|  |  |
| --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **Unión Internacional de Telecomunicaciones****Oficina de Normalización de las Telecomunicaciones** |
|  |  | Ginebra, 23 de julio de 2025 |
| **Ref**.: | **Circular TSB 50**CE 17/XY | **A:**– las Administraciones de los Estados Miembros de la Unión**Copia a:**– los Miembros de Sector del UIT‑T;– los Asociados de la Comisión de Estudio 17 del UIT-T;– las Instituciones Académicas de la UIT;– el Presidente y el Vicepresidente de la Comisión de Estudio 17 del UIT-T;– el Director de la Oficina de Desarrollo de las Telecomunicaciones;– el 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 nuevas Recomendaciones determinadas UIT-T X.1062 (ex X.shcd), X.1238 (ex X.sgc-rcs), X.1128 (ex X.mt‑feature), X.1129 (ex X.mt-integrity), X.1130 (ex X.tg-fdma), X.1457 (ex X.str‑irs), X.1753 (ex X.gdsml) y X.1649 (ex X.sgmc), y de Recomendaciones revisadas UIT-T X.1250 y X.1631, propuestos para su aprobación en la reunión de la Comisión de Estudio 17 del UIT-T (Ginebra, 3-11 de diciembre de 2025)** |

Estimado Señor/Estimada Señora,

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 física que tendrá lugar en Ginebra del 3 al 11 de diciembre de 2025. 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 [4/17](https://www.itu.int/md/T25-SG17-COL-0004/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 – No se ha presentado un documento justificativo de la Recomendación UIT‑T A.5 para ninguno de estos textos determinados.

NOTA 2 de la TSB – En la fecha de la presente Circular, la TSB no había recibido ninguna declaración relativa a los derechos de propiedad intelectual (DPI) en relación con estos textos determinados. Para obtener información actualizada, se invita a los miembros a consultar la base de datos de DPI en [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 su 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 en el **Anexo 2** antes de las 23.59 horas UTC del **21 de noviembre de 2025**.

4 Si el 70 % como mínimo de las respuestas de los Estados Miembros es favorable a que se considere la aprobación, 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 nuevas Recomendaciones determinadas UIT-T X.1062 (ex X.shcd), X.1238 (ex X.sgc-rcs), X.1128 (ex X.mt-feature), X.1129 (ex X.mt-integrity), X.1130 (ex X.tg-fdma), X.1457 (ex X.str-irs), X.1753 (ex X.gdsml) y X.1649 (ex X.sgmc), y de Recomendaciones revisadas UIT-T X.1250 y X.1631

# 1 Proyecto de nueva Recomendación UIT-T X.1062 (ex X.shcd) [[SG17-R6](https://www.itu.int/md/T25-SG17-R-0006/es)]

Marco para el desarrollo de capacidades humanas en materia de seguridad

Resumen

La ciberseguridad es un tema amplio y en constante evolución que requiere aprendizaje continuo y desarrollo de competencias. En esta Recomendación se especifica un marco para el desarrollo de las capacidades humanas en materia de seguridad con el fin de orientar el crecimiento de los especialistas y profesionales de la seguridad mediante el perfeccionamiento de sus competencias y el reconocimiento de sus competencias y conocimientos en materia de seguridad en una organización.

# 2 Proyecto de nueva Recomendación UIT-T X.1238 (ex X.sgc-rcs) [[SG17-R7](https://www.itu.int/md/T25-SG17-R-0007/es)]

Directrices para contrarrestar el correo basura por mensajería del servicio de comunicación mejorado (RCS)

Resumen

En esta Recomendación se especifican orientaciones y habilitadores técnicos que ayudan a los proveedores del servicio de comunicación mejorado (RCS) a evitar la distribución de correo basura sobre la base de las especificidades del RCS y se define el mecanismo de prevención y control del correo basura respaldado por el cliente del RCS.

Esta Recomendación cita la arquitectura del RCS definida en la GSMA [b‑GSMA RCC.07] y se centra en cómo mitigar los riesgos relacionados con el correo basura de la mensajería del RCS.

# 3 Proyecto de nueva Recomendación UIT-T X.1128 (ex X.mt-feature) [[SG17-R8](https://www.itu.int/md/T25-SG17-R-0008/es)]

Funciones de seguridad para evaluar la seguridad de terminales móviles

Resumen

Los terminales móviles, en particular los teléfonos inteligentes, han transformado el modo de trabajar y de vivir. Por ejemplo, los pagos móviles están experimentando un rápido crecimiento, dado que los consumidores utilizan los terminales móviles como parte de sus modernos y dinámicos estilos de vida; cada vez son más las empresas que ayudan a sus empleados a acceder a servicios de empresa con terminales móviles personales; etc. No obstante, la seguridad de los terminales móviles constituye un gran reto para los servicios de aplicaciones móviles propiamente dichos. Por ejemplo, los usuarios pueden exponer de forma inconsciente sus terminales a programas maliciosos y comprometer datos confidenciales.

En la presente Recomendación se proporciona información sobre diversas funciones de seguridad destinadas a la evaluación de la seguridad de terminales móviles, así como la forma en que las partes interesadas pertinentes pueden aplicar esas funciones.

# 4 Proyecto de nueva Recomendación UIT-T X.1129 (ex X.mt-integrity) [[SG17-R9](https://www.itu.int/md/T25-SG17-R-0009/es)]

Directrices de seguridad para la protección de la integridad de terminales móviles

Resumen

El objetivo de la protección de la integridad de los terminales móviles es garantizar que el terminal móvil se comporte de la manera esperada. Esto significa que el *hardware*, el *firmware* y el *software* (por ejemplo, el sistema operativo o aplicaciones preinstaladas) del terminal móvil no se han visto comprometidos por ningún medio ni de ninguna manera. Si un atacante pone en peligro el *firmware* o el *software*, modifica la configuración del *hardware* (por ejemplo, la ROM o las células de retención) o cambia el *hardware* (por ejemplo, la memoria externa), podría controlar o alterar la funcionalidad del terminal móvil.

Cuando se encienden, los terminales móviles inician una fase de arranque para verificar los componentes de *hardware* y cargar uno o más módulos de *software*. A continuación, pasan a una fase de ejecución y alcanzan su estado operativo, por lo que están preparados para el fin previsto. A fin de corregir las vulnerabilidades y deficiencias del *firmware*/*software* (FW/SW), los terminales móviles deben ser actualizados de vez en cuando, lo que se conoce como fase de actualización del FW/SW. En cada una de estas fases el atacante tiene la oportunidad de introducir amenazas a la seguridad de la integridad del terminal móvil.

En esta Recomendación se analizan las amenazas a la seguridad de los terminales móviles durante la fase de arranque, la fase de ejecución y la fase de actualización del FW/SW, se definen los requisitos de seguridad y se proporcionan directrices de seguridad para proteger la integridad de los terminales móviles.

# 5 Proyecto de nueva Recomendación UIT-T X.1130 (ex X.tg-fdma) [[SG17-R10](https://www.itu.int/md/T25-SG17-R-0010/es)]

Directrices técnicas para la detección de actividades maliciosas de aplicaciones móviles

Resumen

Con el uso generalizado de dispositivos y aplicaciones móviles, las aplicaciones se han convertido en uno de los principales vectores de las actividades maliciosas. Por ejemplo, las aplicaciones malintencionadas pueden adoptar la forma de aplicaciones legítimas de crédito o compras para engañar a los usuarios. Para detectar y prevenir estas actividades maliciosas, los enfoques tradicionales se basan en las reseñas de la tienda de aplicaciones y en las alertas del *software* de seguridad instalado en el dispositivo móvil. Sin embargo, esta solución se enfrenta a varios desafíos. Si bien las reseñas de la tienda de aplicaciones pueden ayudar a bloquear aplicaciones malintencionadas, los atacantes desarrollan continuamente nuevas técnicas para evadir la detección y eludir las reseñas de la tienda. Además, algunas aplicaciones malintencionadas se distribuyen a través de plataformas de terceros en las que incitan a los usuarios a descargarlas e instalarlas. El *software* de seguridad móvil se centra principalmente en la detección de virus y vulnerabilidades de las aplicaciones, lo que dificulta la identificación eficaz de aplicaciones malintencionadas diseñadas específicamente para llevar a cabo actividades maliciosas.

Las aplicaciones malintencionadas en dispositivos móviles suelen operar en cuatro etapas: descarga, instalación, ejecución e incitación al pago. Cada etapa presenta riesgos diferenciados.

Durante las etapas de descarga e instalación, las aplicaciones malintencionadas a menudo adoptan la forma de aplicaciones legítimas para evitar ser detectadas por el *software* de seguridad. También pueden introducir troyanos en el dispositivo móvil durante esta fase.

En la etapa de ejecución, estas aplicaciones pueden robar información del usuario a través de los troyanos introducidos o imitar aplicaciones legítimas para engañar a los usuarios y conseguir que revelen información confidencial de forma voluntaria.

En la etapa de incitación al pago, las aplicaciones malintencionadas suelen generar confianza ofreciendo pequeñas recompensas o beneficios a través de diversos mecanismos. Una vez conseguida su confianza, confunden al usuario para que transfiera dinero. En algunos casos, el engaño es directo, por ejemplo, haciéndose pasar por aplicaciones de compras legítimas para explotar a usuarios desprevenidos.

Todo el proceso de detección y prevención de actividades maliciosas es extremadamente complejo y requiere una coordinación estrecha entre los dispositivos móviles y las aplicaciones. En esta Recomendación se analizan las características y los riesgos de las aplicaciones malintencionadas en las diferentes etapas, a saber, descarga, instalación, ejecución e incitación al pago, y se ofrece una solución técnica completa para detectar y prevenir actividades maliciosas basada en las interacciones entre los dispositivos móviles y las aplicaciones.

# 6 Proyecto de nueva Recomendación UIT-T X.1457 (ex X.str-irs) [[SG17-R11](https://www.itu.int/md/T25-SG17-R-0011/es)]

Amenazas y requisitos de seguridad para el servicio de recomendación de información

Resumen

El servicio de recomendación de información se utiliza ampliamente en diversos sitios web y aplicaciones. Por ejemplo, el servicio de recomendación de información educativa es un factor importante para facilitar el intercambio de información educativa. Dentro de la gran cantidad de información educativa disponible, los usuarios pueden encontrar rápidamente los recursos de información educativa que necesitan, satisfacer sus necesidades de aprendizaje y disfrutar de una experiencia de aprendizaje de calidad. Sin embargo, no se deben ignorar los problemas de seguridad asociados al servicio de recomendación de información, como las amenazas a la integridad de los datos, la manipulación de datos, los ataques de evasión, entre otros.

En la presente Recomendación se proporciona un análisis de las amenazas de seguridad y los requisitos para el servicio de recomendación de información. Se identifican las amenazas de seguridad implicadas en el servicio de recomendación de información y se especifican los requisitos de seguridad establecidos para abordar estas amenazas.

# 7 Proyecto de nueva Recomendación UIT-T X.1753 (ex X.gdsml) [[SG17-R12](https://www.itu.int/md/T25-SG17-R-0012/es)]

Directrices sobre seguridad de datos mediante aprendizaje automático en infraestructuras de macrodatos

Resumen

En las infraestructuras de macrodatos, existen numerosas amenazas a la seguridad respecto del proceso de recopilación, almacenamiento, procesamiento y gestión de datos. La manera de supervisar y analizar las amenazas a la seguridad de los datos, así como de responder a ellas, de manera dinámica e inteligente, constituye un problema que ha de resolverse en las infraestructuras de macrodatos. El aprendizaje automático tiene las capacidades del aprendizaje automático y el reconocimiento de patrones, que pueden detectar posibles amenazas a la seguridad y comportamientos anómalos en una gran cantidad de datos de manera que se puedan tomar medidas defensivas proactivas. El uso del aprendizaje automático para mejorar la seguridad de los datos se ha ido gradualmente convirtiendo en una tecnología necesaria para las infraestructuras de macrodatos.

En esta Recomendación se analizan las amenazas a la seguridad de los datos en las infraestructuras de macrodatos y los casos en los que puede aplicarse el aprendizaje automático a la protección de seguridad de datos de las infraestructuras de macrodatos. Asimismo, en ella se ofrecen directrices relativas al uso del aprendizaje automático para proteger la seguridad de los datos de las infraestructuras de macrodatos.

# 8 Proyecto de nueva Recomendación UIT-T X.1649 (ex X.sgmc) [[SG17-R14](https://www.itu.int/md/T25-SG17-R-0014/es)]

Directrices de seguridad para varios sistemas en la nube

Resumen

En esta Recomendación se ofrece una reseña de la multinube, incluida su definición y el contexto en el que apareció. En ella también se analizan los riesgos de seguridad y se especifican orientaciones apropiadas para la multinube a fin de mitigar los riesgos de seguridad.

# 9 Proyecto de Recomendación revisada UIT-T X.1250 [[SG17-R15](https://www.itu.int/md/T25-SG17-R-0015/es)]

Capacidades básicas para una mejor gestión e interoperabilidad de identidades

Resumen

En este documento se exponen las principales disposiciones para crear y desplegar sistemas de gestión de identidades estructurados e interoperables en las redes de telecomunicaciones y TI, garantizando la privacidad y el cumplimiento de las políticas regionales. Abarca temas como los modelos de gestión de identidades estructurados para lograr intercambios de identidades seguros y eficientes, la protección y asignación de atributos de identidad y la detección de proveedores de servicios de identidad. Asimismo, aborda la interoperabilidad entre las plataformas de identidad, medidas de seguridad para mitigar las amenazas, la auditoría con fines de cumplimiento y la importancia de la usabilidad y escalabilidad. El objetivo general consiste en crear sistemas de gestión de identidades robustos, transparentes y adaptables que mejoren la confianza, la seguridad y la experiencia del usuario en las interacciones digitales, y cumplan a su vez las normas reglamentarias.

# 10 Proyecto de Recomendación revisada UIT-T X.1631 [[SG17-R13](https://www.itu.int/md/T25-SG17-R-0013/es)]

Controles de seguridad de la información basados en la ISO/CEI 27002 para los servicios en la nube

Resumen

Las directrices que figuran en esta Recomendación | norma internacional se añaden y completan las directrices proporcionadas en la ISO/CEI 27002:2022.

En concreto, esta Recomendación | norma internacional ofrece directrices para la implementación de controles de seguridad de la información para clientes y proveedores de servicios en la nube (CSC y CSP respectivamente). Algunas directrices se destinan a los CSC que implementan los controles y otras a los CSP para apoyar la implementación de dichos controles. La determinación de los controles de seguridad de la información adecuados y el grado de uso de las directrices proporcionadas dependerá de los resultados de la correspondiente evaluación de riesgos y la existencia de requisitos jurídicos, reglamentarios, contractuales u otros requisitos de seguridad de la información específicos de la computación en la nube.

Anexo 2
Asunto: Respuesta de los Estados Miembros a la Circular TSB 50:
Consulta sobre los proyectos de nuevas Recomendaciones determinadas UIT-T X.1062 (ex X.shcd), X.1238 (ex X.sgc-rcs), X.1128 (ex X.mt-feature), X.1129 (ex X.mt-integrity), X.1130 (ex X.tg-fdma), X.1457 (ex X.str-irs), X.1753 (ex X.gdsml) y X.1649 (ex X.sgmc), y de Recomendaciones revisadas UIT-T X.1250 y X.1631

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

Estimado Señor/Estimada Señora:

En lo que respecta a la consulta a los Estados Miembros sobre los proyectos determinados que se enumeran en la Circular 50 de la TSB, deseo informarle de la opinión de esta Administración, que se refleja en el siguiente cuadro:

|  | Seleccione una de las dos casillas |
| --- | --- |
| **Proyecto de nueva Recomendación X.1062 (ex X.shcd)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 para examinar este texto para aprobación (en cuyo caso, seleccione 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 de esta decisión y las posibles modificaciones que permitirían que prosiguieran los trabajos) |
| **Proyecto de nueva Recomendación X.1238 (ex X.sgc-rcs)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 para examinar este texto para aprobación (en cuyo caso, seleccione 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 de esta decisión y las posibles modificaciones que permitirían que prosiguieran los trabajos) |
| **Proyecto de nueva Recomendación X.1128 (ex X.mt‑feature)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 para examinar este texto para aprobación (en cuyo caso, seleccione 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 de esta decisión y las posibles modificaciones que permitirían que prosiguieran los trabajos) |
| **Proyecto de nueva Recomendación X.1129 (ex X.mt‑integrity)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 para examinar este texto para aprobación (en cuyo caso, seleccione 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 de esta decisión y las posibles modificaciones que permitirían que prosiguieran los trabajos) |
| **Proyecto de nueva Recomendación X.1130 (ex X.tg-fdma)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 para examinar este texto para aprobación (en cuyo caso, seleccione 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 de esta decisión y las posibles modificaciones que permitirían que prosiguieran los trabajos) |
| **Proyecto de nueva Recomendación X.1457 (ex X.str-irs)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 para examinar este texto para aprobación (en cuyo caso, seleccione 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 de esta decisión y las posibles modificaciones que permitirían que prosiguieran los trabajos) |
| **Proyecto de nueva Recomendación X.1753 (ex X.gdsml)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 para examinar este texto para aprobación (en cuyo caso, seleccione 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 de esta decisión y las posibles modificaciones que permitirían que prosiguieran los trabajos) |
| **Proyecto de nueva Recomendación X.1649 (ex X.sgmc)** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 para examinar este texto para aprobación (en cuyo caso, seleccione 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 de esta decisión y las posibles modificaciones que permitirían que prosiguieran los trabajos) |
| **Proyecto de Recomendación revisada X.1250** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 para examinar este texto para aprobación (en cuyo caso, seleccione 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 de esta decisión y las posibles modificaciones que permitirían que prosiguieran los trabajos) |
| **Proyecto de Recomendación revisada X.1631** | [ ]  **Otorga autoridad** a la Comisión de Estudio 17 para examinar este texto para aprobación (en cuyo caso, seleccione 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 de esta decisión y las posibles modificaciones que permitirían que prosiguieran los trabajos) |

Atentamente,

[Nombre]
[Cargo oficial/título]
Administración de [Estado Miembro]