Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1752

(01/2022)

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

Seguridad de datos – Seguridad de los macrodatos

Directrices de seguridad para infraestructuras y plataformas de macrodatos

Recomendación UIT-T X.1752

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web (1)	X.1140–X.1149
Seguridad en las aplicaciones (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Correo certificado	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1399
Seguridad de tecnología de libro mayor distribuido (DLT)	X.1400–X.1429
Seguridad en las aplicaciones (2)	X.1450–X.1459
Seguridad en la web (2)	X.1470–X.1489
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
Ciberdefensa	X.1590-X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	**X.1750–X.1759**
Protección de los datos	X.1770–X.1789
SEGURIDAD DE LAS IMT-2020	X.1800–X.1819

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

Recomendación UIT-T X.1752

Directrices de seguridad para infraestructuras y plataformas de macrodatos

Resumen

En la Recomendación UIT-T X.1752, se analizan las amenazas y los riesgos de seguridad relativos a las infraestructuras y las plataformas de macrodatos y se especifica un marco de referencia para definir la correspondencia de las directrices de seguridad con las amenazas para dichas infraestructuras y plataformas de macrodatos.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1752	2022-01-07	17	11.1002/1000/14806

Palabras clave

Macrodatos, infraestructura, plataforma, directrices de seguridad

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

© UIT 2022

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

Página

1 Alcance 3

2 Referencias 3

3 Definiciones 4

3.1 Términos definidos en otros documentos 4

3.2 Términos definidos en esta Recomendación 5

4 Abreviaturas y acrónimos 5

5 Convenios 6

6 Amenazas y riesgos de seguridad para las infraestructuras y las plataformas de macrodatos 6

6.1 Amenazas y riesgos de seguridad para las infraestructuras de macrodatos ... 6

6.2 Amenazas y riesgos de seguridad para las plataformas de macrodatos 8

7 Directrices de seguridad para infraestructuras y plataformas de macrodatos 9

7.1 Directrices de seguridad para la capa de origen de datos 10

7.2 Directrices de seguridad para la capa de procesamiento 12

7.3 Directrices de seguridad para la capa de aplicación 13

7.4 Directrices de seguridad para la capa de acceso 13

7.5 Directrices para la gestión de la seguridad 14

Bibliografía 13

Recomendación UIT-T X.1752

Directrices de seguridad para infraestructuras y plataformas de macrodatos

1 Alcance

En la presente Recomendación, se describen las infraestructuras y las plataformas de macrodatos a partir de los trabajos de normalización de los foros relevantes. En esta Recomendación, se describe una metodología de evaluación de las amenazas y se especifican directrices de seguridad para la protección de las infraestructuras y las plataformas de macrodatos. También se proporciona en esta Recomendación una correspondencia entre las amenazas y las directrices de seguridad.

2 Referencias

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

[UIT-T X.1279] Recomendación UIT-T X.1279 (2020), *Marco de autenticación mejorada mediante telebiometría con mecanismos de detección antisuplantación.*

[UIT-T X.1601] Recomendación UIT-T X.1601 (2015), *Marco de seguridad para la computación en la nube.*

[UIT-T X.1603] Recomendación UIT-T X.1603 (2018), *Requisitos de seguridad de los datos para el servicio de control de la computación en la nube.*

[UIT-T X.1605] Recomendación UIT-T X.1605 (2020), *Requisitos de seguridad de la infraestructura pública como servicio (IaaS) en la computación en la nube.*

[UIT-T Y.3600] Recomendación UIT-T Y.3600 (2015), *Macrodatos – Requisitos y capacidades basados en la computación en la nube.*

[UIT-T Y.3605] Recomendación UIT-T Y.3605 (2020), *Macrodatos – Arquitectura de referencia.*

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 control de acceso [b-UIT-T X.800]: Prevención del uso no autorizado de un recurso, incluida la prevención del uso de un recurso de una manera no autorizada.

3.1.2 auditoría [b-UIT-T X.800]: Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.

3.1.3 autentificación [b-ISO/CEI 18014-2]: Acción de garantizar la identidad de una entidad.

3.1.4 análisis de macrodatos [b-UIT-T Y.2244]: Análisis realizado sobre un volumen masivo de datos con el fin de obtener resultados significativos, como tendencias o preferencias.

3.1.5 desensibilización de datos [b-UIT-T X.1217]: Proceso para ocultar los datos sensibles.

3.1.6 integridad de los datos [b-UIT-T X.800]: Propiedad que garantiza que los datos no han sido alterados o destruidos de manera no autorizada.

3.1.7 cortafuegos [b-ISO/CEI 27033-1]: Tipo de barrera de seguridad colocada entre entornos de red –que consiste en un dispositivo especial o una combinación de diversos componentes y técnicas– a través de la cual pasa todo el tráfico de un entorno de red a otro, y viceversa, y solo se permite el tráfico autorizado que se defina en la política de seguridad local.

3.1.8 reparto de carga [b-UIT-T Y.2052]: Esquema que permite dividir la carga de tráfico y repartirla para utilizar de manera efectiva los recursos de la red (por ejemplo, la anchura de banda de los enlaces).

3.1.9 sistema de detección de intrusión [b-ISO/CEI 27039]: Sistemas de información utilizados para detectar que se ha producido una intrusión, se está produciendo o ha habido un intento.

3.1.10 sistema de prevención de intrusiones [b-UIT-T X.1361]: Variante de sistema de detección de intrusión diseñada especialmente para ofrecer una capacidad de respuesta activa.

3.1.11 autentificación multifactor [b-UIT-T X.1158]: Autentificación en la que se emplea como mínimo dos factores de autentificación independientes.

3.1.12 redundancia [b-UIT-T E.800]: En un elemento, existencia de más de un medio para realizar una función requerida.

3.1.13 robustez [b-UIT-T J.1014]: Propiedad de la implementación de una función de la interfaz común integrada (ECI) segura especificada que representa el esfuerzo y el costo para poner en riesgo la seguridad de la función segura implementada.

3.1.14 parámetros de la configuración de seguridad [b-UIT-T X.1046]: Conjunto de parámetros que describen las características de la función de seguridad, como el ancho de banda máximo, el número máximo de conexiones, etc., que soportan la función de seguridad, el objeto protegido o las acciones de seguridad de la función de seguridad.

3.1.15 registro único [b-UIT-T Y.2201]: Capacidad que tiene un usuario para utilizar una declaración de autentificación expedida por un operador de red o un proveedor de servicio en otro operador o proveedor, bien sea para acceder a un servicio o para la itinerancia en una red visitada.

3.1.16 amenaza [b-ISO/CEI 27000]: Posible causa de un incidente no deseado, que puede dañar un sistema o perjudicar a una organización.

3.1.17 validación [b-UIT-T Z.450]: Proceso de verificación de una especificación para asegurarse de que es sintáctica y semánticamente correcta y de que representa el comportamiento previsto.

3.1.18 vulnerabilidad [b-UIT-T X.1524]: Punto débil del *software* que puede utilizarse para acceder a un sistema o a la información que contiene.

3.1.19 lista blanca [b-UIT-T X.1245]: Lista identificativa de personas o fuentes vinculadas a servicios de comunicaciones, cuando las identificaciones de la lista son conocidas, fiables o explícitamente autorizadas.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 infraestructura de macrodatos: Sistema que combina dispositivos físicos básicos y un entorno de red para constituir un ecosistema de macrodatos que permite la prestación de servicios de macrodatos con el fin de recopilar datos, procesar datos, gestionar datos, etc.

3.2.2 plataforma de macrodatos: Sistema o conjunto de sistemas distribuidos en un ecosistema de macrodatos para realizar análisis de datos, visualización de datos y otras funciones.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

API	Interfaz de programación de aplicaciones (*application programming interface*)
BDAP	Proveedor de aplicaciones de macrodatos (*big data application provider*)
BDIP	Proveedor de infraestructura de macrodatos (*big data infrastructure provider*)
DDOS	Denegación de servicio distribuida (*distributed denial of service*)
DOS	Denegación de servicio (*denial of service*)
IAM	Gestión de identidades y accesos (*identity and access management*)
IDS	Sistema de detección de intrusiones (*intrusion detection system*)
IP	Protocolo de Internet (*Internet protocol*)
IPS	Sistema de prevención de intrusiones (*intrusion prevention system*)
SSO	Registro único (*single sign-on*)
VM	Máquina virtual (*virtual machine*)

5 Convenios

En esta Recomendación:

La expresión "se recomienda" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio.

6 Amenazas y riesgos de seguridad para las infraestructuras y las plataformas de macrodatos

Como se define en [UIT-T Y.3600] y se muestra en la Figura 6-1 (adaptada de la Figura 7-1 de [UIT-T Y.3600]), una plataforma de macrodatos está proporcionada por un proveedor de plataformas de macrodatos (BDAP) para realizar análisis de datos, visualización de datos y otras funciones. Una infraestructura de macrodatos está proporcionada por un proveedor de infraestructura de macrodatos (BDIP) para prestar servicios de macrodatos como la recopilación de datos, el procesamiento de datos la gestión de los datos, etc.

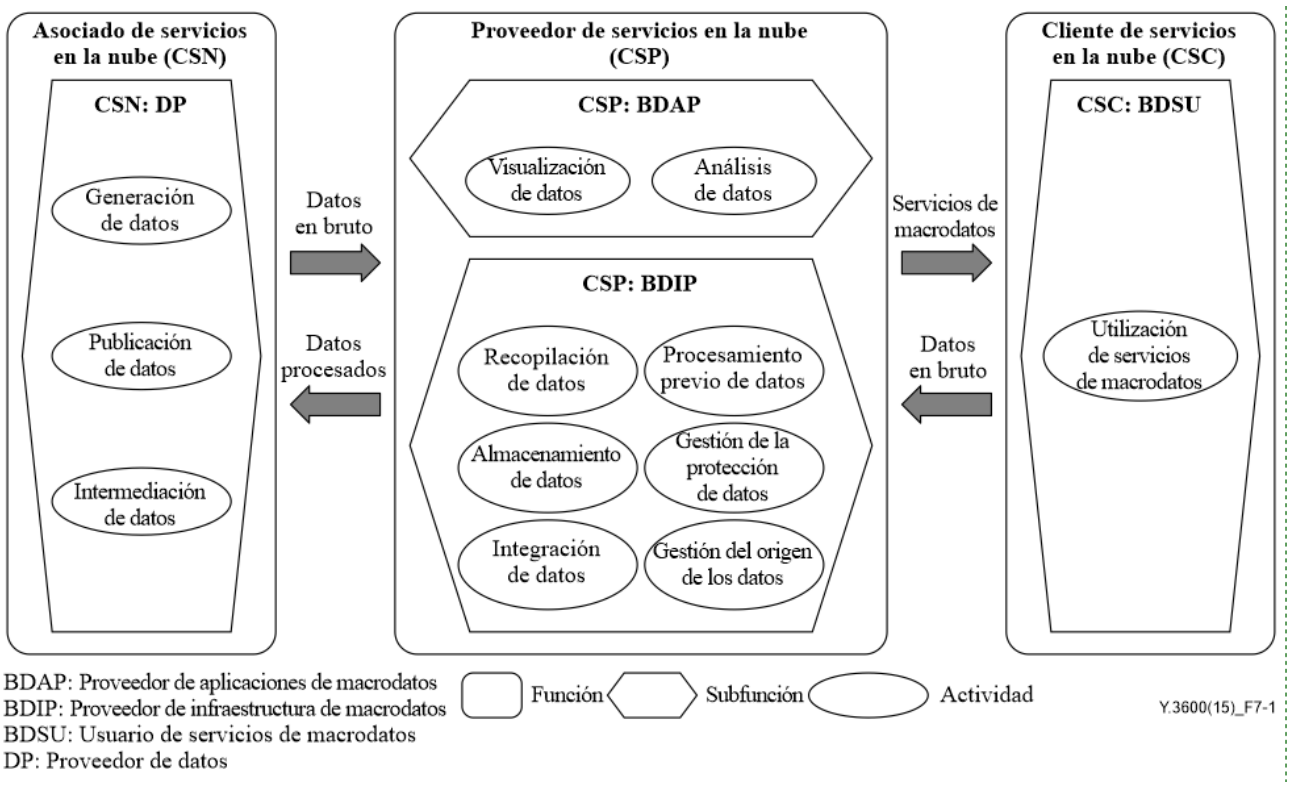

Figura 6-1 – Sistema de macrodatos basado en la computación en la nube

6.1 Amenazas y riesgos de seguridad para las infraestructuras de macrodatos

Las amenazas y los riesgos de seguridad para las infraestructuras de macrodatos incluyen los relativos al almacenamiento de datos, la integración de datos, el procesamiento previo de datos y la gestión de los datos.

6.1.1 Amenazas y riesgos de seguridad para la recopilación de datos

En relación con la seguridad de la recopilación de datos, las amenazas y los riesgos de seguridad incluyen:

a) Recopilación de datos sin autorización: los atacantes pueden recopilar los datos sin permiso o autorización del usuario.

b) Vulnerabilidad de la interfaz de recopilación de datos: los atacantes pueden utilizar una vulnerabilidad de la interfaz de recopilación de datos para acceder al proceso de recopilación y provocar pérdidas de datos.

c) Acceso con derechos de administración no autorizado: el acceso con derechos de administración no autorizados al sistema de recopilación de datos puede provocar pérdidas de datos. Por ejemplo, los atacantes pueden aprovechar una vulnerabilidad del sistema para conseguir acceder con derechos de administración no autorizados al sistema de recopilación de datos y cambiar la dirección IP del destino de la recopilación de datos por la de los atacantes.

6.1.2 Amenazas y riesgos de seguridad para el almacenamiento de datos

En relación con la seguridad del almacenamiento de datos, las amenazas y los riesgos de seguridad incluyen:

a) Pérdidas y filtración de datos: la falta de una gestión adecuada de la información criptográfica, como las claves de encriptación, los códigos de autentificación y los privilegios de acceso, podría dar lugar a daños considerables, como pérdidas de datos o su imprevista filtración al exterior. Además, la convergencia a gran escala de datos de múltiples fuentes

incrementa la dificultad del control de acceso al almacenamiento de datos. Los escenarios complejos del almacenamiento y el flujo de macrodatos hacen que la implementación de la encriptación de los datos sea difícil de llevar a cabo.

b) Indisponibilidad del servicio: un servidor de almacenamiento de datos puede sufrir un ataque de denegación de servicio (DoS) o de denegación de servicio distribuida (DDoS); además, los equipos físicos del almacenamiento pueden fallar y provocar pérdidas y destrucción de datos.

c) Las amenazas y los riesgos de seguridad para las instalaciones físicas de almacenamiento de datos: con respecto a la seguridad de las instalaciones físicas de almacenamiento de datos, éstas se enfrentan a amenazas y riesgos de seguridad similares a lo especificado en la cláusula 9.3 de [UIT-T X.1601] y la cláusula 7 de [UIT-T X.1605].

d) Las amenazas y los riesgos del servicio para el terminal del almacenamiento de datos: en relación con el terminal del almacenamiento de datos, las amenazas y los riesgos de seguridad se centran en los parámetros de la configuración de seguridad del hardware y el software de los terminales, que incluyen los parámetros de la configuración de seguridad del sistema operativo, el software de oficina, los buscadores y el sistema de correo, etc. Las principales amenazas y riesgos de seguridad incluyen los falsos conjuntos de parámetros de la configuración de seguridad, las actualizaciones tardías de los parámetros de la configuración de seguridad, las vulnerabilidades de los parámetros de la configuración de seguridad, etc.

6.1.3 Amenazas y riesgos de seguridad para la integración de datos

En relación con la seguridad de la integración de datos, las amenazas y los riesgos de seguridad incluyen:

a) Utilización indebida de datos: los datos pueden migrar entre diferentes ubicaciones físicas durante la integración de los datos. Es muy importante no permitir que se utilicen indebidamente los datos como resultado de la transmisión de los mismos a diferentes ubicaciones.

b) Suplantación: según la definición de [UIT-T X.1279], la suplantación es la pretensión asumida por una entidad que afirma ser otra entidad diferente, mediante la presentación de una imagen grabada u otra muestra de datos biométricos, o una característica biométrica derivada artificialmente, a fin de hacerse pasar por un individuo. Los atacantes podrían suplantar la identidad del sistema de gestión o del servidor de almacenamiento de datos y provocar la pérdida o el uso indebido de datos durante la integración de datos.

c) Amenazas de seguridad para la red durante la integración de datos: se enfrenta a amenazas de seguridad similares a las especificadas en la cláusula 9.5 de [UIT-T X.1601]. Además, los riesgos de seguridad particulares de la infraestructura de macrodatos se centran en la gestión integrada de la seguridad en toda la red física, la red virtual y los entornos en la nube.

6.1.4 Amenazas y riesgos de seguridad para el procesamiento previo de los datos

En relación con la seguridad del preprocesamiento de los datos, las amenazas y los riesgos de seguridad incluyen:

a) Amenazas internas: un empleado del proveedor de aplicaciones de macrodatos puede hace una utilización indebida de los datos de usuario para unos fines distintos de los previstos durante el procesamiento previo sin el permiso de los usuarios.

b) Vulnerabilidad del sistema: los datos podrían perderse durante el procesamiento previo debido a vulnerabilidades del sistema.

6.1.5 Amenazas y riesgos de seguridad para la gestión de los datos

En relación con la seguridad de la gestión de los datos, las amenazas y los riesgos de seguridad incluyen:

a) Vulnerabilidades del *software*: los atacantes podrían explotar posibles vulnerabilidades de seguridad del *software* utilizado en la gestión de los macrodatos. Los defectos técnicos de la virtualización del sistema podrían provocar diversos riesgos de seguridad; además, una tecnología de operación y mantenimiento inmadura podría aumentar la gravedad de los riesgos. Asimismo, los modelos de computación y almacenamiento a gran escala de las infraestructuras y las plataformas de macrodatos dan lugar a mayores riesgos para los parámetros de la configuración de seguridad del *software* utilizado en la gestión de macrodatos.

b) Errores del control de acceso: los errores del control de acceso de la gestión de los datos pueden dar lugar a la pérdida, la filtración o la utilización indebida de los datos.

c) Acceso con derechos de administración no autorizado: el acceso con derechos de administración no autorizados al sistema de gestión de los macrodatos podría provocar la pérdida, la filtración o la utilización indebida de los datos. Por ejemplo, los atacantes pueden aprovechar una vulnerabilidad del sistema para conseguir acceder con derechos de administración no autorizados al sistema de macrodatos y cambiar la dirección IP de destino de la recopilación de datos por la de los atacantes.

d) Amenazas internas: usuarios descuidados o sin la formación adecuada (o miembros de una familia en los equipos del usuario), o actuaciones malintencionadas de empleados descontentos pueden provocar pérdidas de datos.

6.2 Amenazas y riesgos de seguridad para las plataformas de macrodatos

Las amenazas y los riesgos de seguridad para las plataformas de macrodatos incluyen los relativos al análisis de datos y la visualización de datos.

6.2.1 Amenazas y riesgos de seguridad para el análisis de datos

En relación con la seguridad del análisis de datos, las amenazas y los riesgos de seguridad incluyen:

a) Vulnerabilidad del sistema: los datos podrían perderse debido a una vulnerabilidad en el sistema de análisis de datos.

b) Ataque DoS/DDoS: un servidor de análisis de datos podría sufrir un ataque DoS o DDoS.

c) Utilización compartida de las aplicaciones de análisis de datos: normalmente diferentes usuarios utilizan las aplicaciones de análisis de datos, lo que puede provocar escapes de las máquinas virtuales, perdidas de datos, etc.

d) Acceso inseguro: el acceso inseguro al análisis de macrodatos podría dar lugar a la pérdida, filtración o utilización indebida de los datos de la aplicación.

e) Acceso con derechos de administración no autorizados: el acceso con derechos de administración no autorizados al análisis de macrodatos puede dar lugar a la pérdida de datos.

6.2.2 Amenazas y riesgos de seguridad para la visualización de datos

En relación con la seguridad de la visualización de datos, las amenazas y los riesgos de seguridad incluyen:

a) Utilización indebida de datos: el proveedor de aplicaciones de macrodatos podría utilizar indebidamente (o presentar sin el permiso de los usuarios) los datos durante la visualización de datos.

b) Vulnerabilidad del sistema: los datos de los análisis o de los informes podrían perderse debido a una vulnerabilidad en el sistema de visualización de datos.

c) Interpretación inadecuada: los datos podrían ser interpretados inadecuadamente durante la visualización de los datos sin el permiso de los usuarios debido a un fallo de las políticas de control de acceso.

7 Directrices de seguridad para infraestructuras y plataformas de macrodatos

Como se define en [UIT-T Y.3605], la estructura de capas utilizada en la arquitectura de referencia de los macrodatos tiene cuatro capas, y un conjunto de funciones que abarcan estas diferentes capas. Las cuatro capas son:

– capa de acceso;

– capa de aplicación;

– capa de procesamiento; y

– capa de origen de datos.

Las funciones que abarcan varias capas se llaman funciones multicapas.

La estructura de capas se muestra en la Figura 7-1 (adaptada de la Figura 8-2 de [UIT-T Y.3605]).

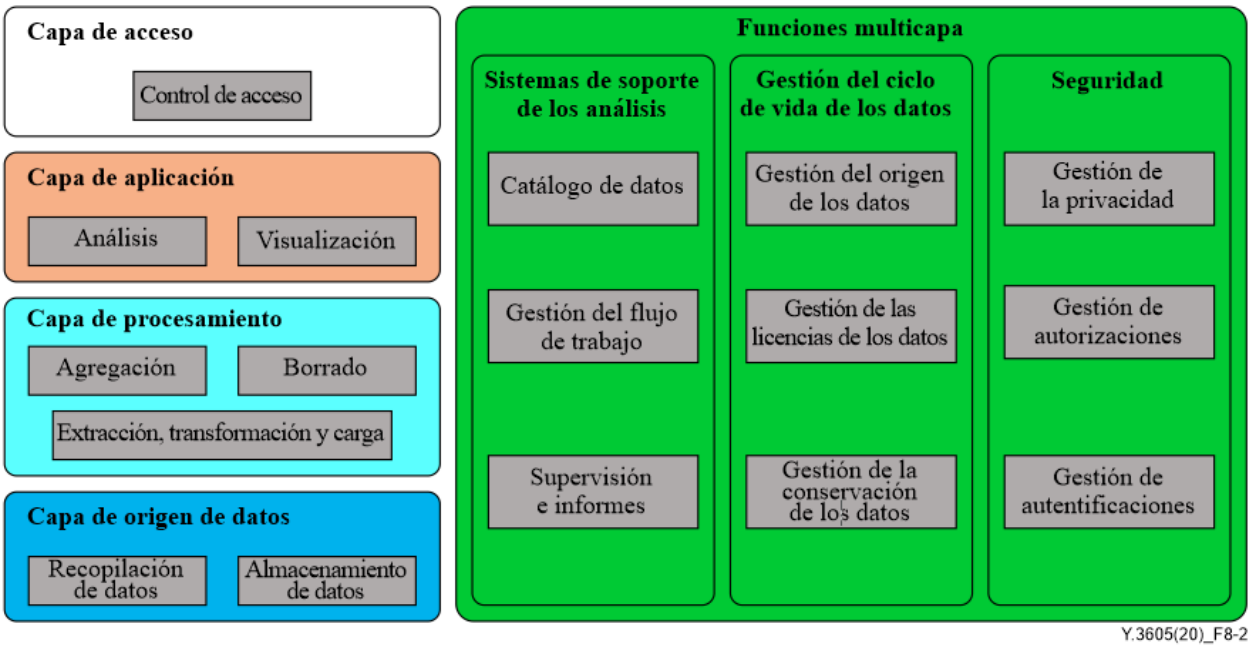

Figura 7-1 – Estructura de capas para los macrodatos

Con base en la estructura de capas indicada en la Figura 7-1, la presente Recomendación utiliza una arquitectura para la seguridad de las infraestructuras y las plataformas de macrodatos que se muestra en la Figura 7-2.

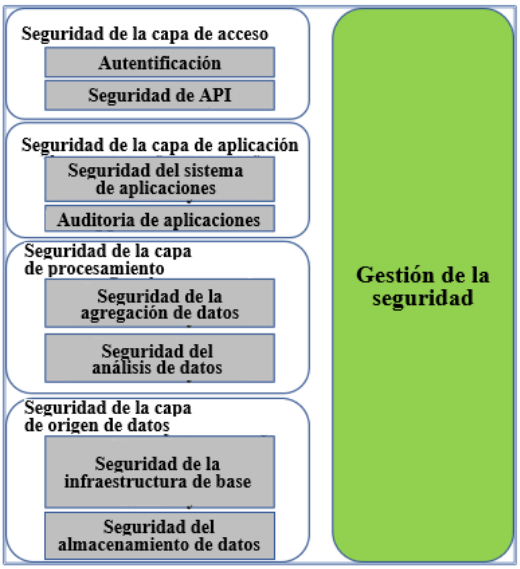

Figura 7-2 – Arquitectura para la seguridad de las infraestructuras y las plataformas de macrodatos

En esta Recomendación se especifican las directrices de seguridad para las infraestructuras y las plataformas de seguridad y se incluyen:

a) directrices de seguridad para la capa de origen de datos;

b) directrices de seguridad para la capa de procesamiento;

c) directrices de seguridad para la capa de aplicación;

d) directrices de seguridad para la capa de acceso;

e) directrices para la gestión de la seguridad.

7.1 Directrices de seguridad para la capa de origen de datos

Las directrices de seguridad para la capa de origen de datos se centran en la seguridad de la infraestructura básica y la seguridad del almacenamiento de datos.

7.1.1 Directrices de seguridad para la infraestructura de base

Las directrices de seguridad para la infraestructura de base incluyen lo siguiente:

a) Se recomienda dividir las infraestructuras virtuales en dominios de seguridad internos y externos y establecer diferentes políticas de seguridad según las necesidades. Se recomienda proporcionar mecanismos de aislamiento efectivos entre los dominios de seguridad internos y externos.

b) Se recomienda implementar unas políticas estrictas de control de acceso entre los dominios de seguridad de las infraestructuras virtuales. Se recomienda utilizar el principio de privilegio mínimo y, por tanto, asignar la autentificación y la autorización de los usuarios en base a las responsabilidades de la función/categoría para permitir el acceso a las infraestructuras virtuales.

c) Se recomienda desplegar *software* de seguridad, como *software* antivirus, en las infraestructuras virtuales para mejorar la protección de la seguridad, y actualizar periódicamente las bases de datos de virus y de código maligno.

d) Se recomienda desplegar equipos de detección de los ataques a la red y de protección frente a los mismos como, por ejemplo, sistemas de prevención de intrusiones (IPS)/sistemas de detección de intrusiones (IDS), cortafuegos, protección frente a DDoS, etc. en las fronteras entre las redes internas y externas, y actualizar periódicamente las bases de datos de firmas de ataques a su última versión.

e) Se recomienda implantar un aislamiento estricto y unas políticas de control de acceso en las fronteras entre las redes internas y externas para evitar accesos no autorizados a las infraestructuras de base.

f) Se recomienda monitorizar los tráficos de red de las infraestructuras de base y realizar una inspección detallada, incluyendo información como las estadísticas de los flujos de red, el tráfico de red inusual, etc.

g) Se recomienda mostrar la información de los ataques, como tipo de ataque, direcciones IP de origen/destino, etiquetas de tiempos, etc. cuando se detectan los ataques.

h) Se recomienda llevar a cabo una supervisión centralizada y en tiempo real de la seguridad que incluya el estado de funcionamiento de los diferentes recursos físicos y virtuales.

7.1.2 Directrices de seguridad para el almacenamiento de datos

Las directrices de seguridad para el almacenamiento de datos incluyen lo siguiente:

a) Se recomienda utilizar componentes seguros de almacenamiento de datos, tales como sistemas de archivos distribuidos seguros, almacenamientos indexados seguros, entre otros, para garantizar la seguridad del entorno de almacenamiento.

b) Se recomienda soportar estrategias de aislamiento para los datos de los diferentes usuarios en un entorno de múltiples clientes.

c) Se recomienda formular políticas de seguridad y reglamentaciones de gestión del almacenamiento de datos, como políticas de control de acceso, políticas de transmisión segura de datos, políticas de integridad de datos, políticas de consistencia de múltiples copias, políticas sobre información personal y encriptación de los datos esenciales, etc.

d) Se recomienda soportar múltiples mecanismos de desensibilización de datos.

e) Se recomienda soportar la encriptación de los sistemas de archivos, para prevenir la corrupción y la fuga de datos. Se recomienda además soportar categorías de encriptación en función del nivel de sensibilidad de los datos: sin encriptación, encriptación parcial, encriptación completa, etc.

f) Se recomienda proporcionar funciones para la detección de los daños a la integridad de los datos del almacenamiento y para el restablecimiento de la integridad de los datos después de que se produzcan daños.

g) Se recomienda soportar opciones para los parámetros de la configuración de seguridad de la encriptación para que los usuarios puedan elegir.

h) Se recomienda dar soporte a los usuarios en la elección de un mecanismo de encriptación de terceros para la encriptación de los datos de las claves.

i) Se recomienda soportar la encriptación de datos mediante claves seguras, así como el almacenamiento y el mantenimiento local de las claves seguras.

j) Se recomienda soportar un algoritmo de encriptación adecuado para la copia de respaldo de los medios en almacenamiento de larga duración, como la utilización de claves de encriptación largas y la planificación de su sustitución por un algoritmo de encriptación mejorado.

k) Se recomienda definir los tiempos oportunos y los derechos para la compartición de los datos, la autorización de la utilización de los datos y el borrado de los datos.

l) Se recomienda autorizar el periodo de validez de la utilización de los datos y notificarlo a los usuarios y los proveedores de macrodatos asociados.

m) Se recomienda soportar las funciones de borrado, copia de respaldo y recuperación de los datos.

7.2 Directrices de seguridad para la capa de procesamiento

Las directrices de seguridad para la capa de procesamiento se centran en seguridad para la agregación de datos y para el análisis de datos.

7.2.1 Directrices de seguridad para la agregación de datos

Las directrices de seguridad para la agregación de datos incluyen lo siguiente:

a) Se recomienda que los componentes de agregación de datos soporten un mecanismo de autentificación, y se recomienda realizar la autentificación y la autorización del terminal del origen de los datos y de los operadores de las plataformas de macrodatos.

b) Se recomienda la aplicación de unas reglamentaciones de seguridad estrictas en los procesos de agregación de datos, que incluyen la clasificación, la transmisión y el almacenamiento temporal.

c) Se recomienda establecer una estrategia de categorización para diferentes orígenes de datos con su correspondiente política de gestión de seguridad, que debe abarcar el proceso de transmisión y almacenamiento temporal. Para cada categoría de origen de datos, se recomienda definir la correspondiente política de gestión de la seguridad con la confidencialidad, la integridad y la disponibilidad de los datos.

d) Se recomienda soportar unas funciones de control de acceso restringido para una carpeta de almacenamiento temporal en los procesos de agregación de datos, de manera que se pueda prohibir el acceso de procesos o de datos de usuarios no deseados, la modificación no autorizada de la dirección de almacenamiento de los componentes de la agregación de datos.

e) Se recomienda proporcionar funciones de reparto de carga para los componentes de agregación de datos, de manera que la carga de grandes flujos de datos pueda aliviarse por múltiples canales.

f) Se recomienda proporcionar funciones de detección y protección como los sistemas de prevención/detección de intrusiones (IPS/IDS) para los componentes de agregación de datos, de manera que puedan aplicarse restricciones a la recopilación excesiva o no deseada de datos.

g) Se recomienda proporcionar mecanismos de conmutación y recuperación en caso de fallo, para los componentes de la agregación, de manera que los flujos de datos transmitidos puedan conmutarse a un componente de reserva.

h) Se recomienda proporcionar un registro de la agregación de datos y generar alarmas ante situaciones anómalas, como en los casos en que: se hayan recopilado datos de manera repetida, los flujos de datos hayan superado el umbral definido, los flujos de datos se hayan interrumpido o se haya superado el límite del almacenamiento de datos recopilados.

7.2.2 Directrices de seguridad para el análisis de datos

Las directrices de seguridad para el análisis de datos incluyen lo siguiente:

a) Se recomienda proporcionar métodos de autentificación para asegurar que solo los usuarios o las aplicaciones legítimos pueden iniciar solicitudes de análisis de datos.

b) Se recomienda implantar un módulo de control de acceso para el análisis de datos, de acuerdo con las políticas de identificación y de autentificación de los usuarios de macrodatos, que incluya la gestión y validación de los tiempos del control de acceso y los mecanismos de validación del cumplimiento de las reglas de acceso a los datos.

c) Se recomienda soportar una auditoría de seguridad del análisis de datos distribuidos y se recomienda que la información de dicha auditoria se almacene y se controle de manera segura.

d) Se recomienda proporcionar un mecanismo de desensibilización para mantener la seguridad y la robustez del análisis de datos, y se recomienda que la continuidad del negocio no se vea afectada. Se recomienda además que la calidad de funcionamiento del sistema no se vea fuertemente afectada después de utilizar el mecanismo de desensibilización.

e) Se recomienda poder establecer diferentes mecanismos de desensibilización de acuerdo con las demandas de los usuarios o los tipos de datos.

f) Se recomienda soportar la configuración del algoritmo de desensibilización después de que se consulten o se soliciten los usuarios.

g) Se recomienda que los mecanismos de desensibilización puedan añadirse o eliminarse de manera dinámica, lo que puede soportar la actualización suave del sistema sin interrupción del negocio.

7.3 Directrices de seguridad para la capa de aplicación

Las directrices de seguridad para la capa de aplicación se centran en los sistemas de aplicaciones y las auditorías de las aplicaciones.

7.3.1 Directrices de seguridad para el sistema de aplicaciones

Las directrices de seguridad para el sistema de aplicaciones incluyen lo siguiente:

a) Se recomienda proporcionar métodos de detección y protección para los sistemas de aplicaciones, como cortafuegos, sistemas antivirus, e IDS/IPS.

b) Se recomienda implantar defensas contra las vulnerabilidades del sistema de aplicaciones.

c) Se recomienda proporcionar métodos de autentificación para prevenir el acceso no autorizado al sistema de aplicaciones.

d) Se recomienda mantener el aislamiento entre diferentes aplicaciones, para evitar las fugas de datos provocadas por los análisis de asociación de datos iniciados por diferentes aplicaciones.

7.3.2 Directrices de seguridad para la auditoria de las aplicaciones

Las directrices de seguridad para la auditoria de las aplicaciones incluyen lo siguiente:

a) Se recomienda auditar las operaciones de los administradores de las aplicaciones, que pueden dejar trazas de eventos y aportar pruebas de incidentes de seguridad.

b) Se recomienda auditar las operaciones de los usuarios de las aplicaciones para permitir detectar comportamientos maliciosos, alertar de ellos y responder rápidamente.

c) Se recomienda auditar la modificación de los parámetros de la configuración de seguridad relativos a las alertas, la respuesta rápida a los comportamientos maliciosos, etc.

7.4 Directrices de seguridad para la capa de acceso

Las directrices de seguridad para la capa de acceso se centran en los mecanismos de autentificación y las interfaces de programación de aplicaciones (API).

7.4.1 Directrices de seguridad para los mecanismos de autentificación

Las directrices de seguridad para los mecanismos de autentificación incluyen lo siguiente:

a) Se recomienda soportar unos servicios mejorados de autentificación, como la autentificación de registro único (*single sign-on*, SSO), la autentificación de múltiples factores, etc.

b) Se recomienda aplicar políticas de contraseñas fuertes, como aumentar la complejidad de las contraseñas, actualizar las contraseñas regularmente, etc.

c) Se recomienda soportar mecanismos de autentificación por listas blancas, como listas blancas de direcciones IP, etc.

7.4.2 Directrices de seguridad para las API

Las directrices de seguridad para las API incluyen lo siguiente:

a) Se recomienda permitir que los administradores autoricen el acceso para las API, como poder configurar el número máximo de veces que un usuario puede acceder a una API, el número total de conexiones que soportan las API, etc.

b) Se recomienda soportar la monitorización en tiempo real de las características de los flujos de red entre clientes e interfaces API, generar alertas y permitir respuestas a los incidentes de tráfico de red anómalo.

c) Se recomienda validar las entradas de las API para prevenir varios tipos de ataques a la seguridad.

d) Se recomienda soportar la transferencia de los datos esenciales por un canal seguro, como un canal encriptado, etc.

e) Se recomienda aplicar un examen y desensibilización de manera bidireccional entre los clientes y las API antes de la transferencia de datos.

f) Se recomienda soportar el control de integridad de los datos y detectar la corrupción de los datos o la pérdida de los mismos durante las transmisiones.

7.5 Directrices para la gestión de la seguridad

Las directrices para la gestión de la seguridad incluyen lo siguiente:

a) Se recomienda utilizar auditorías de la gestión de la identidad y el acceso, y del control de acceso, incluidos los registros de operación y mantenimiento, los registros de accesos a los datos, la inspección de los comportamientos de acceso, la gestión de claves y la encriptación de datos.

b) Se recomienda utilizar mecanismos de detección y protección racionales y eficaces incluida la redundancia de la seguridad de las infraestructuras, el análisis de vulnerabilidades, los IPS/IDS, cortafuegos, y los dispositivos de seguridad de la virtualización.

c) Se recomienda utilizar técnicas de refuerzo de la seguridad para reducir las posibilidades de ataque de las infraestructuras y las plataformas.

d) Se recomienda realizar la actualización de parches y versiones regularmente en las infraestructuras y plataformas de macrodatos.

Bibliografía

[b-UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

[b-UIT-T X.810] Recomendación UIT-T X.810 (1995), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general*.

[b-UIT-T X.1158] Recomendación UIT-T X.1158 (2014), *Mecanismo de autentificación multifactorial utilizando un dispositivo móvil*.

[b-UIT-T X.1217] Recomendación UIT-T X.1217 (2021), *Directrices para la aplicación de la inteligencia sobre amenazas en la explotación de redes de telecomunicaciones*.

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

[b-UIT-T X.1361] Recomendación UIT-T X.1361 (2018), *Marco de seguridad para la Internet de las cosas basado en el modelo de pasarela*.

[b-UIT-T X.1524] Recomendación UIT-T X.1524 (2012), *Lista de puntos débiles comunes*.

[b-UIT-T X.1631] Recomendación UIT-T X.1631 (2015), *Tecnologías de la información - Técnicas de seguridad -Código de prácticas para controles de seguridad de la información basados en SO/IEC 27002 para los servicios en la nube*.

[b-UIT-T Y.2052] Recomendación UIT-T Y.2052 (2008), *Marco para el multidireccionamiento en las NGN IPv6*.

[b-UIT-T Y.2201] Recomendación UIT-T Y.2201 (2009), *Requisitos y capacidades de las NGN del UIT-T*.

[b-UIT-T Y.2244] Recomendación UIT-T Y.2244 (2019), *Modelo de servicio para un servicio de plan de cultivo en la fase de preproducción*.

[b-UIT-T Y.3500] Recomendación UIT-T Y.3500 (2014), *Tecnología de la información – Computación en la nube – Descripción general y vocabulario*.

[b-UIT-T Y.3502] Recomendación ITU-T Y.3502 (2014), *Tecnología de la información – Computación en la nube – Arquitectura de referencia*.

[b-ISO/CEI 18014-2] ISO/CEI 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-ISO/CEI 19440] ISO/CEI 19440:2007, *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/CEI 19944] ISO/CEI 19944:2016, *Information technology – Cloud services and devices: data flow, data categories and data use*.

[b-ISO/CEI 20000-1] ISO/CEI 20000-1:2011, *Information technology – Service management – Part 1: Service management system requirements*.

[b-ISO/CEI 27000] ISO/CEI 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/CEI 27729] ISO/CEI 27729:2012, *Information and documentation – International standard name identifier (ISNI)*.

[b-ISO/CEI 29100] ISO/CEI 29100:2011, *Information technology – Security techniques – Privacy framework*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2022