ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T X.1816 (03/2023)

SERIE X: Redes de datos, comunicaciones de sistemas abiertos y seguridad

Seguridad en las redes IMT-2020

Directrices y requisitos para clasificar las capacidades de seguridad en la segmentación de red IMT-2020

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	X.1000-X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	X.1100-X.1199
SEGURIDAD EN EL CIBERESPACIO	X.1200-X.1299
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	X.1300-X.1499
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	X.1500-X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	X.1600-X.1699
COMUNICACIÓN CUÁNTICA	X.1700-X.1729
SEGURIDAD DE LOS DATOS	X.1750-X.1799
SEGURIDAD EN LAS REDES IMT-2020	**X.1800-X.1819**

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

Recomendación UIT-T X.1816

Directrices y requisitos para clasificar las capacidades de seguridad en la segmentación de red IMT-2020

Resumen

La definición de las funciones y procesos básicos de la tecnología de segmentación de red ha establecido una base sólida para la primera fase del despliegue de las IMT-2020 y la utilización comercial de los servicios de segmentación de red. Dado que se trata de una red lógica de extremo a extremo que se personaliza según la demanda, la segmentación puede ofrecer capacidades de seguridad diferenciada.

En primer lugar, la segmentación de red IMT-2020 ofrece las medidas de seguridad que respaldan la implementación diferenciada de redes. En segundo lugar, la red IMT-2020 soporta algunas medidas de seguridad opcionales a nivel del segmento. Algunas medidas de seguridad también pueden ofrecer múltiples opciones de seguridad y los operadores podrían poseer diferentes recursos de seguridad. Estos podrían aportar diferentes niveles de garantía de seguridad o de calidad de funcionamiento no relacionada con la seguridad.

Los clientes de los segmentos también tienen requisitos de seguridad específicos y podrían solicitar segmentos de red personalizados con diferentes niveles de protección de seguridad a los operadores de los segmentos. Los clientes de los segmentos o los operadores de estos encargados de seleccionar las capacidades de seguridad de sus segmentos, como los costes de gestión y la incoherencia en la definición, etc., se enfrentan a algunas dificultades. El objetivo de la Recomendación UI-T X.1816 es describir las capacidades de seguridad diferenciadas de los segmentos de red IMT-2020 y proporcionar directrices para clasificar las capacidades de seguridad de los segmentos de red IMT-2020 y la seguridad de los segmentos de red IMT-2020 a fin de ayudar al ecosistema de las IMT-2020 a comprender y seleccionar de forma más adecuada las capacidades de seguridad de los segmentos de red.

Historia *

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único
1.0	ITU-T X.1816	2023-03-03	17	11.1002/1000/15114

Palabras clave

Capacidades de seguridad, clasificación, IMT-2020, segmento de red.

* Para acceder a la Recomendación, sírvase digitar el URL https://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación.

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 se pronuncia en lo que respecta a la existencia, validez o aplicabilidad de los derechos de propiedad intelectual reclamados, 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 patentes/derechos de autor de *software*, 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 las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1816

Directrices y requisitos para clasificar las capacidades de seguridad en la segmentación de red IMT-2020

1 Alcance

El objetivo de esta Recomendación es ofrecer orientaciones y requisitos para clasificar la seguridad de los segmentos de red IMT-2020. Esta Recomendación especifica:

- La definición de las capacidades de seguridad diferenciadas de los segmentos de red IMT-2020;
- Los principios y métodos para identificar la clasificación de las capacidades de seguridad de los segmentos de red IMT-2020.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.805] Recomendación UIT-T X.805 (2003), *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo.*

[UIT-T X.1047] Recomendación UIT-T X.1047 (2021), *Requisitos y arquitectura de seguridad para la gestión y orquestación de la segmentación de red.*

[3GPP TS 33.501] Especificación técnica 3GPP TS 33.501 V17.1.0 (2021), *Proyecto de Asociación de 3ª Generación; Servicios del Grupo de Especificación Técnica y Aspectos de Sistemas; Arquitectura y procedimientos de seguridad para el sistema 5G (Versión 17).*

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 segmento de red [b-UIT-T Y.3100]: Red lógica que proporciona capacidades y características de red específicas.

NOTA 1 – Los segmentos de red permiten la creación de redes personalizadas, capaces de ofrecer soluciones flexibles para diferentes casos de mercado, con diversos requisitos, en lo que atañe a las funcionalidades, la calidad de funcionamiento y la atribución de recursos.

NOTA 2 – Un segmento de red puede ser capaz de exponer sus propias capacidades.

NOTA 3 – El comportamiento de un segmento de red se materializa a través de la instancia o instancias del segmento de red en cuestión.

3.1.2 instancia de segmento de red [b-UIT-T Y.3100]: Una instancia de un segmento de red, que se crea sobre la base de un plan de segmentación de red.

3.1.3 subred de segmento de red [b-ETSI TS 128 530]: Una representación de los aspectos de gestión de un conjunto de funciones gestionadas y los recursos necesarios (por ejemplo, recursos de computación, almacenamiento y red).

3.2 Términos definidos en la presente Recomendación

Ninguno.

4 Abreviaturas y acrónimos

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

AAA	Autenticación, autorización y contabilización (*authentication, authorization, and accounting*)
ACL	Lista de control de acceso (*access control list*)
AMF	Función de gestión de acceso y movilidad (*access and mobility management function*)
CN	Red central (*core network*)
CU	Unidad central (*central unit*)
DDoS	Denegación de servicio distribuida (*distributed denial of service*)
DU	Unidad distribuida (*distributed unit*)
EAP	Protocolo de autenticación extensible (*extensible authentication protocol*)
ENSI	Información de segmentación de red externa (*external network slice information*)
gNB	Nodo B NR (*NR node B*)
IMT-2020	Telecomunicaciones móviles internacionales-2020 (*international mobile telecommunications-2020*)
NAT	Conversión de dirección de red (*network address translation*)
NFV	Virtualización de la función de red (*network function virtualization*)
ng-eNB	Nodo B evolucionado de próxima generación (*next generation evolved node-B*)
S-NSSAI	Información de ayuda para la selección de un único segmento de red (*single network slice selection assistance information*)
NSSAI	Información de ayuda para la selección del segmento de red (*network slice selection assistance information*)
PDU	Unidad de datos de protocolo (*protocol data unit*)
PNF	Función de red física (*physical network function*)
RAN	Red de acceso radioeléctrico (*radio access network*)
RB	Portador radioeléctrico (*radio bearer*)
TLS	Seguridad de la capa de transporte (*transport layer security*)
UE	Equipo de usuario (*user equipment*)
URL	Localizador uniforme de recursos (*uniform resource locator*)
VNF	Función de red virtual (*virtual network function*)
WAF	Cortafuegos de aplicaciones web (*web application firewall*)

5 Convenios

En esta Recomendación:

La expresión **"se recomienda"** indica que se trata de un requisito recomendado pero que no es absolutamente obligatorio. Por tanto, el cumplimiento de ese requisito no es necesario para invocar la conformidad.

La expresión **"se tiene la opción de"** u **"opcionalmente"** indica que se trata de un requisito opcional que se permite, sin que ello signifique que se recomienda. El uso de este término no implica que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

6 Introducción sobre la clasificación de las capacidades de seguridad de los segmentos de red IMT-2020

La seguridad de los segmentos de red es un prerrequisito previo de la introducción a la segmentación de red. En cuanto a los clientes de segmentos que utilizan servicios de comunicación por segmentos, estos necesitan la correspondiente garantía de seguridad para la aplicación de sus segmentos y podrían también tener necesidades específicas de seguridad sobre la base de sus servicios que utilizan los segmentos. Por lo tanto, tal vez soliciten segmentos de red personalizados con diferentes niveles de protección de seguridad a sus operadores. Para los operadores de segmentos que diseñan, construyen y operan redes y proporcionan segmentos de red, la segmentación implica múltiples ámbitos (por ejemplo, la comunicación inalámbrica, la transmisión, la red central y la gestión) y puede ofrecer capacidades de seguridad diferenciadas. En primer lugar, la segmentación de red IMT-2020 ofrece medidas de seguridad para la implementación diferenciada de la red. En segundo lugar, la red IMT-2020 soporta algunas medidas de seguridad opcionales a nivel del segmento. Algunas medidas de seguridad también pueden ofrecer múltiples opciones de seguridad y los operadores pueden poseer diferentes recursos de seguridad. Estos pueden aportar diferentes niveles de garantía de seguridad o de calidad de funcionamiento no relacionada con la seguridad. Por consiguiente, las capacidades de seguridad de un segmento han de decidirse sobre la base de las necesidades de los clientes y las capacidades de seguridad que la red es capaz de proporcionar. Hay algunos desafíos a los que se enfrentan los clientes de segmentos y los operadores de segmentos a la hora de elegir las capacidades de seguridad de sus segmentos:

- Los requisitos de seguridad de los clientes tal vez sean imprecisos y escasos y no sean suficientes para establecer la correspondencia con las capacidades de seguridad.
- Los clientes podrían tener demasiados requisitos de seguridad que van más allá de las capacidades de la red.
- El coste que supone para las partes interesadas conocer las capacidades de seguridad y las diferencias puede variar y la combinación de las capacidades que elijan podría no ser razonable. Por ejemplo, la protección proporcionada por las capacidades seleccionadas podría ser incompatible con múltiples ámbitos o partes interesadas.
- El número de combinaciones de capacidades de seguridad de los segmentos podría ser muy grande y el coste de gestión y orquestación para los operadores podría ser relativamente alto.

Se recomendarán capacidades de seguridad diferenciadas para los segmentos de red IMT-2020 y una metodología para clasificarlas y combinarlas, cuya importancia es la siguiente:

- Esto ayuda a la industria a lograr una comprensión unificada de las capacidades de seguridad de los segmentos y la diferencia entre las capacidades de seguridad de los segmentos (por ejemplo, la calidad de funcionamiento).

- Proporciona una clasificación general básica de las capacidades de seguridad de los segmentos IMT-2020 para que la industria comprenda claramente esas capacidades y las adecue mejor a la mayoría de las aplicaciones industriales.
- Ayuda a lograr la itinerancia entre diferentes segmentos, lo cual facilita también la reutilización de los segmentos.
- Proporciona una referencia para que los usuarios industriales elijan segmentos apropiados que pueden atender a sus necesidades.
- Proporciona una referencia para que los supervisores industriales formulen planes de desarrollo y estrategias respecto de los segmentos.
- Proporciona una referencia para que los proveedores de servicios desplieguen sus servicios en segmentos apropiados.
- Proporciona una referencia para que los operadores formulen los planes de desarrollo de los segmentos y evalúen el valor y los precios de los segmentos.
- Proporciona una referencia para que los distribuidores de equipos planifiquen la hoja de ruta de la tecnología y la hoja de ruta de productos de los segmentos.

La metodología incluye los siguientes aspectos:

- Enumerar las capacidades de seguridad diferenciadas generales de los segmentos de una forma estructurada, con inclusión del nombre, la descripción, la dimensión de seguridad y las opciones. Esto se facilita en la cláusula 7.
- Para cada dimensión de seguridad, se pueden establecer múltiples niveles de una única dimensión enumerando combinaciones de las correspondientes capacidades de seguridad de los segmentos con diferentes opciones, sobre la base de los mismos principios. Esto se facilita en la cláusula 8.
- Además, se pueden definir tipos básicos de seguridad de segmentos con dimensiones de seguridad eligiendo un nivel para cada dimensión de seguridad sobre la base de los mismos principios. Esto se facilita en la cláusula 9.
- Las partes interesadas pueden utilizar el principio, los métodos y los resultados de la clasificación para decidir las capacidades de seguridad de un segmento. Esto se facilita en la cláusula 10.

7 Capacidades de seguridad de los segmentos de red IMT-2020

7.1 Modelo para las descripciones de las capacidades de seguridad de los segmentos de red

En la cláusula 7 se enumeran las capacidades generales de seguridad de la red IMT-2020 que pueden variar en función de los segmentos de red. Las descripciones de las capacidades de seguridad deben ser claras, concisas e inequívocas. Cada descripción debe incluir:

- **La descripción de la capacidad**: una descripción detallada de la capacidad de seguridad diferenciada del segmento de red IMT-2020.
- **El nombre de la capacidad:** un nombre único y un acrónimo asignado a cada capacidad de seguridad.
- **La dimensión de seguridad de la capacidad:** un aspecto particular de la seguridad que ha de abordar la capacidad de seguridad. Hay ocho (8) dimensiones de seguridad, a saber, el control de acceso, la autenticación, la no repudiación, la confidencialidad de datos, la seguridad de la comunicación, la integridad de datos, la disponibilidad y la privacidad [UIT-T X.805].

- **Las opciones de la capacidad:** las múltiples opciones que ofrece cada capacidad de seguridad, que pueden variar de un segmento a otro. En esta Recomendación se hace referencia a cada opción mediante un "acrónimo de la capacidad.número de serie".

Nota: Las opciones son genéricas y no se vinculan con implementaciones de red específicas. Además, pueden subdividirse a fin de adecuarse a una implementación específica.

7.2 Capacidades de seguridad diferenciadas de los segmentos IMT-2020

7.2.1 Capacidad de autenticación y autorización de determinados segmentos de red

- **Descripción de la capacidad:** el sistema IMT-2020 ofrece la autenticación y autorización opcionales [3GPP TS 33.501] de determinados segmentos de red entre un equipo de usuario (UE) y un servidor de autenticación, autorización y contabilización (AAA-S) que puede ser propiedad de una empresa tercera externa. La autenticación y autorización de determinados segmentos de red puede activarse sobre la base de la información de ayuda para la selección de un único segmento de red (S-NSSAI) tras la autenticación primaria. El servidor AAA también puede activar la autorización, revocación, reautenticación y reautorización de determinados segmentos.
- **Nombre de la capacidad:** autenticación y autorización de determinados segmentos de red (NSSAA).
- **Dimensión de seguridad de la capacidad:** autenticación, control de acceso.
- **Opción de la capacidad:**
  - NSSAA.0: desactivada
  - NSSAA.1: activada

7.2.2 Capacidad de aislamiento de los recursos de red en la segmentación de red

- **Descripción de la capacidad**: los segmentos de red IMT-2020 se ejecutan en los recursos de infraestructura unificados de los operadores. Existen diversas soluciones de aislamiento para evitar que elementos de red de un segmento accedan o influyan en los de diferentes segmentos a través de recursos de infraestructura compartidos. En cuanto a los dominios de las subredes de segmentos:
  - Red de acceso (AN): para la interfaz aérea, las opciones de compartición de recursos de portadores radioeléctricos (RB) dinámicos y de reserva de RB estáticos se encuentran disponibles para la asignación de recursos. La primera opción ofrece resultados mejores y más flexibles respecto de la cobertura y la utilización de recursos, mientras que la segunda es más fiable y más costosa. En cuanto a la estación de base, la unidad central (CU) y la unidad distribuida (DU) de diferentes segmentos pueden ser las mismas. Para obtener mayores niveles de aislamiento, se pueden aislar físicamente asignando hardware específico o aislado de manera lógica utilizando la virtualización de la función de red (NFV) (mediante una máquina virtual / contenedor) para compartir el hardware.
  - Red de transporte (TN): el aislamiento en redes de transporte puede ser inexistente (sin aislamiento), o tratarse de un aislamiento físico (por ejemplo, aislamiento de la función de red física, aislamiento del enlace de red física, etc.), un aislamiento lógico (por ejemplo, aislamiento de la función de red lógica, aislamiento del enlace de red lógica/virtual, etc.) [UIT-T X.1047].
  - Red central (CN): el aislamiento físico de recursos de la red central abarca uno o varios aislamientos específicos de la función de red física (PNF), aislamientos específicos del enlace de red física, el aislamiento de la ubicación geográfica, el aislamiento de la computación, el aislamiento de la memoria, el aislamiento del almacenamiento, el aislamiento de la PNF basado en la seguridad, etc. El aislamiento lógico de los recursos de la red central abarca uno o varios aislamientos de la función de red virtual (VNF), el

aislamiento del enlace virtual, el aislamiento de las tecnologías de virtualización, el aislamiento de la computación virtual, el aislamiento de la memoria virtual, el aislamiento del almacenamiento virtual, el aislamiento de la ubicación geográfica del HW que se ha virtualizado para proporcionar recursos virtuales, y el aislamiento de la VNF basado en la seguridad, etc. [UIT-T X.1047].

En cuanto a los tipos de recursos y técnicas de aislamiento:

– Recursos de la interfaz aérea: compartición de RB o reserva de RB.

– Recursos de la función de red de las redes AN/TN/CN: aislamiento físico, aislamiento lógico o sin aislamiento.

- Nombre de la capacidad: aislamiento de los recursos de red en segmentos (SIR).
- Dimensión de seguridad de la capacidad: control del acceso, disponibilidad, privacidad.
- Opciones de la capacidad y calidad de funcionamiento correspondiente:
  – SIR.0: sin aislamiento
  – SIR.1: aislamiento lógico + compartición de RB
  – SIR.2: aislamiento lógico y físico + compartición de RB
  – SIR.3: aislamiento físico + compartición de RB
  – SIR.4: aislamiento lógico + reserva de RB
  – SIR.5: aislamiento lógico y físico + reserva de RB
  – SIR.6: aislamiento físico + reserva de RB

7.2.3 Capacidad de protección de datos del plano de usuario

- Descripción de la capacidad: el sistema IMT-2020 puede proporcionar capacidades de protección diferenciadas de los datos del plano de usuario a nivel de los segmentos. El Nodo B evolucionado de próxima generación (ng-eNB) / Nodo B NR (gNB) puede decidir activar la confidencialidad del plano de usuario y/o la protección de la integridad del plano de usuario en cada sesión de las unidades de datos de protocolo (PDU) en función de la política de seguridad del plano de usuario recibida. La política de seguridad del plano de usuario puede configurarse para indicar "Requerida" o "No necesaria". Hay algoritmos de cifrado opcionales [3GPP TS 33.501].
- Nombre de la capacidad: protección de datos del plano de usuario (UPDP).
- Dimensión de seguridad de la capacidad: confidencialidad de datos, integridad de datos.
- Opción de la capacidad:
  – UPDP.0: no activar la confidencialidad del plano de usuario ni/o la protección de la integridad del plano de usuario.
  – UPDP.1: activar la confidencialidad del plano de usuario y/o la protección de la integridad del plano de usuario con algoritmos de cifrado opcionales.

7.2.4 Capacidad de protección de los límites

- Descripción de la capacidad: es importante proteger un segmento de red contra los ataques de red implementando funciones/características de seguridad en el límite, especialmente en el límite de la CN (por ejemplo, configuración de la protección N6 para la interfaz N6) [b-3GPP TS 28.541]. Para los diferentes clientes de segmentos de red, las funciones/características de control de la seguridad podrían ser diferentes y podrían cambiar dinámicamente en función de las necesidades. Las funciones de control de la seguridad pueden ser los cortafuegos, la conversión de dirección de red (NAT), el antimalware, el control parental, la función de protección de la denegación de servicio distribuida, etc. [b-3GPP TS 28.541]. Las características se refieren a las reglas de reenvío, las reglas de

filtrado, la configuración de parámetros, etc. Las necesidades podrían ser el control del acceso a la red de datos y el mecanismo de tunelización.

- Nombre de la capacidad: protección de los límites (BP).
- Dimensión de seguridad de la capacidad: control del acceso, disponibilidad, seguridad de las comunicaciones.
- Opción de la capacidad:
  - BP.0: ausencia de funciones de control de la seguridad.
  - BP.1: funciones/características de control de la seguridad implementadas.

7.2.5 Capacidades de protección de los servicios de aplicaciones

- Descripción de la capacidad: los operadores pueden implementar dispositivos o módulos de seguridad en la red para proporcionar diferentes niveles de protección de la seguridad a los servicios de aplicaciones que utilizan los segmentos y a los usuarios que utilizan los servicios de aplicaciones. Por ejemplo, la red del operador puede proporcionar la detección de anomalías en el terminal, la limpieza del tráfico de red, la detección de localizador uniforme de recursos (URL), cortafuegos de aplicaciones web (WAF), anti-DDoS, etc.
- Nombre de la capacidad: protección de servicios de aplicaciones (ASP)
- Dimensión de seguridad de la capacidad: seguridad de las comunicaciones, control de acceso, disponibilidad.
- Opción de la capacidad:
  - ASP.0: ausencia de protección de los servicios de aplicaciones.
  - ASP.1: implementación de protecciones de los servicios de aplicaciones.

7.2.6 Capacidad de protección de la privacidad del ID del EAP durante la NSSAA

- Descripción de la capacidad: se pueden utilizar múltiples métodos de protocolo de autenticación extensible (EAP) [b-IETF RFC 3748] para la autenticación de segmentos específicos. Se puede elegir un método EAP capaz de proteger la privacidad, por ejemplo, el protocolo EAP de seguridad de la capa de transporte (TLS) [b-IETF RFC 5216] o el EAP-TTLS [b-IETF RFC 5281]) para proteger la privacidad del ID del EAP utilizado para la NSSAA basada en el EAP [3GPP TS 33.501].
- Nombre de la capacidad: protección de la privacidad del ID del EAP durante la NSSAA (PPEAP)
- Dimensión de seguridad de la capacidad: privacidad.
- Opción de la capacidad:
  - PPEAP.0: no utilizar métodos EAP capaces de proteger la privacidad
  - PPEAP.1: utilizar métodos EAP capaces de proteger la privacidad

7.2.7 Capacidad de protección de la privacidad de la información de ayuda para la selección de un (único) segmento de red

- Descripción de la capacidad: la información de ayuda para la selección de un segmento de red (NSSAI) se utiliza para identificar un tipo de segmento/servicio de red. Determinada información sobre la red del operador y los clientes podría obtenerse a partir de la NSSAI y su utilización. La red IMT-2020 proporciona las capacidades para proteger la privacidad de la información de ayuda para la selección de un (único) segmento de red ((S-)NSSAI) al no permitir que se utilice la NSSAI o utilizar información alternativa fuera del dominio del operador. Durante el procedimiento de registro, la función de gestión de acceso y movilidad (AMF) podría proporcionar al equipo del usuario en el mensaje de aceptación del registro, un parámetro sobre el modo de inclusión de la NSSAI en el momento del establecimiento de

la conexión del estrato de acceso, con indicación de si el equipo del usuario debe incluir información NSSAI en el establecimiento de la conexión del estrato de acceso y en qué momento debe hacerlo, según los diferentes modos. Por defecto, el equipo del usuario no proporcionará información NSSAI en el estrato de acceso de 3GPP, a menos que haya sido proporcionada con la indicación de operar en otros modos [b-3GPP TS 23.502]. Durante la autenticación y autorización de determinados segmentos de red (NSSAA), si el servidor AAA utilizado pertenece a un tercero, dado que la S-NSSAI forma parte del núcleo interno IMT-2020, se puede establecer una correspondencia entre la información en la red del operador y la información de un segmento de red exterior (ENSI) que se transmite y utiliza fuera del dominio del operador [3GPP TS 33.501].

- Nombre de la capacidad: protección de la privacidad de la (S-)NSSAI (PPSI)
- Dimensión de seguridad de la capacidad: privacidad.
- Opción de la capacidad:
  - PPSI.0: utilizar la NSSAI fuera del dominio del operador
  - PPSI.1: no utilizar la NSSAI o utilizar información alternativa fuera del dominio del operador.

7.3 Clasificación de las capacidades de seguridad de los segmentos IMT-2020

Las capacidades de seguridad de los segmentos IMT-2020 pueden clasificarse según su dimensión de seguridad, como se indica en el Cuadro 7-1.

Cuadro 7-1 – Clasificación de las capacidades de seguridad de los segmentos IMT-2020 según la dimensión de seguridad

Dimensión de seguridad **Capacidad de seguridad del segmento**	**Autenticación y autorización de determinados segmentos de red (NSSAA)**	**Aisla-miento de segmentos para los recursos (SIR)**	**Protección de datos del plano de usuario (UPDP)**	**Protección de los límites (BP)**	**Protección de los servicios de aplica-ciones (ASP)**	**Protección de la privacidad del ID del EAP durante la NSSAA (PPEAP)**	**Protección de la privacidad de la (S-) NSSAI (PPSI)**
Control del acceso	√	√		√	√		
Autenticación	√						
No repudio							
Confidencialidad de datos			√				
Seguridad de la comunicación				√	√		
Integridad de los datos			√				
Disponibilidad		√		√	√		
Privacidad		√				√	√

8 Clasificación para las dimensiones de seguridad logradas por las capacidades de seguridad de los segmentos

8.1 Método y principio de clasificación de las dimensiones de seguridad en función de las capacidades de seguridad de los segmentos

El método para clasificar cada dimensión de seguridad es el siguiente:

1) Se recomienda enumerar las capacidades de seguridad y las opciones conexas pertenecientes a la dimensión de seguridad. Si hay una ligera posibilidad de que una capacidad de seguridad afecte a alguna dimensión de seguridad, dicha capacidad de seguridad puede opcionalmente

no enumerarse en la dimensión de seguridad e incluirse únicamente en las demás dimensiones de seguridad principalmente afectadas.

2) Se recomienda enumerar la combinación de diferentes opciones de las capacidades y formar los diferentes niveles de la dimensión de seguridad. Si múltiples capacidades de seguridad logran una dimensión de seguridad, cada nivel de protección debe mantenerse en coherencia para múltiples ámbitos o partes interesadas cuando se combinen las opciones de las capacidades de seguridad. El xx.nn (por ej., AC.1, …, DI.0) hace referencia al nombre del nivel de la dimensión de seguridad xx.

En la cláusula 8.2 se ofrece la lista genérica de las ocho dimensiones de seguridad con niveles basados en las capacidades de seguridad y las opciones que figuran en la cláusula 7.

8.2 Dimensiones de seguridad con niveles basados en las capacidades de seguridad de los segmentos IMT-2020

8.2.1 Control del acceso basado en las capacidades de seguridad de los segmentos IMT-2020

El control del acceso puede ser conseguido por capacidades con opciones, por ejemplo: la autenticación y autorización de determinados segmentos de red, el aislamiento de recursos de red en segmentos, la protección de límites y la protección de servicios de aplicaciones. Existen diversas combinaciones de capacidades con distintas opciones para conseguir diferentes niveles de control del acceso. Esto se muestra a continuación sobre la base de la cláusula 7.

Cuadro 8-1 – Niveles de control del acceso

Dimensión de seguridad: Control del acceso (AC)															
Capacidad	**Autenticación y autorización de determinados segmentos de red (NSSAA)**		**Protección de los servicios de aplicaciones (ASP)**		**Aislamiento de segmentos para los recursos (SIR)**							**Protección de los límites (BP)**		**Nombre del nivel**
Opciones	**NSSAA.0**	**NSSAA.1**	**ASP.0**	**ASP.1**	**SIR.0**	**SIR.1**	**SIR.2**	**SIR.3**	**SIR.4**	**SIR.5**	**SIR.6**	**BP.0**	**BP.1**	
Combinación	NSSAA.0		ASP.0		SIR.0							BP.0		AC.0000
					SIR.0							BP.1		AC.0001
					SIR.1 SIR.4							BP.0		AC.0010 AC.0040
					SIR.1 SIR.4							BP.1		AC.0011 AC.0041
					SIR.2 SIR.5							BP.0		AC.0020 AC.0050
					SIR.2 SIR.5							BP.1		AC.0021 AC.0051
					SIR.3 SIR.6							BP.1		AC.0031 AC.0061
			ASP.1		SIR.0							BP.0		AC.0100
					SIR.0							BP.1		AC.0101
					SIR.1 SIR.4							BP.0		AC.0110 AC.0140

Cuadro 8-1 – Niveles de control del acceso

Dimensión de seguridad: Control del acceso (AC)																
Capacidad	**Autenticación y autorización de determinados segmentos de red (NSSAA)**		**Protección de los servicios de aplicaciones (ASP)**		**Aislamiento de segmentos para los recursos (SIR)**							**Protección de los límites (BP)**		**Nombre del nivel**
Opciones	**NSSAA.0**	**NSSAA.1**	**ASP.0**	**ASP.1**	**SIR.0**	**SIR.1**	**SIR.2**	**SIR.3**	**SIR.4**	**SIR.5**	**SIR.6**	**BP.0**	**BP.1**	
					SIR.1 SIR.4							BP.1		AC.0111 AC.0141
					SIR.2 SIR.5							BP.0		AC.0120 AC.0150
					SIR.2 SIR.5							BP.1		AC.0121 AC.0151
					SIR.3 SIR.6							BP.1		AC.0131 AC.0161
	NSSAA.1		ASP.0		SIR.0							BP.0		AC.1000
					SIR.0							BP.1		AC.1001
					SIR.1 SIR.4							BP.0		AC.1010 AC.1040
					SIR.1 SIR.4							BP.1		AC.1011 AC.1041
					SIR.2 SIR.5							BP.0		AC.1020 AC.1050
					SIR.2 SIR.5							BP.1		AC.1021 AC.1051
					SIR.3 SIR.6							BP.1		AC.1031 AC.1061
			ASP.1		SIR.0							BP.0		AC.1100
					SIR.0							BP.1		AC.1101
					SIR.1 SIR.4							BP.0		AC.1110 AC.1140
					SIR.1 SIR.4							BP.1		AC.1111 AC.1141
					SIR.2 SIR.5							BP.0		AC.1120 AC.1150
					SIR.2 SIR.5							BP.1		AC.1121 AC.1151
					SIR.3 SIR.6							BP.1		AC.1131 AC.1161

8.2.2 Autenticación basada en las capacidades de seguridad de los segmentos IMT-2020

La autenticación puede ser conseguida por capacidades como la autenticación y autorización de determinados segmentos de red. Hay dos niveles de autenticación. Se muestran a continuación:

Cuadro 8-2 – Niveles de autenticación

Dimensión de seguridad: Autenticación (Au)			
Capacidad	**Autenticación y autorización de determinados segmentos de red (NSSAA)**		**Nombre del nivel**
Opciones	**NSSAA.0**	**NSSAA.1**	
Combinación	NSSAA.0		Au.0
	NSSAA.1		Au.1

8.2.3 No repudio basado en las capacidades de seguridad de los segmentos IMT-2020

Ninguna capacidad establecida en la cláusula 7 consigue el no repudio.

8.2.4 Confidencialidad de datos basada en las capacidades de seguridad de los segmentos IMT-2020

La confidencialidad de datos puede ser conseguida por capacidades como la protección de datos del plano de usuario. Hay dos niveles de autenticación. Se muestran a continuación:

Cuadro 8-3 – Niveles de confidencialidad de datos

Dimensión de seguridad: Confidencialidad de datos (DC)			
Capacidad	**Protección de datos del plano de usuario (UPDP)**		**Nombre del nivel**
Opciones	**UPDP.0**	**UPDP.1**	
Combinación	UPDP.0		DC.0
	UPDP.1		DC.1

8.2.5 Seguridad de la comunicación basada en las capacidades de seguridad de los segmentos IMT-2020

La seguridad de la comunicación puede ser conseguida por capacidades como la protección de los límites y la protección de los servicios de aplicaciones. Existen diversas combinaciones de capacidades con distintas opciones para conseguir diferentes niveles de seguridad de la comunicación. Se muestran a continuación:

Cuadro 8-4 – Niveles de seguridad de la comunicación

Dimensión de seguridad: Seguridad de la comunicación (CS)					
Capacidades	**Protección de los límites (BP)**		**Protección de los servicios de aplicaciones (ASP)**		**Nombre del nivel**
Opciones	**BP.0**	**BP.1**	**ASP.0**	**ASP.1**	
Combinaciones	BP.0		ASP.0		CS.00
	BP.0		ASP.1		CS.01
	BP.1		ASP.0		CS.10
	BP.1		ASP.1		CS.11

8.2.6 Integridad de datos basada en las capacidades de seguridad de los segmentos IMT-2020

La integridad de los datos puede ser conseguida por capacidades como la protección de datos del plano de usuario. Hay dos niveles de integridad de los datos. Se muestran a continuación:

Cuadro 8-5 – Niveles de integridad de datos

Dimensión de seguridad: Integridad de datos (DI)			
Capacidad	**Protección de datos del plano de usuario (UPDP)**		**Nombre del nivel**
Opciones	**UPDP.0**	**UPDP.1**	
Combinación	UPDP.0		DI.0
	UPDP.1		DI.1

8.2.7 Disponibilidad basada en las capacidades de seguridad de los segmentos IMT-2020

La disponibilidad puede ser conseguida por capacidades como el aislamiento de segmentos para los recursos de red, la protección de los límites y la protección de los servicios de aplicaciones. Existen diversas combinaciones de capacidades con distintas opciones para conseguir diferentes niveles de disponibilidad. Se muestran a continuación:

Cuadro 8-6 – Niveles de disponibilidad

Dimensión de seguridad: Disponibilidad (Av)							
Capacidad	**Protección de los servicios de aplicaciones (ASP)**		**Aislamiento de segmentos para los recursos (SIR)**		**Protección de los límites (BP)**		**Nombre del nivel**
Opciones	**ASP.0**	**ASP.1**	**SIR.1/SIR.2/SIR.3**	**SIR.4/SIR.5/SIR.6**	**BP.0**	**BP.1**	
Combinación	ASP.0		SIR.1/SIR.2/SIR.3		BP.0		Av.000
					BP.1		Av.001
			SIR.4/SIR.5/SIR.6		BP.0		Av.010
					BP.1		Av.011
	ASP.1		SIR.1/SIR.2/SIR.3		BP.0		Av.100
					BP.1		Av.101
			SIR.4/SIR.5/SIR.6		BP.0		Av.110
					BP.1		Av.111

8.2.8 Privacidad basada en las capacidades de seguridad de los segmentos IMT-2020

La privacidad puede ser conseguida por capacidades como la protección de la privacidad del ID del EAP durante la NSSAA y la protección de la privacidad de la (S-)NSSAI. Existen diversas combinaciones de capacidades con distintas opciones para conseguir diferentes niveles de privacidad. Se muestran a continuación:

Cuadro 8-7 – Niveles de privacidad

Dimensión de seguridad: privacidad (Pr)					
Capacidades	**Protección de la privacidad del ID del EAP durante la NSSAA (PPEAP)**		**Protección de la privacidad de la (S-)NSSAI (PPSI)**		**Nombre del nivel**
Opciones	**PPEAP.0**	**PPEAP.1**	**PPSI.0**	**PPSI.1**	
Combinaciones	PPEAP.0		PPSI.0		Pr.00
	PPEAP.0		PPSI.1		Pr.01
	PPEAP.1		PPSI.0		Pr.10
	PPEAP.1		PPSI.1		Pr.11

9 Directrices y requisitos para los tipos de seguridad de segmentos

Un conjunto de dimensiones de seguridad puede caracterizar a un tipo de seguridad del segmento de red y puede diferenciarse por una categoría de servicio. Habrá muchas clases de tipos de seguridad de segmentos a raíz de la combinación de las dimensiones de seguridad con diferentes niveles. Sin embargo, no todas las combinaciones son razonables.

El método y el principio para formar los tipos de seguridad de segmentos son:

1) Se recomienda determinar los niveles de las dimensiones de seguridad con mayor prioridad en primer lugar según los requisitos de servicio y la calidad de funcionamiento de todos los niveles.
2) Se recomienda determinar los niveles de las demás dimensiones de seguridad según los requisitos de servicio y la calidad de funcionamiento de los niveles.
3) Se recomienda comprobar si hay un conflicto entre cada dimensión de seguridad a efectos de coordinación. En un segmento, para diferentes dimensiones de seguridad con la misma capacidad de seguridad, las opciones de la capacidad de seguridad deben ser coherentes.
4) Cuando la opción de algunas capacidades o el nivel de algunas dimensiones de seguridad se actualizan para un tipo de seguridad del segmento, se recomienda cambiar las capacidades conexas y la dimensión de seguridad para mantener la coherencia.

10 Directrices y requisitos para las partes interesadas en relación con la clasificación de las capacidades de seguridad de los segmentos de red

Se recomienda que los operadores de segmentos preparen su propia lista de capacidades de seguridad de segmentos sobre la base de la lista de capacidades de seguridad de segmentos que figura en la cláusula 7 y sus capacidades de seguridad privadas.

Se recomienda que los operadores de segmentos preparen su propia lista de dimensiones de seguridad con niveles sobre la base de la lista genérica de dimensiones de seguridad con niveles y sus capacidades de seguridad privadas u otras dimensiones con arreglo al método indicado en la cláusula 8.

Se recomienda que los operadores de segmentos preparen su propia lista de tipos de seguridad de segmentos según el método indicado en la cláusula 9.

Se recomienda que los operadores de segmentos decidan sobre las capacidades de seguridad y las opciones para una instancia de segmento (por ejemplo, durante el suministro [b-ETSI TS 128 531]) sobre la base de su lista de capacidades de seguridad o su lista de dimensiones de seguridad con

niveles o sus listas de tipos de seguridad de segmentos estableciendo la correspondencia con los niveles de las dimensiones de seguridad o los tipos de seguridad de los segmentos.

Se recomienda que los clientes de segmentos elijan combinaciones de capacidades de seguridad y opciones de la lista genérica de capacidades de seguridad de los segmentos o de la lista de capacidades de seguridad de los segmentos del operador si desean conocer exactamente sus requisitos de seguridad y las correspondientes capacidades de seguridad.

Se recomienda que los clientes de segmentos elijan niveles de las dimensiones de seguridad conexas según la calidad de funcionamiento de los niveles a partir de la lista genérica de dimensiones de seguridad con niveles o de la lista de dimensiones de seguridad del operador, si desean conocer el efecto de alguna dimensión de seguridad que desean conseguir.

Se recomienda que los clientes de segmentos elijan un tipo a partir de la lista de tipos de seguridad de segmentos del operador, si apenas conocen el contenido de seguridad detallado.

Apéndice I

Calidad de funcionamiento de las opciones relativas a las capacidades de seguridad de los segmentos de red IMT-2020

(Este apéndice no forma parte integrante de esta Recomendación.)

NOTA – La calidad de funcionamiento depende de detalles específicos de la implementación y puede variar con el avance de la tecnología.

- Calidad de funcionamiento de las opciones relativas a la NSSAA:
  - NSSAA.0: nivel básico.
  - NSSAA.1: mayor autonomía (para la industria vertical).
- Calidad de funcionamiento de las opciones relativas al SIR:
  - SIR.0: ausencia de aislamiento: nivel básico.
  - SIR.1: aislamiento lógico + compartición de RB: SIR.1 es más flexible y puede implicar menos costes que SIR.2 y SIR.3.
  - SIR.2: aislamiento lógico y físico + compartición de RB: SIR.2 es más flexible y puede implicar menos costes que SIR.3. SIR.2 ofrece más fiabilidad que SIR.1.
  - SIR.3: aislamiento físico + compartición de RB: SIR.3 ofrece más fiabilidad e implica mayores costes de recursos que SIR.1 y SIR.2.
  - SIR.4: aislamiento lógico + reserva de RB: SIR.4 es más flexible y puede implicar menos costes que SIR.5 y SIR.6.
  - SIR.5: aislamiento lógico y físico + reserva de RB: SIR.5 es más flexible y puede implicar menos costes que SIR.6. SIR.5 ofrece más fiabilidad que SIR.4.
  - SIR.6: aislamiento físico + reserva de RB: SIR.6 ofrece menor latencia, mayor fiabilidad e implica mayores costes que las demás opciones.

Es posible que las opciones con aislamiento lógico impliquen menos costes en recursos del servidor que las opciones con aislamiento físico, mientras que las primeras tal vez necesiten gastar más en contramedidas de seguridad que las segundas para conseguir un efecto de protección similar.

Las opciones con aislamiento físico pueden conseguir un mayor nivel de control del acceso que las opciones con aislamiento lógico.

Las opciones con compartición de RB resultan mejores y más flexibles respecto del efecto de cobertura y la utilización de recursos que las opciones con reserva de RB.

- Calidad de funcionamiento de las opciones relativas a la UPDP:
  - UPDP.0: no hay protección de datos en la interfaz aérea y la latencia es menor que con la opción UPDP.1
  - UPDP.1: hay protección de datos en la interfaz aérea con diferentes efectos de protección en función de los algoritmos de cifrado opcionales.
- Calidad de funcionamiento de las opciones relativas a la BP:
  - BP.0: nivel básico
  - BP.1: hay protección de los límites con diferentes efectos de protección en función de las funciones/características de control de seguridad opcionales que se hayan instalado.
- Calidad de funcionamiento de las opciones relativas a la ASP:
  - ASP.0: nivel básico

  - ASP.1: hay una protección de servicios de aplicaciones con diferentes efectos de protección en función de las protecciones opcionales de servicios de aplicaciones.
- Calidad de funcionamiento de las opciones relativas a la PPEAP:
  - PPEAP.0: se expone la identidad del UE
  - PPEAP.1: la identidad del UE es anónima
- Calidad de funcionamiento de las opciones relativas a la PPSI:
  - PPSI.0: se expone la (S-)NSSAI
  - PPSI.1: la (S-)NSSAI no se muestra

Apéndice II

Ejemplo de tipos básicos de seguridad de los segmentos IMT-2020

(Este apéndice no forma parte integrante de esta Recomendación.)

El siguiente cuadro relativo a los tipos básicos de seguridad de los segmentos se ha elaborado sobre la base del método establecido en la cláusula 9, que las partes interesadas pueden utilizar directamente o adaptarlo para elaborar sus propios tipos básicos de seguridad de los segmentos.

Cuadro II.1 – Ejemplos de tipos básicos de seguridad de los segmentos

Tipo de seguridad de los segmentos	Control del acceso	Autenti-cación	Disponi-bilidad	Seguridad de la comunicación	Confiden-cialidad de datos	Integridad de los datos	No repudio	Privacidad	Opinión	Servicios adecuados
0	AC.0	Au.0	Av.0	CS.0	DC.0	DI.0	–	Pr.0	Seguridad básica	Red pública
1	AC.1161	Au.1	Av.111	CS.11	DC.1	DI.1	–	Pr.11	Alta seguridad, mayores costes	Tipos que requieran un alto nivel de seguridad, como las líneas privadas para clientes de los gobiernos, las finanzas, los valores y el suministro eléctrico.
2	AC.0000	Autor.0	Av.0	CS.0	–	–	–	–	Coste bajo	Tipos de servicios de coste bajo, acceso a Internet y vídeo OTT
3	AC.xx61	–	Av.x11	–	–	–	–	Pr.xx4 Pr.xx6	Alto nivel de aislamiento, coste alto	Tipos de servicios que requieren alto nivel de aislamiento
4	–	–	Av.x1x	–	DC.0	DI.0	–	–	Baja latencia	Tipos de servicios que requieren baja latencia, como los juegos en la nube

NOTA – en el número de serie del nombre del nivel, x se refiere a cualquier valor.

Bibliografía

[b-UIT-T Y.3100] Recomendación UIT-T Y.3100 (2017), *Condiciones y definiciones relativas a las redes IMT-2020.*

[b-3GPP TS 23.502] 3GPP TS 23.502, *Procedimientos para el Sistema 5G (5GS).* <https://www.3gpp.org/ftp/Specs/archive/23_series/23.502>

[b-3GPP TS 28.541] 3GPP TS 28.541, *Gestión y orquestación; Modelo de recursos de la red 5G (NRM); etapas 2 y 3.* <https://www.3gpp.org/ftp/Specs/archive/28_series/28.541>

[b-IETF RFC 3748] IETF RFC 3748, *Protocolo de autenticación extensible (EAP).* <https://tools.ietf.org/html/rfc3748>

[b-IETF RFC 5216] IETF RFC 5216, *El protocolo de autenticación EAP-TLS.* <https://www.rfc-editor.org/rfc/rfc5216.html>

[b-IETF RFC 5281] IETF RFC 5281, *Versión 0 del protocolo de seguridad autenticado de la capa de transporte tunelizada a través del protocolo de autenticación extensible (EAP-TTLSv0).* <https://datatracker.ietf.org/doc/html/rfc5281>

[b-ETSI TS 128 530] Especificación técnica ETSI TS 128 530 V17.1.0 (2022), *5G; Gestión y orquestación; Conceptos, casos de uso y requisitos* (3GPP TS 28.530 versión 17.2.0 Edición 17). <https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/17.02.00_60/ts_128530v170200p.pdf>

[b-ETSI TS 128 531] Especificación técnica ETSI TS 128 531 V16.9.0 (2021), *5G; Gestión y orquestación; aprovisionamiento;* (3GPP TS 28.531 versión 16.6.0 Edición 16). <https://www.etsi.org/deliver/etsi_ts/128500_128599/128531/16.06.00_60/ts_128531v160600p.pdf>

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, 2023