Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1812

(05/2022)

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

Marco de seguridad basado en las relaciones de confianza para el ecosistema IMT-2020

Recomendación UIT-T X.1812

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 de 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.1319
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 de 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 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.1812

Marco de seguridad basado en las relaciones de confianza para el ecosistema IMT-2020

Resumen

En la Recomendación UIT-T X.1812 se identifican las partes interesadas en el ecosistema de las Telecomunicaciones Móviles Internacionales 2020 (IMT-2020; también conocidas como la quinta generación), se analizan las relaciones de confianza entre ellas, se identifican las amenazas y se aclaran las responsabilidades en materia de seguridad de cada parte interesada, se especifican las fronteras de seguridad entre las partes, y se establece un marco de seguridad basado en las relaciones de confianza.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1812	2022-05-20	17	11.1002/1000/14808

Palabras clave

Confianza, ecosistema, IMT-2020, marco.

* 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 http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

El conjunto de partes interesadas en el sistema de las Telecomunicaciones Móviles Internacionales 2020 (IMT-2020; también denominado de quinta generación (5G)) es más amplio y variado que el de los anteriores sistemas de comunicación. En las generaciones segunda, tercera y cuarta (2G, 3G y 4G) puede decirse que las principales partes interesadas son los proveedores de servicios, los operadores de red, los fabricantes de equipos y los abonados. Sin embargo, en el ecosistema IMT-2020 también participan agentes verticales, como las empresas industriales y comerciales. Además, los proveedores de servicios pueden subdividirse en operadores de plataformas en la nube, empresas de análisis de datos, proveedores de aplicación, etc. Por otra parte, en el extremo terminal, los abonados no son solo los usuarios finales como ocurría anteriormente. Dentro de la categoría de abonados pueden incluirse diversas partes interesadas, en particular cuando se trata de terminales comerciales, por ejemplo, en el caso de la comunicación vehicular compartida. Estas diferencias dan lugar a relaciones complejas entre las distintas partes y plantean una serie de nuevos problemas de seguridad para los ecosistemas IMT-2020.

La red IMT-2020 ofrece además nuevas funcionalidades. Por ejemplo, la introducción de la virtualización de red en las IMT-2020 rompe las conexiones fijas entre entidades de red y permite las redes definidas por software. Otro ejemplo es la arquitectura de servicio, que permite la integración en una red IMT-2020 de más funcionalidades relacionadas con la nube. Asimismo, la segmentación puede facilitar una cooperación más efectiva entre la red IMT-2020 y los servicios.

Con el tiempo cada vez se aplicarán más técnicas de tecnología de la información (TI) a los sistemas IMT-2020, no solo sus servicios sino también su red. La red IMT-2020 se basa íntegramente en el protocolo Internet. La especificación de su arquitectura se basa en servicios en lugar de puntos de referencia, como ocurría con las anteriores arquitecturas de red. Con cada vez más frecuencia las señales se transfieren de Internet, en lugar de las redes dedicadas. El protocolo de transporte de las redes IMT-2020 ya no es Diameter [b-IETF RFC 6733], menos popular que el protocolo de transporte de hipertexto, que se utiliza ampliamente en todo el mundo. Todos estos cambios serán benéficos para el despliegue y el funcionamiento de redes y servicios IMT-2020.

Sin embargo, la utilización de protocolos populares y la apertura del entorno de conexión también pueden facilitar los ataques. Un atacante no tendrá que pasar mucho tiempo estudiando complejos protocolos de comunicación y posiblemente le sea más fácil encontrar un punto de intrusión en la red. Por consiguiente, en las redes IMT-2020 no es razonable asumir que la comunicación interna sigue siendo fiable. Así, la transición de la 4G a IMT-2020 rompe la relación de confianza entre operadores de red.

Además, la red IMT-2020 está diseñada para ser más flexible a fin de cumplir requisitos de servicio diversos. Concretamente, en las redes IMT-2020 se ha introducido la segmentación. Las redes IMT-2020 pueden además exponer algunas capacidades a los servicios; y dicha exposición permitirá a un servicio IMT-2020 controlar algunas de las funciones de red. Estas nuevas características difuminarán la frontera de seguridad entre la red IMT-2020 y los servicios.

En esta Recomendación se identifican las partes interesadas en un ecosistema IMT-2020, se analizan las relaciones de confianza entre ellas, se identifican las amenazas y se aclaran las responsabilidades en materia de seguridad de cada parte interesada, se especifican las fronteras de seguridad entre las partes, y se establece un marco de seguridad basado en dichas relaciones de confianza.

Recomendación UIT-T X.1812

Marco de seguridad basado en las relaciones de confianza para el ecosistema IMT-2020

1 Alcance

En esta Recomendación se especifica un marco de seguridad basado en las relaciones de confianza para un ecosistema de Telecomunicaciones Móviles Internacionales 2020 (IMT-2020). Se describe un enfoque general para lo siguiente:

– identificación de hipótesis de prestación de servicios IMT-2020;

– identificación de partes interesadas en un ecosistema IMT-2020;

– análisis de las relaciones de confianza entre partes interesadas;

– identificación de las amenazas que se pueden plantear a cada parte interesada;

– aclaración de las responsabilidades de seguridad de cada parte interesada;

– especificación de las fronteras de seguridad entre las partes;

– especificación de los requisitos de seguridad sobre la base del modelo de confianza; y

– establecimiento de un marco de seguridad basado en las relaciones de confianza entre las partes interesadas.

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 demás referencias están sujetas a revisión; por consiguiente, 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.

Ninguna.

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 unidad comercial [b-ISO/TS 21089]: Función o subfunción discreta y responsable dentro de una organización.

NOTA – Una unidad comercial puede ser un departamento, servicio o especialidad de una organización que presta servicios de atención sanitaria.

3.1.2 despliegue [b-ISO/CEI/IEEE 24765]: Fase de un proyecto en la que el sistema se pone en marcha y se resuelven los problemas de la transición.

3.1.3 creador [b-NIST SP 800-53]: Entidad que comprende: i) creadores o fabricantes de sistemas de información, componentes de sistemas o servicios de sistemas de información; ii) integradores de sistemas; iii) distribuidores; y iv) vendedores de productos.

3.1.4 dominio [b-ISO/CEI 14888-1]: Conjunto de entidades que opera en el marco de una política de seguridad única.

EJEMPLO – Certificados de clave pública creados por una única autoridad o por un conjunto de autoridades que utilizan la misma política de seguridad.

3.1.5 sistema de información [b-ISO/CEI 27000]: Conjunto de aplicaciones, servicios, bienes de tecnología de la información u otros componentes de tratamiento de la información.

3.1.6 vida útil [b-ISO/CEI/IEEE 15288]: Evolución de un sistema, producto, servicio, proyecto u otra entidad artificial desde su concepción hasta su eliminación.

3.1.7 función de red [b-UIT-T Y.3100]: En el contexto de las IMT-2020 una función de procesamiento en una red.

NOTA 1 – Las funciones de red pueden incluir, entre otras, las funcionalidades de nodo de red, por ejemplo, gestión de sesión, gestión de movilidad y funciones de transporte, cuyo comportamiento funcional e interfaces están definidos.

NOTA 2 – Las funciones de red pueden implementarse en un hardware dedicado o como funciones de software virtualizadas.

NOTA 3 – Las funciones de red no se consideran recursos, sino que cualquier función de red puede instanciarse utilizando los recursos.

3.1.8 parte interesada [b-ISO/PAS 19450]: Persona, organización o grupo de personas interesados en el sistema considerado, creado o desplegado, o que puede verse afectado por él.

3.1.9 proveedor [b-ISO 10393]: Organización o persona que ofrece un producto o servicio.

3.1.10 desarrollo de sistemas [b-ISO/CEI 2382]: Proceso que suele incluir el análisis de requisitos, el diseño de sistemas, la implementación, la documentación y la garantía de calidad.

3.1.11 confianza [b-ISO/CEI 25010]: Grado en que un usuario u otra parte interesada confía en que un producto o sistema se comportará como está previsto.

3.1.12 nivel de confianza [b-ISO 28598-1]: Estimación que realiza el cliente a partir de pruebas históricas, suplementarias e indirectas de la capacidad del proveedor para cumplir los requisitos de calidad especificados.

3.2 Términos definidos en la presente Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 proveedor de servicio externo: Conjunto de entidades que comprende: a) las entidades pertenecientes a la organización, pero que están fuera de las fronteras de autorización de seguridad establecidas para los sistemas de información de la organización; b) las entidades externas a la organización, ya sean del sector público (por ejemplo, agencias federales) o del sector privado (por ejemplo, proveedores de servicio comerciales); o c) una combinación de entidades del sector público y el sector privado.

NOTA – Adaptado de [b-NIST SP 800-53].

3.2.2 cadena de producción: Red de organizaciones implicadas mediante vínculos verticales en los procesos y actividades que generan valor en forma de productos y servicios en manos del consumidor extremo.

3.2.3 ciclo de desarrollo de sistemas: Enfoque estructurado de planificación, creación, pruebas, despliegue y mantenimiento de un sistema de información.

3.2.4 modelo de confianza: Modelo formado por los componentes que describen las relaciones de confianza y las cadenas entre partes interesadas.

4 Abreviaturas y acrónimos

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

2G Segunda generación

3G Tercera generación

4G Cuarta generación

5G Quinta generación

5GC Quinta generación principal

CAB Órgano de evaluación de la conformidad (*Conformity Assessment Body*)

E2E Extremo a extremo (*End to End*)

EB Estación de base

HO Operador propio (*Home Operator*)

IIP Información de identificación personal

IMT-2020 Telecomunicaciones móviles internacionales-2020 (*International Mobile Telecommunications-2020*)

IoT Internet de las cosas (*Internet of Things*)

IoV Internet de los vehículos (*Internet of Vehicles*)

IPX Intercambio de paquetes entre redes (*Internetwork Packet Exchange*)

NE Elemento de red (*Network Element*)

NESAS Esquema de garantía de seguridad de equipos de red (*Network Equipment Security Assurance Scheme*)

NF Función de red (*Network Function*)

NFV Virtualización de la función de red (*Network Function Virtualization*)

NPN Red no pública (*Non-Public Network*)

PCI Proveedor de contenidos de Internet

PSI Proveedor de servicios de Internet

RPMT Red pública móvil terrestre

SCAS Especificación de garantía de seguridad (*Security Assurance Specification*)

SDL Ciclo de desarrollo de seguridad (*Security Development Lifecycle*)

TI Tecnología de la información

TIC Tecnología de la información y la comunicación

UICC Tarjeta de circuito integrado universal (*Universal Integrated Circuit Card*)

VNF Función de red virtualizada (*Virtualized Network Function*)

VO Operador visitado (*Visited Operator*)

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. Su cumplimiento no es indispensable para poder declarar la conformidad.

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

6 Generalidades

Antes de la era 5G, los sistemas de telecomunicaciones se utilizaban principalmente para ofrecer servicios de telefonía, acceso a Internet y servicios conexos. Dadas las capacidades y limitaciones de velocidad de estos sistemas, las hipótesis de uso eran, por lo general, sencillas. Concretamente, en un sistema de comunicación solo participaba un pequeño número de funciones. Para un servicio de llamada, los actores implicados eran el llamante, el llamado y la red móvil. Para un servicio de datos, los actores eran el terminal, la red móvil y los proveedores de servicios o aplicaciones. Además, los distribuidores participaban para sustentar la creación de redes y sistemas de aplicación. En el terminal intervenían los fabricantes de terminales y los proveedores de tarjetas de circuito integrado universales (UICC). Estas eran las principales funciones implicadas en los sistemas de telecomunicaciones 2G, 3G y 4G.

Sin embargo, en el ecosistema IMT-2020 las cosas son diferentes. En este ecosistema participan no solo todas las partes interesadas del sistema de telecomunicaciones, desde el terminal hasta el servicio, pasando por la red, sino también otras partes interesadas. En el lado terminal los abonados no son los únicos usuarios finales, como ocurría antes, porque el dispositivo móvil puede ser uno de los muchos tipos de equipos distintos que pueden compartirse entre múltiples partes y no simplemente un teléfono. En la red, las IMT-2020 introducen toda una gama de nuevas funcionalidades. Por ejemplo, la virtualización de la red en las IMT-2020 pone fin a la conexión fija entre entidades de red y permite las redes definidas por software, que rompen la frontera de seguridad del despliegue de red. Además, los atacantes pueden utilizar cada vez más técnicas de la tecnología de la información (TI) aplicadas en las redes IMT-2020. El servicio de exposición de red abre al atacante interfaces en el plano de control en lugar de en el plano de usuario. En los servicios también intervienen agentes verticales, como las empresas industriales y comerciales. Esto divide a los proveedores de servicio en operadores de plataformas de red, empresas de análisis de datos, proveedores de aplicación, etc., como se ilustra en la Figura 1.

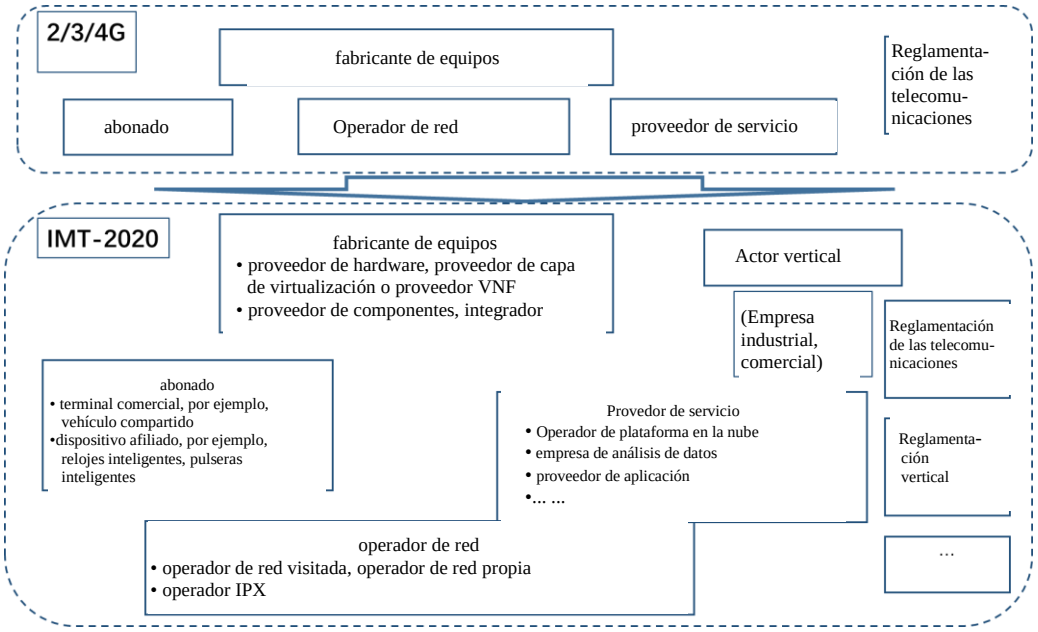


Figura 1 – Evolución del ecosistema de la 2G, 3G y 4G a las IMT-2020

En este caso, la relación de confianza del sistema IMT-2020 es diferente. Los usuarios o abonados y los sistemas de redes o servicios son mucho más cercanos que antes. La compleja y larga cadena de producción obliga a los operadores a tener más en cuenta la evaluación de los proveedores. La estrecha relación entre los servicios y las redes hace que las industrias verticales dependan mucho de las redes y exige mayores niveles de confianza y seguridad. El suministro de un nuevo modelo de confianza para el ecosistema IMT-2020 debe examinarse, a fin de formular un requisito de seguridad claro y una frontera de seguridad inequívoca entre las partes interesadas. De esta manera se puede mejorar la eficacia de la comunicación, tanto como sea posible, con la garantía de la seguridad de los datos.

Hay cinco propiedades, a saber, la resiliencia, la seguridad de la comunicación, la gestión de identidades, la protección de la información de identificación personal (IIP) y la garantía de seguridad, que afectan a la fiabilidad de un sistema IMT-2020.

- Resiliencia: La resiliencia es la capacidad de resistencia de una organización a verse afectada por interrupciones. Hay muy diversas características complementarias y parcialmente duplicadas de las IMT-2020 que pueden contribuir a lograr la resiliencia de un sistema IMT-2020 a ciberataques y otros incidentes benignos.
- Seguridad de la comunicación: La seguridad de la comunicación se aplica a la comunicación de datos en las IMT-2020. En un sistema IMT-2020 es fundamental para los dispositivos y para la propia infraestructura que las comunicaciones sean seguras.
- Gestión de identidades: Un sistema de gestión de identidades consiste en los procesos y políticas necesarios para gestionar la vida útil, el valor, el tipo y los metadatos optativos de los atributos que conforman las identidades de las entidades de un sistema IMT-2020. Se recomienda el suministro de la gestión de identidades de manera segura para identificar y autentificar a los abonados, se esté o no en itinerancia, y garantizar que solo los abonados genuinos puedan acceder a los servicios de red. Esos sistemas se basan en primitivas criptográficas y características de seguridad sólidas.
- Protección de la IIP: La privacidad de los datos se define en [b-ISO/TS 21719-2] como los derechos y obligaciones de los particulares y organizaciones con respecto a la obtención,

utilización, conservación, divulgación y eliminación de información personal. La protección de la IIP consiste en proteger la IIP que partes no autorizadas pueden utilizar para identificar a los abonados.

- Garantía de seguridad: La garantía de seguridad sirve de base para justificar la confianza en la afirmación de que se cumplen o van a cumplir los objetivos de seguridad. La garantía de seguridad es un medio de asegurar que un equipo de red cumple los requisitos de seguridad y que ello se consigue adoptando procesos de desarrollo y de vida útil del producto seguros.

7 Marco de seguridad soportado por el modelo de confianza

En esta Recomendación se analizan y determinan las funciones de las partes interesadas en el ecosistema IMT-2020 y las relaciones de confianza entre funciones, examinando varios casos típicos. A continuación, se procura determinar el nivel de confianza con los factores clave que han de considerarse. Sobre esta base, se dan recomendaciones sobre cómo determinar los requisitos de seguridad basados en el nivel de confianza, y elaborar un marco de seguridad basado en relaciones de confianza, como se ilustra en la Figura 2.

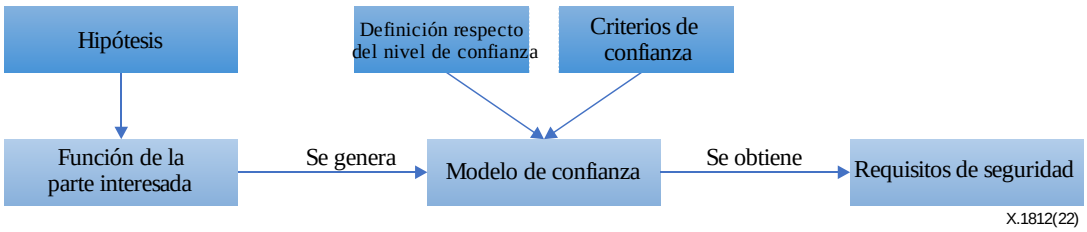


Figura 2 – Metodología para construir un marco de seguridad basado en relaciones de confianza para el ecosistema IMT-2020

Sobre la base de las funciones y relaciones, el modelo de confianza y los requisitos de seguridad de todas las partes interesadas, en la Figura 3 se ilustra un marco de seguridad soportado por el modelo de confianza establecido en la presente Recomendación. Todos los componentes del marco se describen en: la cláusula 8, en relación con las funciones de las partes interesadas; la cláusula 9, en relación con el modelo de confianza; y la cláusula 10, en relación con los requisitos de seguridad.

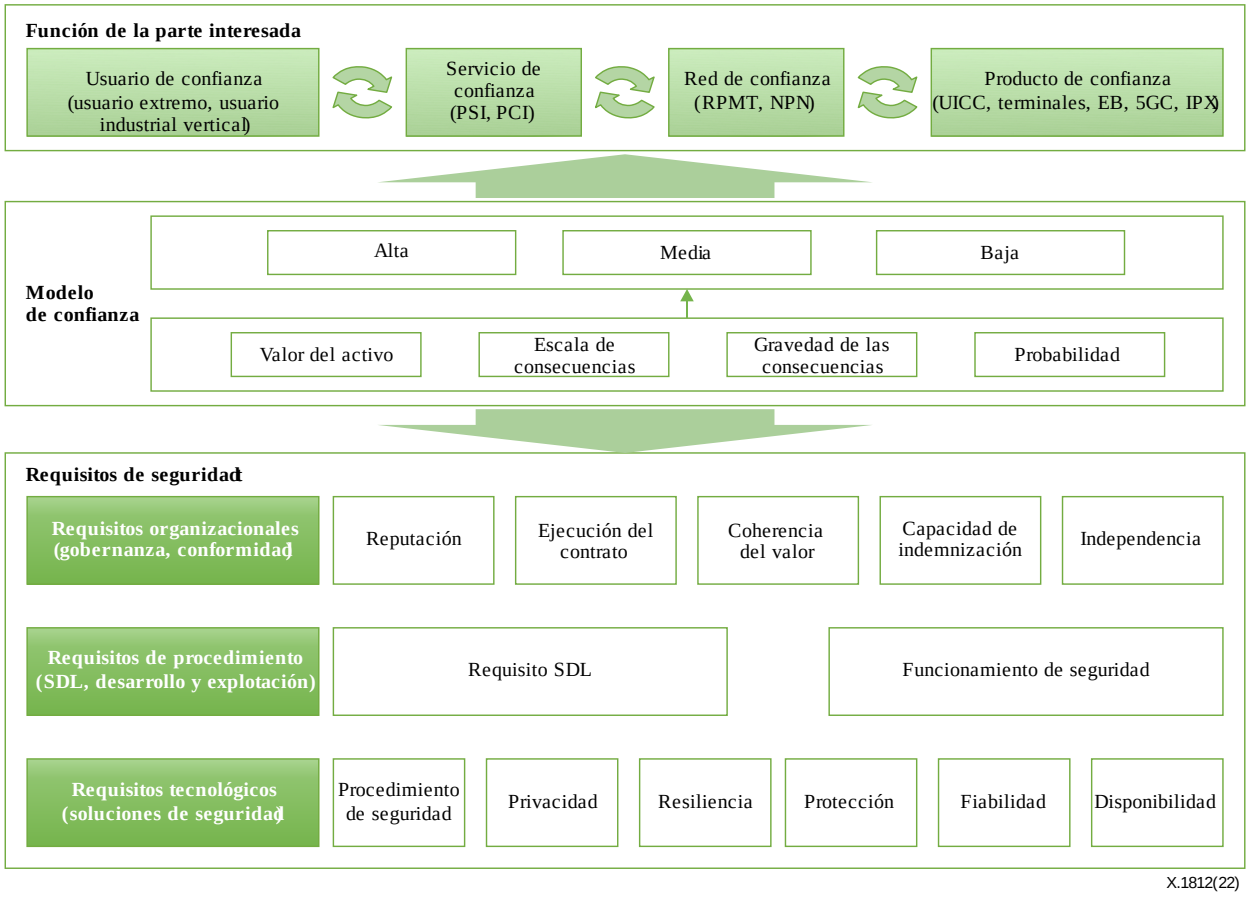


Figura 3 – Marco de seguridad soportado por el modelo de confianza basado en las relaciones de confianza entre las partes interesadas

5GC: Quinta generación principal; EB: Estación de base; PCI: Proveedor de contenidos de Internet; PSI: Proveedor de servicios de Internet; NPN: Red no pública (*Non-Public Network*); SDL: Ciclo de desarrollo de seguridad (*Security Development Lifecycle*)

8 Función de las partes interesadas en las hipótesis de funcionamiento del ecosistema IMT-2020

8.1 Generalidades

El actual sistema de telecomunicaciones puede estar subdividido en tres subsistemas: terminal, red y servicio. Es necesario considerar las relaciones posibles tanto entre los subsistemas como dentro de un mismo subsistema. No se aborda en esta cláusula la relación terminal-red, pues ya ha sido estudiada por otros organismos de normalización, como el Proyecto común de tecnologías inalámbricas de la tercera generación (3GPP).

En conjunto, las cinco hipótesis consideradas en esta cláusula abarcan todas las relaciones entre sistemas posibles, a excepción de la relación terminal-red.

8.2 Hipótesis 1: Despliegue de red de virtualización en un dominio de operador de red

8.2.1 Generalidades

Esta hipótesis se centra principalmente en la relación interna de la red.

En las redes de telecomunicaciones actuales, los elementos de red (NE) desplegados en una red suelen implementarse como dispositivos físicos dedicados. Cada NE se implementa como uno o más servidores de entidad físicos, según sus capacidades. Se utilizan cables, fibras, conmutadores y encaminadores para conectar esos dispositivos de red mediante interfaces físicas. En esta hipótesis, las principales partes interesadas son: los usuarios o abonados, los fabricantes de terminales móviles,

los proveedores de UICC, los distribuidores de dispositivos de red y los operadores. Esto se ilustra en la Figura 4.

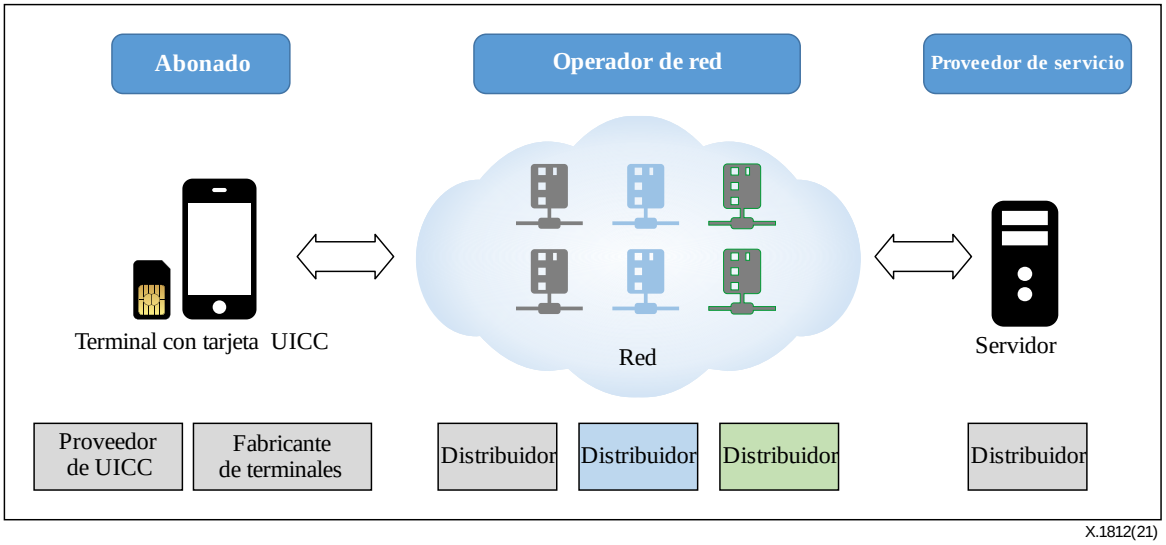


Figura 4 – Principales partes interesadas en un dominio de operador de red

En las IMT-2020, la tecnología de redes definidas por software/virtualización de las funciones de red está muy desarrollada y se ha ido desplegando gradualmente en la red. Las redes de telecomunicaciones también se están desarrollando con el uso creciente de la tecnología de la información (TI). Cuando se diseñó la arquitectura de red IMT-2020, se introdujo una novedosa arquitectura de servicio para utilizar mejor la TI para el despliegue y el mantenimiento. Los NE son sustituidos por las funciones de red (NF), más flexibles de explotar y mantener. Las NF pueden implementarse como funciones de red virtualizadas (VNF) e incluso como aplicaciones de software que se ejecutan en una máquina virtual, lo que sugiere que la virtualización de red se utilizará ampliamente en el despliegue de las redes IMT-2020. Así, la implementación ha pasado de los dispositivos integrados de hardware y software originales a una combinación triple de hardware, capa virtual y VNF. Por consiguiente, las principales partes interesadas en esta hipótesis son: los usuarios o abonados, los fabricantes de terminales móviles, los proveedores de UICC, los distribuidores de NE (proveedores de hardware, proveedores de capa de virtualización, proveedores VNF) y los operadores de red. Esto se resume en la Figura 5.

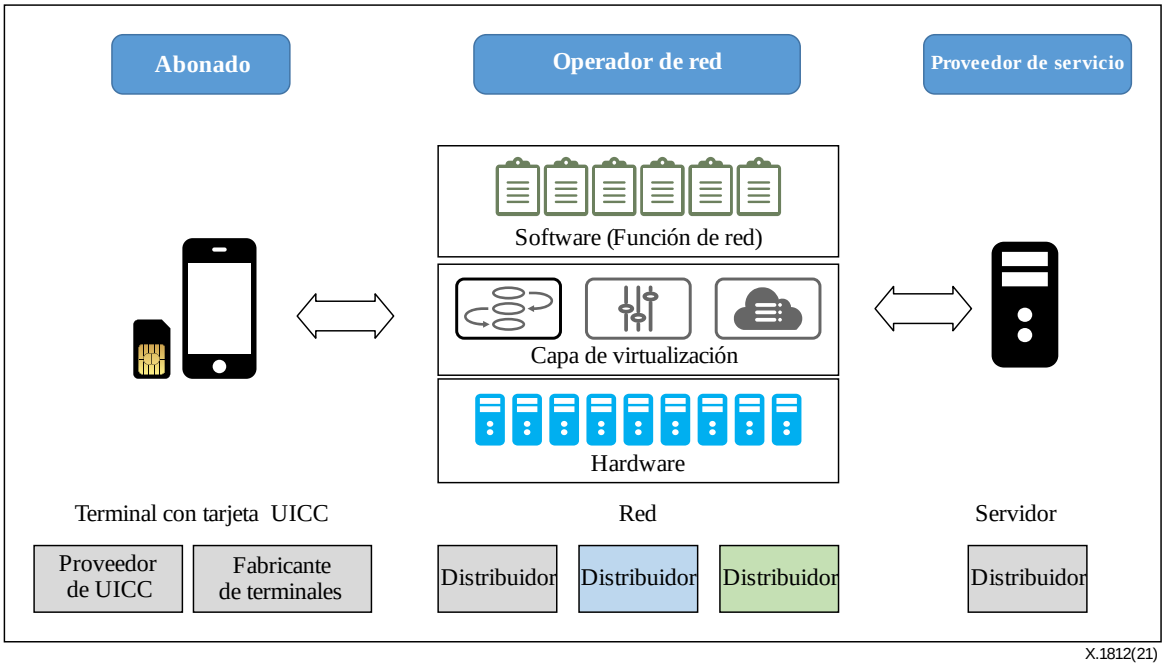


Figura 5 – Principales partes interesadas en el despliegue de red de virtualización de un dominio de operador de red

8.2.2 Funciones de las partes interesadas en esta hipótesis

En esta hipótesis las partes interesadas mencionadas asumen las siguientes funciones.

- Usuarios o abonados: Se trata de los usuarios extremos, es decir, los clientes, de los servicios de telecomunicaciones. El equipo de abonado consiste en un terminal móvil suministrado por un fabricante y una UICC suministrada por un distribuidor de tarjetas.
- Fabricante de terminales móviles: Esta entidad facilita los terminales que pueden utilizar los usuarios o abonados que se comunican con una red.
- Proveedor UICC: Esta entidad facilita las UICC que pueden utilizarse para representar las identidades de los abonados.
- Distribuidor de elementos de red: Esta entidad ofrece dispositivos o componentes de dispositivos que pueden combinarse para crear un sistema de telecomunicaciones o una plataforma/sistema de servicio.

  NOTA – De facilitar los componentes, puede inscribirse en cualquiera de las siguientes categorías: proveedor de hardware, proveedor de capa de virtualización o proveedor VNF.
- Operador de red: Esta entidad posee o controla todos los elementos necesarios para vender y prestar servicios de telecomunicaciones a los abonados y proveedores de servicio.

8.3 Hipótesis 2: Interconexión e itinerancia

8.3.1 Generalidades

Esta hipótesis se centra principalmente en la relación interna de la red.

La red de telecomunicaciones móviles puede ofrecer servicios a usuarios de todo el mundo gracias a la interconexión y coordinación entre operadores mundiales. Dicha interconexión y coordinación entre operadores implica la coordinación y cooperación en las capas de servicio y de transporte.

Hasta ahora, el principio de diseño de la interconexión entre los operadores de redes públicas móviles terrestres (RPMT) asumía que los operadores (a nivel de servicio) podían confiar plenamente unos en otros y que la transmisión de los datos de usuario y de señalización también era fiable. Para garantizar el reenvío correcto de mensajes de señalización a un operador concreto se introdujo el

proveedor de intercambio de paquetes entre redes (IPX). Sin embargo, el crecimiento de la red y la utilización de Internet han hecho que las conexiones IPX sean cada vez más complejas y susceptibles de ser atacadas por Internet. Por consiguiente, los operadores solo pueden garantizar la seguridad de las conexiones IPX que les atañen directamente, pero no de los enlaces entre operadores ni de todos los demás enlaces de esos operadores. Esto se ilustra en la Figura 6.

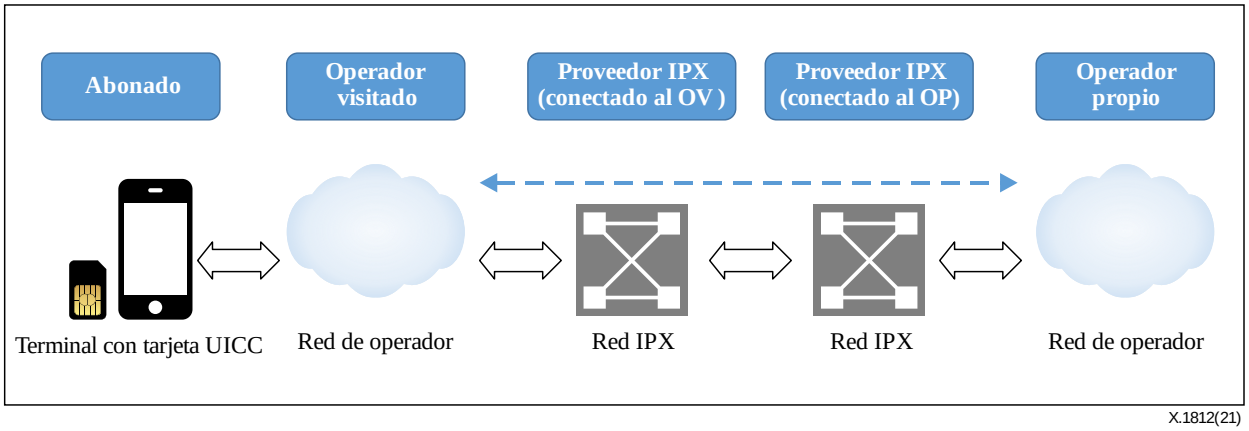


Figura 6 – Principales partes interesadas en la hipótesis de interconexión e itinerancia
HO: Operador propio; VO: Operador visitado

Además, se han descubierto y explotado numerosas vulnerabilidades de los operadores que han permitido el lanzamiento de ataques a otros operadores utilizando los dispositivos comprometidos como trampolín. Así, los operadores ya no confían en los mensajes de la capa de servicios [b-3GPP TS 33.501].

En esta hipótesis los principales actores son los usuarios o abonados, los operadores visitados, los operadores propios y los operadores IPX (incluido el IPX conectado al operador visitado y el IPX conectado al operador propio).

8.3.2 Funciones de las partes interesadas en esta hipótesis

En esta hipótesis las partes interesadas mencionadas asumen las siguientes funciones.

- Usuario o abonado: Se trata del usuario extremo, es decir, el cliente, de los servicios de telecomunicaciones.
- Operadores visitados: Son los operadores que facilitan al abonado acceso a los servicios cuando éste se encuentra fuera de la cobertura de su operador de red propio.
- Operador propio: Operador titular de las suscripciones de los abonados y que les presta servicios.
- Operador IPX (IPX conectado a los operadores visitados o IPX conectado al operador propio): Entidad que ofrece el servicio de intercambio de paquetes entre redes a los operadores.

8.4 Hipótesis 3: Alquiler de coche con funcionamiento a distancia

8.4.1 Generalidades

Esta hipótesis se centra principalmente en la relación interna del terminal y la relación terminal-servicio.

Cada vez hay más vehículos que se comunican con la plataforma remota gracias a un módulo de comunicación integrado durante o después de su fabricación. Esos vehículos pueden telecargar estados específicos o recibir instrucciones de una plataforma remota. En este caso, el vehículo consta

de dos partes: una relacionada con las telecomunicaciones, facilitada por el fabricante de terminales, y la otra, que es el vehículo mismo, procedente de la fábrica de vehículos.

La red de comunicaciones móviles tradicional ofrece principalmente servicios de voz, mensajes breves o acceso a la red de datos a los abonados. El abonado es el usuario extremo del terminal. En el caso de los servicios de alquiler de coches, los conductores que utilizan los vehículos con terminales de comunicación no son abonados. Además, los arrendadores de coches normalmente tendrán que utilizar una aplicación en su terminal móvil para interactuar con la plataforma a través de una red de comunicación para obtener a distancia información del vehículo o dirigirlo a distancia, para localizarlo, abrir o cerrar las puertas sin llave, o activar o desactivar el aire acondicionado.

Por consiguiente, en este caso, como se muestra en la Figura 7, las principales partes interesadas son los arrendadores de coches, el vehículo (que ejerce de terminal móvil), los fabricantes de terminales móviles, los proveedores de UICC, los fabricantes de automóviles, los distribuidores de elementos de red, los operadores de red y los proveedores de aplicaciones.

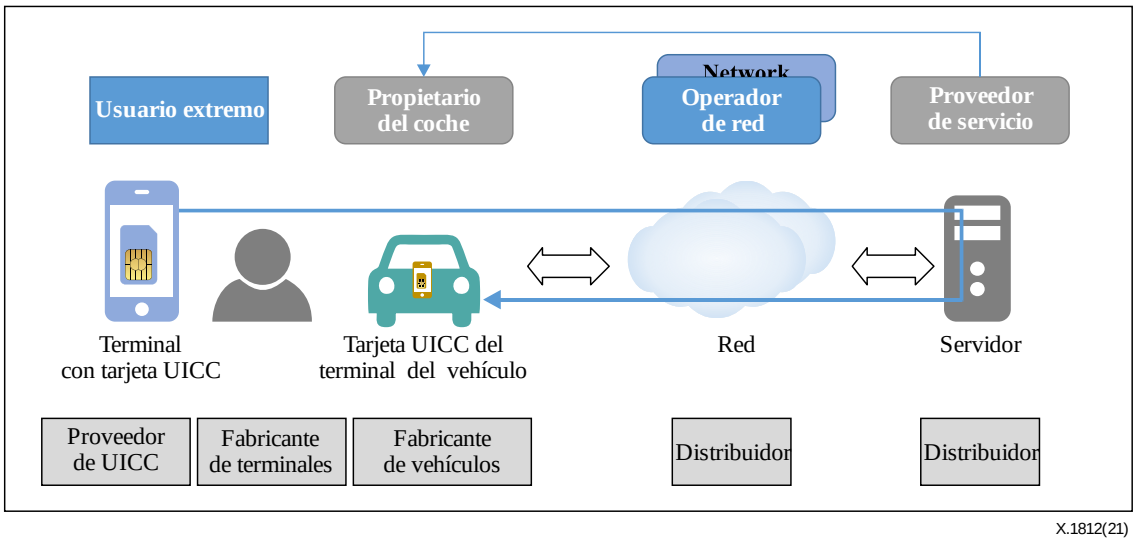


Figura 7 – Principales partes interesadas en la hipótesis del alquiler de coches con funcionamiento a distancia

8.4.2 Funciones de las partes interesadas en esta hipótesis

En esta hipótesis, las partes interesadas mencionadas asumen las siguientes funciones.

- Arrendador de coches: Un usuario específico alquila un coche a una empresa de alquiler de coches. Esa persona es también un abonado a una red móvil con un terminal móvil.
- Vehículo: El vehículo pertenece a una empresa de alquiler de coches y lleva incorporado un terminal móvil específico, que puede considerarse un abonado de red.
- Fabricante de terminales móviles: Entidad que facilita los terminales que pueden utilizar los abonados que comunican con la red.
- Proveedor UICC: La entidad facilita las UICC que pueden utilizarse para representar las identidades de los abonados.
- Fabricante de automóviles: La entidad que produce vehículos que pueden o no llevar integrado un terminal móvil.
- Distribuidor de elementos de red: La entidad que ofrece dispositivos o componentes de dispositivos que pueden combinarse en un sistema de telecomunicaciones o una plataforma o sistema de servicios.

- Operador de red: La entidad que posee o controla todos los elementos necesarios para vender y prestar servicios de telecomunicaciones a los abonados y proveedores de servicios.
- Proveedor de aplicaciones: La entidad que facilita las aplicaciones del servicio de alquiler de coches para los usuarios.

8.5 Hipótesis 4: Exposición de las capacidades de red para la industria

8.5.1 Generalidades

Esta hipótesis se centra principalmente en la relación red-servicio y la relación interna del servicio.

Las IMT-2020 poseen nuevas funcionalidades, como la banda ancha móvil mejorada, la conexión masiva a Internet de las cosas (IoT) y la comunicación de baja latencia ultrafiable, gracias a las que una red IMT-2020 puede ofrecer un mejor soporte de conexión a la red a sectores verticales, como la industria.

En comparación con las comunicaciones personales, las comunicaciones de la industria verticales tienen necesidades diferentes, como la diversidad de servicios, la diferenciación funcional y la heterogeneidad tecnológica. La comunicación vertical en la capa de aplicación suele tener unos requisitos de seguridad estrictos, por ejemplo, el aislamiento de la comunicación con otros usuarios industriales, una mayor capacidad de gestión o la colaboración con operadores de red con características específicas, como la exposición de capacidades. etc.

A diferencia de los servicios tradicionales, los servicios industriales verticales pueden cooperar con los operadores de red, de manera que también intervienen los proveedores de aplicaciones, así como los proveedores de servidores de aplicación o los proveedores de plataforma en la nube.

En el lado del terminal, como ocurre en la hipótesis 3, el dispositivo terminal también puede constar de dos partes, una relacionada con las comunicaciones, facilitada por el fabricante de terminales, y otra relacionada con las aplicaciones verticales dedicadas, facilitada por otros fabricantes de terminales industriales.

En este caso, como se ilustra en la Figura 8, las principales partes interesadas son: los usuarios industriales verticales, los fabricantes de terminales de comunicación, los proveedores de UICC, los fabricantes de terminales industriales, los distribuidores de elementos de red, los proveedores de servidores de aplicación o los proveedores de servicio de plataforma en la nube, los proveedores de aplicaciones y los operadores de red.

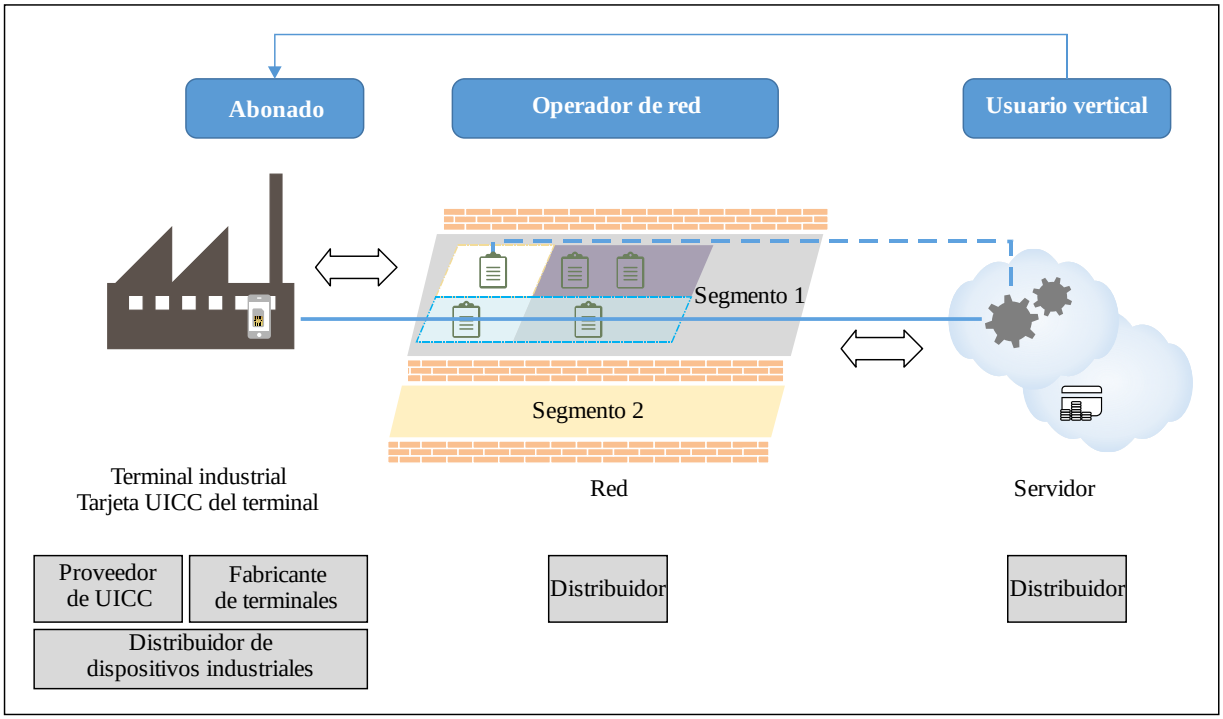


Figura 8 – Principales partes interesadas en la hipótesis de exposición de capacidades de red

8.5.2 Funciones de las partes interesadas en esta hipótesis

En esta hipótesis las principales partes interesadas asumen las siguientes funciones:

- Usuario industrial vertical: El usuario industrial vertical controla a distancia un terminal industrial a través de la red de telecomunicaciones utilizando aplicaciones dedicadas que se ejecutan en servidores de aplicación o en plataformas en la nube públicas o privadas.
- Fabricante de terminales de comunicación: La entidad que facilita los terminales que pueden utilizar los abonados que comunican con la red.
- Proveedor UICC: La entidad que facilita las UICC que pueden utilizarse para representar las identidades de los abonados.
- Fabricante de terminales industriales: La entidad que facilita las máquinas, redes o sistemas industriales a las fábricas o empresas.
- Distribuidor de elementos de red: La entidad que ofrece dispositivos o componentes de dispositivos que pueden combinarse en un sistema de telecomunicaciones o una plataforma o sistema de servicios.
- Proveedor de servidor de aplicaciones o proveedor de servicios de plataforma en la nube: La entidad que posee la infraestructura y la plataforma que ofrecen los servicios de almacenamiento y recursos de computación para las aplicaciones de capa superior.
- Proveedor de aplicaciones: La fábrica o las empresas que recaban información u ofrecen la señalización de control a los terminales industriales.
- Operador de red: La entidad que posee o controla todos los elementos necesarios para vender y prestar servicios de telecomunicaciones a los abonados y proveedores de servicios.

8.6 Hipótesis 5: Cadenas de producción

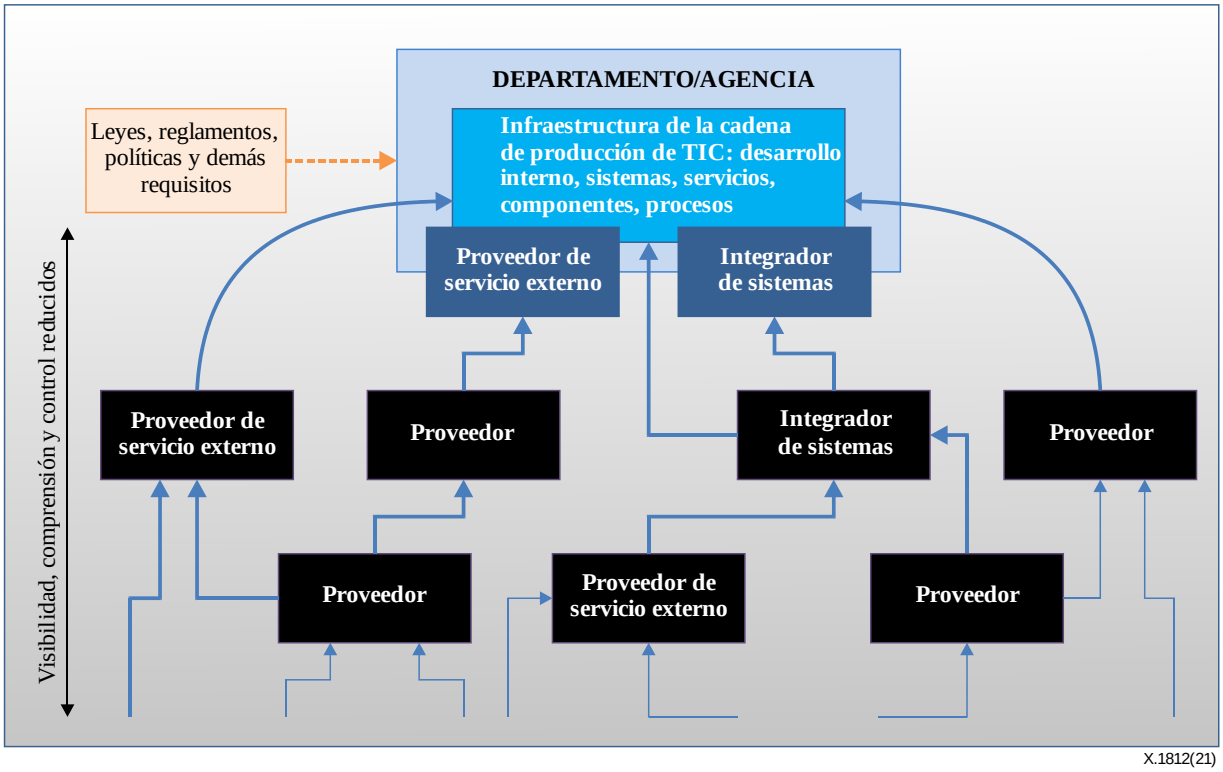
8.6.1 Generalidades

El ecosistema IMT-2020 es una comunidad compuesta por múltiples organizaciones que aportan grandes cantidades de tecnologías y conocimientos a fin de que los servicios y aplicaciones IMT-2020 funcionen.

Una cadena de producción es un sistema de organizaciones, personas, actividades, informaciones y recursos implicados en llevar un producto o servicio del proveedor al cliente. La gestión de riesgos en la cadena de producción es el esfuerzo coordinado que realiza una organización para identificar, supervisar, detectar y contrarrestar las amenazas a la continuidad y rentabilidad de la cadena de producción. La gestión de riesgos en la cadena de producción del ecosistema IMT-2020 se asienta sobre los cuatro pilares de seguridad siguientes:

- Seguridad: Esto atañe a la confidencialidad, integridad y disponibilidad de la información que a) describe la cadena de producción (por ejemplo, información sobre los trayectos transversales de los productos y servicios IMT-2020 tanto lógicos como físicos); o b) atraviesa la cadena de producción (por ejemplo, la propiedad intelectual de los productos y servicios IMT-2020), así como la información sobre las partes interesadas que intervienen en la cadena de producción (todos los relacionados de un modo u otro con un producto o servicio IMT-2020 a lo largo de su vida útil);
- Integridad: Esto garantiza que los productos o servicios IMT-2020 de la cadena de producción son genuinos, están inalterados, funcionarán de acuerdo con las especificaciones del comprador y no tendrán funcionalidades adicionales no deseadas.
- Resiliencia: Esto garantiza que la cadena de producción ofrezca los productos y servicios requeridos bajo presión y en caso de fallo;
- Calidad: Esto reduce las vulnerabilidades que puedan limitar el funcionamiento previsto de un componente, causar el fallo de un componente u ofrecer oportunidades para su explotación.

Esta hipótesis se centra principalmente en la cadena de producción y sus relaciones. En la Figura 9 se muestran las partes intervinientes en la cadena de producción.



TIC: Tecnología de la información y la comunicación

Figura 9 – Principales partes interesadas en las hipótesis de la cadena de producción

8.6.2 Funciones de las partes interesadas en esta hipótesis

En la cadena de producción participan varias partes: el creador o fabricante, el integrador de sistemas, el distribuidor, los vendedores de productos, el proveedor y el proveedor de servicios externos.

Por creador o fabricante se entiende: i) los creadores o fabricantes de sistemas de información, componentes de sistemas o servicios de sistemas de información; ii) los integradores de sistemas; iii) los distribuidores; o iv) los vendedores de productos.

Un integrador de sistemas es una persona o empresa que reúne los subsistemas componentes en uno y garantiza que esos subsistemas funcionan juntos. Este proceso se denomina integración de sistemas.

Un distribuidor es una entidad que ofrece bienes o servicios a una empresa o particular. El distribuidor suele fabricar los elementos y venderlos al cliente. Una empresa es una entidad jurídica distinta de la empresa contratante que ofrece servicios tales como consultoría o desarrollo de software.

Un vendedor de productos es una empresa o particular que adquiere bienes o servicios con la intención de venderlos, en lugar de consumirlos o utilizarlos.

Un proveedor es una entidad que ofrece bienes y servicios a otra entidad.

Por proveedor de servicio externo se entiende: i) las entidades pertenecientes a la organización, pero que están fuera de las fronteras de autorización de seguridad establecidas para los sistemas de información de la organización; ii) las entidades externas a la organización, ya sean del sector público (por ejemplo, agencias federales) o del sector privado (por ejemplo, proveedores de servicio comerciales); o iii) una combinación de entidades del sector público y el sector privado.

8.7 Partes interesadas en el ecosistema IMT-2020

De acuerdo con los casos de uso descritos en las cláusulas 8.2 a 8.6, el ecosistema IMT-2020 puede dividirse en los cuatro tipos de partes interesadas que se ilustran en la Figura 10, a saber: el fabricante, el operador de red, el proveedor de servicios y el usuario final.

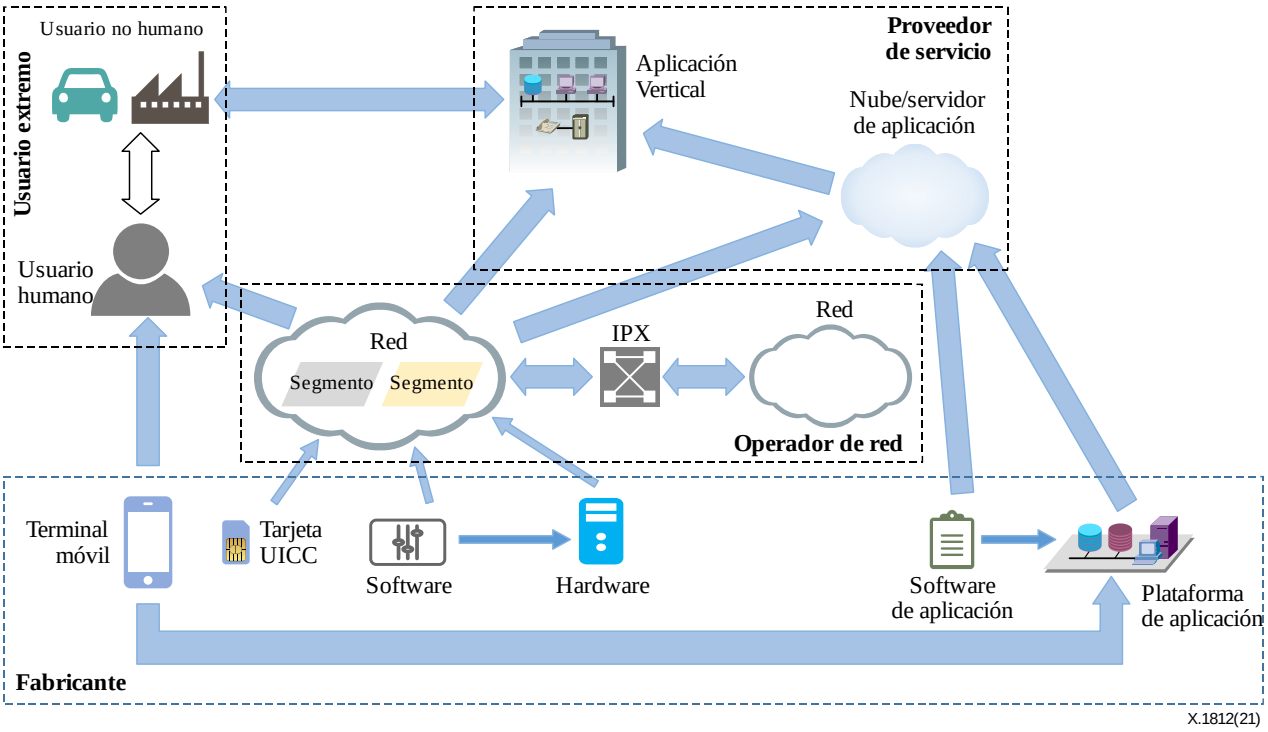


Figura 10 – Partes interesadas en el ecosistema IMT-2020

Una parte interesada puede estar relacionada directamente con otra e indirectamente con otras a través de otra parte interesada, por ejemplo, actuando como parte de la cadena de producción.

En el ecosistema IMT-2020 el fabricante puede considerarse un grupo de creadores o fabricantes, integradores de sistemas o distribuidores. Los operadores de red pueden contemplarse como vendedores de productos y proveedores de servicios de red. Los proveedores de servicios pueden considerarse externos.

Los fabricantes de componentes facilitan los bloques de construcción tecnológicos a los fabricantes de dispositivos inalámbricos y los fabricantes de equipos de red. Esos fabricantes de componentes también pueden facilitar los bloques de construcción directamente a los operadores de red. Los fabricantes de dispositivos inalámbricos ofrecen equipos para los usuarios extremos o como componentes de máquinas industriales, mientras que los fabricantes de equipos de red producen equipos que sustentan la infraestructura de red (tanto alámbrica como inalámbrica). Los operadores de red combinan estos dispositivos, componentes de red, equipos de red y redes de otros operadores a través del IPX en una red operativa mundial para dar servicio a los usuarios extremos. Los usuarios extremos hacen llamadas vocales, envían mensajes de texto y ejecutan aplicaciones por la red. Los operadores de red también ofrecen servicios de comunicaciones y otros servicios conexos a los proveedores de servicio externos gracias al servicio de exposición de capacidades de la red y otros servicios específicos.

9 Nivel de confianza, criterios de confianza y modelo de confianza

9.1 Generalidades

Como se define en la cláusula 3.1.11, la confianza es el grado en que un usuario u otra parte interesada confía en que un producto o sistema se comportará como está previsto. La confianza también desempeña un papel importante en el ecosistema IMT-2020. En esta Recomendación se especifica un modelo de confianza del ecosistema IMT-2020 que permite a las partes interesadas tomar decisiones con conocimiento de causa sobre confianza y seguridad.

Este modelo de confianza del ecosistema IMT-2020 se divide en tres niveles.

- El primer nivel de confianza atañe a los requisitos en la materia de los gobiernos y órganos reglamentarios. Los principales factores que rigen la confianza son, entre otros, la adopción de normas internacionales y la certificación pública y transparente.
- El segundo nivel de confianza afecta a los requisitos de las organizaciones industriales. Para esas entidades los factores clave son la definición de las partes interesadas, el propietario de la solución de extremo a extremo (E2E), el usuario comercial extremo, el modelo comercial, los niveles de confianza y las relaciones de confianza, entre otros.
- El tercer nivel de confianza consiste en proteger esa confianza mediante soluciones técnicas basadas en los factores clave de los dos anteriores niveles.

Esta Recomendación se centra en los niveles segundo y tercero, es decir, las organizaciones industriales y las soluciones técnicas.

El operador de red IMT-2020 necesita confiar en los dispositivos o equipos facilitados por los fabricantes para crear su sistema de red. Así, debe confiar en que los fabricantes facilitan dispositivos que se ajustan a los requisitos del operador de red.

El proveedor de servicio confía en que la red transmita la información, por lo que debe confiar en que el operador de red garantice la correcta y puntual transmisión de los datos. El proveedor de servicio también debe confiar en los dispositivos facilitados por los fabricantes para implantar sus servicios, por lo que debe confiar en que esos fabricantes ofrezcan dispositivos que cumplen los requisitos del proveedor de servicio.

Los usuarios extremos deben confiar en la transmisión de red y las aplicaciones de servicio, por lo que deben confiar en que el acceso a la red ofrecido por el operador de red sea legal y efectivo. Estos mismos requisitos se aplican al proveedor de servicio.

9.2 Niveles de confianza

Resulta esencialmente difícil cuantificar la confianza de manera significativa. En el modelo de confianza de esta Recomendación se introduce la noción cualitativa de nivel de confianza para poder razonar las implicaciones de los distintos grados de confianza.

Los servicios IMT-2020 funcionan en diversos contextos, por lo que deben ajustarse a distintos requisitos de confianza. Por ejemplo, los distintos verticales transportan servicios diferentes y operan en situaciones distintas, por lo que sus necesidades de confianza son variables. Además, algunas industrias se consideran parte de la infraestructura nacional esencial, como la red eléctrica inteligente, mientras que otras intervienen en aspectos menos críticos de la vida cotidiana, como las empresas de alquiler de vehículos.

Si una industria concreta se considera parte de la infraestructura esencial, es evidente que necesitará un mayor nivel de confianza en que el sistema IMT-2020 se comportará como está previsto. Dicho de otro modo, se ha de fijar un nivel de confianza más elevado para esa industria, pues cualquier daño afectará a la estabilidad nacional. Por otra parte, puede establecerse un nivel de confianza más bajo para las industrias cuyos fallos tengan repercusiones relativamente menores.

Por ejemplo, los servicios de Internet de las cosas en banda estrecha, como la Internet de los vehículos (IoV), la Internet industrial, la red eléctrica inteligente y el riego de flores, tienen distintos niveles de confianza, pues los daños causados a estas industrias repercutirán en distinto grado en la sociedad o los usuarios.

El nivel de confianza en cada caso dependerá principalmente del grado en que un daño causado a la industria de que se trate repercutirá en la sociedad y el país. Ese grado de incidencia quien mejor lo podrá determinar será probablemente la organización vertical en cuestión, pues dispondrá de representantes de múltiples campos y de la experiencia profesional necesaria para hacer el análisis

del caso; también forma parte de su diligencia debida especificar el nivel de confianza. Por tanto, en los casos en que el nivel de confianza sea más elevado, también será mayor la responsabilidad de cada una de las partes interesadas implicadas; dicho de otro modo, también se habrá de definir un nivel de confianza mayor para esas partes interesadas.

A los efectos del modelo de confianza propuesto aquí, se supone que el nivel de confianza de cada una de las partes puede fijarse a uno de los tres niveles cualitativos: alto, medio o bajo. Este supuesto se asienta en dos motivos principales:

- en primer lugar, la asignación de valores cuantitativos a los niveles de confianza puede resultar muy problemática, pues no existe una métrica evidente de la confianza (a diferencia, por ejemplo, del análisis de riesgos, donde la métrica puede basarse en una combinación de probabilidad de ocurrencia y una evaluación de la repercusión financiera anualizada);
- en segundo lugar, esta escala de tres niveles basta para abarcar la mayoría de los casos de uso existentes y es también la adoptada por otras entidades, por ejemplo, en el esquema de garantía de seguridad de equipos de red (NESAS) [b-GSMA FS.13], [b-GSMA FS.14], [b-GSMA FS.15], [b-GSMA FS.16], para medir los requisitos de confianza.

Permanece el problema de determinar el significado de estos tres niveles de confianza a fin de poder utilizar de manera coherente el modelo establecido en esta Recomendación. En la cláusula 9.3 se indican los criterios de confianza diseñados para determinar los niveles de confianza.

Dada la diversidad de activos y el amplio abanico de hipótesis de despliegue de cada industria vertical, en la práctica el nivel de confianza general debe perfilarse en función del contexto. Por ejemplo, el nivel de confianza necesario para la conducción autónoma evidentemente depende de la red IoV concreta, la red del complejo o la macrorred.

En el siguiente ejemplo se ilustra también la necesidad de contar con una definición de nivel de confianza compleja y adaptada al contexto. Supongamos que un operador escoge al fabricante de equipos de red en función del nivel de confianza especificado. Si solo se especifica un nivel, todos los fabricantes de equipos de red deben ser escogidos en función de un único nivel de confianza. Sin embargo, la red troncal es más sensible, valiosa e influyente que, por ejemplo, las antenas, por lo que, en un caso típico, el nivel de confianza del fabricante de red troncal deberá ser superior al del fabricante de antenas.

Si ahondamos más, el nivel de confianza se especifica independientemente para la unidad comercial y para la hipótesis comercial. En el caso de una industria vertical esto significa que hay que especificar por un lado el nivel de confianza de toda la industria vertical y por otro el nivel de la industria vertical de que se trate. En el Cuadro 1 se muestran las combinaciones posibles de niveles de confianza para estos dos casos.

Cuadro 1 – Nivel de confianza de la unidad comercial y de las hipótesis comerciales, y relación entre ellos

Nivel de confianza de la unidad comercial	Nivel de confianza de la hipótesis comercial
Alto	Alto
	Medio
	Bajo
Medio	Medio
	Bajo
Bajo	Bajo

A fin de que la especificación del nivel sea más práctica y universal, se recomienda definir el nivel de confianza del componente de manera flexible. Por ejemplo, el nivel de confianza del componente puede definirse en función del valor del activo o de la zona de despliegue.

Por poner un ejemplo concreto, el nivel de confianza de toda la red eléctrica inteligente es alto, pero dentro de la red misma, los cables y postes eléctricos no tienen tanto valor como los sensores y la infraestructura de transmisión de la señal de la red IMT-2020. Incluso considerando los sensores y la infraestructura de transmisión de la señal, una red eléctrica inteligente desplegada en una ciudad pequeña no es tan sensible como una red de ese tipo desplegada en una gran ciudad.

En el Cuadro 2 se indican los posibles niveles de confianza en la relación entre una industria vertical y una parte interesada.

Cuadro 2 – Posibles niveles de confianza entre una industria vertical y una parte interesada

Nivel de confianza del sistema	Nivel de confianza del componente	Nivel de confianza de la parte interesada
Alto	Alto	Alto
	Medio	Medio
	Bajo	Bajo
Medio	Medio	Medio
	Bajo	Bajo
Bajo	Bajo	Bajo

9.3 Criterios de confianza

Para determinar si un nivel de confianza es alto, medio o bajo es necesario evaluar las relaciones de confianza entre las partes interesadas. La relación de confianza entre dos partes cualesquiera se ve afectada por múltiples factores, y el grado de confianza entre las distintas partes de una categoría y las partes de otra categoría también será diferente. Por consiguiente, los criterios de evaluación se han de especificar para cada caso concreto.

Dado que el nivel de confianza se escoge para minimizar los daños que las posibles amenazas y riesgos podrían causar, entre los criterios pueden incluirse el valor de los activos, la escala de consecuencias, la gravedad de las consecuencias y la probabilidad de materialización del riesgo, de acuerdo con las normas de gestión de riesgo como [b-NIST SP800-30], [b-ISO 31000] y [b-ISO/CEI 27005].

- Activos: La importancia de este factor es evidente. Cuanto más importante sea un activo, mayor será la necesidad de mantenerlo bajo control estricto de la parte interesada y más elevado será el nivel de confianza necesario.
- Escala de consecuencias: En el caso de una parte interesada de gran tamaño, cuanto mayor sea su ámbito de influencia, mayores serán las consecuencias de un eventual fallo. Por consiguiente, se necesita un nivel de confianza alto si el ámbito de influencia es amplio. Por ejemplo, un operador necesitará un nivel de confianza más bajo en un distribuidor que venda células pequeñas que dan cobertura a zonas minúsculas que si este vende elementos de red troncal que dan cobertura a zonas inmensas.
- Gravedad de las consecuencias: Si la parte interesada forma parte de una infraestructura esencial, las consecuencias de los daños serán más graves, por lo que se ha de invertir un mayor esfuerzo en evitar que ese daño ocurra. Esto genera una mayor necesidad de evaluar cuidadosamente las interacciones con otras partes. Así, cuanto mayor sea la consecuencia de un fallo en una relación, mayor será el nivel de confianza necesario.
- Probabilidad de materialización del riesgo: Cuanto mayor sea esa probabilidad, más posibilidades habrá de que el riesgo se materialice.

El ecosistema IMT-2020 es muy complejo. Hay diversas clases de partes interesadas, por ejemplo, usuarios extremos, fabricantes de equipos, operadores de red y proveedores de servicio, y cada una de ellas contiene diversas instancias específicas. Dado que la confianza es un concepto subjetivo, esta

resulta difícil de medir y de normalizar, y el nivel de confianza entre dos instancias también es diferente. Sin embargo, es necesario definir un conjunto de niveles de confianza generales que abarque la mayoría de las situaciones a fin de poder orientar a cada entidad del ecosistema IMT-2020. Esos niveles son: bajo, medio y alto.

En el Cuadro 3 se muestra un ejemplo de la manera en que se puede determinar un nivel de confianza en función de los diversos criterios de confianza.

Cuadro 3 – Criterios de nivel de confianza

Nivel de confianza global	Criterios de nivel de confianza			
	Valor de los activos	Escala de consecuencias	Gravedad de las consecuencias	Probabilidad de materialización del riesgo
Alto	Alto	Alto	Alto	Alto
Medio	Medio	Medio	Medio	Medio
Bajo	Bajo	Bajo	Bajo	Bajo

Al utilizar las correspondencias del Cuadro 3 es importante que el nivel de riesgo de los criterios de confianza tenga en cuenta las medidas de reducción de riesgos ya implantadas o que se implantarán. Por ejemplo, cuando la Internet existente se utiliza para el comercio electrónico de gran valor, deberá otorgarse al valor de los activos, la escala de consecuencias y la gravedad de las consecuencias un nivel muy elevado; además, a primera vista podría decirse que la probabilidad de ataque también será muy elevada, dado que los protocolos de comunicación Internet no contienen funcionalidades de seguridad robustas. De acuerdo con el Cuadro 3, entonces, el nivel de confianza de Internet debe ser alto para ajustarse a las necesidades del comercio electrónico. Sin embargo, a pesar de que el nivel de confianza en el mundo real de Internet es en realidad bajo, pues Internet no ofrece garantías de confidencialidad, integridad o disponibilidad de los canales de comunicación, el comercio electrónico se utiliza ampliamente y con gran éxito para realizar enormes volúmenes de transacciones.

De hecho, el motivo por el que esta hipótesis funciona es que los riesgos que corren la confidencialidad e integridad de la transferencia de datos están cubiertos por la utilización rutinaria de la seguridad de la capa de transporte [b-IETF RFC 5246] para proteger las comunicaciones entre puntos extremos, lo que puede considerarse como parte de los requisitos de seguridad especificados en la cláusula 10.2.

En conclusión, el cálculo del nivel de confianza requerido debe tomar en consideración el nivel real de la amenaza tras la aplicación de medidas de reducción de riesgos específicas a cada caso. En caso contrario podrían formularse demandas irrealistas en cuanto al nivel de confianza requerido de los proveedores de equipos y servicios, lo que causaría un aumento notable de los costes.

9.4 Correspondencias en el modelo de confianza basado en las relaciones de confianza

A fin de definir la frontera de seguridad y las medidas de seguridad en las IMT-2020 de manera interoperable y normalizada, es necesario desarrollar y utilizar adecuadamente el modelo de confianza. Para que el modelo de confianza sea efectivo, hay que analizar las relaciones de confianza.

A partir de los factores señalados en la cláusula 9.2 la relación de confianza entre dos partes es en general unidireccional, más que bidireccional. En el Cuadro 4 se muestra un ejemplo de análisis de las relaciones de confianza entre diversas partes interesadas.

Cuadro 4 – Relaciones de confianza entre partes interesadas

Sujeto	Objeto			
	Usuario extremo	**Fabricante**	**Operador de red**	**Proveedor de servicios**
Usuario extremo		Medio/bajo	Alto/medio/bajo	Alto/medio/bajo
Fabricante	–		Alto	Alto
Operador de red	Bajo	Alto/medio/bajo		Alto/medio/bajo
Proveedor de servicios	Alto/medio/bajo	Alto/medio/bajo	Alto/medio/bajo	

Las relaciones de confianza entre los diversos intervinientes en un ecosistema IMT-2020 suelen ser muy complejas, por lo que es necesario establecer un modelo de confianza que refleje dicha complejidad. Así, la relación de confianza global puede detallarse para obtener valores de confianza a nivel del subsistema. En el Cuadro 5 se presenta un ejemplo de análisis de las relaciones de confianza a nivel del subsistema.

Cuadro 5 – Relación de confianza a nivel del subsistema dentro del fabricante

Sujeto	Objeto			
	Chip/módem	**Módulo**	**Proveedor de dispositivos**	**Proveedor de software**
Chip/módem		–	–	–
Módulo	Alto/medio		–	–
Proveedor de dispositivos	Alto/medio	Alto/medio		–
Proveedor de software	Alto/medio	Alto/medio	Alto/medio	

Tomando este modelo, en el Cuadro 6 se muestra un ejemplo de extremo a extremo de la hipótesis de alquiler de coche.

Cuadro 6 – Modelo de confianza basado en las relaciones de confianza en la hipótesis de alquiler de coche

Sujeto		Objeto						
		Proveedor de servicios (vehículo)	**Arrendador**	**Fabricante**			**Operador de red**	**Proveedor de servicios**
				Terminal/ UICC	**Automóvil (excluidos el terminal y la UICC)**	**Equipo de red**		
Vehículo			Medio/bajo	Medio	Alto/medio	–	Alto/medio/bajo	Alto
Arrendador		Alto/medio		Medio/bajo	Medio/bajo	–	Alto/medio/bajo	Alto/medio/bajo
Fabricante	**Terminal/UICC**	–	–		–	–	Alto	Alto
	Automóvil	–	–	–		–	–	Alto
	Equipo de red	–	–	–	–		Alto	–
Operador de red		Bajo	Bajo	Alto/medio/bajo	–	Alto/medio/bajo		Alto/medio/bajo
Proveedor de servicios		Alto	Medio/bajo	Alto/medio/bajo	Alto/medio	–	Alto/medio/bajo	

10 Requisitos de seguridad soportados por el modelo de confianza basado en las relaciones de confianza

10.1 Generalidades

En cualquier hipótesis concreta, el sistema está establecido por una serie de partes interesadas que ofrecen distintos servicios y funciones para garantizar que el sistema se comporte y funcione como está previsto, reportando beneficios a las partes interesadas. El conjunto de esas partes representa el ecosistema.

Durante el funcionamiento del ecosistema puede haber peligros y amenazas de bloqueo del funcionamiento corriente. Para evitar que las amenazas causen daños, todas las partes interesadas deben contribuir a garantizar el funcionamiento continuo del ecosistema respetando la legalidad y ofreciendo productos, servicios y soluciones seguros siguiendo un procedimiento de desarrollo seguro.

El modelo de confianza que se establece en la cláusula 9 puede utilizarse para determinar los requisitos de seguridad basados en la confianza de cada una de las partes interesadas.

10.2 Requisitos de seguridad a partir del nivel de confianza

10.2.1 Generalidades

Puede utilizarse el nivel de confianza de una parte interesada para evaluar si podrá ofrecer una capacidad de defensa ante daños suficiente. Pueden definirse requisitos de seguridad para paliar esos daños. Así, los requisitos de seguridad pueden basarse en las capacidades de la organización, incluido el nivel profesional de su personal, la utilización de procesos de desarrollo seguros, como el ciclo de desarrollo de seguridad o las capacidades procesales de funcionamiento de seguridad y las capacidades tecnológicas necesarias para una solución fiable. Puede encontrarse más información al respecto en normas y prácticas como [b-NIST FICIC], [b-BSIMM]. Véase el Cuadro 7.

Cuadro 7 – Nivel de confianza y categorías de requisitos de seguridad

Nivel de confianza	**Categorías de requisitos de seguridad**		
Sujeto	**Objeto**		
	Capacidad de la organización (buena reputación)	Seguridad del desarrollo del sistema y seguridad de la vida útil del producto o capacidad de funcionamiento seguro (buen procedimiento)	Capacidad tecnológica necesaria para una solución fiable (buena solución)
Alto	√	√	√
Medio	√	√	–
Bajo	√	–	–

10.2.2 Requisitos de la organización

10.2.2.1 Introducción

Las capacidades de seguridad relacionadas con la confianza de una organización pueden desglosarse en: su reputación, su capacidad para ejecutar contratos, la coherencia del valor, la posible indemnización por ruptura de contrato y su independencia.

10.2.2.2 Reputación

La reputación refleja el grado de respeto histórico de los objetivos especificados para un producto o sistema. La reputación es una medida que podría derivarse del conocimiento directo o indirecto de

las interacciones previas de las partes interesadas y se utiliza para evaluar el nivel de confianza en una parte interesada. Como representación de la confianza, suele depender de la información histórica para inferir la probabilidad de fiabilidad futura. Por consiguiente, cuando una parte interesada concreta ya ha actuado de manera correcta según los términos de un acuerdo, su reputación en la industria aumentará y obtendrá una mayor confianza de la otra parte. Los datos necesarios para gestionar la reputación pueden obtenerse de fuentes fiables y ampliamente aceptadas basadas en las pruebas, como los certificados o los informes anuales y financieros oficiales. Sin embargo, una parte concreta puede tener reputaciones distintas en función del ámbito que se trate. Por ejemplo, la relación entre un fabricante de dispositivos y un operador de red o proveedor de servicio es una relación vendedor-cliente, mientras que la relación entre distintos fabricantes puede ser de naturaleza competitiva. Así, un fabricante de dispositivos puede tener una buena reputación ante un operador de red o proveedor de servicio y una mala reputación para la competencia. Por consiguiente, al examinar la información sobre reputación procedente de fuentes externas, los operadores de red o proveedores de servicio no pueden considerar como fuente primaria la información de reputación obtenida de un fabricante competidor.

10.2.2.3 Ejecución de contratos

En el caso de la ejecución cooperativa continua o de la ejecución cooperativa intermitente repetida, la calidad de la ejecución de los contratos repercutirá en la confianza de ambas partes. También tendrá repercusiones en la relación de confianza entre las partes. Cuando el contrato se ejecute correctamente, aumentará la confianza mutua y la relación de confianza será estrecha. Por el contrario, cuando un contrato no se ejecute correctamente, la confianza mutua resultará mermada, así como la relación de confianza. En el caso de la cooperación múltiple continua, por ejemplo, cuando los usuarios recurren repetidamente a un proveedor de servicio, la experiencia histórica de los usuarios tendrá consecuencias directas para su confianza en el sistema de servicio. En ese caso, se recomienda considerar la información relativa a la experiencia histórica del usuario como un factor correspondiente a la ejecución del contrato del usuario, más que un factor de reputación.

10.2.2.4 Coherencia del valor

Cuando las partes interesadas comparten los mismos valores, la relación entre ellas es más estrecha y sus expectativas de futuro a largo plazo son más coherentes. Por consiguiente, se alcanza una confianza mutua mayor y se establecerá entre ellas una mejor relación de confianza.

10.2.2.5 Indemnización

Por capacidad de indemnización se entienden las expectativas de indemnización en caso de que no se respete un compromiso adquirido. La expectativa de indemnización puede considerarse otra garantía de que la parte interesada procurará ejecutar el contrato incluso en circunstancias anormales. Por norma general, cuanto mayor sea la indemnización, menores serán las pérdidas para la otra parte. Esa capacidad aumentará la confianza y la seguridad respecto de esa otra parte. Por ejemplo, en la legislación regional en materia de ciberseguridad pueden definirse el nivel y la gravedad de las sanciones o indemnizaciones aplicables a las distintas partes a fin de fomentar la fiabilidad.

10.2.2.6 Independencia

La independencia de una parte refleja su autonomía para ejecutar un contrato. Dentro de la independencia se incluye la capacidad de una empresa matriz para controlar a su filial, así como la influencia de las autoridades en la entidad comercial. Cuantas más partes interesadas intervengan, mayor influencia recibirá de ellas y más se verá afectada su relación de confianza.

10.2.2.7 Resumen

En el Cuadro 8 se muestra un ejemplo de las maneras en que los niveles de confianza pueden relacionarse con las capacidades de una organización. En la práctica, los aspectos concretos necesarios para los niveles de confianza medio y bajo dependerán del ámbito de aplicación. Por

ejemplo, en algunos casos puede ser necesaria una reputación del proveedor adecuada para alcanzar un nivel de confianza bajo, mientras que en otros casos ese aspecto puede no tener importancia, aunque se necesite un nivel de confianza medio.

Cuadro 8 – Niveles de confianza y requisitos de seguridad relacionados con las capacidades de la organización

Nivel de confianza	Requisitos de seguridad de la capacidad de la organización				
	Reputación	Ejecución de contratos	Coherencia del valor	Capacidad de indemnización	Independencia
Alto	√	√	√	√	√
Medio	(√)	√	–	√	(√)
Bajo	–	√	–	(√)	–

10.2.3 Requisitos de procedimiento

10.2.3.1 Introducción

La capacidad de funcionamiento seguro puede ejecutarse empleando las siguientes capacidades: seguridad del desarrollo y la vida útil del producto; y capacidad de funcionamiento seguro.

10.2.3.2 Seguridad del desarrollo y la vida útil del producto

Dentro del esquema de garantía de seguridad de equipos de red (NESAS), el desarrollo y la vida útil del producto abarcan todos los aspectos que pueden influir en la vida útil de un producto de red, incluidos la planificación, el diseño, la implementación, la entrega, la actualización y, en su caso, la eliminación. En la actualidad, para la red IMT-2020, en NESAS, producto conjunto de la Asociación del Sistema Mundial para Comunicaciones Móviles (GSMA) y el 3GPP, se ha determinado una seguridad del desarrollo y la vida útil del producto para los equipos de red IMT-2020 que abarca las fases que siguen estos productos de red a lo largo de su desarrollo (como la planificación, el diseño, la implementación, las pruebas, la comercialización, la producción y la entrega), y la vida útil del producto (abarcando las fases que siguen los productos de red desarrollados hasta el final de su vida útil, incluidos el mantenimiento y las actualizaciones). Se recomienda tomar esto como referencia a la hora de evaluar el desarrollo y la vida útil del producto de un distribuidor.

10.2.3.3 Capacidad de funcionamiento seguro

La capacidad de funcionamiento seguro implica que el producto o la red deben estar bien gestionados cuando se utilizan a título comercial, entre otras cosas mediante el despliegue de seguridad, las restricciones y las limitaciones del control del acceso.

10.2.3.4 Resumen

Así, respecto de la capacidad de funcionamiento seguro, se recomiendan los requisitos de seguridad que se indican en el Cuadro 9.

Cuadro 9 – Nivel de confianza y requisitos de seguridad para la capacidad de funcionamiento seguro

Nivel de confianza	Requisitos de seguridad para la capacidad de funcionamiento seguro	
	Seguridad del desarrollo del sistema y la vida útil del producto	Funcionamiento seguro
Alto	√	√
Medio	(√)	√
Bajo	=	√

10.2.4 Requisitos tecnológicos

La capacidad de fiabilidad puede alcanzarse si se respetan adecuadamente los siguientes factores: procedimientos de seguridad, privacidad, resiliencia, protección, fiabilidad y disponibilidad. Se trata de atributos clave que se recomienda que tengan los productos y soluciones de seguridad ofrecidos por la parte interesada desde el punto de vista de la fiabilidad, como se estipula en una serie de documentos como [b-BSI 10754-1] y [b-NIST SP800-160v1].

En el Cuadro 10 se presenta un ejemplo de cómo pueden alcanzarse los niveles de confianza relacionados con la fiabilidad de una organización. Como en el caso anterior, en la práctica, los aspectos concretos necesarios para alcanzar niveles de confianza medios o bajos dependerán del ámbito de aplicación. Por ejemplo, en algunos casos puede ser necesario ofrecer un nivel adecuado de protección de la privacidad de los datos para alcanzar un nivel de confianza bajo, mientras que en otros casos este aspecto puede no ser tan importante, aunque se necesite un nivel de confianza medio.

Cuadro 10 – Nivel de confianza y requisitos de seguridad para la capacidad de fiabilidad

Nivel de confianza	Requisitos de seguridad para la capacidad de fiabilidad					
	Procedimiento de seguridad	Privacidad	Resiliencia	Protección	Fiabilidad	Disponibilidad
Alto	√	√	√	√	√	√
Medio	√	(√)	(√)	(√)	(√)	√
Bajo	√	–	–	(√)	(√)	–

En la práctica, los requisitos concretos dependerán de las hipótesis de servicio y de las necesidades de flexibilidad. Como se ha indicado anteriormente, si el nivel de confianza es bajo, aunque los requisitos de seguridad puedan ser relativamente bajos, puede ser necesario cumplir requisitos más estrictos, como el de la privacidad.

10.3 Interpretación de la confianza en función de los requisitos de garantía concretos

Una vez determinado el nivel de confianza necesario para un caso de uso concreto, es necesario interpretarlo para tomar decisiones operativas o sobre la implementación.

Para ello puede establecerse una correspondencia entre el nivel de confianza requerido y los requisitos específicos enumerados en la cláusula 10.2, que pueden cumplirse mediante la garantía de productos y sistemas. Hay una amplia gama de técnicas normalizadas e implantadas para garantizar la fiabilidad de los productos y sistemas mediante pruebas y evaluaciones, por ejemplo, las que llevan a cabo especialistas terceros. Estas pueden servir de base para establecer la correspondencia entre el nivel de confianza requerido, derivado de un análisis como el descrito en la cláusula 9.4, y los requisitos de garantía específicos aplicables a la adquisición y uso de equipos y servicios.

El objetivo del ejemplo que se ilustra en el Cuadro 11 es la integración de los niveles de confianza necesarios en las decisiones de orden comercial y operativo basadas en la confianza a partir de las evaluaciones de productos y sistemas.

Cuadro 11 – Ejemplo de correspondencia entre los niveles de confianza necesarios y los requisitos de garantía

Nivel de confianza necesario	Tipo de entidad garante	Ejemplos de esquemas de garantía de la seguridad
Alto	Evaluación por un organismo público reconocido	Criterios comunes [b-ISO/CEI 15408 (todas las partes)] Organismo nacional de reglamentación [b-ISO/CEI 27001] NESAS Especificación de garantía de seguridad (SCAS) [b-3GPP TS33.511] [b-3GPP TS33.512] [b-3GPP TS33.513] [b-3GPP TS33.514] [b-3GPP TS33.515] [b-3GPP TS33.516] [b-3GPP TS33.517] [b-3GPP TS33.518] [b-3GPP TS33.519]
Medio	Evaluación por un órgano de evaluación de la conformidad (CAB) acreditado	Criterios comunes [b-ISA/CEI 62443 (todas las partes)] [b-ISO/CEI 27001] NESAS/SCAS
Bajo	Evaluación por un CAB o autoevaluación	Criterios comunes NESAS/SCAS

Incluso dentro de un mismo esquema de garantía, a cada nivel de confianza pueden convenir distintos grados o tipos de garantías.

- Algunas técnicas, en particular las que se especifican en [b-ISO/CEI 15408 (todas las partes)], permiten especificar múltiples tipos de garantías, por lo que distintos niveles de confianza pueden exigir opcionalmente distintos niveles de evaluación [b-ISO/CEI 15408 (todas las partes)]. Sin embargo, otros esquemas, como [b-ISO/CEI 27001], solo permiten un único nivel de evaluación.
- El grado de garantía que puede obtenerse de una evaluación puede depender opcionalmente del órgano que la realice (como se indica en la columna del medio del Cuadro 11). Por ejemplo, para un nivel de confianza bajo puede bastar con una autoevaluación de los requisitos de [b-ISO/CEI 27001].

Además, el peso otorgado a una evaluación puede verse influido por otros factores, como, por ejemplo:

- si el equipo o servicio es esencial para la ejecución de la misión o es solo una de las múltiples maneras en que puede realizarse una función concreta (por ejemplo, por redundancia);
- si hay múltiples evaluaciones de garantía relacionadas con distintos aspectos de un producto, sistema o servicio concreto.

Bibliografía

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

[b-ISO 10393] ISO 10393:2013, *Consumer product recall – Guidelines for suppliers.*

[b-ISO 28598-1] ISO 28598-1:2017, *Acceptance sampling procedures based on the allocation of priorities principle (APP) – Part 1: Guidelines for the APP approach.*

[b-ISO 31000] ISO 31000:2018, *Risk management – Guidelines*. Disponible [consultado el 18-07-2022] en: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

[b-ISO/CEI 2382] ISO/CEI 2382:2015, *Information technology – Vocabulary*.

[b-ISO/CEI 14888-1] ISO/CEI 14888-1:2008, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General.*

[b-ISO/CEI/IEEE 15288] ISO/CEI/IEEE 15288:2015, *Systems and software engineering – System life cycle processes*.

[b-ISO/CEI 15408(todas las partes)] ISO/CEI 15408, *Information technology – Security techniques – Evaluation criteria for IT security*

[b-ISO/CEI/IEEE 24765] ISO/CEI/IEEE 24765:2017, *Systems and software engineering – Vocabulary*.

[b-ISO/CEI 25010] ISO/CEI 25010:2011, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*.

[b-ISO/CEI 27000] ISO/CEI 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/CEI 27001] ISO/CEI 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/CEI 27005] ISO/CEI 27005:2018, *Information technology – Security techniques – Information security risk management*.

[b-ISO/PAS 19450] Especificación Disponible al Público ISO/PAS 19450:2015, *Automation systems and integration – Object-process methodology*.

[b-ISO/TS 21089] Especificación técnica ISO/TS 21089:2018, *Health informatics – Trusted end-to-end information flows.*

[b-ISO/TS 21719-2] Especificación técnica ISO/TS 21719-2:2018, *Electronic fee collection – Personalization of on-board equipment (OBE) Part 2: Using dedicated short-range communication*.

[b-ISO/TS 22318] Especificación técnica ISO/TS 22318:2021, *Security and resilience – Business continuity management systems – Guidelines for supply chain continuity management*.

[b-ISA/CEI 62443] ISA/CEI 62443 (todas las partes) [series de normas de ciberseguridad en los sistemas de automatización y control].

[b-GSMA FS.13] Asociación GSM (2022). *Network equipment security assurance scheme – Overview*, Documento oficial FS.13, versión 2.1. Londres: Asociación GSM. 29 págs. Disponible [consultado el 17-07-2022] en: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.13-v2.1.pdf.

[b-GSMA FS.14] Asociación GSM (2022). *Network equipment security assurance scheme –Security test laboratory accreditation*, Documento oficial FS.14, versión 2.1. Londres: Asociación GSM. 15 págs. Disponible [consultado el 17-07-2022] en: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.14-v2.1.pdf.

[b-GSMA FS.15] Asociación GSM (2022). *Network equipment security assurance scheme – Development and lifecycle assessment methodology*, Documento oficial FS.15, versión 2.1. Londres: Asociación GSM. 33 págs. Disponible [consultado el 17-07-2022] en: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.15-v2.1.pdf.

[b-GSMA FS.16] Asociación GSM (2022). *Network equipment security assurance scheme – Development and lifecycle security requirements*, Documento oficial FS.16, versión 2.1. Londres: Asociación GSM. 22 págs. Disponible [consultado el 17-07-2022] en: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.16-v2.1.pdf.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) protocol – Version 1.2*.

[b-IETF RFC 6733] IETF RFC 6733 (2012), *Diameter base protocol*.

[b-3GPP TS 33.501] Especificación técnica 3GPP TS 33.501 V17.6.0 (2022), *Security architecture and procedures for 5G system*.

[b-3GPP TS 33.511] Especificación técnica 3GPP TS 33.511 V17.1.0 (2022), *Security assurance specification (SCAS) for the next generation node B (gNodeB) network product class*.

[b-3GPP TS 33.512] Especificación técnica 3GPP TS 33.512 V17.3.0 (2022), *5G security assurance specification (SCAS); Access and mobility management function (AMF)*.

[b-3GPP TS 33.513] Especificación técnica 3GPP TS 33.513 V17.0.0 (2022), *5G security assurance specification (SCAS); User plane function (UPF)*.

[b-3GPP TS 33.514] Especificación técnica 3GPP TS 33.514 V17.0.0 (2022), *5G security assurance specification (SCAS) for the unified data management (UDM) network product class*.

[b-3GPP TS 33.515] Especificación técnica 3GPP TS33.515 V17.0.0 (2022), *5G security assurance specification (SCAS) for the session management function (SMF) network product class*.

[b-3GPP TS 33.516] Especificación técnica 3PGP TS33.516 V17.0.0 (2022), *5G security assurance specification (SCAS) for the authentication server function (AUSF) network product class*.

[b-3GPP TS 33.517] Especificación técnica 3GPP TS33.517 V17.0.0 (2022), *5G security assurance specification (SCAS) for the security edge protection proxy (SEPP) network product class*.

[b-3GPP TS 33.518] Especificación técnica 3GPP TS33.518 V17.0.0 (2022), *5G security assurance specification (SCAS) for the network repository function (NRF) network product class*.

[b-3GPP TS 33.519] Especificación técnica 3GPP TS33.519 V17.0.0 (2022), *5G security assurance specification (SCAS) for the network exposure function (NEF) network product class*.

[b-BSI 10754-1] BS 10754-1:2018, *Information technology. Systems trustworthiness – Governance and management specification*.

[b-BSIMM] Instituto Británico de Normas (2021). *Building security in maturity model*, BSIMM 12. Londres: Instituto Británico de Normas.

[b-NIST FICIC] NIST (2018). *Framework for improving critical infrastructure cybersecurity*, Versión 1.1. Gaithersburg, MD: Instituto Nacional de Normas y Tecnología. 48 págs. Disponible [consultado el 18-07-2022] en: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[b-NIST SP800-30] Joint Task Force Transformation Initiative (2012). *Guide for conducting risk assessments,* Publicación especial del Instituto Nacional de Normas y Tecnología, NIST SP800-30 Rev.1. Gaithersburg, MD: Instituto Nacional de Normas y Tecnología. 95 págs. Disponible [consultado el 18-07-2022] en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[b-NIST SP 800-53] Instituto Nacional de Normas y Tecnología SP 800-53 Rev 5 2020, *Security and privacy controls for information systems and organization*s.

[b-NIST SP800-160v1] Ross, R., McEvilley, M., Carrier Oren, J. (2018). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems – Volume 1*, Publicación especial del Instituto Nacional de Normas y Tecnología, NIST SP800-160v1. Gaithersburg, MD: Instituto Nacional de Normas y Tecnología. 243 págs. Disponible [consultado el 18-07-2022] en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.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, 2022