



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.509

Corrigendum 1
(10/2001)

SERIE X: REDES DE DATOS Y COMUNICACIÓN
ENTRE SISTEMAS ABIERTOS

Directorio

Tecnología de la información – Interconexión de
sistemas abiertos – El directorio: Marcos para
certificados de claves públicas y atributos

Corrigendum técnico 1

Recomendación UIT-T X.509 (2000) – Corrigendum 1

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE X
REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1–X.19
Interfaces	X.20–X.49
Transmisión, señalización y conmutación	X.50–X.89
Aspectos de redes	X.90–X.149
Mantenimiento	X.150–X.179
Disposiciones administrativas	X.180–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200–X.209
Definiciones de los servicios	X.210–X.219
Especificaciones de los protocolos en modo conexión	X.220–X.229
Especificaciones de los protocolos en modo sin conexión	X.230–X.239
Formularios para declaraciones de conformidad de implementación de protocolo	X.240–X.259
Identificación de protocolos	X.260–X.269
Protocolos de seguridad	X.270–X.279
Objetos gestionados de capa	X.280–X.289
Pruebas de conformidad	X.290–X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.369
Redes basadas en el protocolo Internet	X.370–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	
Gestión de redes	X.600–X.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–X.649
Denominación, direccionamiento y registro	X.650–X.679
Notación de sintaxis abstracta uno	X.680–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999

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

**Tecnología de la información – Interconexión de sistemas abiertos –
El directorio: Marcos para certificados de claves públicas y atributos**

CORRIGENDUM TÉCNICO 1

Resumen

Este corrigendum técnico trata las resoluciones tomadas con relación a los informes de defectos 272, 273, 274, 275, 276, 277, 278, y 279.

Orígenes

El corrigendum 1 a la Recomendación UIT-T X.509 (2000), preparado por la Comisión de Estudio 7 (2001-2004) del UIT-T, fue aprobado el 7 de octubre de 2001. Se publica también un texto idéntico como corrigendum técnico 1 a la Norma Internacional ISO/CEI 9594-8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) 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 Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), 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 CMNT.

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.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido 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.

© UIT 2002

Es propiedad. Ninguna parte de esta publicación puede reproducirse o utilizarse, de ninguna forma o por ningún medio, sea éste electrónico o mecánico, de fotocopia o de microfilm, sin previa autorización escrita por parte de la UIT.

ÍNDICE

	<i>Página</i>
1) Esto corrige los defectos señalados en el informe de defectos 272	1
2) Esto corrige los defectos señalados en el informe de defectos 273	1
3) Esto corrige los defectos señalados en el informe de defectos 274	4
4) Esto corrige los defectos señalados en el informe de defectos 275	4
5) Esto corrige los defectos señalados en el informe de defectos 276	4
6) Esto corrige los defectos señalados en el informe de defectos 277	5
7) Esto corrige los defectos señalados en el informe de defectos 278	5
8) Esto corrige los defectos señalados en el informe de defectos 279	5

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

**Tecnología de la información – Interconexión de sistemas abiertos –
El directorio: Marcos para certificados de claves públicas y atributos**

CORRIGENDUM TÉCNICO 1

(Trata las resoluciones tomadas con relación a los informes de defectos 272, 273, 274, 275, 276, 277, 278 y 279)

1) Esto corrige los defectos señalados en el informe de defectos 272

*En 8.4.2.1, añádase el siguiente texto al final del párrafo que comienza por "El componente **pathLenConstraint** estará presente solamente si..."*

La constricción comienza a surtir efecto con el siguiente certificado en el trayecto. La constricción restringe la longitud del segmento del trayecto de certificación entre el certificado que contiene esta extensión y el certificado de la entidad final. No influye en el número de certificados CA en el trayecto de certificación entre el fiduciario fundamental y el certificado que contiene esta extensión. En consecuencia, la longitud de un trayecto de certificación completo puede exceder la longitud máxima del segmento constreñido por esta extensión. La constricción controla el número de certificados CA no autoexpedidos entre el certificado CA que contiene la constricción y el certificado de la entidad final. Por lo tanto, la longitud total de este segmento del trayecto, excluyendo los certificados autoexpedidos, puede ser superior al valor de la constricción hasta en dos certificados. (Esto incluye los certificados en los dos puntos extremos del segmento más los certificados CA entre los dos puntos extremos que están constreñidos por el valor de esta extensión.)

*En 15.5.2.1, en el párrafo que comienza por "El componente **pathLenConstraint** tiene sentido únicamente si...", sustitúyanse las dos últimas oraciones por lo siguiente:*

La constricción restringe la longitud del segmento del trayecto de delegación entre el certificado que contiene esta extensión y el certificado de la entidad final. No influye en el número de certificados AA en el trayecto de delegación entre el fiduciario fundamental y el certificado que contiene esta extensión. Por lo tanto, la longitud de un trayecto de delegación completo puede ser superior a la longitud máxima del segmento constreñido por esta extensión. La constricción controla el número de certificados AA entre el certificado AA que contiene la constricción y el certificado de la entidad final. En consecuencia, la longitud total de este segmento del trayecto puede ser superior al valor de la constricción hasta en dos certificados. (Esto incluye los certificados en los dos puntos extremos del segmento más los certificados AA entre los dos puntos extremos que están constreñidos por el valor de esta extensión.)

2) Esto corrige los defectos señalados en el informe de defectos 273

Sustitúyase 8.4.2.2 por lo siguiente:

8.4.2.2 Extensión de constricciones de nombre

Este campo, que se utilizará solamente en un certificado CA, indica un espacio de nombres dentro del cual deben estar ubicados todos los nombres de sujeto en certificados subsiguientes en un trayecto de certificación. Este campo se define como sigue:

```
nameConstraints EXTENSION ::= {
    SYNTAX          NameConstraintsSyntax
    IDENTIFIED BY    id-ce-nameConstraint }
```

```
NameConstraintsSyntax ::= SEQUENCE {
    permittedSubtrees      [0]  GeneralSubtrees OPTIONAL,
    excludedSubtrees       [1]  GeneralSubtrees OPTIONAL,
    requiredNameForms      [2]  NameForms OPTIONAL }
```

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
 base **GeneralName,**
 minimum [0] **BaseDistance DEFAULT 0,**
 maximum [1] **BaseDistance OPTIONAL }**

BaseDistance ::= INTEGER (0..MAX)

NameForms ::= SEQUENCE {
 basicNameForms [0] **BasicNameForms OPTIONAL,**
 otherNameForms [1] **SEQUENCE SIZE (1..MAX) OF OBJECT IDENTIFIER OPTIONAL }**

(ALL EXCEPT ({ -- néant; c'est-à-dire: au moins un composant doit être présent -- })))

BasicNameForms ::= BIT STRING {
 rfc822Name (0),
 dnsName (1),
 x400Address (2),
 directoryName (3),
 ediPartyName (4),
 uniformResourceIdentifier (5),
 iPAddress (6),
 registeredID (7) } (SIZE (1..MAX))

Si están presentes, cada uno de los componentes **permittedSubtrees** y **excludedSubtrees** especifica uno o más subárboles de denominación, cada uno definido por el nombre de la raíz del subárbol y, facultativamente, dentro de ese subárbol, una zona que está limitada por un nivel superior, por un nivel inferior, o por ambos niveles. Si **permittedSubtrees** está presente, los nombres de sujeto dentro de estos subárboles son aceptables. Si **excludedSubtrees** está presente, todo certificado expedido por la CA sujeto o por CA subsiguientes en el trayecto de certificación que tiene un nombre de sujeto dentro de estos subárboles es inaceptable. Si ambos subárboles, **permittedSubtrees** y **excludedSubtrees**, están presentes y los espacios de nombres se superponen, tiene preferencia la instrucción de exclusión para los nombres en la región en que existe tal superposición. Si no están especificados subárboles permitidos ni subárboles excluidos para una forma de nombre, es aceptable cualquier nombre dentro de esa forma de nombre. Si está presente **requiredNameForms**, todos los certificados subsiguientes en el trayecto de certificación deben incluir un nombre de al menos una de las formas de nombre requeridas.

Si está presente **permittedSubtrees**, se aplica lo siguiente a todos los certificados subsiguientes en el trayecto. Si cualquier certificado contiene un nombre de sujeto (en el campo **subject** o en la extensión **subjectAltNames**) de una forma de nombre para la cual se especifican subárboles permitidos, el nombre debe estar dentro de al menos uno de los subárboles especificados. Si cualquier certificado contiene solamente nombres de sujeto de formas de nombre distintas de aquellas para las cuales están especificados subárboles permitidos, no se requiere que los nombres de sujeto caigan dentro de alguno de los subárboles especificados. Por ejemplo, supóngase que se especifican dos subárboles permitidos, uno para la forma de nombre DN y el otro para la forma de nombre rfc822, no se especifican subárboles excluidos, pero se especifica **requiredNameForms** con el bit **directoryName** y el bit **rfc822Name** presentes. Un certificado que contuviera solamente nombres distintos de un nombre de directorio o de un nombre rfc822 sería inaceptable. Sin embargo, si no se especificara **requiredNameForms**, tal certificado sería aceptable. Por ejemplo, supóngase que se especifican dos subárboles permitidos, uno para la forma de nombre DN y el otro para la forma de nombre rfc822, no se especifican subárboles excluidos, y no está presente **requiredNameForms**. Un certificado que contuviera solamente un DN y en el que el DN estuviera dentro del subárbol permitido especificado, sería aceptable. Un certificado que contuviera tanto un nombre DN como un nombre rfc822 y en el que solamente uno de ellos está dentro de su subárbol permitido especificado sería inaceptable. Un certificado que contuviera solamente nombres distintos de un nombre DN o de un nombre rfc822 sería también aceptable.

Si está presente **excludedSubtrees**, todo certificado expedido por la CA sujeto o por CA subsiguientes en el trayecto de certificación, que tenga un nombre de sujeto (en el campo **subject** o en la extensión **subjectAltNames**) dentro de estos subárboles es inaceptable. Por ejemplo, supóngase que se especifican dos subárboles excluidos, uno para la forma de nombre DN y el otro para la forma de nombre rfc822. Un certificado que contuviera solamente un DN y en el que el DN estuviera dentro del subárbol excluido especificado sería inaceptable. Un certificado que contuviera tanto un nombre DN como un nombre rfc822 y en el que al menos uno de ellos está dentro de su subárbol excluido especificado sería inaceptable.

Cuando un sujeto de certificado tiene múltiples nombres de la misma forma de nombre (incluido, en el caso de la forma de nombre **directoryName**, el nombre en el campo sujeto del certificado, si no es nulo), se probará la coherencia de todos esos nombres con una restricción de nombre de esa forma de nombre.

Si está presente **requiredNameForms**, todos los certificados subsiguientes en el trayecto de certificación deben incluir un nombre de sujeto de al menos una de las formas de nombre requeridas.

De las formas de nombre disponibles mediante el tipo **GeneralName**, solamente las formas de nombre que tienen una estructura jerárquica bien definida se pueden utilizar en los campos **permittedSubtrees** y **excludedSubtrees**. La forma de nombre **directoryName** satisface este requisito; cuando se utiliza esta forma de nombre, un subárbol de denominación corresponde a un subárbol del DIT.

El campo **minimum** especifica el límite superior de la zona dentro del subárbol. Ningún nombre cuyo componente de nombre final está por encima del nivel especificado está contenido en la zona. Un valor de **minimum** igual a cero (el valor por defecto) corresponde a la base, es decir, al nodo superior del subárbol. Por ejemplo, si **minimum** está puesto a uno, el subárbol de denominación no incluye el nodo de base pero sí incluye nodos subordinados.

El campo **maximum** especifica el nivel inferior de la zona dentro del subárbol. Los nombres cuyo último componente está por debajo del nivel especificado no están contenidos en la zona. Un valor de **maximum** de cero corresponde a la base, es decir, a la parte superior del subárbol. Un componente **maximum** ausente indica que no se debe imponer un límite inferior en la zona dentro del subárbol. Por ejemplo, si **maximum** está puesto a uno, el subárbol de denominación excluye todos los nodos, excepto la base del subárbol y sus subordinados inmediatos.

A opción del expedidor del certificado, esta extensión puede ser crítica o no crítica. Se recomienda que se señale como crítica; de lo contrario, un usuario de certificado no podría comprobar que los certificados subsiguientes en un trayecto de certificación están situados en el espacio de nombres previsto por la CA expedidora.

Las implementaciones conformes no están obligadas a reconocer todas las formas de nombre posibles.

Si la extensión está presente y está señalada como crítica, una implementación que emplea certificados debe reconocer y procesar todas las formas de nombre para las cuales hay una especificación de subárbol (permitido o excluido) en la extensión y un valor correspondiente en el campo **subject** o en la extensión **subjectAltNames** de cualquier certificado subsiguiente en el trayecto de certificación. Si aparece una forma de nombre no reconocida en una especificación de subárbol y en un certificado subsiguiente, ese certificado se debe tratar como si se hubiera encontrado una extensión crítica no reconocida. Si cualquier nombre de sujeto en el certificado está dentro de un subárbol excluido, el certificado es inaceptable. Si un subárbol está especificado para una forma de nombre que no está contenida en ningún certificado subsiguiente, ese subárbol puede ser ignorado. Si el componente **requiredNameForms** especifica solamente formas de nombre no reconocidas, ese certificado se debe tratar como si se hubiera encontrado una extensión crítica no reconocida. De lo contrario, al menos una de las formas de nombre reconocidas debe aparecer en todos los certificados subsiguientes en el trayecto.

Si la extensión está presente y está señalada como no crítica, y una implementación que emplea certificado no reconoce una forma de nombre utilizada en cualquier componente **base**, esa especificación de subárbol puede ser ignorada. Si la extensión está señalada como no crítica y la implementación que emplea certificados no reconoce alguna de las formas de nombre especificadas en el componente **requiredNameForms**, el certificado se tratará como si estuviese ausente el componente **requiredNameForms**.

En 10.3, añádase la siguiente nueva variable de procesamiento de trayecto y renumérense los incisos subsiguientes como corresponda:

- d) *required-name-forms*: Un conjunto (que puede estar vacío) de conjuntos de formas de nombre. Para cada conjunto de formas de nombre, todo certificado subsiguiente debe contener un nombre de una de las formas de nombre en el conjunto.

En 10.4, añádase el siguiente nuevo paso de inicialización y renumérense los incisos subsiguientes como corresponda:

- d) Inicializar *required-name-forms* como un conjunto vacío.

En la cláusula 10.5.1, añádase el siguiente paso a las comprobaciones que se aplican a todos los certificados:

- h) Si el certificado no es un certificado autoexpedido intermedio, y si no es un conjunto vacío, para cada conjunto de formas de nombre en *required-name-forms* se comprueba que en el certificado hay un nombre de sujeto de una de las formas de nombre en el conjunto.

En 10.5.2, añádase el siguiente paso a las acciones de registro de restricción que se aplican a los certificados intermedios:

- c) Si la extensión **nameConstraints** con un componente **requiredNameForms** está presente en el certificado, la variable *required-name-forms* se fija a la unión (lógica) de su valor anterior y el conjunto constituido por el conjunto de formas de nombre especificadas en la extensión de certificado. Si el componente **requiredNameForms** contiene más de una forma de nombre, la variable *required-name-forms* señalará que un nombre de al menos una de las formas de nombre indicadas en esta extensión estará presente en todos los certificados subsiguientes. La unión (lógica) de un valor anterior de la variable *required-name-forms* y el valor de la extensión del certificado actual es un conjunto de conjuntos que señalan requisitos para todos los certificados subsiguientes. Por ejemplo, si el *required-name-forms* actual se fija de manera que requiera que ya sea un nombre DN o un nombre rfc822 esté presente en certificados y la extensión actual en el certificado que se está procesando indica que se requieren ya sean nombres rfc822 o nombres DNS, la unión (lógica) resultante que es el nuevo *required-name-forms* indica que cada uno de los certificados subsiguientes debe tener ya sea un nombre rfc822 o ambos nombres, es decir, un nombre DN y un nombre DNS.

En el anexo A, módulo **certificateExtensions**, actualícese la ASN.1 para la extensión **nameConstraints** como se ha indicado.

En el anexo A, módulo **certificateExtensions**, añádase lo siguiente:

id-ce-nameConstraint OBJECT IDENTIFIER ::= {id-ce 30 1}

En el anexo A, módulo **certificateExtensions**, suprimase lo siguiente:

id-ce-nameConstraints OBJECT IDENTIFIER ::= {id-ce 30}

En el anexo A, módulo **certificateExtensions**, añádase lo siguiente al conjunto de OIDs no utilizados en esta Especificación:

id-ce 30

3) Esto corrige los defectos señalados en el informe de defectos 274

En anexo A, sustitúyase la producción ASN.1 **AttCertVersion** por:

AttCertVersion ::= INTEGER {v2(1)}

4) Esto corrige los defectos señalados en el informe de defectos 275

En 8.2.2.4, añádase lo siguiente como un nuevo segundo párrafo a continuación de la ASN.1 para la extensión **extKeyUsage**:

Una CA puede afirmar any-extended-key-usage utilizando el identificador **anyExtendedKeyUsage**. Esto permite a la CA expedir un certificado que contenga OIDs para utilizaciones de claves extendidas que puedan ser requeridas por aplicaciones que emplean certificado, sin restringir el certificado a esas utilizaciones de clave solamente. Si la utilización de la extensión **extendedKeyUsage** restringiera la utilización claves, la inclusión de este OID eliminaría esa restricción.

anyExtendedKeyUsage OBJECT IDENTIFIER ::= { 2 5 29 37 0 }

5) Esto corrige los defectos señalados en el informe de defectos 276

En 8.1.5:

En la última oración, sustitúyase "y los indicadores *explicit-policy-pending*" por "indicadores *explicit-policy-pending* e *inhibit-any-policy*".

En 8.4.2.4, primera oración:

Sustitúyase "para todos los certificados en el trayecto de certificación" por "para todos los certificados no autoexpedidos en el trayecto de certificación".

En 10.5.1, primera enumeración, inciso e):

Sustitúyase "o si *inhibit-any-policy-indicator* está puesto a uno, suprimase" por "o si *inhibit-any-policy-indicator* está puesto a uno y el certificado no es un certificado intermedio autoexpedido, suprimase".

6) Esto corrige los defectos señalados en el informe de defectos 277

En 8.4.2.3, última oración del primer párrafo:

Sustitúyase "que es el sujeto de un certificado subsiguiente" por "que es el expedidor de un certificado subsiguiente".

7) Esto corrige los defectos señalados en el informe de defectos 278

En 8.6.2.6, primera oración:

Sustitúyase "se utilizará únicamente como una extensión de certificado y podrá utilizarse..." por "podrá utilizarse ya sea como un certificado o como una extensión CRL. Dentro de certificados, esta extensión podrá utilizarse...".

8) Esto corrige los defectos señalados en el informe de defectos 279

En la cláusula 7, añádase lo siguiente inmediatamente después de la producción ASN.1 **CrossCertificates**:

PkiPath ::= SEQUENCE OF Certificate

Se utiliza **PkiPath** para representar un trayecto de certificación. Dentro de la secuencia, el orden de los certificados es tal que el sujeto del primer certificado es el expedidor del segundo certificado, y así sucesivamente.

En 11.1.6:

Sustitúyase "clase de objeto estructural **pkiCA**" por "**pkiCA** o **pkiUser** estructurales".

En la última oración del último párrafo de la cláusula 7:

Sustitúyase "en el componente de **CertPath**" por "en el componente de **CertPath** o un valor de **Certificate** en **PkiPath**".

En 11.2.10:

Suprimase la producción ASN.1 **PkiPath**.

En la primera oración de 11.2.10:

Sustitúyase "certificados cruzados" por "certificados".

En 11.2.10, sustitúyase el texto a continuación de la ASN.1 por lo siguiente:

Este atributo se puede almacenar en un asiento de directorio de la clase de objeto **pkiCA** o **pkiUser**.

Cuando se almacenan en asientos **pkiCA**, valores de este atributo contienen trayectos de certificación que excluyen certificados de entidad final. Como tal, el atributo se utiliza para almacenar trayectos de certificación que son utilizados frecuentemente por partes confiantes asociadas con esa CA. Un valor de este atributo se puede utilizar junto con cualquier certificado de entidad final expedido por el último sujeto de certificado en el valor de atributo.

Cuando se almacenan en asientos **pkiUser**, valores de este atributo contienen trayectos de certificación que incluyen el certificado de entidad final. En este caso, la entidad final es el usuario cuyo asiento contiene este atributo. Los valores del atributo representan trayectos de certificación completos para certificados expedidos a este usuario.

En 11.3.9, última oración del primer párrafo:

Sustitúyase "expedido por la CA que expidió el certificado de entidad final que se está validando." por "expedido al sujeto especificado."

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
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 multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
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 y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación