|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **Unión Internacional de Telecomunicaciones**  **Oficina de Normalización de las Telecomunicaciones** | |  |
|  | |  | |

Ginebra, 29 de enero de 2015

|  |  |  |
| --- | --- | --- |
| Ref.: | **Addéndum 1 a la Carta Colectiva TSB 5/17** |  |
| Tel.: | +41 22 730 5866 | A: |
| Fax:  Correo-e: | +41 22 730 5853  [tsbsg17@itu.int](mailto:tsbsg17@itu.int) | * – las Administraciones de los Estados Miembros de la Unión; * – los Miembros del Sector UIT‑T; * – los Asociados que participan en los trabajos de la Comisión de Estudio 17 y a * – las Instituciones Académicas del UIT-T |

|  |  |
| --- | --- |
| Asunto: | **Reunión de la Comisión de Estudio 17; Ginebra, 8-17 de abril de 2015** |

Estimado(a) Señor(a):

Los siguientes dos trabajos sometidos al proceso de aprobación alternativo (AAP) recibieron comentarios de la última llamada y se someterán a la consideración de la reunión de la Comisión de Estudio 17 que tendrá lugar en Ginebra, del 8 al 17 de abril de 2015.

1) **Proyecto de nueva Recomendación UIT-T X.1341 (X.mail)**, *Protocolos de transporte de correo certificado y de oficina postal certificada*.

**Localización de los comentarios de la última llamada y texto del proyecto:**  
[COM 17 – TD 1634 Rev.1](http://www.itu.int/md/meetingdoc.asp?lang=en&parent=T13-SG17-150408-TD-PLEN-1634).

**Resumen**

El objetivo de esta Recomendación es definir el Protocolo de transporte de correo certificado (CMTP) y el Protocolo de oficina postal certificada (CPOP) con el fin de fomentar los intercambios de correos electrónicos certificados en todo el mundo y de manera segura proporcionando confidencialidad, identificación de los corresponsales, integridad y evitando el repudio.

2) **Proyecto de nueva Recomendación UIT-T X.1157 (X.sap-7)**, *Capacidades técnicas de detección de fraudes y de respuesta para servicios con requisitos de alto nivel de seguridad*.

**Localización de los comentarios de la última llamada y texto del proyecto:**  
[COM 17 – TD 1638](http://www.itu.int/md/meetingdoc.asp?lang=en&parent=T13-SG17-150408-TD-PLEN-1638).

**Resumen**

En la Recomendación UIT-T X.1157 se facilitan capacidades necesarias para la detección del fraude y el servicio de respuesta en servicios de aplicación de tecnologías de la información y la comunicación (TIC) que requieren seguridad. Los servicios de detección del fraude y respuesta sirven de base para la detección, el análisis y la gestión del fraude entre usuarios, cuentas, productos, procesos y canales. Realizan un seguimiento y analizan la actividad y el comportamiento del usuario en el plano de la aplicación (en lugar de hacerlo en el plano del sistema, de la base de datos o de la red), y supervisa lo que ocurre dentro de las cuentas y entre ellas utilizando cualquier canal disponible para un usuario. También analiza el comportamiento entre usuarios, cuentas u otras entidades relacionados, en busca de actividades anormales, corrupción o uso indebido. Suele utilizarse en áreas verticales de gestión de dinero de usuario, tales como las ciberfinanzas, el acceso remoto a la empresa, etc., pero se aplica también frecuentemente para detectar el fraude interno y otros tipos de actividades no autorizadas.

Atentamente.

Chaesub Lee  
Director de la Oficina de Normalización   
de las Telecomunicaciones