|  |  |
| --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **Unión Internacional de Telecomunicaciones****Oficina de Normalización de las Telecomunicaciones** |
|  |  | Ginebra, 23 de abril de 224 |
| Ref.: | **Circular TSB 195**CE 17/XY | - A las Administraciones de los Estados Miembros de la Unión**Copia:**- A los Miembros del Sector del UIT‑T;- A los Asociados de la Comisión de Estudio 17;- Al Presidente y a los Vicepresidentes de laComisión de Estudio 17 del UIT-T;- Al Director de la Oficina de Desarrollo de las Telecomunicaciones;- Al Director de la Oficina de Radiocomunicaciones |
| Tel.: | +41 22 730 6206 |
| Fax: | +41 22 730 5853 |
| Correo-e: | tsbsg17@itu.int |
| **Asunto:** | **Consulta a los Estados Miembros sobre los proyectos de nueva Recomendación determinada** **UIT‑T X.1237 (X.tsfpp), X.1283 (X.gpwd), X.1353 (X.ztd-iot), X.1354 (X.sc-iot), X.1384 (X.itssec-5), X.1471 (X.websec-7), X.1819 (X.5Gsec-netec) y X.1820 (X.5Gsec-srocvs), propuestos para aprobación en la reunión de la Comisión de Estudio 17 del UIT-T (Ginebra, 2-6 de septiembre de 2024)** |

Muy Señora mía/Muy Señor mío,

1 La Comisión de Estudio 17 (Seguridad) tiene previsto aplicar el procedimiento de aprobación tradicional descrito en la Sección 9 de la Resolución 1 (Rev. Ginebra, 2022) de la AMNT a efectos de la aprobación de los proyectos de Recomendación indicados en el asunto durante la próxima reunión que tendrá lugar en Ginebra del 2 al 6 de septiembre de 2024. El orden del día y toda la información pertinente sobre la reunión de la Comisión de Estudio 17 del UIT-T figurarán en la Carta Colectiva [8/17](https://www.itu.int/md/T22-SG17-COL-0008/en).

2 El **Anexo 1** contiene los títulos, resúmenes y ubicaciones de los proyectos de Recomendación UIT-T propuestos para aprobación.

NOTA 1 de la TSB – A excepción del proyecto de nueva Recomendación X.1820 (X.5Gsec-srocvs), no se ha presentado la justificación con arreglo a la UIT-T A.5 de los textos determinados.

NOTA 2 DE LA TSB– En la fecha de la presente Circular, la TSB no había recibido ninguna declaración de DPI en relación con este proyecto de texto t. Para obtener información actualizada, se invita a los miembros a consultar la base de datos de DPI: [www.itu.int/ipr/](http://www.itu.int/ipr/).

3 Con esta Circular se inicia la consulta oficial con los Estados Miembros de la UIT sobre si estos textos pueden considerarse para aprobación en la próxima reunión, de acuerdo con la cláusula 9.4 de la Resolución 1. Se ruega a los Estados Miembros que cumplimenten y devuelvan el formulario incluido el Anexo 2 antes de las 23.59 horas UTC del **21 de agosto de 2024.**

4 Si al menos el 70% de las respuestas de los Estados Miembros es favorable a que se considere la aprobación de este proyecto de Recomendación, se dedicará una sesión plenaria a la aplicación del procedimiento de aprobación. Los Estados Miembros que no otorguen autoridad para proceder deben informar al Director de la TSB de los motivos de su decisión e indicar los posibles cambios que harían posible el avance de los trabajos.

Atentamente,

Seizo Onoe
Director de la Oficina de
Normalización de las Telecomunicaciones

**Anexos:** 2

Anexo 1

Resumen y ubicación de los proyectos de nueva Recomendación determinada
UIT-T X.1237 (X.tsfpp), X.1283 (X.gpwd), X.1353 (X.ztd-iot), X.1354 (X.sc-iot), X.1384 (X.itssec-5), X.1471 (X.websec-7), X.1819 (X.5Gsec-netec)
y X.1820 (X.5Gsec-srocvs)

# 1 Proyecto de nueva Recomendación UIT-T X.1237 (X.tsfpp) [[R62](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0062)]

Requisitos de seguridad para la protección de la información de identificación personal en el marco de la lucha contra el spam en la mensajería móvil

Resumen

Hoy en día, el contenido spam, guiado por el interés comercial (publicidad), se infiltra en todos los medios para llegar hasta nosotros. Operadores, desarrolladores de software y organizaciones de diversa índole están estudiando distintos tipos de tecnologías, plataformas, servicios y aplicaciones para luchar contra el spam. No obstante, si no se tiene en cuenta la protección de la información de identificación personal (IIP) en el diseño y la aplicación de estos enfoques, su funcionalidad y eficacia podrían verse mermadas.

La presente Recomendación tiene en cuenta la protección de la IIP en el diseño y la aplicación de soluciones para contrarrestar el spam en la mensajería móvil. Proporciona una visión general de los procesos de lucha contra el spam en la mensajería móvil y propone requisitos de seguridad para contrarrestar este fenómeno. Además, presenta las funciones de las entidades y los procedimientos de gestión.

# 2 Proyecto de nueva Recomendación UIT-T X.1283 (X.gpwd) [[R66](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0066)]

Análisis de amenazas y directrices para la seguridad de soluciones de autenticación con contraseñas o sin ellas

Resumen

En la esfera de la seguridad se han logrado amplios avances para sustituir la autenticación mediante contraseñas por otras soluciones basadas en autenticación sin contraseñas. Lamentablemente, muchas de las soluciones propuestas adolecen de las mismas limitaciones que las actuales soluciones basadas en contraseñas. Dichas soluciones son vulnerables, en particular, frente a ataques mediante intermediarios o por suplantación de identidad.

En la Recomendación UIT-T X.1283 (X.gpwd) se analiza la seguridad de soluciones de autenticación basadas en la compartición de datos secretos, así como las amenazas asociadas a las mismas. Se evalúan pormenorizadamente los riesgos de seguridad de sistemas de contraseñas y de soluciones incipientes que no se basan en la utilización de contraseñas.

En la presente Recomendación se abordan amenazas de índole diversa y se formulan directrices y prácticas idóneas para la protección de usuarios y cuentas con arreglo a esos métodos. Ello puede ser útil para facilitar la utilización de soluciones actuales a medida que se implantan métodos de autenticación más eficaces basados en infraestructuras de clave pública (en particular, UIT‑T X.1277 y UIT-T X.1278).

# 3 Proyecto de nueva Recomendación UIT-T X.1353 (X.ztd-iot) [[R63](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0063)]

Metodología de seguridad basada en cadenas de bloques para instalaciones sin intervención de IoT masiva

Resumen

La Internet de las cosas masiva (mIoT) es una importante aplicación de las futuras redes de comunicaciones. A la vista de numerosos casos de uso previstos de mIoT, resulta difícil para los fabricantes preinstalar sus dispositivos IoT prefabricados con información específica del operador móvil y/o información específica del servicio (por ejemplo, identidades y claves), ya que los fabricantes pueden desconocer dónde se desplegarán y se activarán finalmente sus dispositivos. El enfoque actual se basa en una configuración manual realizada por los clientes, que es aceptable para aplicaciones de IoT a pequeña escala. Sin embargo, en el caso de dispositivos mIoT, dicho enfoque es inaceptable debido a que la configuración manual lleva mucho tiempo, es poco rentable y engorrosa. Por lo tanto, la mIoT requiere la provisión automática de credenciales sin la participación del usuario, conocida como "sin intervención".

La presente Recomendación proporciona una metodología de seguridad para el diseño de sistemas descentralizados de gestión de identidades que permitan futuras tecnologías basadas en cadenas de bloques de IoT masiva. Este es un enfoque factible y prometedor para lograr la instalación sin intervención para la futura IoT masiva. La instalación sin intervención permitirá a los dispositivos IoT encontrar automáticamente su operador de red móvil y su proveedor de servicios, y conectarse automáticamente a la red y al servicio. Esto facilitará en gran medida la futura instalación de dispositivos mIoT en ámbitos verticales. El contenido de esta Recomendación abarca la arquitectura de seguridad, las consideraciones sobre la seguridad y los procedimientos de seguridad conexos (como las acreditaciones de dispositivos, la autenticación y la provisión de credenciales), que son necesarios para crear la plataforma para instalaciones sin intervención para la Internet de las cosas masiva (mIoT).

# 4 Proyecto de nueva Recomendación UIT-T X.1354 (X.sc-iot) [[R64](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0064)]

Controles de seguridad para sistemas IoT

Resumen

La Recomendación UIT-T X.1354 (X.sc-iot) contiene directrices prácticas de seguridad para tres partes interesadas en los sistemas de Internet de las cosas (IoT), a saber, el proveedor, el desarrollador y el usuario del servicio, y describe asimismo el concepto, los riesgos y los controles de seguridad de estos sistemas.

Los sistemas IoT presentan retos particulares en lo que respecta a la seguridad de la información debido a que están muy distribuidos y engloban a numerosas y diversas entidades. Siendo tan grande la superficie de ataque, la aplicación y el mantenimiento de controles de seguridad adecuados en todo el sistema suponen un reto considerable para el sistema de gestión de la seguridad de la información.

# 5 Proyecto de nueva Recomendación UIT-T X.1384 (X.itssec-5) [[R67](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0067)]

Requisitos y directrices de seguridad para la computación periférica vehicular

Resumen

La Recomendación UIT-T X.1384 (antes X.itssec-5) proporciona requisitos y directrices de seguridad para la computación periférica vehicular (CPV). La CPV se refiere a un paradigma informático que despliega capacidad de procesamiento en la periferia de la red para distribuir recursos informáticos en una nube central en entorno STI. La CPV también proporciona servicios de almacenamiento y aplicaciones más localizados a los usuarios de la carretera, lo que permite lograr menores retrasos de latencia, tiempos de respuesta más rápidos, conocimiento de ubicación, alta disponibilidad y calidad de servicio para aplicaciones de transmisión en tiempo real, ya que el procesamiento de datos se realiza más cerca del vehículo.

La CPV enfrenta muchos desafíos y problemas de seguridad, ya que requiere un tiempo de respuesta de servicio más rápido a los usuarios finales. En esta Recomendación se analizan las amenazas y vulnerabilidades identificadas en la CPV y se establecen requisitos de seguridad para el mismo. Además, también proporciona casos de uso para los servicios de CPV.

# 6 Proyecto de nueva Recomendación UIT-T X.1471 (X.websec-7) [[R65](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0065)]

Supervisión de referencia de servicios de análisis en línea

Resumen

El servicio de análisis de macrodatos se basa en datos no estructurados y no definidos, como datos sobre el comportamiento de los usuarios o sobre la adquisición, el pago, la ubicación y el consumo de diferentes contenidos de Internet. Puede aportar conocimientos nuevos que no se habían descubierto previamente y predice los estados futuros. Sin embargo, cabe la posibilidad de que se haga un uso malicioso de algunos datos no autorizados durante el proceso de análisis.

# En esta Recomendación se describe la supervisión de referencia aplicable en el análisis y las operaciones de macrodatos a fin de detectar el uso de datos no autorizados. Además, se analizan las amenazas y los problemas de seguridad del análisis de macrodatos y se describen las consideraciones de seguridad que podrían mitigar estas amenazas y contrarrestar los problemas de seguridad mediante mecanismos de control de acceso. Se facilita una metodología de supervisión de referencia basada en el control de acceso para determinar qué capacidades de seguridad se requieren para mitigar las amenazas de seguridad y contrarrestar los problemas de seguridad en el análisis de macrodatos.

# 7 Proyecto de nueva Recomendación UIT-T X.1819 (X.5Gsec-netec) [[R60](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0060)]

Funciones de seguridad de la capa de red para computación periférica IMT-2020/5G

Resumen

La computación periférica para redes IMT-2020/5G (5G EC) desempeñará un papel clave en servicios de baja latencia y servicios de descarga de tráfico en las próximas generaciones de redes IMT. Existen varios factores destacados que podrían dar lugar a un aumento de la complejidad y de los riesgos de seguridad de la capa de red que soporta las 5G EC, o plantear nuevos retos de seguridad en la red. Dichos factores incluyen arquitecturas de red flexibles IMT‑2020/5G, estructuras de despliegue de EC variables y la existencia de diversos escenarios de aplicación y de varios tipos de redes privadas y de acceso de clientes, entre otros. Los límites entre las redes de telecomunicaciones y las redes privadas serían menos claros, y su exposición sería mayor. En consecuencia, cabe especificar los requisitos y las medidas de seguridad de la capa de red, incluidas las redes de telecomunicaciones y las redes privadas.

# 8 Proyecto de nueva Recomendación UIT-T X.1820 (X.5Gsec-srocvs) [[R61](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T22-SG17-R-0061)]

Requisitos de seguridad para la explotación de la red medular IMT-2020/5G en apoyo de los servicios verticales

Resumen

Con el desarrollo del sistema IMT‑2020/5G, los servicios verticales han adquirido una importancia clave como escenarios de la IMT‑2020/5G. En el caso de los servicios verticales para fábricas inteligentes y ciudades inteligentes que utilizan una red IMT‑2020/5G, muchos dispositivos de usuario utilizan servicios verticales con comunicaciones masivas tipo máquina y comunicaciones ultrafiables y de ultrabaja latencia (URLLC).

Como apoyo a los casos de uso verticales que requieren URLLC, cabe la posibilidad de desplegar algunas funciones de la red medular IMT‑2020/5G en emplazamientos locales más cercanos a los usuarios verticales, mientras otras funciones de la red medular IMT‑2020/5G continúan desplegadas en un emplazamiento central. A diferencia de la red medular IMT‑2020/5G desplegada como conjunto, las redes medulares IMT‑2020/5G que funcionan en esa configuración pueden enfrentarse a amenazas de seguridad específicas.

A fin de garantizar la seguridad durante la explotación de la red medular IMT‑2020/5G en apoyo de los servicios verticales, es preciso analizar las amenazas de seguridad específicas y definir los requisitos de seguridad pertinentes.

En esta Recomendación se analizan las amenazas de seguridad de datos, las amenazas de seguridad de red y las amenazas de seguridad física que son específicas de la red medular IMT‑2020/5G, la cual se encuentra desplegada tanto en un emplazamiento central como en emplazamientos locales en apoyo de los servicios verticales. Además, se especifican los requisitos de seguridad aplicables.

Este proyecto de texto determinado incluye referencias normativas que requieren una justificación UIT-T A.5, la cual puede encontrarse en SG17-[TD1739](https://www.itu.int/md/T22-SG17-240220-TD-PLEN-1739/en).

Anexo 2

Asunto: Respuesta de Estado Miembro a la Circular TSB 195:
Consulta sobre los proyectos de nuevas Recomendaciones determinadas UIT-T X.1237 (X.tsfpp), X.1283 (X.gpwd), X.1353 (X.ztd-iot), X.1354 (X.sc-iot), X.1384 (X.itssec-5), X.1471 (X.websec-7), X.1819 (X.5Gsec-netec) y X.1820 (X.5Gsec-srocvs)

|  |  |  |  |
| --- | --- | --- | --- |
| **A**: | Director de la Oficina deNormalización de las Telecomunicaciones,Unión Internacional de TelecomunicacionesPlace des NationsCH 1211 Ginebra 20, Suiza | **De**: | [Nombre][Cargo oficial /título][Dirección] |
| **Fax**:**Correo-e**: | +41-22-730-5853tsbdir@itu.int  | **Fax**:**Correo-e**: |  |
|  |  | **Fecha**: | [Lugar,] [Fecha] |

Muy Señora mía/Muy Señor mío:

En lo que respecta a la consulta a los Estados Miembros sobre los proyectos determinados que se enumeran en la Circular 195 de la TSB, deseo informarle de la opinión de esta Administración, que se refleja en el siguiente cuadro:

|  | Seleccione una de las dos casillas para cada texto |
| --- | --- |
| **Proyecto de nueva Recomendación UIT-T X.1237 (X.tsfpp)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (en cuyo caso seleccionará una de las dos opciones ⃝):⃝ Sin comentarios o cambios sugeridos⃝ Se adjuntan los comentarios o cambios sugeridos |
| [ ]  **No otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (se adjuntan los motivos en que se fundamenta esta opinión y las modificaciones que podrían permitir el proseguimiento de los trabajos) |
| **Proyecto de nueva Recomendación UIT-T X.1283 (X.gpwd)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (en cuyo caso seleccionará una de las dos opciones ⃝):⃝ Sin comentarios o cambios sugeridos⃝ Se adjuntan los comentarios o cambios sugeridos |
| [ ]  **No otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (se adjuntan los motivos en que se fundamenta esta opinión y las modificaciones que podrían permitir el proseguimiento de los trabajos) |
| **Proyecto de nueva Recomendación UIT-T** **X.1353(X.ztd-iot)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (en cuyo caso seleccionará una de las dos opciones ⃝):⃝ Sin comentarios o cambios sugeridos⃝ Se adjuntan los comentarios o cambios sugeridos |
| [ ]  **No otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (se adjuntan los motivos en que se fundamenta esta opinión y las modificaciones que podrían permitir el proseguimiento de los trabajos) |
| **Proyecto de nueva Recomendación UIT-T X.1354(X.sc-iot)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (en cuyo caso seleccionará una de las dos opciones ⃝):⃝ Sin comentarios o cambios sugeridos⃝ Se adjuntan los comentarios o cambios sugeridos |
| [ ]  **No otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (se adjuntan los motivos en que se fundamenta esta opinión y las modificaciones que podrían permitir el proseguimiento de los trabajos) |
| **Proyecto de nueva Recomendación UIT-T X.1384 (X.itssec-5)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (en cuyo caso seleccionará una de las dos opciones ⃝):⃝ Sin comentarios o cambios sugeridos⃝ Se adjuntan los comentarios o cambios sugeridos |
| [ ]  **No otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (se adjuntan los motivos en que se fundamenta esta opinión y las modificaciones que podrían permitir el proseguimiento de los trabajos) |
| **Proyecto de nueva Recomendación UIT-T X.1471 (X.websec-7)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (en cuyo caso seleccionará una de las dos opciones ⃝):⃝ Sin comentarios o cambios sugeridos⃝ Se adjuntan los comentarios o cambios sugeridos |
| [ ]  **No otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (se adjuntan los motivos en que se fundamenta esta opinión y las modificaciones que podrían permitir el proseguimiento de los trabajos) |
| **Proyecto de nueva Recomendación UIT-T X.1819 (X.5Gsec-netec)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (en cuyo caso seleccionará una de las dos opciones ⃝):⃝ Sin comentarios o cambios sugeridos⃝ Se adjuntan los comentarios o cambios sugeridos |
| [ ]  **No otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (se adjuntan los motivos en que se fundamenta esta opinión y las modificaciones que podrían permitir el proseguimiento de los trabajos) |

|  |  |
| --- | --- |
| **Proyecto de nueva Recomendación UIT-T X.1820 (X.5Gsec-srocvs)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (en cuyo caso seleccionará una de las dos opciones ⃝):⃝ Sin comentarios o cambios sugeridos⃝ Se adjuntan los comentarios o cambios sugeridos |
| [ ]  **No otorga autoridad** a la Comisión de Estudio 17 a fin de examinar este texto para aprobación (se adjuntan los motivos en que se fundamenta esta opinión y las modificaciones que podrían permitir el proseguimiento de los trabajos) |

Atentamente,

[Nombre]

[Cargo oficial/Título]

Administración de [Estado Miembro]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_