Unión Internacional de Telecomunicaciones

# UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

# X.1361

(09/2018)

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

Aplicaciones y servicios con seguridad (2) – Seguridad en la Internet de las cosas (IoT)

## Marco de seguridad para la Internet de las cosas basado en el modelo de pasarela

Recomendación UIT-T X.1361

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 | X.1140–X.1149 |
| Protocolos de seguridad | X.1150–X.1159 |
| Seguridad en las comunicaciones punto a punto | X.1160–X.1169 |
| Seguridad de la identidad en las redes | X.1170–X.1179 |
| Seguridad en la TVIP | X.1180–X.1199 |
| SEGURIDAD EN EL CIBERESPACIO | |
| Ciberseguridad | X.1200–X.1229 |
| Lucha contra el correo basura | X.1230–X.1249 |
| Gestión de identidades | X.1250–X.1279 |
| APLICACIONES Y SERVICIOS CON SEGURIDAD (2) | |
| Comunicaciones de emergencia | X.1300–X.1309 |
| Seguridad en las redes de sensores ubicuos | X.1310–X.1339 |
| Recomendaciones relacionadas con la PKI | X.1340–X.1349 |
| **Seguridad en la Internet de las cosas (IoT)** | **X.1360–X.1369** |
| Seguridad en los sistema de transporte inteligente (ITS) | X.1370–X.1379 |
| INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD | |
| Aspectos generales de la ciberseguridad | X.1500–X.1519 |
| Intercambio de estados/vulnerabilidad | X.1520–X.1539 |
| Intercambio de eventos/incidentes/heurística | X.1540–X.1549 |
| Intercambio de políticas | X.1550–X.1559 |
| Petición de heurística e información | X.1560–X.1569 |
| Identificación y descubrimiento | X.1570–X.1579 |
| Intercambio asegurado | X.1580–X.1589 |
| SEGURIDAD DE LA COMPUTACIÓN EN NUBE | |
| Visión general de la seguridad de la computación en nube | X.1600–X.1601 |
| Diseño de la seguridad de la computación en nube | X.1602–X.1639 |
| Prácticas óptimas y directrices en materia de seguridad de la computación en nube | X.1640–X.1659 |
| Aplicación práctica de la seguridad de la computación en nube | X.1660–X.1679 |
| Otras cuestiones de seguridad de la computación en nube | X.1680–X.1699 |

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

# Recomendación UIT-T X.1361

## Marco de seguridad para la Internet de las cosas basado en el modelo de pasarela


**Resumen**

En la Recomendación UIT-T X.1361 se describe un marco de seguridad para la Internet de las cosas (IoT) utilizando pasarelas de seguridad. La Internet de las cosas (IoT) es la infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) sobre la base de tecnologías de la información y comunicación compatibles existentes o en fase de desarrollo.

En la presente Recomendación se analizan las amenazas y los problemas de seguridad en un entorno de Internet de las cosas y se describen las capacidades con las que se podrían abordar y reducir esas amenazas y resolver esos problemas. Se facilita una metodología marco para determinar qué capacidades de seguridad se necesitan para abordar y reducir esos problemas y amenazas en la Internet de las cosas.



**Historia**

| Edición | Recomendación | Aprobación | Comisión de Estudio | ID único* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1361 | 2018-09-07 | 17 | 11.1002/1000/13607 |

**Palabras clave**

Internet de las cosas, marco de seguridad, requisitos de seguridad


* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

## PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

## NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

## PROPIEDAD INTELECTUAL

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

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

## ÍNDICE

**Página**

# Recomendación UIT-T X.1361

## Marco de seguridad para la Internet de las cosas basado en el modelo de pasarela

### 1 Alcance

En la presente Recomendación se describe un marco de seguridad para la Internet de las cosas (IoT) utilizando pasarelas de seguridad.

También se analizan los problemas y amenazas de seguridad en un entorno de Internet de las cosas y se describen las capacidades de seguridad necesarias para abordar y reducir esos problemas y amenazas. Se facilita una metodología marco para determinar qué capacidades de seguridad se necesitan para abordar y reducir esos problemas y amenazas en la Internet de las cosas.

La presente Recomendación se centra en las capacidades de seguridad IoT que se obtienen al utilizar pasarelas de seguridad y en ella se estudia el modelo de referencia descrito en [b-UIT-T Y.4401], centrando la atención en cuestiones técnicas y no de gestión.

### 2 Referencias

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

[UIT-T Y.4100] Recomendación UIT-T Y.4100/Y.2066 (2014), *Requisitos comunes de la Internet de las cosas.*

### 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 ataque** [b-ISO13491-1]: Intento realizado por un adversario en el dispositivo para obtener o modificar información sensible o un servicio que no está autorizados a obtener o modificar.

**3.1.2 autentificación** [b-NIST-SP-800-53]: Verificación de la identidad de un usuario, proceso o dispositivo, que suele ser condición necesaria para acceder a recursos de un sistema de información.

**3.1.3 capacidad** [b-ISO 19440]: Concepto que representa la reunión de características de capacidad (expresadas como atributos de capacidad) de un recurso (su capacidad ofrecida) o de una actividad empresarial (su capacidad requerida).

NOTA – Se pueden agregar capacidades.

**3.1.4 contexto** [UIT-T X.1252]: Entorno con condiciones de contorno definidas en las que existen e interactúan entidades.

**3.1.5 algoritmo criptográfico** [b-ISO/IEC 19790]: Procedimiento informático bien definido que toma insumos variables, que pueden incluir claves criptográficas, y produce un resultado.

**3.1.6 número aleatorio de calidad criptográfica** [b-UIT-T X.667]: Número aleatorio o número seudoaleatorio generado por un mecanismo que garantiza una separación suficiente de valores generados repetidamente para que sean aceptables para su uso en criptografía (y que se utilizan efectivamente).

**3.1.7 criptografía** [b-UIT-T X.800]: Disciplina que abarca los principios, medios y métodos para la transformación de los datos con el fin de esconder su contenido de información, impedir su modificación no detectada y/o su uso no autorizado.

NOTA – La criptografía determina los métodos utilizados en el cifrado y descifrado. Un ataque a los principios, medios y métodos criptográficos es criptoanálisis.

**3.1.8 criptosistema** [b-ISO 11568-1]: Conjunto de primitivos criptográficos utilizados para proporcionar servicios de seguridad de la información.

**3.1.9 dispositivo** [b-UIT-T Y.4000]: En el contexto de Internet de los objetos se trata de una pieza de equipo con las capacidades obligatorias de comunicación y las capacidades opcionales de detección, de accionamiento y de adquisición, almacenamiento y procesamiento de datos.

**3.1.10 gestión de identidad** [b-UIT-T X.1250]: Conjunto de funciones y capacidades (por ejemplo, administración, gestión y mantenimiento, descubrimiento, intercambios de comunicación, correlación y vinculación, cumplimiento de una política, autentificación y asertos) que se utilizan para:

– garantizar la información de identidad (por ejemplo, identificadores, credenciales, atributos);

– garantizar la identidad de una entidad (por ejemplo, usuarios/abonados, grupos, dispositivos de usuario, organizaciones, proveedores de red y servicios, elementos y objetos de red, y objetos virtuales); y

– apoyar aplicaciones de negocios y de seguridad.

**3.1.11 Internet de las cosas (IoT)** [b-UIT-T Y.4000]: Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras.

NOTA 1 – Gracias a la identificación, la adquisición y el procesamiento de datos y a las capacidades de comunicación, IoT hace pleno uso de los objetos para ofrecer servicios a todo tipo de aplicaciones, garantizando a su vez el cumplimiento íntegro de los requisitos de seguridad y privacidad.

NOTA 2 – Desde una perspectiva más amplia, IoT puede considerarse una noción con repercusiones tecnológicas y sociales.

**3.1.12 detección de intrusión** [b-ISO/CEI 27039]: Proceso formal de detección de intrusión, caracterizado generalmente por una recopilación de conocimientos sobre pautas de utilización anormales, y de las vulnerabilidades aprovechadas, y del modo en que se han utilizado, para presentar información sobre cuándo y cómo se produjo la intrusión.

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

**3.1.14 prevención de intrusiones** [b-ISO/CEI 27033-1]: Proceso formal de respuesta activa destinado a prevenir intrusiones.

**3.1.15 sistema de prevención de intrusiones** [b-ISO/CEI 27039]: Variante de sistema de detección de intrusión diseñada especialmente para ofrecer una capacidad de respuesta activa.

**3.1.16 gestión de claves** [b-UIT-T X.800]: Generación, almacenamiento, distribución, supresión, archivo y aplicación de claves de acuerdo con una política de seguridad.

**3.1.17 criptografía ligera** [b-ISO/CEI 29192-1]: Un algoritmo criptográfico realizado especialmente para ser aplicado en entornos limitados.

**3.1.18 software maligno** [b-ISO/CEI 27033-1]: Software maligno diseñado específicamente para dañar o interrumpir un sistema atacando su confidencialidad, integridad y/o disponibilidad.

NOTA – Los virus y los troyanos son ejemplos de software maligno.

**3.1.19 monitorización de red** [b-ISO/CEI 27033-1]: Proceso de observar y revisar continuamente los datos registrados en operaciones y actividades de red, incluidos ficheros cronológico de auditoría y alertas y análisis afines.

**3.1.20 información de identificación personal (IIP)** [b-ISO/CEI 29100]: Toda información que a) puede utilizarse para identificar el titular de la información de identificación personal (IIP) con quien está relacionada esa información, o b) está o puede estar relacionada directa o indirectamente con el titular de la IIP.

NOTA – Para determinar si un titular de IIP es identificable, se deben tener en cuenta todos los medios utilizables, razonablemente, por el interesado en la privacidad que posea los datos, o por cualquier otra parte, para identificar a esa persona física.

**3.1.21 asociación de seguridad con máscara (SAM)** [b-UIT-T X.1362]: Conjunto de parámetros específicos del protocolo de seguridad. La SAM permite definir los servicios y mecanismos necesarios para la protección del tráfico mediante encriptación con datos de máscara asociados (EAMD). La SAM guarda relación con su protocolo asociado, dependiendo de las capas de protocolo tales como la capa de transporte o la capa del protocolo Internet (IP). Dichos parámetros pueden incluir los identificadores y modos de algoritmos y los identificadores de capa a los que se aplica la EAMD, así como las claves criptográficas.

**3.1.22 sensor** [b-UIT-T Y.4105]: Dispositivo electrónico que detecta una condición física o un componente químico y transmite una señal electrónica proporcional a la característica observada.

**3.1.23 objeto** [b-UIT-T Y.4000]: En el contexto de Internet de los objetos se trata de un objeto del mundo físico (objetos físicos) o del mundo de la información (objetos virtuales) que se puede identificar e integrar en las redes de comunicaciones.

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

**3.1.25 vulnerabilidad** [b-ISO/CEI 27000]: Debilidad de un activo o control que puede ser aprovechada por una o más amenazas.

## 3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

**3.2.1 negociación de algoritmo criptográfico**: Mecanismo para determinar el tipo de algoritmo criptográfico y la longitud de las claves criptográficas que deben utilizarse en una sesión de comunicaciones encriptada e integrada y para determinar el algoritmo criptográfico más adecuado disponible en ambos lados.

NOTA – Adaptación de [b-ISO/CEI 27033-1] y conocida como "pasarela" en la presente Recomendación.

**3.2.2 gestión de parches**: Proceso que abarca la adquisición, prueba e instalación de múltiples parches en sistemas de información.

NOTA – Puede estudiarse una capacidad de gestión de vulnerabilidad.

**3.2.3 violación de IIP**: Situación en la que se procesa información de identificación personal incumpliendo uno o más requisitos de protección de IIP importantes.

**3.2.4 modelo de preferencia de privacidad**: Modelo que permite a los sitios web declarar el uso que pretenden hacer de los datos personales que recopilan para ofrecer un mayor control de la información personal que poseen.

**3.2.5 configuración segura**: Proceso por el que los dispositivos de red deberían configurarse para reducir el nivel de vulnerabilidades inherentes y prestar únicamente los servicios requeridos para desempeñar su función.

NOTA – Incorpora la eliminación o desactivación de soporte lógico y cuentas de usuario innecesarios, el cambio de cualquier contraseña predeterminada a una contraseña alternativa y segura, la activación de cortafuegos y la configuración para desactivar (bloquear) conexiones no aprobadas de forma predeterminada por defecto y la desactivación de la función de ejecución automática.

**3.2.6 pasarela de seguridad**: Punto de conexión entre redes o entre subgrupos dentro de redes o entre aplicaciones de soporte lógico dentro de diferentes dominios de seguridad destinado a proteger una red según una determinada política de seguridad particular en el entorno IoT.

**3.2.7 ataque de canal paralelo**: Ataque que se realiza utilizando información obtenida de la ejecución física de un criptosistema.

NOTA – La información sobre tiempo computacional, consumo de energía y fugas electromagnéticas puede utilizarse para penetrar al criptosistema.

**3.2.8 gestión de vulnerabilidad**: Proceso de detección, clasificación, remedio y reducción de vulnerabilidades.

## 4 Abreviaturas y acrónimos

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

DoS Negación de servicio (*denial of service*)

EAMD Encriptación con datos de máscara asociados (*encryption with associated mask data*)

IDS Sistema de detección de intrusión (*intrusion detection system*)

IP Protocolo Internet (*Internet protocol*)

IPS Sistema de prevención de intrusiones (*intrusion prevention system*)

PII Información de identificación personal (*personally identifiable information*)

## 5 Convenios

Ninguno.

## 6 Resumen

La Internet de las cosas (IoT) se define como una infraestructura mundial para la sociedad de la información que permite prestar servicios avanzados mediante la interconexión de objetos (tanto físicos como virtuales) sobre la base de tecnologías de la información y comunicación compatibles existentes o en fase de desarrollo.

Una IoT típica consta de dispositivos de borde equipados con sensores en una red de cable o inalámbrica que envía datos a través de una pasarela a una nube pública o privada. Los aspectos de la topología variarán ampliamente de una aplicación a otra. En algunos casos, por ejemplo, la pasarela puede encontrarse en el dispositivo. Los dispositivos basados en esas topologías pueden construirse desde cero para aprovechar la IoT o pueden ser dispositivos heredados con capacidades de IoT añadidas después de la puesta en funcionamiento.

## 7 Marco y arquitectura funcional

La presente Recomendación se basa en la arquitectura funcional de IoT mostrada en la Figura 1.

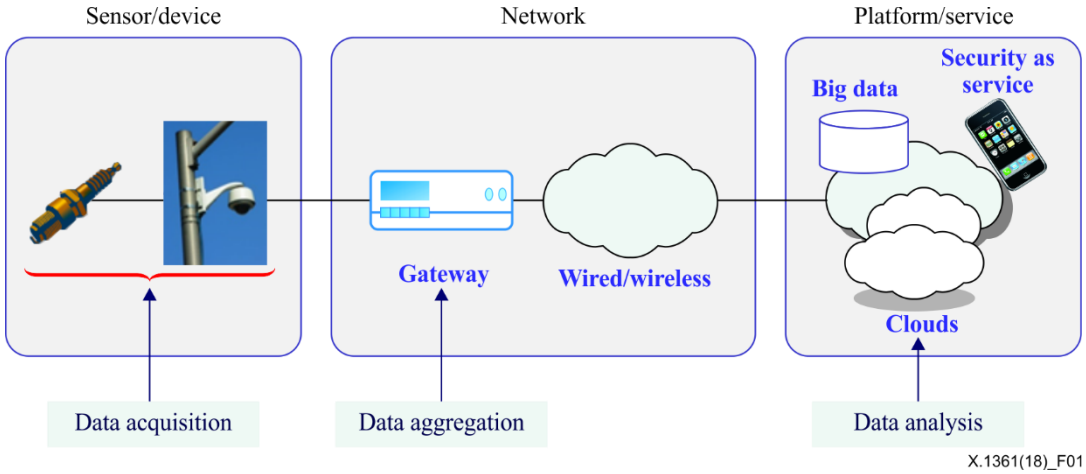


**Figura 1 – Arquitectura funcional de IoT (simplificada)**

Los datos entre el punto extremo de la IoT (sensor o dispositivo) y la pasarela pueden comunicarse a través de dos tipos de redes de comunicación: red basada en un protocolo Internet (IP) o una red no basada en IP. Se supone que la comunicación entre la pasarela y el componente de IoT en la plataforma de IoT, desplegado en un centro de datos, debería realizarse utilizando un protocolo basado en IP. Así, en el caso de una red que no sea IP, debe finalizarse la conexión de comunicación a través de esa red y restablecerse a través de una red IP en la pasarela.

La arquitectura funcional puede elaborarse como se muestra en la Figura 2.

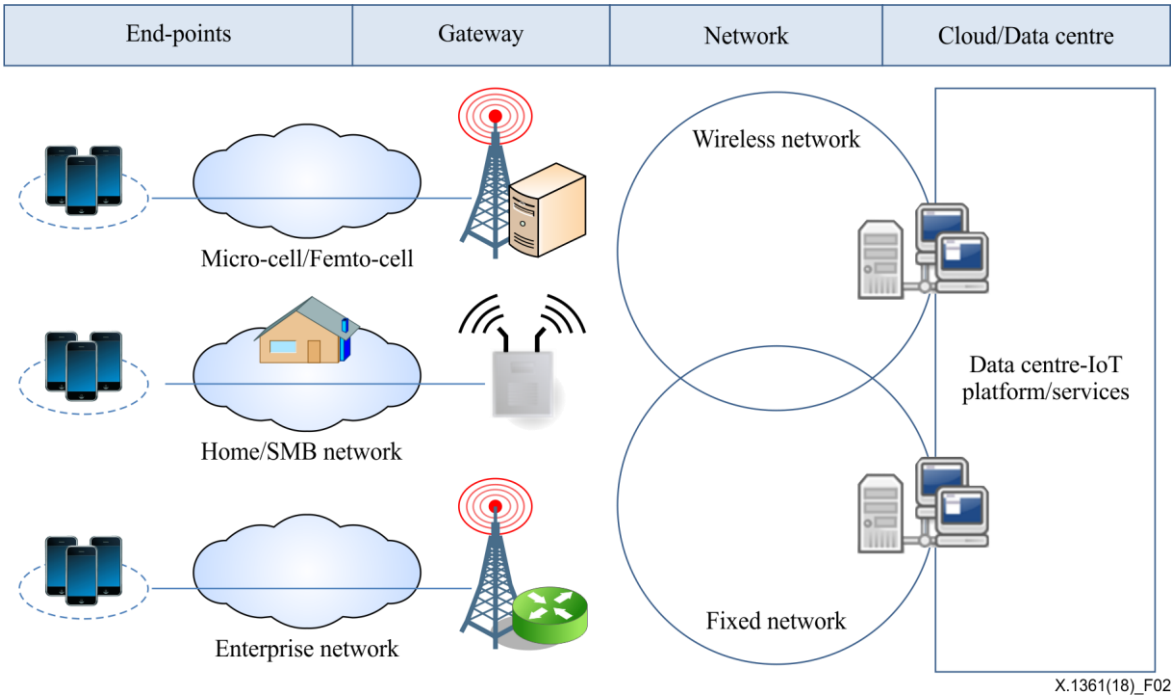


**Figura 2 – Arquitectura funcional práctica**

Por ejemplo, en un sistema de transporte inteligente, la pasarela mostrada en la Figura 2 podría actuar de pasarela móvil de vehículo para conectar una red de área (vehículo) interna y una red abierta externa.

Tendrá que haber una capacidad de cortafuego en la pasarela para controlar el tráfico destinado a terminar en el dispositivo. Algunos dispositivos de IoT tienen protocolos de transporte únicos diferentes a los protocolos IP/protocolos de control de transmisión TCP. Los protocolos patentados pueden utilizarse para controlar el modo en que los dispositivos IoT se comunican entre sí. Así, deben existir capacidades de filtrado de protocolos específicos del sector para detectar cargas útiles maliciosas que podrían esconderse en protocolos no IP.

La pasarela debería ejercer una función de filtrado de datos concretos destinados a finalizar en ese dispositivo de modo que se utilicen al máximo los recursos computacionales disponibles y limitados.

La pasarela participa como un elemento único en la arquitectura funcional. A menudo es el primer punto de seguridad fiable en un sistema IoT porque los puntos extremos son más vulnerables a la manipulación física. La pasarela desempeña un papel en la IoT que justifica su distinción como activo de seguridad especial aparte de la red. Debe tener en cuenta las limitaciones de los nodos de sensor. A menudo puede realizar algunas funciones de seguridad por cuenta de puntos extremos limitados como: gestión de claves, negociación criptográfica, prevención de intrusiones, etc.

La pasarela tendrá capacidades de seguridad muy diversas dependiendo de factores como: la potencia y las capacidades de los puntos extremos, el diseño de servicio, el diseño de red, las ubicaciones físicas y el contexto de utilización.

## 8 Amenazas de seguridad a la Internet de las cosas

### 8.1 Amenazas de seguridad a sensores/dispositivos IoT

Amenazas propias de sensor/dispositivo:

– Captura de dispositivo: Se produce cuando un dispositivo se ve afectado físicamente o cuando se pierden sus claves.

– Ataque de sumidero (*sinkhole*): Se produce cuando un dispositivo afectado atrae tráfico de comunicación para formar un agujero negro o introducir una retransmisión selectiva. En un ataque de sumidero el intruso accede al dispositivo, o introduce un dispositivo falsificado en la red, y lo utiliza para lanzar un ataque. El dispositivo atacado intenta atraer todo el tráfico de datos de los nodos vecinos basándose en la métrica de encaminamiento utilizada en el protocolo de encaminamiento. Si lo consigue, el dispositivo afectado lanza un ataque. Los ataques de sumidero son un tipo de ataque de red de capa en los que un dispositivo afectado envía información de encaminamiento falsa a sus vecinos para atraer el tráfico de red hacia él. Debido a las redes *ad hoc* y a los patrones de comunicación de muchos a uno de las redes inalámbricas en las que muchos nodos envían datos a una única estación de base, esas redes son particularmente vulnerables a los ataques de sumidero. Basándose en flujos de comunicación en una red inalámbrica, el ataque de sumidero no necesita dirigirse a todos los nodos de la red sino sólo a los cercanos a la estación de base.

– Ataque Sybil: Es un ataque en el que un dispositivo malicioso adopta de forma ilegítima múltiples identidades. La identidad adicional de un dispositivo malicioso se llama "nodo Sybil". El ataque se lanza junto con otros ataques para reducir la eficacia de los mecanismos tolerantes a fallos, como el almacenamiento distribuido, el encaminamiento multitrayecto y el mantenimiento de la topología.

– Ataque por inundación: Es una forma de ataque de negación de servicio en el que un atacante envía una sucesión de paquetes "hello" a un dispositivo objetivo para consumir los suficientes recursos para que no pueda responder a un ataque de verdad.

– Ataque de retransmisión selectiva: En este ataque, un nodo afectado filtra al azar paquetes recibidos y envía algunos de ellos al siguiente nodo. Si el nodo filtra (excluye) todos los paquetes que recibe, se llama ataque de agujero negro.

– Ataque de agujero de gusano (*wormhole attack*): Los ataques de agujero de gusano se producen cuando dos nodos atacados/maliciosos anuncian tener un trayecto muy corto entre ellos. El túnel es una ruta de datos entre dos dispositivos conectados en red que se establece a través de una infraestructura de red existente. Una red obtiene datos de otra y los transmite por un túnel a una tercera, donde los replica, con lo que puede producirse confusión en esa red. Es en ese momento cuando un ciberdelincuente puede entrar fácilmente en la red para atacar. Si se utiliza con un ataque de sumidero y un ataque Sybil, puede producirse una retransmisión selectiva o la creación de un sumidero.
– Suplantación de sensor/dispositivo: Este ataque se produce cuando un atacante se hace pasar por un sensor/dispositivo legítimo.

## 8.2 Amenazas de seguridad a pasarelas IoT

Amenazas propias de pasarela:

– Acceso no autorizado: El acceso no autorizado a una pasarela puede producir la divulgación de información confidencial, la modificación de datos, la negación de servicio o el uso ilícito de recursos. Por ejemplo, una vez que un atacante ha accedido a una pasarela, la monitorización de los datos no encriptados en ese momento puede poner en peligro nombres de usuario, contraseñas y datos de configuración segura.
– Pasarela maligna (*Rogue gateway*): Incluso si todas las pasarelas inalámbricas son seguras, los atacantes pueden desplegar fácilmente una pasarela maligna por sí solos. Por ejemplo, un empleado muy motivado puede instalar un punto de acceso inalámbrico en su oficina sin tener en cuenta cuestiones de seguridad. Ello dará al traste con muchas de las medidas de seguridad vigentes y ocasionará incluso, posiblemente, interferencias radioeléctricas con la instalación de la organización o la empresa. Un punto de acceso inalámbrico maligno también puede instalarse de forma deliberada y encubierta para facilitar un acceso fácil a la red, local o remota. El ciberdelincuente podría reemplazar un punto de acceso inalámbrico existente por uno (conocido como "gemelo malvado", *evil twin*) en el que tuviera una configuración completa y acceso de monitorización o incluso configurar un punto de acceso inalámbrico maligno con configuraciones similares pero con una relación de potencia lo suficientemente mayor como para superar la señal de punto de acceso inalámbrico legítimo. Una vez que se engaña al dispositivo legítimo para que se conecte a una pasarela maligna, puede recopilarse información confidencial de la conexión.
– Ataque de negación de servicio: El ataque de negación de servicio hace que el objetivo reduzca notablemente sus servicios o, idealmente, que los detenga del todo agotando su capacidad de computación y/o memoria. El objetivo se mantiene ocupado respondiendo al tráfico ilegítimo que los atacantes están enviando. La red de sensores inalámbrica es particularmente vulnerable a ese tipo de ataque por sus características de topología de cambio dinámico y medio abierto y por no tener una línea de defensa clara. Los ataques de negación de servicio son actualmente un problema creciente en las redes. Muchas de las técnicas de defensa elaboradas para las redes de cable fijas no pueden aplicarse a entornos de redes móviles.

## 8.3 Amenazas de seguridad a la red

Amenazas propias de red:

– Acceso no autorizado: El acceso no autorizado a una red de sensores inalámbrica puede hacer que se divulgue información confidencial, se modifiquen datos, se denieguen servicios y se utilicen ilícitamente recursos. Por ejemplo, una vez que un atacante ha accedido a una red de sensores, la monitorización de los datos no encriptados en ese momento puede afectar a nombres de usuario y contraseñas.

– Rastreo de paquetes: En el caso de redes de sensores inalámbricas que no tienen capacidades de encriptado, es muy fácil para los atacantes escuchar ilegítimamente las comunicaciones de red. Para ello necesitan una antena, herramientas de red inalámbrica normal y un rastreador de paquetes de red. Un rastreador de paquetes de red es una herramienta que establece la tarjeta de red en "modo promiscuo". Eso significa que la interfaz recibirá y procesará todo el tráfico en lugar de sólo el tráfico destinado a ella. El rastreador de red mostrará a su usuario todos los paquetes de red y los decodificará para facilitar su lectura. Todo el tráfico de texto en lenguaje claro se entiende fácilmente y pueden definirse filtros para buscar determinadas palabras clave o valores.
– *Bluejacking*: Ataque realizado en dispositivos móviles Bluetooth, como teléfonos móviles. Un atacante inicia un *bluejacking* enviando mensajes no solicitados a usuarios de dispositivos Bluetooth. Los mensajes enviados no dañan el dispositivo objetivo pero pueden inducir al usuario a responder de alguna manera o a añadir el nuevo contacto a la agenda del dispositivo.
– *Bluesnarfing*: Este tipo de ataque provoca un acceso no autorizado a información de un dispositivo inalámbrico objetivo a través de una conexión Bluetooth, a menudo teléfonos, ordenadores, portátiles y agendas digitales personales (PDA). Un ataque exitoso puede dar lugar a un acceso no autorizado a información privada y confidencial de esos dispositivos.

### 8.4 Amenazas de seguridad a plataformas/servicios

En Internet, la principal tarea de la capa de aplicación es recopilar y procesar un gran número de datos de usuario, incluida información personal de usuarios o información confidencial de diversas transacciones. El objetivo del atacante es robar, manipular o dañar los datos. Es necesario protegerlos utilizando mecanismos de protección de privacidad. Entre las amenazas de capa de aplicación encontramos: procesamiento de datos en masa, dispositivos inteligentes fuera de control, intervención humana no autorizada y dispositivos fuera de control incapaces de recuperarse de un desastre.

Amenazas propias de plataformas/servicios:

– Elaboración de perfiles: Proceso explorador utilizado para reunir información en plataformas/servicios.
– Negación de servicio: Ataque en el que la plataforma/servicio se ve superada por peticiones de servicio en masa y no puede responder a peticiones de clientes verdaderos.
– Ejecución de código arbitrario: Un ataque con el que se intenta ejecutar código malicioso en una plataforma/servicio para dañar sus recursos y lanzar luego más ataques.
– Ejecución de código malicioso: Todo guion o parte de un sistema de soporte lógico destinado a causar efectos no deseados, a la violación de la información de seguridad o de identificación personal (IIP) o a dañar un sistema. Los ejemplos típicos son virus, gusanos y troyanos.
– Elevación de privilegios: Un ataque en el que se ejecuta un código utilizando una cuenta de proceso privilegiada para elevar los privilegios del atacante.
– Inyección de lenguaje de consulta estructurado (SQL): Un ataque que aprovecha las vulnerabilidades en el código de acceso de datos y validación de entrada de una aplicación para ejecutar comandos arbitrarios que inyectan o extraen información.
– Escuchas clandestinas de red: Un ataque que captura paquetes transmitidos desde la red y lee el contenido de los datos en busca de información confidencial: contraseñas, testigos (*tokens*) de sesión o cualquier tipo de información confidencial.
– Acceso no autorizado: Un ataque por el que se obtiene acceso a una plataforma/servicio utilizando la cuenta de otra persona u otro método de acceso. Por ejemplo, cuando alguien intenta adivinar una contraseña o nombre de usuario de una cuenta que no es suya hasta conseguirlo.

– Fuerza bruta: Un ataque por el que se prueban sistemáticamente todas las claves posibles hasta encontrar la correcta.
– Ataque de diccionario de nombres de usuarios/contraseñas: Un ataque sistemático para superar los mecanismos de cifrado o autenticación que consiste en probar como contraseña todas las palabras de un diccionario.
– Uso de nombres de usuario o contraseñas por defecto/uso de contraseñas débiles: Ataque en el que se prueban nombres de usuario y contraseñas por defecto o débiles para acceder a la plataforma o a los servicios.
– Ataque de interferencia: Se produce cuando un usuario es capaz de inferir información protegida a partir de trozos de información accesibles correctamente de clasificación inferior.
– Fuga IIP: divulgación intencional o accidental de IIP en un entorno no fiable.

## 9 Requisitos de la Internet de las cosas

La presente Recomendación se basa en los requisitos de alto nivel descritos en [UIT-R Y.4100], como se explica en el Anexo A.

## 10 Capacidades de seguridad de la Internet de las cosas

### 10.1 Resumen

En la presente Recomendación solo se estudian requisitos de seguridad y se tiene en cuenta la fiabilidad y la calidad de los servicios. Se amplían las capacidades de seguridad de la IoT respecto de las descritas en [b-UIT-T Y.4401].

*Capacidades generales*

En la arquitectura de la IoT debería figurar:

– una capacidad de comunicación segura para soportar comunicaciones seguras, fiables y con protección de la privacidad;
– una capacidad de gestión de claves segura para soportar comunicaciones seguras;
– una capacidad de gestión de datos segura para proporcionar una gestión de datos segura, fiable y con protección de privacidad;
– una capacidad de autenticación para la autenticación de dispositivos;
– una capacidad de autorización (control de acceso) para autorizar dispositivos;
– una capacidad de auditoría para monitorizar el acceso a datos o los intentos de acceder a las aplicaciones de IoT de manera totalmente transparente, rastreable y reproducible, basándose en reglamentos y leyes apropiados;
– una capacidad de prestación de servicios segura para prestar servicios de modo seguro, fiable y con protección de privacidad;
– una capacidad de integración segura para integrar diferentes políticas y técnicas de seguridad relativas a la variedad de componentes funcionales IoT;
– una capacidad de implementar protocolos seguros utilizando algoritmos criptográficos normalizados y a disposición del público;
– una capacidad de implementar protocolos seguros basándose en criptografía ligera;
– una capacidad de actualización de soporte lógico segura y estructurada para actualizar módulos de soporte lógico o aplicaciones;
– una capacidad de gestión de identidades para dispositivos/sensores de IoT, pasarelas y plataformas/servicios;

– una capacidad de análisis de la vulnerabilidad;
– una capacidad de monitorizar el acceso a datos o los intentos de acceder a las aplicaciones de IoT de manera totalmente transparente, rastreable y reproducible;
– una capacidad de seguridad de soporte físico (por ejemplo, módulo de plataforma de confianza) para evitar los riesgos de seguridad física que acompañan la virtualización de pasarela y red;
– una capacidad de encaminamiento multitrayecto para evitar ataques de retransmisión selectiva;
– una capacidad de protección IIP contra ataques IIP en todo el ciclo de vida IIP;
– una capacidad de configuración segura;
– una capacidad que utiliza criptografía ligera; y
– una capacidad de encriptación simple con encriptación con datos de máscara asociados (EAMD) [b-UIT-T X.1362] para comunicar con otras entidades, incluida la pasarela.

*Algoritmo criptográfico relativo a capacidades*

En la arquitectura de la IoT debería figurar:
– una capacidad de producción de un número aleatorio de calidad criptográfica para soportar la gestión de claves [b-IETF RFC 4086];
– una capacidad de actualización periódica de las claves criptográficas necesarias para trenes de radiodifusión; y
– una capacidad de utilizar algoritmos criptográficos normalizados.

*Capacidades relativas a contexto*

En la arquitectura de la IoT debería figurar:
– una capacidad de resistir ataques de canal paralelo;
– una capacidad de soportar prácticas de codificación segura para que se aplique una validación rigurosa de datos en sistemas y servicios, aplicaciones de bases de datos y servicios web; y
– una capacidad de realizar una evaluación del riesgo planificado para determinar riesgos en contextos operativos.

### 10.2 Capacidades de seguridad de sensores/dispositivos

Los sensores/dispositivos IoT deberían incorporar:
– una capacidad de gestión de claves;
– una capacidad de negociación de algoritmo criptográfico;
– una capacidad de encriptación de datos y en algunos casos de datos de plano de señalización, control y gestión para reducir los problemas de seguridad relativos a la confidencialidad de los datos transmitidos por redes inalámbricas;
– una capacidad de integridad de datos para datos transmitidos por redes inalámbricas utilizando programas de protección de integridad adecuados que ofrecen garantías de que los datos de usuario o de señalización, control o gestión no han sido manipulados ni alterados;
– una capacidad de autenticación del origen de los datos o de las identidades de los sensores/dispositivos de IoT y de los administradores y personal de mantenimiento de esas redes;
– una capacidad de gestión de parches, incluidos módulos de soporte lógico seguros de actualización y transformación;
– capacidad de implementar protocolos seguros sobre la base de criptografía ligera;

– una capacidad de control de acceso para que sólo los usuarios o dispositivos autorizados pueden acceder a elementos de red, información almacenada, flujos de información, servicios y aplicaciones;
– una capacidad de prevención y/o detección de manipulación;
– una capacidad de producir números aleatorios de calidad criptográfica para soportar la gestión de claves;
– una capacidad de resistir a ataques de canal paralelo;
– una capacidad de protección y detección de software maligno;
– una capacidad de protección IIP frente a violaciones IIP; y

Los dispositivos IoT deberían incluir:

– una capacidad de verificar la autenticidad e integridad del soporte lógico en un dispositivo utilizando firmas digitales generadas criptográficamente [b-ISO/CEI 9796-3];
– una capacidad de cortafuego, detección de intrusión, protección contra intruso o inspección detallada de paquetes para controlar el tráfico destinado a terminar en un dispositivo; y
– una capacidad de realizar configuraciones seguras.

### 10.3 Capacidades de seguridad de pasarelas

La pasarela debería incorporar:

– una capacidad de sistema de detección de intrusión (IDS)/de sistema de prevención de intrusiones (IPS);
– una capacidad de gestión de claves;
– una capacidad de realizar una configuración segura;
– una capacidad de negociación de algoritmo criptográfico;
– una capacidad de encriptar datos y, en algunos casos, datos de plano de señalización, control y gestión con dispositivos y componentes IoT en el centro de datos para reducir los problemas de seguridad relativos a la confidencialidad de los datos transmitidos por redes inalámbricas;
– una capacidad de integridad de los datos transmitidos por redes inalámbricas utilizando programas de protección de la integridad adecuados para garantizar que los datos de usuario o de señalización, control o gestión no han sido manipulados ni alterados;
– una capacidad de disponibilidad para gestionar ataques de negación de servicio, desde el uso de técnicas de codificación de fuente seguras, pruebas de análisis de código de fuente y pruebas de vulnerabilidad hasta el uso de IDS/IPS basados en red o huésped;
– una capacidad de autenticación del origen de los datos o de las identidades de los sensores/dispositivos de IoT y de los administradores y personal de mantenimiento de esas redes;
– una capacidad de control de acceso para que sólo los usuarios o dispositivos autorizados pueden acceder a elementos de red, información almacenada, flujos de información, servicios y aplicaciones; y
– una capacidad de responsabilización de dispositivo IoT para que toda infracción en materia de políticas pueda rastrearse hasta un dispositivo en concreto.

La pasarela es necesaria para soportar una capacidad de actualizar módulos de soporte lógico seguros.

### 10.4 Capacidades de seguridad de la red

Las capacidades de seguridad de la red están fuera del ámbito de la presente Recomendación.

NOTA – Podrían utilizarse capacidades de seguridad para cumplir las dimensiones de seguridad descritas en [b-UIT-T X.805].

## 10.5 Capacidades de seguridad de plataformas/servicios

La plataforma/servicio debería incorporar:

– una capacidad de proteger una credencial de operaciones criptográficas, que es un grupo de datos presentados como prueba de títulos y/o identidades alegados;
– una capacidad de modificar nombres de usuarios y contraseñas por defecto durante la configuración inicial;
– una capacidad de aplicar contraseñas seguras y políticas de control de acceso granular;
– una capacidad de poner a disposición puertos no necesarios;
– una capacidad de soportar una configuración segura, por ejemplo, para eliminar servicios y soporte lógico innecesario;
– una capacidad de protección ante infecciones de software maligno utilizando soporte lógico de protección ante esas amenazas;
– una capacidad de aplicar políticas de gestión de parches;
– una capacidad de gestionar vulnerabilidades;
– una capacidad de actualizar módulos y aplicaciones de soporte lógico seguros;
– una capacidad de gestionar claves para transferir mensajes de forma segura entre una pasarela y una plataforma/servicio;
– una capacidad de negociación de algoritmo criptográfico para establecer una tunelización segura entre la pasarela y la plataforma/servicio en caso de que se necesite una transferencia de mensajes segura entre ambas;
– una capacidad de disponibilidad para gestionar ataques de negación de servicio;
– una capacidad de monitorizar la red;
– una capacidad de proteger IIP en reposo;
– una capacidad de nivel de seguridad de aplicación para evitar los ataques y amenazas de nivel de aplicación descritos en la cláusula 8.4; y
– una capacidad de ofrecer apoyo para reducir los ataques de inferencia.

# Anexo A

## Requisitos de seguridad y privacidad descritos en UIT-T Y.4100/Y.2066

(Este anexo forma parte integrante de la presente Recomendación.)

Los requisitos de seguridad y protección de la privacidad hacen referencia a los requisitos funcionales durante la captura, almacenamiento, transferencia, agregación y procesamiento de los datos de objetos, y a la prestación de servicios que implican objetos. Esos requisitos están relacionados con todos los actores IoT.

En el presente Anexo se presentan los requisitos de seguridad y privacidad de alto nivel descritos en el Anexo A de [UIT-T Y.4100] y los términos entre paréntesis que figuran en las siguientes cláusulas se refieren al elemento del Anexo A de [UIT-T Y.4100].

### A.1 Seguridad de comunicación

Se requiere una capacidad de comunicación segura, fiable y con protección de la privacidad para prohibir el acceso no autorizado al contenido de datos, garantizar la integridad de los datos y proteger su contenido relativo a la privacidad durante la transmisión o transferencia de datos en IoT [SP1].

### A.2 Seguridad de gestión de datos

Se requiere una capacidad de gestión de datos segura, fiable y con protección de la privacidad para prohibir el acceso no autorizado al contenido de datos, garantizar la integridad de los datos y proteger su contenido relativo a la privacidad al almacenar o procesar datos en IoT [SP2].

### A.3 Seguridad de prestación de servicio

Se requiere una capacidad de prestación de servicio segura, fiable y con protección de la privacidad para prohibir el acceso no autorizado al servicio y a la prestación de servicio fraudulento y proteger la información de privacidad relativa a los usuarios IoT [SP3].

### A.4 Integración de técnicas y políticas de seguridad

Se requiere una capacidad de integrar diferentes políticas y técnicas de seguridad, a fin de garantizar un control de seguridad coherente sobre la variedad de dispositivos y redes de usuarios en la IoT [SP4].

### A.5 Autenticación y autorización mutua

Antes de que un dispositivo (o un usuario IoT) pueda acceder a la IoT, debe realizarse una autenticación y autorización mutua entre el dispositivo (o el usuario IoT) y la IoT de acuerdo con las políticas de seguridad predefinidas [SP5].

### A.6 Auditoría de seguridad

Se requiere que la auditoría de seguridad esté soportada en IoT. Todo acceso a los datos o intento de acceso a aplicaciones de IoT debe ser totalmente transparente, rastreable y reproducible de conformidad con reglamentos y leyes apropiados. En particular, la IoT debe soportar la auditoría de seguridad para el acceso a la aplicación, procesamiento, almacenamiento y transmisión de datos [SP6].

# Apéndice I

# Capacidades de seguridad y privacidad descritas en UIT-T Y.4401/Y.2068

(Este apéndice no forma parte integrante de la presente Recomendación.)

En el presente Apéndice se muestran las capacidades de privacidad y seguridad de alto nivel descritas en [b-UIT-T Y.4401] y los términos entre paréntesis de las siguientes cláusulas se refieren al elemento particular de [UIT-T Y.4401].

## I.1 Capacidad de seguridad de comunicación

La capacidad de seguridad de comunicación implica la habilidad de soportar comunicaciones seguras, fiables y con protección de la privacidad [C-7-1].

## I.2 Capacidad de seguridad de gestión de datos

La capacidad de seguridad de gestión de datos implica la habilidad de proporcionar una gestión de datos segura, fiable y con protección de la privacidad [C-7-2].

## I.3 Capacidad de seguridad de prestación de servicio

La capacidad de seguridad en la prestación de servicios implica la habilidad de ofrecer una prestación de servicios segura, fiable y con protección de la privacidad [C-7-3].

## I.4 Capacidad de integración de seguridad

La capacidad de integración de seguridad implica la habilidad de integrar diferentes políticas y técnicas de seguridad relacionadas con la variedad de componentes funcionales de la IoT [C-7-4].

## I.5 Capacidad de autenticación y autorización mutua

La capacidad de autenticación y autorización mutua implica la habilidad de autenticación y autorización de todos los dispositivos antes de que accedan a la IoT basándose en políticas de seguridad predefinidas [C-7-5].

## I.6 Capacidad de auditoría de seguridad

La capacidad de auditoría de seguridad implica la habilidad de monitorizar el acceso a datos o los intentos de acceder a aplicaciones de IoT de manera totalmente transparente, rastreable y reproducible de conformidad con reglamentos y leyes [C-7-6].

NOTA – Entre las capacidades de seguridad y protección de la privacidad hay también la habilidad de hacer frente a problemas de protección de privacidad y seguridad en operaciones en diferentes dominios.

# Apéndice II

## Panorama de aplicación del marco funcional IoT que amplía la arquitectura funcional de red de próxima generación descrita en UIT-T Y.4401/Y.2068

(Este apéndice no forma parte integrante de la presente Recomendación.)

En la Figura II.1 se muestra un panorama de aplicación del marco funcional IoT que amplía las entidades funcionales descritas en [b-UIT-T Y.4401] sobre arquitectura funcional de red de próxima generación (NGN), relacionada con el marco funcional de seguridad en la presente Recomendación. En la presente Recomendación se muestran las capacidades de la capa de soporte de servicio y la capa de dispositivo en la Figura 7-2 de [b-UIT-T Y.4401].

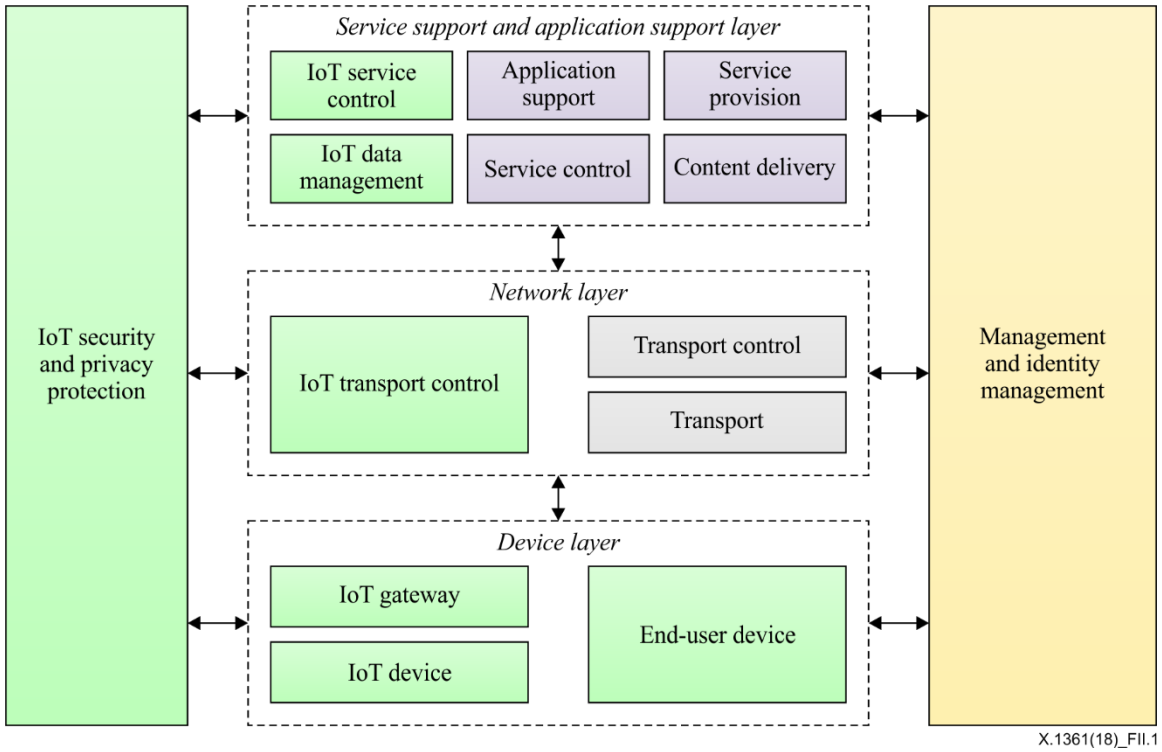


**Figura II.1 – Panorama de aplicación del marco funcional IoT que amplía la arquitectura funcional NGN**

# Bibliografía


[b-UIT-T X.667] Recomendación UIT-T X.667 (2012), *Tecnología de la información – Procedimientos para el funcionamiento de las autoridades de registro de los identificadores de objeto: Generación de identificadores únicos universales y su utilización como componentes de identificador de objetos.*

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

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

[b-UIT-T X.1250] Recomendación UIT-T X.1250 (2009), *Capacidades básicas para una interoperabilidad y una gestión mejoradas de la identidad global*.

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones sobre gestión de identidad de referencia*.

[b-UIT-T X.1311] Recomendación UIT-T X.1311 (2011) | ISO/CEI 29180:2012, *Tecnología de la información – Marco de seguridad para red de sensores ubicuos*.

[b-UIT-T X.1362] Recomendación UIT-T X.1362 (2017), *Procedimiento de encriptación simple para la Internet de las cosas (IoT)*.

[b-UIT-T Y.4000] Recomendación UIT-T Y.4000/Y.2060 (2012), *Visión general de la Internet de las cosas*.

[b-UIT-T Y.4050] Recomendación UIT-T Y.4050/Y.2221 (2010), *Términos y definiciones para la Internet de las cosas*.

[b-UIT-T Y.4105] Recomendación UIT-T Y.4105/Y.2221 (2010), *Requisitos para el soporte de los servicios y aplicaciones de redes de sensores ubicuos en el entorno de las redes de próxima generación*.

[b-UIT-T Y.4113] Recomendación UIT-T Y.4113 (2016), *Requisitos de red para la Internet de las cosas*.

[b-UIT-T Y.4400] Recomendación UIT-T Y.4400/Y.2063 (2012), *Marco de la web de las cosas*.

[b-UIT-T Y.4401] Recomendación UIT-T Y.4401/Y.2068 (2015), *Functional framework and capabilities of the Internet of things*.

[b-IETF RFC 4086] IETF RFC 4086 (2005), *Randomness Requirements for Security*.

[b-ISO 11568-1] ISO 11568-1:2005, *Banking – Key management (retail) – Part 1: Principles*.

[b-ISO 13491-1] ISO 13491-1:2016, *Financial services – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods*.

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

[b-ISO/IEC 9796-3] ISO/IEC 9796-3:2006, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms*.

[b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.

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

[b-ISO/CEI 27033-1] ISO/CEI 27033-1:2015, *Information technology –Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/CEI 27033-6] ISO/CEI 27033-6:2016, *Information technology – Security techniques – Network security – Part 6: Securing wireless IP network access*.

[b-ISO/CEI 27039] ISO/CEI 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS)*.

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

[b-ISO/IEC 29192-1] ISO/IEC 29192-1:2012, *Information technology – Security techniques – Lightweight cryptography – Part 1: General*.

[b-NIST SP 800-53] NIST Special Publication 800-53 (2013), *Security and Privacy Controls for Federal Information Systems and Organizations*.

[b-ZT] Zhang Li, Tong Xin (2013), *Threat Modeling and Countermeasures Study for the Internet of Things, Journal of Convergence Information Technology (JCIT), Vol. 8, No. 5, marzo*.

## 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, 2019

Impreso en Suiza
Ginebra,