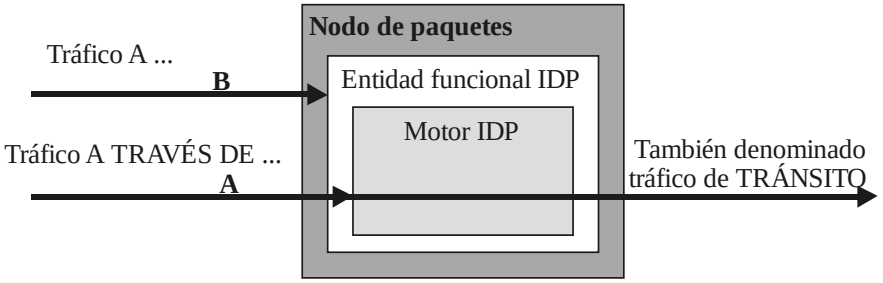


Figura 7-2 – Tráfico A TRAVÉS DE (A) y HACIA (B) un nodo IDP

7.2.2 Requisitos relacionados con el plano de gestión

R-7.2.2/1: Se requiere que la DPI-FE admita protocolos de gestión para gestionar la configuración de reglas políticas IDP.

R-7.2.2/2: Se recomienda que la DPI-FE gestione información sobre la identidad del usuario y la relación entre el usuario y las aplicaciones de usuario.

R-7.2.2/3: Se recomienda que la DPI-FE pueda gestionar aplicaciones y servicios:

- generar, modificación y publicar plantillas de aplicaciones;
- mantener la relación entre aplicaciones y estrategias; y
- realizar y gestionar reservas de servicio del usuario;

R-7.2.2/4: Se recomienda que la DPI-FE pueda gestionar estrategias predefinidas o generadas dinámicamente. (Se tiene la opción de que estas estrategias estén relacionadas con la identificación de aplicaciones, el control de aplicaciones y la gestión de usuarios.)

R-7.1.2/5: Se recomienda que la DPI-FE pueda gestionar la autoridad de administración. Para poder realizar una gestión jerárquica, cada administrador tiene distintas autoridades de gestión.

7.2.3 Requisitos relativos al plano de control

R-7.2.3/1: La DPI-FE tiene la opción de dar soporte a protocolos de control de políticas (como el [b-ITU-T H.248.1] en el punto de referencia *Rw* del UIT-T definido en [ITU-T Y.2111]) para el control y la señalización de reglas políticas IDP.

7.2.4 Requisitos relativos al plano (de datos) de usuario

Los requisitos optativos del plano (de datos) de usuario son los siguientes:

R-7.2.4/1: La DPI-FE tiene la opción de admitir diferentes tecnologías de paquetes (por ejemplo, xDSL, UMTS, CDMA2000, cable, LAN, WLAN, Ethernet, MPLS, IP, ATM).

7.2.5 Requisitos en diferentes planos

R-7.2.5/1: La DPI-FE tiene la opción de admitir gramática de protocolo armonizada para la especificación de reglas políticas IDP. Se recomienda que la sintaxis utilizada en la interfaz de control de políticas (plano de control) y en la interfaz de gestión de políticas (plano de gestión) sea preferiblemente idéntica. Esto no implica que se haya de utilizar el mismo protocolo, sino que tiene que ver con el lenguaje de especificación para reglas políticas (IDP) (a menudo denominado lenguaje de especificación de filtro (FSL), o lenguaje de especificación de políticas (PSL); véase la Nota).

NOTA – Ejemplos de lenguajes de programación son SIEVE [b-IETF RFC 5228], PERL, XML y XACML (*eXtensible access control markup language*).

La gramática de protocolo armonizada permite utilizar un modelo de datos/objeto común en el trayecto de aplicación de políticas dentro de un nodo IDP, que es una condición necesaria para la ejecución rápida y eficiente, así como para las operaciones de actualización sin interrupción en la biblioteca de firmas IDP.

8 Interfaces de la entidad funcional IDP

Los requisitos descritos en las cláusulas anteriores implican a las siguientes interfaces:

- entre la DPI-FE y las entidades de red distantes (véase la cláusula 8.1); y
- entre los componentes internos de la DPI-FE (véase la cláusula 8.2).

8.1 Interfaces DPI-FE externas

En la Figura 8-1 se muestran las interfaces externas de la DPI-FE:

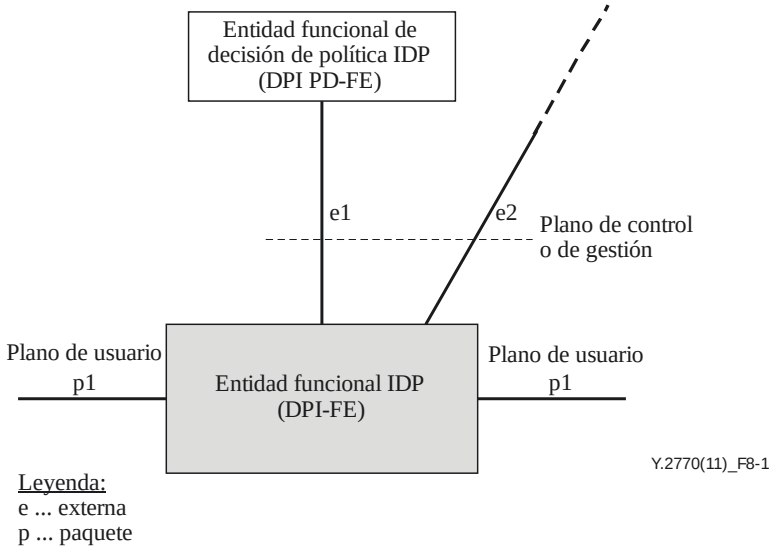


Figura 8-1 – Interfaces DPI-FE externas

8.1.1 Tráfico inspeccionado (p1)

La DPI-FE intercambia paquetes con los nodos de paquetes remotos a través de *p1*. El trayecto de paquetes tiene una topología punto a punto para la DPI-FE que actúa en modo *IDP en el trayecto*. No se admiten topologías multipunto. La interfaz *p1* abarca los trayectos de paquetes *bidirectionales*.

La topología de trayecto de paquetes de la DPI-FE que actúa en modo *IDP fuera del trayecto* está relacionada con el punto extremo.

8.1.2 Control/gestión de la inspección de tráfico (e1)

La entidad función de decisión política IDP (DPI-PDFE) tiene por objeto controlar o gestionar la DPI-FE. Así, la información intercambiada a través de *e1* está relacionada con instrucciones para controlar/configurar la gestión de paquetes en la DPI-FE. Estas instrucciones podrían describirse en una política de IDP.

La interfaz *e1* también podría dar soporte a la notificación y comunicación de información de la DPI-FE a la DPI-PDFE.

8.1.3 Notificación a otras entidades de red (e2)

La interfaz *e2* comprende todas las posibles interfaces de comunicación con entidades de red remotas distintas de la DPI-PDFE. Esta interfaz se emplea principalmente para la notificación.

8.2 Interfaces internas de DPI-FE

En la Figura 8-2 se muestran las posibles interfaces internas de acuerdo con los requisitos IDP:

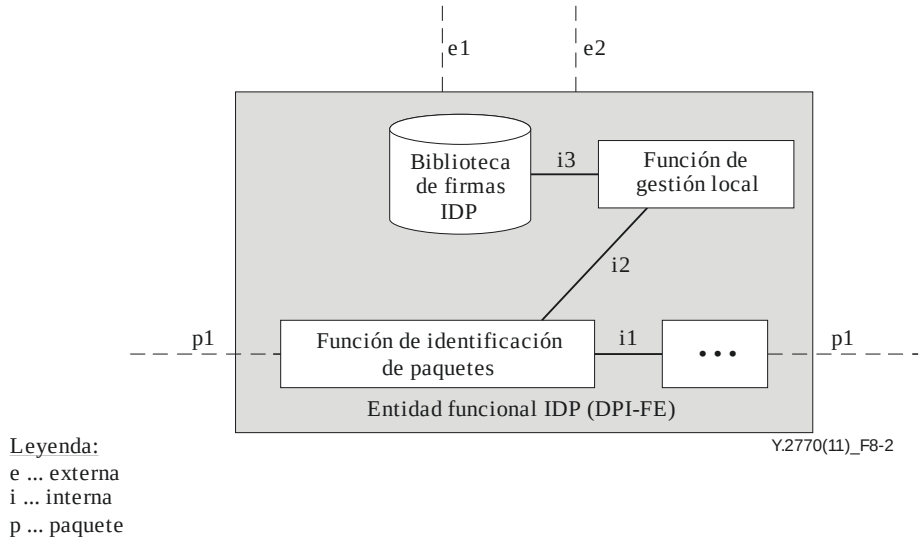


Figura 8-2 – Interfaces internas de DPI-FE

Puede haber otras interfaces internas y componentes funcionales internos de la DPI-FE. Las interfaces internas serán objeto de un estudio ulterior.

8.3 Requisitos de las interfaces

R-8.3/1: Se recomienda que la interfaz e1 cumpla los requisitos estipulados en la cláusula 6.5.

R-8.3/2: Se recomienda que la interfaz e2 cumpla los requisitos estipulados en la cláusula 6.4.1.

9 Consideraciones y requisitos de seguridad

En la presente cláusula se describen las amenazas de seguridad y los requisitos de seguridad de las entidades IDP en las NGN.

9.1 Amenazas a la seguridad de las entidades IDP

Las entidades funcionales relacionadas con la IDP suelen estar situadas en una *zona de confianza* del operador NGN o en una *zona de confianza pero vulnerable* definida en la [UIT-T Y.2701]. La Recomendación identifica las amenazas a la seguridad a la NGN y define los requisitos de protección contra las mismas. Dado que las entidades IDP forman parte de la NGN, la conclusión de [ITU-T Y.2701] son aplicables a ellos. Según la [ITU-T Y.2701] las amenazas a la seguridad de las entidades IDP son las siguientes:

- Destrucción de información relacionada con la IDP.
- Corrupción o modificación de la información relacionada con la IDP.
- Robo, supresión o pérdida de información IDP.
- Revelación de información IDP.
- Interrupción de los servicios.

La información relativa a las operaciones IDP comprende reglas políticas IDP con sus firmas e información exportada sobre la aplicación y el flujo IDP. La destrucción, corrupción o modificación, el robo, la supresión o la pérdida de dicha información puede convertirla en inutilizable para las operaciones IDP. En muchos países se recomienda que dicha información no debe revelarse y que debe gestionarse con arreglo a normativa nacional y los requisitos de política.

La interrupción de servicios puede deberse a ataques de denegación del servicio (DoS). Toda entidad que recibe datos puede ser objeto de un ataque DoS. Por ejemplo, el atacante puede inundar indirectamente una entidad IDP con un inmenso volumen de tráfico causando así la degradación o la interrupción de los servicios IDP para los usuarios legítimos.

9.2 Requisitos de seguridad para las entidades IDP

Los principales requisitos de seguridad para entidades IDP son los siguientes:

R-9.2/1: Se requiere que la información relacionada con IDP que resida en las entidades IDP se mantenga protegida.

R-9.2/2: Cuando se intercambie información fuera de la *zona de confianza* del operador NGN, se requiere la información IDP se mantenga protegida entre las entidades IDP y las entidades funcionales remotas (por ejemplo, DPI PD-FE, NMS).

R-9.2/3: Se tiene la opción de exigir mecanismos para mitigar los ataques por inundación contra la DPI FE.

R-9.2/4: Se requiere que al aplicar la presente Recomendación los fabricantes, operadores y proveedores de servicio tengan en cuenta la reglamentación nacional y los requisitos de política.

R-9.2/5: Se recomienda a los ingenieros que utilicen mecanismos existentes de eficacia probada para cumplir los requisitos de seguridad definidos en la presente Recomendación. Por ejemplo, los especificados en la Recomendación UIT-T Y.2704 [ITU-T Y.2704].

Anexo A

Especificación del descriptor del flujo

(El presente anexo forma parte integrante de esta Recomendación.)

A.1 Perspectiva sintáctica del protocolo

El descriptor del flujo está relacionado con la *estructura de datos* (objeto de datos), que se puede representar con un modelo de *k-tupla* (véase la Figura A.1). La estructura de datos consta de *k* elementos de información (IE) (Nota). El valor de *k* es variable y mayor que cero[1], pero se mantiene constante para un determinado flujo. Los *elementos de información* son los que figuran en el registro IPFIX de la IANA. Existe un *valor* relacionado con cada elemento de información. la *asociación* se suele indicar mediante el símbolo matemático de igualdad ('='), aunque no se excluyen otras relaciones matemáticas.

NOTA – Los elementos de información IPFIX del IETF pueden atribuirse como "campo esencial" o "campo no esencial".

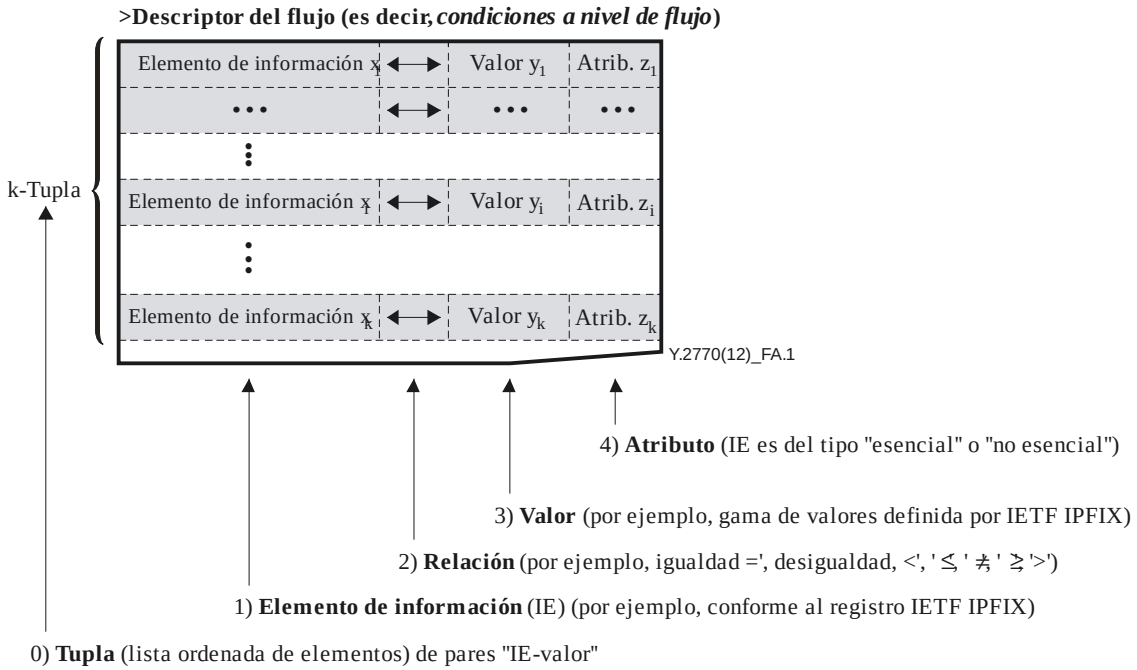


Figura A.1 – El descriptor del flujo (condiciones a nivel de flujo) desde el punto de vista sintáctico del protocolo

Por consiguiente, los descriptores a nivel de flujo en forma de *k*-tupla representan una lista de *k* "*pares nombre-valor*" (NVP); es decir una secuencia de pares ("< *IE* ↔ *valor* >")[2].

---

1 NOTA – N = 0 indica "independiente del flujo".

2 Similar a otras estructuras como AVP (<nombre del atributo, valor>), o el par parámetro-valor (<parm=valor>), etc.

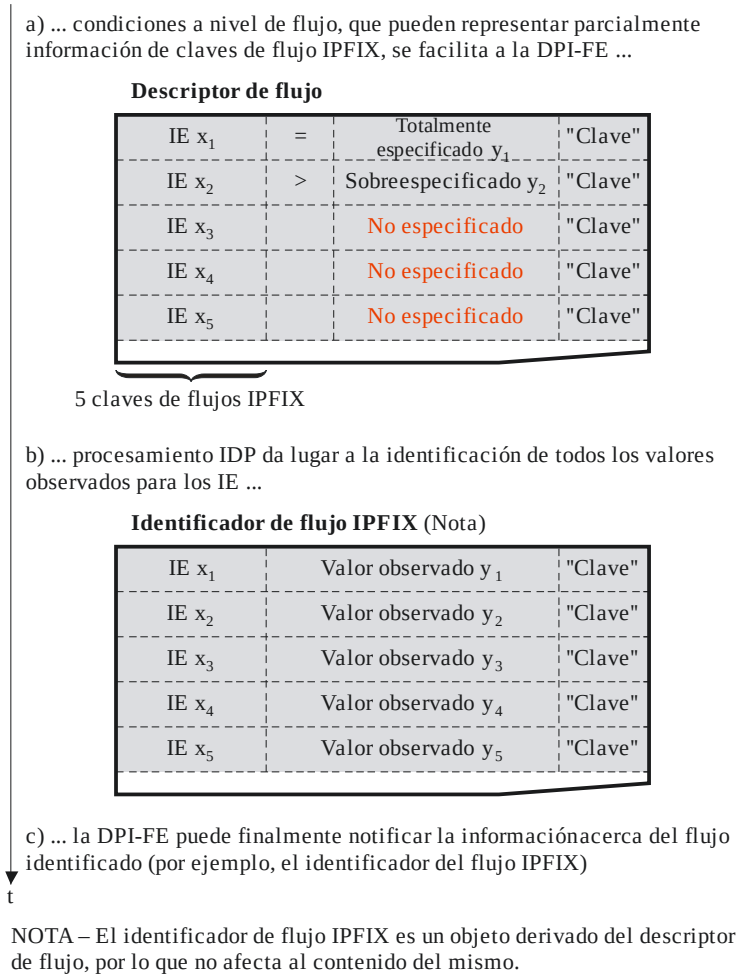
A.2 Especificación de valores de los elementos de información

En las condiciones a nivel de flujo, el valor de un IE puede:

- Especificarse íntegramente
  Totalmente especificado representa el caso de un conjunto completo de nombre-valor.
- No especificarse
  "*No especificado*" representa el caso en el que *aún no hay ningún valor* asignado al IE.
- Sobreespecificado
  Sobreespecificado indica que hay múltiples valores posibles para un determinado IE.
- Subespecificado
  Subespecificado indica que existen comodines (por ejemplo, todos los posibles valores, o seleccione un valor).

A.3 Relación entre el descriptor del flujo, el identificador de flujo IPFIX y la clave de flujo IPFIX

En la Figura A.2 se muestra un ejemplo de descriptor del flujo de 5-tuplas que contiene 5 claves de flujo IFPIX. Para identificar un determinado flujo, el descriptor impone ciertas condiciones a los valores de estas claves de flujo, como se define en la cláusula A.2: el primer IE de clave de flujo x_1 está "totalmente especificado", el segundo IE de clave de flujo está "sobreespecificado", en tanto que los otros IE están "no especificados", como se muestra en la parte a) de la Figura A.2.



NOTA – El identificador de flujo IPFIX es un objeto derivado del descriptor de flujo, por lo que no afecta al contenido del mismo.

Figura A.2 – Ejemplo de descriptor del flujo, identificador de flujo IPFIX y clave de flujo IPFIX

Obsérvese que el descriptor del flujo no impone condiciones a las claves de flujo IPFIX exclusivamente: de hecho, en algunas circunstancias, pueden requerirse descriptores de flujo en claves ajenas al flujo, por ejemplo cuando se exige una condición de los indicadores TCP del primer paquete del flujo. En el ejemplo de la Figura A.2, la diferencia fundamental entre el descriptor del flujo y el identificador de flujo IPFIX es que el descriptor del flujo contiene la condición "mayor que" en el IE x_2, ("IE x_2 > valor y_2"), mientras que el identificador de flujo IPFIX contiene el valor observado para el IE x_2, es decir, el valor yy_2. El identificador de flujo IPFIX está formado por el conjunto de valores observados de las claves de flujo, una vez que la entidad funcional IDP ha procesado los paquetes y los ha clasificado en un flujo.

Obsérvese que si la información exportada (por ejemplo, por medio de un registro de flujo IPFIX) contiene cada IE con los correspondientes valores asociados, o si el IE es o no una clave de flujo IPFIX, no hay necesidad de asignar el identificador de flujo IPFIX especificado, ya que el identificador de flujo IPFIX es la suma de toda esta información.

Bibliografía

[b-ITU-T H.248.1] Recomendación UIT-T H.248.1 v3 (2005), *Protocolo de control de las pasarelas: Versión 3*.

[b-ITU-T X.734] Recomendación UIT-T X.734 (1992), *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de gestión de informes de eventos*.

[b-ITU-T X.1141] Recomendación UIT-T X.1141 (2006), *Lenguaje de marcaje de aserción de seguridad (SAML 2.0)*.

[b-ITU-T Y.2011] Recomendación UIT-T Y.2011 (2004), *Principios generales y modelo de referencia general de las redes de próxima generación*.

[b-ITU-T Y.2121] Recomendación UIT-T Y.2121 (2008), *Requisitos para el soporte de la tecnología de transporte con conocimiento del estado del flujo en la red de próxima generación*.

[b-ETSI ES 282 003] ETSI ES 282 003 (2011), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture*.

[b-ETSI TS 123 203] ETSI TS 123 203 (2011), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control architecture (3GPP TS 23.203 version 10.4.0 Release 10)*.

[b-ETSI TS 124 229] ETSI TS 124 229 (2009), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE;IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229 version 9.4.0 Release 9)*.

[b-IETF IANA IPFIX] IETF IANA IPFIX (2007), IP Flow Information Export (IPFIX) Entities. <http://www.iana.org/assignments/ipfix/ipfix.xhtml>

[b-IETF opsec] IETF draft-ietf-opsec-filter-caps (2007), *Filtering and Rate Limiting Capabilities for IP Network Infrastructure*. <http://tools.ietf.org/html/draft-ietf-opsec-filter-caps-09>

[b-IETF RFC 1950] IETF RFC 1950 (1996), *ZLIB Compressed Data Format Specification version 3.3*.

[b-IETF RFC 3198] IETF RFC 3198 (2001), *Terminology for Policy-Based Management*.

[b-IETF RFC 3320] IETF RFC 3320 (2003), *Signaling Compression (SigComp)*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[b-IETF RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure*.

[b-IETF RFC 4268] IETF RFC 4268 (2005), *Entity State MIB*.

[b-IETF RFC 4778] IETF RFC 4778 (2007), *Operational Security Current Practices in Internet Service Provider Environments*.

[b-IETF RFC 4867] IETF RFC 4867 (2007), *RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs*.

[b-IETF RFC 5102] IETF RFC 5102 (2008), *Information Model for IP Flow Information Export*.

[b-IETF RFC 5103] IETF RFC 5103 (2008), *Bidirectional Flow Export Using IP Flow Information Export (IPFIX)*.

[b-IETF RFC 5228] IETF RFC 5228 (2008), *Sieve: An Email Filtering Language*.

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The Syslog Protocol*.

[b-IETF RFC 5426] IETF RFC 5426 (2009), *Transmission of Syslog Messages over UDP*.

[b-IETF RFC 5476] IETF RFC 5476 (2009), *Packet Sampling (PSAMP) Protocol Specifications*.

[b-PacketTypes] McCann, P.J., and Chandra S. (2000), *Packet Types: Abstract Specification of Network Protocol Messages*; in SIGCOMM '00: Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pp. 321-333, ACM Press, New York.

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, 2014