Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1541

(09/2017)

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

Intercambio de información de ciberseguridad – Intercambio de eventos/incidentes/heurística

Formato para el intercambio de descripciones de objetos de incidentes, versión 2

Recomendación UIT-T X.1541

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistema de transporte inteligente (ITS)	X.1370–X.1379
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	**X.1540–X.1549**
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

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

Recomendación UIT-T X.1541

Formato para el intercambio de descripciones de objetos de incidentes, versión 2

Resumen

La Recomendación UIT-T X.1541 describe el modelo de información para el formato de intercambio de descripciones de objetos de incidentes (IODEF), versión 2, y proporciona un modelo de datos asociado especificado en lenguaje XML. El IODEF especifica una representación de modelo de datos para compartir información que suele intercambiarse en caso de incidentes de seguridad informática o de otro tipo. A tal efecto se ha establecido una lista de las secciones pertinentes de IETF RFC 7970 y se indica si son normativas o informativas.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1541	2012-09-07	17	11.1002/1000/11375
2.0	ITU-T X.1541	2017-09-06	17	11.1002/1000/13264

* 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

En la Recomendación UIT-T X.1500, "Aspectos generales del intercambio de información de ciberseguridad" se dan orientaciones para el intercambio de información de seguridad, en particular la relativa a incidentes e indicadores que se indican en la presente Recomendación. El formato de intercambio de descripciones de objetos de incidentes (IODEF) es un modelo de datos para representar la información que suele intercambiarse en caso de incidentes de seguridad informática. Se especifica un modelo de datos XML para comunicar información sobre incidentes entre las entidades que tienen la responsabilidad operativa de tomar medidas proactivas defensivas, paliativas y de observancia y alerta a una comunidad determinada. El modelo de datos proporciona un método para codificar la información acerca de las computadoras centrales, las redes y los servicios que corren en estos sistemas; la metodología de explotación y los datos conexos; las repercusiones del incidente; y procedimientos limitados para documentar el flujo de trabajo.

La finalidad principal del IODEF es desarrollar las capacidades operativas y aumentar el conocimiento de la situación. La adopción de IODEF por parte de la comunidad mejora su capacidad para resolver incidentes y comunicar la situación general de las amenazas, gracias a que simplifica la colaboración y el intercambio de información. El formato estructurado de IODEF permite:

– una mayor automatización en el procesamiento de la información sobre incidentes a través del intercambio de información estructural sobre el incidente, eliminando así la necesidad de recurrir a analistas de seguridad para analizar documentos de texto exentos de formato;

– un menor esfuerzo para establecer la correlación entre datos similares (incluso cuando están muy estructurados) procedentes de distintas fuentes, lo que permite conocer mejor la situación; y

– un formato común que hace posible la compatibilidad de herramientas para el tratamiento y análisis de los incidentes, especialmente cuando la información procede de distintas entidades.

Hay numerosas consideraciones de procedimiento, fiabilidad, políticas y legales que pueden limitar o impedir el intercambio de información. El IODEF es una especificación técnica y no trata de resolver estos problemas. Sin embargo, al elaborar los acuerdos de intercambio de información, habrá que considerar este contexto más amplio a efectos de la aplicación práctica del IODEF y de los formatos y protocolos asociados.

Recomendación UIT-T X.1541

Formato para el intercambio de descripciones de objetos de incidentes, versión 2

1 Alcance

El formato de intercambio de descripciones de objetos de incidentes (IODEF) especifica una representación del modelo de datos para compartir información que suele intercambiarse en caso de incidentes de seguridad informática o de otro tipo. En esta Recomendación se describe el modelo de información para el IODEF y el modelo de datos correspondiente especificado en lenguaje XML.

Toda representación de modelo de datos o todo marco que permita el intercambio de información sobre seguridad informática o incidentes de otro tipo de ofrecer las capacidades necesarias para cumplir con todas las políticas, reglamentaciones y legislaciones regionales y nacionales aplicables.

Los encargados de la aplicación y los usuarios de todas las Recomendaciones UIT-T, incluidas la Recomendación UIT-T X.1541 y las técnicas subyacentes, deberán cumplir con todas las políticas, reglamentaciones y legislaciones regionales y nacionales aplicables.

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.

[IETF RFC 7970] IETF RFC 7970 (2016), *The Incident Object Description Exchange Format Version 2*.
<https://datatracker.ietf.org/doc/rfc7970/>

3 Definiciones

3.1 Términos definidos en otros documentos

Ninguno.

3.2 Términos definidos en esta Recomendación

Ninguno.

4 Abreviaturas y acrónimos

Esta Recomendación utiliza las abreviaturas y acrónimos siguientes:

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

IODEF Formato de intercambio de descripciones de objetos de incidentes (*incident object description exchange format*)

5 Convenios

Los siguientes términos se consideran equivalentes:

– En la UIT, los requisitos obligatorios se expresan con el futuro simple del verbo principal (futuro de mandato) u otras expresiones con significado de obligación y sus equivalentes negativos.

– En la UIT, el uso de la palabra inglesa "shall" es equivalente al uso que se hace en el IETF de la palabra "MUST".

– En la UIT, el uso de la expresión inglesa "shall not" es equivalente al uso que se hace en el IETF de la expresión "MUST NOT".

NOTA – En el IETF las palabras inglesas "shall" y "must" (en minúsculas) se utilizan para textos de carácter informativo.

6 Descripción de objetos de incidentes y formato de intercambio

En la cláusula 6 se define el formato de intercambio de descripciones de objetos de incidentes (IODEF), versión 2, con referencias directas a [IETF RFC 7970] mediante la alineación de las cláusulas con los números de la sección. Así, por ejemplo, la cláusula 6.x se corresponde con la sección x de [IETF RFC 7970] con títulos idénticos.

6.1 Introducción

La sección 1 de [IETF RFC 7970] es informativa.

6.1.1 Terminología

La sección 1.1 [IETF RFC 7970] es informativa.

6.1.2 Notaciones

La sección 1.2 de [IETF RFC 7970] es informativa.

6.1.3 Sobre el modelo de datos IODEF

La sección 1.3 de [IETF RFC 7970] es informativa.

6.1.4 Diferencias respecto de la RFC 5070

La sección 1.4 de [IETF RFC 7970] es informativa.

6.2 Tipos de datos IODEF

La sección 2 de [IETF RFC 7970] es informativa, pero sus subsecciones, es decir, secciones 2.1-2.15 son normativas y definen los siguientes tipos de datos:

– Enteros (se definen en [IETF RFC 7970], sección 2.1)

– Números reales (se definen en [IETF RFC 7970], sección 2.2)

– Caracteres y cadenas (se definen en [IETF RFC 7970], sección 2.3)

– Cadenas multilingües (se definen en [IETF RFC 7970], sección 2.4)

– Cadenas binarias (se definen en [IETF RFC 7970], sección 2.5)
  – Bytes Base64 (se definen en [IETF RFC 7970], sección 2.5.1)
  – Bytes hexadecimales (se definen en [IETF RFC 7970], sección 2.5.2)

– Tipos enumerados (se definen en [IETF RFC 7970], sección 2.6)

– Cadena fecha-hora (se define en [IETF RFC 7970], sección 2.7)

– Cadena de zona horaria (se define en [IETF RFC 7970], sección 2.8)

- Lista de puertos (se define en [IETF RFC 7970], sección 2.9)
- Dirección postal (se define en [IETF RFC 7970], sección 2.10)
- Número de teléfono (se define en [IETF RFC 7970], sección 2.11)
- Cadena correo electrónico (se define en [IETF RFC 7970], sección 2.12)
- Cadenas de localizador uniforme de recursos (se definen en [IETF RFC 7970], sección 2.13)
- Indicadores y referencias a indicadores (se definen en [IETF RFC 7970], sección 2.14)
- Software (se define en [IETF RFC 7970], sección 2.15)
  - Clase SoftwareReference (se define en [IETF RFC 7970], sección 2.15.1)
- Extensión (se define en [IETF RFC 7970], sección 2.16)

6.3 El modelo de información IODEF

La sección 3 de [IETF RFC 7970] es informativa, pero sus subsecciones, es decir, secciones 3.1-3.29 son normativas y definen los siguientes tipos de datos:

- Clase IODEF-Document (se define en [IETF RFC 7970], sección 3.1)
- Clase Incident (se define en [IETF RFC 7970], sección 3.2)
- Atributos comunes (se definen en [IETF RFC 7970], sección 3.3)
  - atributo restricción (se define en [IETF RFC 7970], sección 3.3.1)
  - atributo id observable (se define en [IETF RFC 7970], sección 3.3.2)
- Clase IncidentID (se define en [IETF RFC 7970], sección 3.4)
- Clase AlternativeID (se define en [IETF RFC 7970], sección 3.5)
- Clase RelatedActivity (se define en [IETF RFC 7970], sección 3.6)
- Clase ThreatActor (se define en [IETF RFC 7970], sección 3.7)
- Clase Campaign (se define en [IETF RFC 7970], sección 3.8)
- Clase Contact (se define en [IETF RFC 7970], sección 3.9)
  - Clase RegistryHandle (se define en [IETF RFC 7970], sección 3.9.1)
  - Clase PostalAddress (se define en [IETF RFC 7970], sección 3.9.2)
  - Clase Email (se define en [IETF RFC 7970], sección 3.9.3)
  - Clase Telephone (se define en [IETF RFC 7970], sección 3.9.4)
- Clase Discovery (se define en [IETF RFC 7970], sección 3.10)
  - Clase DetectionPattern (se define en [IETF RFC 7970], sección 3.10.1)
- Clase Method (se define en [IETF RFC 7970], sección 3.11)
  - Clase Reference (se define en [IETF RFC 7970], sección 3.11.1)
- Clase Assessment (se define en [IETF RFC 7970], sección 3.12)
  - Clase SystemImpact (se define en [IETF RFC 7970], sección 3.12.1)
  - Clase BusinessImpact (se define en [IETF RFC 7970], sección 3.12.2)
  - Clase TimeImpact (se define en [IETF RFC 7970], sección 3.12.3)
  - Clase MonetaryImpact (se define en [IETF RFC 7970], sección 3.12.4)
  - Clase Confidence (se define en [IETF RFC 7970], sección 3.12.5)
- Clase History (se define en [IETF RFC 7970], sección 3.13)
  - Clase HistoryItem (se define en [IETF RFC 7970], sección 3.13.1)
- Clase EventData (se define en [IETF RFC 7970], sección 3.14)

  - Clase relativa al incidente y EventData (se define en [IETF RFC 7970], sección 3.14.1)
  - Definición recursiva de EventData (se define en [IETF RFC 7970], sección 3.14.2)
- Clase Expectation (se define en [IETF RFC 7970], sección 3.15)
- Clase Flow (se define en [IETF RFC 7970], sección 3.16)
- Clase System (se define en [IETF RFC 7970], sección 3.17)
- Clase Node (se define en [IETF RFC 7970], sección 3.18)
  - Clase Address (se define en [IETF RFC 7970], sección 3.18.1)
  - Clase NodeRole (se define en [IETF RFC 7970], sección 3.18.2)
  - Clase Counter (se define en [IETF RFC 7970], sección 3.18.3)
- Clase DomainData (se define en [IETF RFC 7970], sección 3.19)
  - Clase Nameservers (se define en [IETF RFC 7970], sección 3.19.1)
  - Clase DomainContacts (se define en [IETF RFC 7970], sección 3.19.2)
- Clase Service (se define en [IETF RFC 7970], sección 3.20)
  - Clase ServiceName (se define en [IETF RFC 7970], sección 3.20.1)
  - Clase ApplicationHeader (se define en [IETF RFC 7970], sección 3.20.2)
- Clase EmailData (se define en [IETF RFC 7970], sección 3.21)
- Clase Record (se define en [IETF RFC 7970], sección 3.22)
  - Clase RecordData (se define en [IETF RFC 7970], sección 3.22.1)
  - Clase RecordPattern (se define en [IETF RFC 7970], sección 3.22.2)
- Clase WindowsRegistryKeysModified (se define en [IETF RFC 7970], sección 3.23)
  - Clase Key (se define en [IETF RFC 7970], sección 3.23.1)
- Clase CertificateData (se define en [IETF RFC 7970], sección 3.24)
  - Clase Certificate (se define en [IETF RFC 7970], sección 3.24.1)
- Clase FileData (se define en [IETF RFC 7970], sección 3.25)
  - Clase File (se define en [IETF RFC 7970], sección 3.25.1)
- Clase HashData (se define en [IETF RFC 7970], sección 3.26)
  - Clase Hash (se define en [IETF RFC 7970], sección 3.26.1)
  - Clase FuzzyHash (se define en [IETF RFC 7970], sección 3.26.2)
- Clase SignatureData (se define en [IETF RFC 7970], sección 3.27)
- Clase IndicatorData (se define en [IETF RFC 7970], sección 3.28)
- Clase Indicator (se define en [IETF RFC 7970], sección 3.29)
  - Clase IndicatorID (se define en [IETF RFC 7970], sección 3.29.1)
  - Clase AlternativeIndicatorID (se define en [IETF RFC 7970], sección 3.29.2)
  - Clase Observable (se define en [IETF RFC 7970], sección 3.29.3)
  - Clase IndicatorExpression (se define en [IETF RFC 7970], sección 3.29.4)
  - Clase Expresiones con IndicatorExpression (se define en [IETF RFC 7970], sección 3.29.5)
  - Clase ObservableReference (se define en [IETF RFC 7970], sección 3.29.6)
  - Clase IndicatorReference (se define en [IETF RFC 7970], sección 3.29.7)
  - Clase AttackPhase (se define en [IETF RFC 7970], sección 3.29.8)

6.4 Consideraciones de procesamiento

La sección 4 de [IETF RFC 7970] es normativa, aunque algunas de sus subsecciones son informativas, como se indica en las siguientes subsecciones.

6.4.1 Codificación

La sección 4.1 de [IETF RFC 7970] es normativa.

6.4.2 IODEF Namespace

La sección 4.2 de [IETF RFC 7970] es normativa.

6.4.3 Validación

La sección 4.3 de [IETF RFC 7970] es normativa.

6.4.4 Incompatibilidades con la v1

La sección 4.4 [IETF RFC 7970] es informativa.

6.5 Ampliación del IODEF

La sección 5 de [IETF RFC 7970] es informativa.

En [b-UIT-T X.1500], "Aspectos generales del intercambio de información de ciberseguridad" se dan orientaciones para el intercambio de información de seguridad, en particular la relativa a incidentes e indicadores que se indican en la presente Recomendación (UIT-T X.1541). Esta Recomendación (UIT-T X.1541) describe el formato básico para el intercambio de información sobre incidentes, pero no comprende todos los casos de utilización con arreglo a [b-UIT-T X.1500]. Podrían ser necesarias extensiones para satisfacer las necesidades de ciertos casos de utilización.

6.5.1 Ampliación de los valores enumerados de los atributos

La sección 5.1 de [IETF RFC 7970] y sus subsecciones son normativas.

6.5.2 Ampliación de clases

La sección 5.2 de [IETF RFC 7970] y sus subsecciones son normativas.

6.6 Cuestiones de internacionalización

La sección 6 de [IETF RFC 7970] es normativa.

6.7 Ejemplos

La sección 7 de [IETF RFC 7970] y sus subsecciones, que describen ejemplos de documentos IODEF, son informativas.

6.8 El modelo de datos IPDEF (esquema XML)

La sección 8 de [IETF RFC 7970] es normativa.

6.9 Consideraciones de seguridad

La sección 9 de [IETF RFC 7970] y sus subsecciones son normativas.

En las implementaciones acordes con el UIT-T, el formato y protocolo de mensaje subyacentes utilizados para el intercambio de ejemplos del IODEF deberán prever garantías apropiadas de confidencialidad, integridad y autenticidad.

NOTA – En el IETF la palabra "must" (en minúsculas) se utiliza para el texto informativo.

6.10 Consideraciones IANA

La sección 10 de [IETF RFC 7970] y sus subsecciones son normativas.

6.11 Referencias

6.11.1 Referencias normativas

La sección 11.1 de [IETF RFC 7970] es informativa.

Esta Recomendación UIT-T ha identificado la sección 11.1 de [IETF RFC 7970] como informativa, ya que el UIT-T no elaboró ninguna posición respecto de ninguna de estas referencias en lo que respecta a esta Recomendación. No obstante, se reconoce que el IETF ha identificado una serie de referencias normativas para [IETF RFC 7970].

6.11.2 Referencias informativas

La sección 11.2 de [IETF RFC 7970] es informativa.

Bibliografía

[b-UIT-T X.1500] Recomendación UIT-T X.1500 (2011), Aspectos generales del intercambio de información de ciberseguridad.

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, 2018