|  |  |  |
| --- | --- | --- |
| itu_logo | **Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT-16)****Hammamet, 25 de octubre - 3 de noviembre de 2016** | CCITT/ITU-T 60th Anniversary logo |
|  |  |
|  |  |
| SESIÓN PLENARIA | **Revisión 1 al Documento 58-S** |
|  | **27 de octubre de 2016** |
|  | **Original: inglés** |
|  |
| Director de la TSB |
| CONCLUSIONES DEL TERCER SIMPOSIO MUNDIAL DE NORMALIZACIÓN |
|  |
|  |

|  |  |
| --- | --- |
| **Resumen:** | En el presente informe se resumen las conclusiones del tercer Simposio Mundial de Normalización. (SMN). En la Revisión 1 a este documento se incluye un resumen de todas las presentaciones del SMN que figuran en el Apéndice 1. |

Conclusiones del 3º Simposio Mundial de Normalización

El 3º Simposio Mundial de Normalización, Hammamet (Túnez), 24 de octubre de 2016, congregó a líderes de opinión en el campo de la normalización que abordaron la mejor manera de incorporar en las actividades de normalización las consideraciones de seguridad, privacidad y confianza.

# 1 Introducción

El Simposio Mundial de Normalización (SMN) consiste en debates sobre política de normalización de alto nivel en los que se investiga la dinámica evolutiva de la tecnología de la información y la comunicación (TIC) y sus repercusiones en la normalización técnica. El SMN se celebra al principio de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT) que la UIT organiza cada 4 años. Las anteriores ediciones se celebraron en Johannesburgo el año 2008 y en Dubái el 2012.

El tema del SMN-12 – *Normalización en la intersección del sector de las TIC con otros sectores, como la atención sanitaria, las instalaciones y el transporte* – ha resultado ser muy oportuno y las conclusiones del Simposio ofrecen orientaciones importantes para los trabajos de normalización en la UIT de 2013 a 2016. En el SMN-12 se abordaron los aspectos de seguridad, privacidad y confianza en los servicios e infraestructura de TIC cuando se debatieron temas tales como la transmisión inalámbrica de datos médicos, el almacenamiento de datos sobre los desplazamientos de vehículos conectados y la recopilación de datos sobre el usuario por las tiendas en línea. En dichos entornos, se precisa de marcos normalizados para garantizar que el servicio posee atributos de seguridad fiables y que se protege la seguridad y privacidad del usuario.

El SMN-16 examinó las opciones de colaboración entre las partes interesadas para crear marcos internacionales de seguridad, privacidad y confianza. El Simposio congregó a líderes expertos en los campos de la seguridad, la privacidad y la confianza, representantes de gobiernos, reguladores, órganos de normalización e industria. Los participantes cambiaron impresiones acerca de los componentes fundamentales de dichos marcos y cuáles deben considerarse prioritarios en los trabajos de normalización de la UIT de 2017 a 2020.

El **Excmo. Sr. Mohamed Anouar Maarouf**, Ministro de Tecnologías de Comunicación y Economía Digital de la República de Túnez, pronunció unas palabras de bienvenida. El Secretario General de la UIT, **Sr.** **Houlin Zhao** y el Director de la Oficina de Normalización de las Telecomunicaciones de la UIT, **Sr. Chaesub Lee** pronunciaron discursos de apertura. Presidió el Simposio el **Sr.** **Mongi Marzoug**, ex Ministro de TIC de Túnez.

Tras la ceremonia de apertura del SMN-16 tuvieron lugar tres sesiones que giraron en torno al tema del Simposio desde las perspectivas de reglamentación y política, de la industria y de la normalización. A continuación se examina, en la Sección 2, el tema del SMN-16 en el contexto de las Naciones Unidas, y en la Sección 3 se resumen las principales conclusiones y recomendaciones de cada sesión del Simposio. En el Apéndice I se adjunta un resumen detallado de los debates del SMN-16.

El programa definitivo y las biografías y ponencias de los oradores están disponibles en la siguiente dirección: <http://itu.int/en/ITU-T/wtsa16/gss/>.

De conformidad con la Resolución 122 (Rev. Guadalajara, 2010) de la Conferencia de Plenipotenciarios y la Resolución 1272 (MOD) del Consejo de la UIT, las conclusiones del SMN‑16 que figuran en el presente informe se someterán a la consideración de la AMNT-16.

# 2 Seguridad, privacidad y confianza en las TIC en el contexto de las Naciones Unidas

Las TIC han hecho posible que miles de millones de personas intercambien información digital a escala mundial. La utilización de estas tecnologías, que dependen en gran medida de normas técnicas, ha acarreado innumerables dificultades en lo que respecta a la privacidad y seguridad de las comunicaciones y, en última instancia, ha afectado a la confianza del usuario en las TIC.

La UIT está comprometida a resolver estas dificultades en cuanto organismo de normalización encargado de elaborar normas[[1]](#endnote-1) internacionales en materia de TIC, de observancia voluntaria, que propicien la privacidad y, también, en su calidad de organización intergubernamental encargada de fomentar la confianza y la seguridad en la utilización de las TIC.[[2]](#endnote-2) La Cumbre Mundial sobre la Sociedad de la Información asignó a la UIT la responsabilidad de actuar de facilitador de la línea de acción C.5, para colaborar con los Estados Miembros de la UIT y otros interesados con miras a *"fortalec[er] el marco de confianza y seguridad con iniciativas complementarias y de apoyo mutuo en los ámbitos de la seguridad en el uso de las TIC, con iniciativas o directrices sobre el derecho a la privacidad y la protección de los datos y de los consumidores"*.

Los fundamentos de la normativa internacional para la protección de la privacidad se basan principalmente en los tratados sobre los derechos humanos, tales como la Declaración Universal de los Derechos Humanos de las Naciones Unidas de 1948[[3]](#endnote-3) y la Convención Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos de 1966[[4]](#endnote-4), los cuales contienen disposiciones sobre el derecho a la privacidad y a la vida privada (artículos 12 y 17, respectivamente). Ahora bien, estos textos no hacen referencia explícita al procesamiento digital de información personal, concepto este que en el contexto del sistema de la Naciones Unidas sólo se ha abordado en un documento orientativo no vinculante, a saber, Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales de 1990.[[5]](#endnote-5)

Si bien varios convenios internacionales vinculantes tratan del derecho a la privacidad – por ejemplo, el Convenio del Consejo de Europa para la Protección de las personas respecto del tratamiento automático de datos personales[[6]](#endnote-6) y el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales [[7]](#endnote-7) y la Convención Americana de Derechos Humanos [[8]](#endnote-8) – estos instrumentos jurídicos se elaboraron y adoptaron a escala regional en lugar de mundial. Muchos de estos acuerdos regionales se basan en los mismos principios fundamentales de privacidad, como el concepto de consentimiento informado del individuo y la adopción de medidas de seguridad adecuadas antes del procesamiento de la información personal.[[9]](#endnote-9)

Diversas partes interesadas han pedido que se preste mayor atención a la necesidad de llegar a un acuerdo común a escala mundial sobre el procesamiento de información personal. Por ejemplo, la Conferencia Internacional de Comisarios para la Protección de Datos y de la Privacidad ha apelado a) a las Naciones Unidas a preparar un instrumento jurídico vinculante, a saber, el "*convenio universal para la protección de las personas con respecto al tratamiento de datos personales*"; b) a las organizaciones internacionales "*a que se comprometan a cumplir los principios que son compatibles con los principales instrumentos internacionales que tratan la protección de datos y la privacidad*"; y c) a los fabricantes de hardware y software "*a que fabriquen productos y sistemas que integren tecnologías de fomento de la privacidad*".[[10]](#endnote-10)

La Asamblea General de las Naciones Unidas atendió esta petición en su 68º periodo de sesiones (2013) mediante la adopción de la Resolución titulada "*el derecho a la privacidad en la era digital*", en la que se exhorta a los Estados Miembros de las Naciones Unidas a "*respetar y proteger el derecho a la privacidad en las comunicaciones digitales*"[[11]](#endnote-11). En virtud de esta Resolución, El Consejo de Derechos Humanos de las Naciones Unidas nombró un relator especial con el mandato de, entre otras cosas, informar sobre las presuntas infracciones del derecho a la privacidad, en particular sobre los problemas que plantean las nuevas tecnologías.

# 3 Principales conclusiones del SMN-16

## 3.1 Principios normativos de seguridad, privacidad y confianza

*Recordando que la privacidad y la protección de los datos constituyen valores fundamentales de las personas y de las sociedades y que la Declaración Universal de los Derechos Humanos consagra la privacidad como un derecho fundamental;*

*Observando que prácticamente todos los aspectos de la vida dependen hoy en día de los servicios e infraestructura de TIC y que, por consiguiente, se verán afectados si no se consigue mantener la confianza; y,*

*Reconociendo la alarmante tendencia de filtración de datos e incidentes de seguridad que afectan negativamente a la confianza de las personas,*

*Los participantes en el SMN insisten en:*

– Recurrir a **marcos internacionales** que contengan los principios básicos de seguridad, privacidad y confianza y establecer mecanismos para cumplir esos principios.

– Fomentar la adhesión a **principios de privacidad en el diseño, evaluación del impacto sobre la privacidad y el desarrollo de tecnologías que mejoran la privacidad** (PET), es decir, tecnologías que cuando se integran en los servicios e infraestructura de TIC minimizan el procesamiento de información de identificación personal.

– Establecer mecanismos para la **compartición de información entre los sectores público y privado** sobre las amenazas a los servicios e infraestructura de TIC, prácticas idóneas y estrategias de mitigación.

– Movilizar a la comunidad internacional y establecer alianzas para **crear capacidades nacionales** a fin de protegernos contra ciberataques, aumentar la capacidad de los países a detectar incidentes de seguridad y coordinar la reacción ante tales incidentes.

– Crear un equilibrio entre la necesidad de proteger la privacidad de las personas y fomentar **la utilización innovadora de datos** para impulsar la economía digital. Cuando están incorporadas en el diseño de nuevos servicios y tecnologías, las prácticas idóneas de privacidad y seguridad se convierten en argumentos de venta atractivos para los clientes y contribuyen a mejorar toda la red.

– Contribuir a la elaboración de **normas internacionales que aborden problemas mundiales**, reconociendo que los ciberataques trascienden las fronteras nacionales, que las infracciones de privacidad y seguridad menoscaban la confianza en las TIC y que se precisan marcos de seguridad normalizados a escala internacional para garantizar la fiabilidad de los atributos de seguridad de los servicios y la protección transfronteriza de la seguridad y la privacidad necesarias del usuario.

– Promover el desarrollo de **normas para la "desidentificación" de datos personales** y la **portabilidad de datos**, normas que puedan contribuir a aumentar la protección del consumidor y aumentar sus posibilidades de suscribirse a servicios TIC y desinscribirse de ellos.

# 3.2 Cómo se satisfacen en el sector privado las expectativas de seguridad, privacidad y confianza del usuario

*Reafirmando el enorme potencial de la digitalización y las tecnologías de información y la comunicación para mejorar la vida y la sociedad;*

*Reconociendo que los fallos de seguridad, la infracción de la privacidad y la falta de confianza en los servicios e infraestructura de TIC representan amenazas serias a la reputación y la actividad de las empresas; y,*

*Exhortando que se creen normas internacionales aplicables,*

*Los participantes en el SMN insisten en:*

– Apoyar y promover principios de **transparencia** e **integridad tecnológica.** Reconociendo que no puede haber confianza sin transparencia, los usuarios deben saber cómo se utilizan sus datos y aceptar o no dicha utilización. La integridad tecnológica potencia la gran seguridad necesaria en los servicios e infraestructura de TIC, refrenda las medidas de privacidad y rechaza la perspectiva de funcionalidad oculta, con objeto de impedir la modificación no autorizada de información y crear confianza en la exactitud, integridad y fiabilidad de la información.

– Mitigar los riesgos que plantean los **robots IoT** mediante la adopción de normas de seguridad. Los casos denunciados de abuso de dispositivos de Internet de las cosas (IoT) en ataques a gran escala distribuidos de denegación del servicio (DDoS) están aumentando. Estos ataques pueden dar lugar a la filtración de datos y considerables daños económicos y a la reputación de las organizaciones afectadas. Es necesario estudiar cómo aprovechar los adelantos en campos tales como la criptografía ligera y métodos de seguridad normalizados para lograr mayores niveles de seguridad utilizando poca potencia de cálculo.

– Evaluar la incidencia de la **computación cuántica** en la seguridad, la privacidad y la confianza y estudiar las **tecnologías** **cuánticas seguras**. Si bien la computación cuántica se encuentra aún en sus albores, se reconoce ampliamente que una vez se comience a utilizar esta tecnología en la práctica, los métodos de encriptación convencionales que protegen hoy en día los pagos, transacciones bancarias y las conversaciones telefónicas y por correo electrónico resultarán rápidamente ineficaces. Ha llegado el momento de evaluar la incidencia de la computación cuántica e investigar, ensayar, normalizar y preparar la transición hacia nuevos modelos de seguridad que resistan ataques cuánticos, mucho antes de que los sistemas sean vulnerables a dichos ataques.

# 3.3 Postura de los organismos de normalización respecto de la seguridad, la privacidad y la confianza

*Reconociendo el papel esencial que desempeñan las normas para garantizar la seguridad, la protección de la privacidad y la creación de confianza en los servicios e infraestructura de TIC;*

*Destacando que la seguridad, la privacidad y la confianza son esferas de trabajo consolidadas de muchos organismos internacionales de normalización que se dedican al campo de las TIC y otras tecnologías; y*

*Exhortando que la normalización aborde los problemas de seguridad, privacidad y confianza,*

*Los participantes en el SMN insisten en:*

– Apoyar el concepto de **privacidad en el diseño**, teniendo debidamente en cuenta las consideraciones de privacidad en todo el proceso de normalización. La privacidad en el diseño puede promoverse en las normas que incorporen funciones de privacidad y protección de datos, y las normas también pueden ser eficaces para garantizar la interoperatividad entre funciones de seguridad.

– Reconocer el papel que desempeña el **software de código fuente abierto** a la hora de abordar los problemas de seguridad, privacidad y confianza. El software de código fuente abierto y las normas contribuyen de manera complementaria al crecimiento e innovación de la industria de las TIC. El software es cada vez más complejo y si bien las comunidades de normalización y código fuente abierto colaboran en muchos campos, es preciso redoblar esfuerzos para facilitar el intercambio de trabajos entre estas dos comunidades y garantizar así software de alta calidad y gran seguridad.

– **Reforzar la colaboración** entre organismos de normalización en el desarrollo de marcos internacionales de seguridad, privacidad y confianza, reconocer sus mandatos y virtudes y aprovechar su actual labor. Los organismos de normalización deben atenerse a los principios de debido procedimiento, amplio consenso, transparencia, equilibrio y apertura en la elaboración de normas; comprometerse a velar por la excelencia técnica, la interoperatividad, la competencia, la innovación y el beneficio colectivo, así como por la disponibilidad universal de normas y su adopción voluntaria. Los organismos de normalización también deben colaborar en sus esfuerzos por reducir la disparidad entre países desarrollados y en desarrollo en cuanto al acceso y aplicación de normas y marcos de seguridad, privacidad y confianza en los servicios e infraestructura de TIC, y participar en pie de igualdad en la preparación de dichas normas y marcos.

Apéndice I
Resumen detallado de los debates del SMN-16

(El presente Apéndice no forma parte del Informe)

Sesión 1: Bienvenida y discursos

**El Excmo. Sr. Mohamed Anouar Maarouf**, Ministro de Tecnologías de Comunicación y Economía Digital de la República de Túnez, [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Maarouf)] dio calurosamente la bienvenida a todos los participantes y agradeció a los miembros de la UIT que hubieran escogido Hammamet (Túnez) para acoger el Simposio Mundial de Normalización y la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT). Subrayó la necesidad de propiciar la confianza en la infraestructura y los servicios de las TIC, reconociendo la importancia de la temática del SMN-16: *Seguridad, privacidad y confianza en la normalización.*

En su discurso de apertura, el Presidente del SMN-16, **Sr. Mongi Marzoug** (Exministro de TIC de Túnez) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Marzoug)], dio la bienvenida a Túnez a todos los participantes y les deseó una agradable estancia en Hammamet. Insistió en el importante papel que las tecnologías de la información y la comunicación (TIC) desempeñan en nuestra vida diaria y cómo lo seguirán haciendo en el futuro. Subrayó la relevancia para el desarrollo mundial en todos los ámbitos (por ejemplo, sanidad, finanzas, servicios públicos, Internet de las cosas) de contar con servicios de TIC abiertos, seguros y fiables. En ese contexto, señaló, la normalización tiene un papel fundamental que desempeñar para mejorar la seguridad de las TIC, proteger la privacidad y crear en los ciudadanos, gobiernos y empresas confianza en los servicios de TIC. Señaló que el objetivo de este tercer SMN es presentar y tratar de las contribuciones a la seguridad, la privacidad y la confianza en la infraestructura y los servicios de TIC de las tres principales partes interesadas, a saber, los gobiernos y los reguladores, la industria y los organismos de normalización, para posteriormente presentar sus conclusiones y recomendaciones al respecto a la AMNT-16.

El **Sr. Houlin Zhao** (Secretario General de la UIT) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Zhao)] agradeció a la República de Túnez, anfitriona del SMN y de la AMNT, su apoyo a la labor de la UIT. Al mencionar el resultado positivo de las contribuciones de las anteriores ediciones del SMN, describió el modo en que el SMN proporciona una plataforma internacional para debatir la política de normalización, congregando a líderes de los sectores público y privado para abordar el modo en que la normalización técnica debería dar respuesta a la evolución de las prioridades del sector de las TIC. Las conclusiones y recomendaciones del SMN-08 y del SMN-12 han pasado a ser primordiales para el programa de trabajo de normalización en la UIT. También señaló que un entorno de las TIC fiable ofrecerá confianza a los usuarios y a las empresas para aprovechar plenamente el potencial de las TIC, y que la labor de normalización en la UIT desempeña un papel importante para cumplir el mandato de la UIT de "crear confianza y seguridad en la utilización de las TIC". Al concluir, manifestó su gratitud a todos los oradores, moderadores y participantes por su contribución al SMN-16.

En su discurso de bienvenida, el **Sr. Chaesub Lee** (Director de la Oficina de Normalización de las Telecomunicaciones de la UIT) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Lee)] describió cómo las redes futuras tendrán que soportar un gran volumen de aplicaciones de TIC y un muy amplio espectro de servicios. Miles de millones de dispositivos, cosas y objetos interconectados permitirán a los sistemas comunicarse y aprender unos de otros, creando así ecosistemas inteligentes que adaptarán su comportamiento en pro de la eficacia. Las comunicaciones de la próxima generación tendrán aplicaciones en ámbitos que irán de los servicios de voz y vídeo a la robótica industrial, el transporte inteligente, la cirugía a distancia y la realidad virtual, por mencionar sólo algunos. El Sr. Lee señaló que esta creciente sofisticación de las TIC y su ubicuidad, que está alcanzando niveles sin precedentes, necesitarán importantes transformaciones de los servicios y la infraestructura de red. En una sociedad global en la que prácticamente todos los aspectos de la actividad socioeconómica van a depender de las TIC, es fundamental que creemos servicios e infraestructuras de TIC que merezcan nuestra confianza. Destacó el papel que desempeñan las normas técnicas para evitar que surjan "silos" de datos en diversos sectores de nuestras economías y señaló que los expertos que participan en las actividades de normalización de la UIT trabajan en pro del desarrollo de un ecosistema de datos compartido e integrado.

Sesión 2: Principios reglamentarios para la seguridad, la privacidad y la confianza

Esta sesión, en la que se presentaron los principios reglamentarios para la seguridad, la privacidad y la confianza, fue moderada por el **Sr. Bilel Jamoussi** (Jefe de Comisiones de Estudio de la Oficina de Normalización de las Telecomunicaciones de la UIT) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Jamoussi)].

En su discurso, el **Sr. John Edwards** (Comisionado de Privacidad de Nueva Zelandia y Presidente del Comité Ejecutivo de la Conferencia Internacional de Protección de Datos y Comisionados de Privacidad) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Edwards)] reconoció avances paulatinos y cada vez mayores para alcanzar un consenso entre organizaciones anteriormente dispares, y convenir en que la privacidad reviste cada vez más importancia en nuestra época. Edwards destacó que la Asamblea General de las Naciones Unidas atendió esta petición en su 68º periodo de sesiones (2013) mediante la adopción de la Resolución titulada "*el derecho a la privacidad en la era digital*", en la que se exhorta a los Estados Miembros de las Naciones Unidas a "*respetar y proteger el derecho a la privacidad en las comunicaciones digitales*". Presentó el trabajo de la organización que representa, la Conferencia Internacional de Comisarios para la Protección de Datos y de la Privacidad, y propuso varias ideas para propiciar la confianza mediante la aplicación de principios sobre privacidad y, tal vez, la elaboración de normas en el sector de las telecomunicaciones, en particular:

– Fomentar la adhesión a principios sobre privacidad en el diseño, evaluación del impacto en la privacidad y desarrollo de tecnologías que mejoren la privacidad (PET).

– Velar por que el acceso a las redes, los sistemas, el contenido, las comunicaciones y los metadatos por los agentes estatales tenga lugar exclusivamente de conformidad con la autoridad jurídica pertinente, únicamente en los casos en que dicho acceso sea necesario y proporcional.

– Promover la transparencia con respecto al acceso a datos personales, o su utilización, para fines que no sean aquellos para los que el titular de los datos ha otorgado su consentimiento.

– Elaborar y promover normas y salvaguardias adecuadas para la "desidentificación" de datos personales y para la prevención de la "reidentificación" de personas en conjuntos de datos no identificados.

– Elaborar normas sobre portabilidad de datos y normas que puedan contribuir a mejorar la protección del consumidor y a ampliar sus opciones con respecto a la suscripción a servicios TIC y la anulación de dicha subscripción.

– Garantizar que los ciudadanos y los consumidores sigan beneficiándose de la transparencia necesaria en lo concerniente a las decisiones automatizadas que les afecten.

En su intervención, el **Sr. Víctor Manuel Martínez Vanegas** (Director de Política Internacional del Instituto Federal de Telecomunicaciones de México) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Vanegas)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSS_IFT_Draft_Presentation.pdf)] abordó el SMN desde una perspectiva global, habló de las iniciativas adoptadas a nivel regional y presentó el contexto nacional para la seguridad, la privacidad y la confianza en las TIC.

Posteriormente describió cómo el desarrollo y la adopción de las TIC han repercutido positivamente en el crecimiento socioeconómico, pero dijo que también hay amenazas y trampas que pueden poner en peligro esos beneficios. La seguridad, la privacidad y la confianza se han convertido en puntos clave que hay que abordar adecuadamente. Se remitió a publicaciones, declaraciones y acuerdos sobre este tema de la Asamblea General de las Naciones Unidas, las actividades de normalización del UIT-T y la CEI, así como al *Information Economy Report* de 2015 de la UNCTAD, donde se dice que la seguridad y la confianza son fundamentales para crear un entorno propicio para el comercio electrónico. El Sr. Martínez Vanegas señaló que en su región, América Latina y el Caribe, es donde la población de Internet crece más rápido de todo el mundo, por lo que el tema de la seguridad, la privacidad y la confianza en las TIC es clave para el desarrollo socioeconómico de la región. Insistió además en que la experiencia en esa región ha demostrado que ningún país puede por sí solo asegurar adecuadamente sus redes y que la cooperación es fundamental.

El **Sr. Ilias Chantzos** (Director Jefe, Asuntos Gubernamentales, EMEA, Global CIP y Privacy Advisor, Symantec, Estados Unidos) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Chantzos)/[Documento de referencia](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/InternationalCyberNorms_Ch10%20-%20Symantec.pdf)] describió cómo los factores políticos y reglamentarios influyen en los adelantos tecnológicos que, a su vez, influyen sobre esos factores. Citó la Reglamentación general de protección de datos de la EU como uno de los ejemplos más evidentes de esa dinámica. La Directiva sobre privacidad en vigor tiene más de 20 años y es necesario adaptarla a la evolución o, más bien, revolución, que la tecnología y otros factores, como los medios sociales, han experimentado. Al mismo tiempo, la utilización de la tecnología y los medios sociales tendrá que conformarse a la nueva Reglamentación con modificaciones esenciales de la manera en que las organizaciones públicas y privadas ejercerán la gobernanza de datos, incluida la protección de los datos de carácter personal contra los ciberataques. Chantzos también presentó el concepto de integridad tecnológica en apoyo a la necesidad de contar con una elevada seguridad en los servicios e infraestructura de las TIC, refrendando las medidas de privacidad y rechazando la perspectiva de funcionalidad oculta, con objeto de impedir la modificación no autorizada de información y crear confianza en la exactitud, integridad y fiabilidad de la información.

El **Sr. James M. Kilaba** (Director General a.i. de la Autoridad de Reglamentación de las Comunicaciones de Tanzanía (TCRA)) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Kilaba)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSSWTSA2016-Kilaba.pdf)] destacó los retos en materia de seguridad y privacidad que plantean los avances tecnológicos registrados desde el momento en que únicamente había unos pocos ordenadores personales conectados a Internet hasta las comunicaciones de hoy en día entre todas las personas y todas las cosas, en cualquier lugar y en todo momento. Describió las iniciativas adoptadas en los planos nacional y regional para proteger la privacidad, la seguridad de los datos y las infraestructuras de las TIC, en particular: el establecimiento de un equipo informático nacional de respuesta a situaciones de emergencia, con objeto de fomentar los conocimientos, la información y las competencias sobre ciberseguridad entre diversas partes interesadas; la implantación de DNSSEC en el sistema de registro de nombres de dominio de Internet; y el debate sobre ciberseguridad en la Organización para las Comunicaciones de África Oriental. Kilaba pidió un enfoque global para abordar estos retos, y subrayó la necesidad de armonizar las normas internacionales en apoyo a los países en desarrollo.

El **Sr. Chawki Gaddes** (Presidente de la Autoridad Nacional para la Protección de la Información personal de Túnez) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Gaddes)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSS-Gaddes.pdf)] describió el papel primordial de Túnez para garantizar, en el marco de su Constitución, la protección de la privacidad y de los datos personales (Artículo 24, 2014), el acceso a la información y a las redes de comunicaciones (Artículo 32, 2004) y el acceso a documentos gubernamentales (entrada en vigor prevista para 2017). Destacó la forma en que Túnez atribuye gran importancia a la creación de un espacio de confianza entre sus ciudadanos, el sector privado y el gobierno.

Sesión 3: Cómo cumple la industria las expectativas de seguridad, privacidad y confianza de los usuarios finales

El **Sr. Ilias Chantzos** (Director Jefe, Asuntos Gubernamentales, EMEA, Global CIP and Privacy Advisor, Symantec, Estados Unidos) moderó las dos partes de esta sesión dedicada a considerar cómo cumple la industria las expectativas de seguridad, privacidad y confianza de los usuarios finales.

El **Sr. Ammar Alkassar** (Director General, Rohde & Schwarz Cybersecurity, Alemania) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Alkassar)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/3-1201601024_ITU%20GSS16_ALKASSAR_2.pptx)] destacó las tendencias en las TIC que repercutirán notablemente a nivel internacional. Describió la utilidad de la ciberseguridad para propiciar ese cambio, que será aún más trascendental en el futuro. El Sr. Alkassar señaló que las herramientas de seguridad utilizadas actualmente no son las más adecuadas con respecto al valor económico que es necesario proteger. Señaló la necesidad de definir nuevos conjuntos de normas a raíz del cambio de paradigma en la seguridad de las TI con objeto de hacer frente al mayor nivel de sofisticación de las amenazas. De acuerdo con Rohde & Schwarz, dicho cambio de paradigma radica en los elementos siguientes: implantación de la seguridad en el diseño y adopción de medidas preventivas, en lugar de reactivas; fomento del control del flujo de información, en lugar del control de acceso; y exención de responsabilidades inasumibles a los usuarios en materia de ciberseguridad. Señaló que la comunidad de la UIT puede realizar aportaciones notables al respecto, especialmente mediante actividades de normalización y vinculando la comunidad tradicional de las telecomunicaciones con los nuevos actores de las TIC.

El **Sr. Thomas Kremer** (Miembro de la Junta de Administración para la Privacidad de los Datos, Asuntos Jurídicos y Conformidad, Deutsche Telekom, Alemania) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Kremer)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Deutsche%20Telekom%20-%20final.pptx)/[Documento de referencia](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Getting%20out%20of%20the%20digital%20trust%20trap%20-%20deutsche%20telekom.pdf)] hizo hincapié en que la transparencia es un requisito *sine qua non* de la confianza. Las personas tienen que poder saber cómo se utilizan sus datos y poder decidir con conocimiento de causa si aceptan o no tal utilización. Sin embargo, la transparencia por sí sola no basta. El Dr. Kremer abogó por sistemas fiables que anonimicen los datos en todos los casos sin necesidad de intervención directa del interesado. En su opinión, la encriptación es otra manera de lograr la confianza del cliente, sobre todo cuando se trata de datos sensibles, como los sanitarios. La postura de Deutsche Telekom es que cualquier propuesta para facilitar a las autoridades "llaves maestras" o "puertas traseras" para asegurar los sistemas será contraproductiva y minará los esfuerzos invertidos en aumentar la seguridad, pues rápidamente podrán ser explotados por los adversarios. El Sr. Kremer dijo que se han de encontrar soluciones inteligentes, prácticas y oportunas en el ámbito de la ciberseguridad. Con las nuevas tecnologías (IoT, aprendizaje automático, computación cuántica, etc.) aparecerán ataques cada vez más sofisticados. Se necesitan métodos normalizados de detección y mitigación de riesgos y ataques.

El **Sr. David Francis** (Director de ciberseguridad Europea, Huawei Technologies, China) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Francis)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Huawei%20-%20final.pptx)] explicó lo que la protección de la privacidad y la seguridad implican desde el punto de vista del fabricante de tecnología. Habló de las políticas y procedimientos que utiliza hoy en día una empresa como Huawei Technologies para garantizar la seguridad y resiliencia de sus productos, lo que, en último término, contribuirá a proteger la privacidad y los datos de los usuarios finales. Cabe considerar los siguientes elementos clave para lograr un enfoque global: dispositivos seguros; la arquitectura – las redes están formadas por diversos productos complejos; y las personas, que aplican, gestionan, actualizan, fijan y evalúan el entorno. El Sr. Francis habló de la necesidad de gestionar la cadena de producción mundial de la que depende enteramente el sector de TI a fin de prevenir cualquier riesgo de seguridad; del papel de la transparencia y las normas mundiales; y de lo necesaria que es la cooperación internacional para mejorar la ciberseguridad en todo el planeta.

La **Sra. Jaya Baloo** (Directora Jefa de Seguridad de la Información de KPN, Países Bajos) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Baloo)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/3-4ITU-GSS-Tunesia.pdf)] expuso los avances sobre tecnologías cuánticas, en particular la computación y la criptografía cuánticas. La disponibilidad de computadores cuánticos planteará un riesgo de seguridad a los países y las empresas que utilicen aplicaciones de criptografía asimétrica (RSA, ECC). Para dar respuesta a ello es necesario adoptar soluciones post-cuánticas en tres fases. En primer lugar, aumentando la longitud de la clave de los actuales algoritmos criptográficos. En segundo lugar, utilizando la distribución cuántica de claves en puntos críticos específicos de las redes. Y en tercer lugar, desarrollando e impulsando futuros algoritmos criptográficos post-cuánticos. La comunidad internacional de la seguridad de la información está logrando avances muy significativos en materia de innovación en el campo de las tecnologías cuánticas. No obstante, existe el riesgo de que ello conlleve una nueva brecha digital en materia de seguridad que permita a los países con los recursos financieros y académicos necesarios para poseer computadores cuánticos descifrar los sistemas criptográficos de otros países al tiempo que protegen sus propias comunicaciones, y que haga que algunos países no puedan atacar ni defenderse.

El **Sr. James Snow** (Estratega en Seguridad y Conformidad, Google, Estados Unidos) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Snow)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Google-final.pptx)/[Documento de referencia](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GoogleExecSummary_2016.pdf)] dijo que una de las principales prioridades de Google es ganar y conservar la confianza de sus clientes gracias al procesamiento de los datos en un entorno seguro, fiable y legal. La seguridad y la privacidad revisten una importancia fundamental para Google, motivo por el que la empresa está invirtiendo masivamente en la protección de los datos de sus clientes, para lo que se utilizan servidores e infraestructuras de red fabricados *ex profeso* y la encriptación de los datos, ya se estén en disco, almacenados en servidores de seguridad, en movimiento por Internet o en tránsito entre centros de datos.

El Sr. Snow describió cómo la confianza del cliente empieza con la comprensión, que sólo se puede conseguir mediante la transparencia, por ejemplo, facilitando documentación detallada, informes de auditoría y certificados. Google es consciente de la importancia de la cooperación internacional y aplica diversas normas internacionales de seguridad y privacidad como:

– ISO 27001:2013, Tecnología de la Información – Técnicas de Seguridad – Sistema de Gestión de la Seguridad de la Información – Requisitos";

– ISO 27017: Tecnologías de la información – Técnicas de seguridad – Código de conducta para los controles de seguridad de la información de servicios de computación en la nube basados en ISO/CEI 27002;

– ISO 27018:2014 Tecnologías de la información – Técnicas de seguridad – Código de conducta parala protección de la información de identificación personal (IIP); y

– SOC 2/SOC 3 – Marco de auditoría sobre principios de no privacidad en materia de seguridad, disponibilidad, integridad de procesamiento y confidencialidad.

El **Sr. Yuejin Du** (Vicepresidente de Seguridad, Alibaba Group, China) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Du)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Yuejin-DU.pptx)] habló de la importancia de la seguridad y la privacidad en la infraestructura que Alibaba ofrece a sus clientes comerciales y de tecnología de datos. Por ejemplo, Alibaba facilita productos y normas de seguridad de la información a sus socios en la alianza de seguridad del ecosistema de comercio electrónico a fin de que puedan aprovechar los modelos de detección de riesgos establecidos para examinar e identificar amenazas.

El **Sr. Bernard** **Benoit** (Director General, WhiteNoise/Kudelski Security, Suiza) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Benoit)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Kudelski%20-%20final.pdf)] explicó el posible conflicto entre los intereses de los usuarios, los proveedores de servicios y los gobiernos y cómo las redes de seguridad actuales están dominadas por los fallos de seguridad, por lo que no pueden garantizar la seguridad y la privacidad de las comunicaciones. Para reforzar la seguridad y aumentar la privacidad en redes no fiables, dijo optar por un componente de hardware de seguridad adaptable basado en la superposición, que funcionaría con independencia de las redes y protocolos subyacentes. El Sr. Benoit recordó a los presentes la necesidad de encontrar soluciones independientes de las plataformas con interfaces normalizadas compatibles para ajustarse a los requisitos de intercepción legítima aplicables sin poner en peligro la integridad tecnológica mediante puertas traseras, llaves maestras, etc.

Sesión 4: Enfoque adoptado por los organismos de normalización en relación con la seguridad, la privacidad y la confianza

En la Sesión 4 se examinó cómo los diversos organismos de normalización enfocan sus trabajos en relación con la seguridad, la privacidad y la confianza. El moderador de la sesión fue el **Sr. Toni Eid** (Editor Jefe, Telecom Review) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Eid)].

La **Sra. Sophie Clivio** (Directora, Política Técnica y de Normalización, Organización Internacional de Normalización (ISO)) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Eid)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/ISO%20-%20final.PPTX)] presentó el amplio y multisectorial enfoque adoptado por la ISO en relación con la seguridad, la privacidad y la confianza. Subrayó el trabajo realizado por los comités de la ISO sobre la seguridad y la resiliencia, la gestión de riesgos, las tecnologías de cadena de bloques y contabilidad electrónica distribuida; así como las actividades que realizan conjuntamente la ISO y la CEI sobre la seguridad y la privacidad en el seno del Comité Mixto sobre Tecnología de la Información (ISO/CEI JTC 1). Los principales temas tratados por el JTC 1 son la gestión de la seguridad de la información, la gestión criptográfica y de seguridad, las tecnologías de gestión de la identidad y de privacidad, la biometría, las tarjetas y la identificación personal, la gobernanza de TI, los mecanismos de seguridad, privacidad y confianza para la computación en la nube, los macrodatos y la IoT. La Sra. Clivio señaló que la ISO y sus normas están presentes en numerosos sectores de la economía, incluidos la sanidad, el transporte (por ejemplo, la aviación, los sistemas de transporte inteligentes, la tecnología marítima), la energía, la construcción y la industria (incluida la aditiva), y que se han concluido acuerdos de cooperación con las organizaciones que se ocupan de las necesidades y particularidades de esos sectores.

El **Sr. Frans Vreeswijk** (Secretario General y Director Ejecutivo, Comisión Electrotécnica internacional (CEI)) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Vreeswijk)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/IEC%20-%20final.pptx)] describió el modo en que la CEI reúne a todas las partes interesadas en la electrotecnología con objeto de propiciar la confianza en productos y sistemas seguros y eficientes mediante la utilización de las normas internacionales de la CEI y de sus sistemas de evaluación de conformidad. La CEI ha publicado más de 200 normas sobre ciberseguridad que hacen hincapié en la protección frente a ciber-vulnerabilidades y ataques de infraestructuras esenciales tales como los sistemas de generación y distribución de electricidad, la gestión del agua y de residuos, los hospitales y sistemas sanitarios y los centros de producción y de datos. La CEI también contribuye notablemente a la seguridad de todos los equipos eléctricos y electrónicos que permiten obtener datos, el acceso a protocolos y el control de los mismos. Ello incluye sensores, dispositivos médicos, dispositivos inteligentes portátiles y tecnologías de computación y almacenamiento de datos. Las normas internacionales de la CEI son clave para propiciar la resiliencia, la gestión de riesgos y la mejora de la eficiencia.

La CEI colabora estrechamente con la ISO en el marco del Comité Mixto sobre Tecnología de la Información (ISO/CEI JTC1) en esferas como la gestión de la seguridad de la información, la gestión de identidad, la criptografía y la identificación de seguridad, las tecnologías relativas a la privacidad, los sistemas biométricos, las tarjetas y la identificación personal, la computación en la nube y las grandes cantidades de datos, entre otras muchas. La CEI colabora actualmente con la UIT y la ISO en el marco de la Cooperación Mundial sobre Normas.

El Sr. Vreeswijk pidió una amplia colaboración entre todas las organizaciones normativas para abordar temas relativos a la seguridad, la privacidad y la confianza, puesto que ninguna organización será capaz de elaborar por sí sola todas las normas necesarias en esta esfera.

La **Sra. Karen McCabe** (Directora General, Política tecnológica y Asuntos Internacionales, IEEE Standards Association (IEEE-SA)) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#McCabe)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/IEEE-final.pptx)] insistió en que las normas tienen un papel crucial que desempeñar a la hora de garantizar la seguridad y la privacidad y propiciar la confianza en las TIC. Para ello, lo mejor es trabajar en el marco de una serie de principios en torno a los cuales se crea una comunidad de interesados que cooperan voluntariamente, lo que da pie a la excelencia técnica, la interoperatividad mundial y la innovación. Entre esos principios se cuentan la participación directa, los procedimientos reglamentarios, el amplio consenso, el equilibrio, la transparencia, la apertura universal, la coherencia y la dimensión de desarrollo.

Señaló que los procesos abiertos son convenientes desde una perspectiva de seguridad, pues cuantos más expertos puedan examinarlos, más posibilidades habrá de descubrir los posibles fallos y de mejorar las normas durante su fase de elaboración. La transparencia en el proceso de creación de normas abiertas fomenta la confianza en las plataformas, servicios y productos que responden y se ajustan a ellas. Del mismo modo, las normas abiertas hacen que las tecnologías que aumentan la seguridad y la privacidad se generalicen, pues fomentan la interoperatividad. En conclusión, las normas abiertas alimentan la innovación, que puede dar lugar a soluciones a los problemas de seguridad, privacidad y confianza.

El IEEE tiene en su haber una amplia gama de normas, desde las consideraciones sobre seguridad privacidad y confianza de la serie IEEE 802 de normas sobre redes, hasta la criptografía de la serie IEEE 1363 (centrada en los algoritmos basados en la infraestructura de clave pública (PKI)) y la serie IEEE 1619, entre muchas otras. El Grupo de Seguridad de Conexiones de la Industria del IEEE (ICSG) es un grupo de entidades de seguridad informática que se han reunido para poner en común su experiencia y sus recursos para luchar contra la rápida y sistemática aparición de amenazas de seguridad informática. Recientemente se puso en marcha la *IEEE Internet Initiative* para aumentar la especialización de la organización en materia de política tecnológica mundial, así como su influencia en esferas tales como la gobernanza de Internet, la ciberseguridad y la definición de políticas de privacidad, aportando sólidos conocimientos técnicos y científicos, además de orientaciones, al proceso. La *IEEE Global Initiative for Ethical Considerations in the Design of Autonomous Systems* y su Comité ad hoc sobre Ética, Sociedad y Tecnología están estudiando nuevas normas y soluciones, certificaciones y códigos de conducta, creando además consenso en torno a la implementación ética de las tecnologías inteligentes, incluidos los sistemas autónomos y la inteligencia artificial.

Por último, la Sra. McCabe abogó por la integración de una nueva generación de profesionales de la privacidad, la seguridad y la ética interdisciplinarios en el proceso de normalización; y por la incorporación de dimensiones de privacidad, seguridad y ética en las normas mismas a fin de aumentar la confianza en las TIC.

El **Sr. Ashok Ganesh** (Director de Innovación, CEN-CENELEC) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Ganesh)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/CEN-CENELEC-final.pptx)] dijo que todos los sectores industriales están transformándose a medida que adoptan métodos y tecnologías digitales (por ejemplo, Internet de las cosas, computación en la nube, robótica, tecnologías de sensores) que modifican radicalmente sus procesos, sistemas e, incluso, sus modelos comerciales. Esos sectores industriales verticales tradicionales (por ejemplo, la manufactura, la energía, el transporte) que no solían utilizar de manera importante las TIC y las tecnologías digitales, buscan soluciones de normalización sobre las que basar esa transformación. El Sr. Ganesh señaló que los organismos de normalización como ISO, CEI y CEN-CENELEC en Europa han dejado una importante huella en esos sectores verticales y buscan mejorar sus métodos para colmar las necesidades relacionadas con las TIC/tecnologías digitales. La adopción de esas tecnologías conlleva el empleo de sistemas para la planta industrial y los procesos de fabricación, así como la generación, el procesamiento, la compartición y el almacenamiento de grandes cantidades de datos. El Sr. Ganesh subrayó que los organismos de normalización se enfrentan a múltiples retos: mantener el compromiso de los interesados tradicionales, atraer a nuevos participantes del sector TIC/digital y modificar sus métodos para poder facilitar directa e indirectamente soluciones de normalización en una esfera cada vez más compleja y que evoluciona rápidamente. Una de las prioridades de los organismos de normalización es centrarse en las necesidades y aplicaciones verticales, incluido el vínculo entre la ciberseguridad y la seguridad funcional, la fiabilidad de los productos y la seguridad y privacidad de los datos.

El **Sr. Reinhard Scholl** (Director Adjunto de la Oficina de Normalización de las Telecomunicaciones de la UIT) [[Biografía](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Scholl)/[Presentación](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Reinhard-final.pptx)] recordó a todos los participantes un simposio sobre ciberseguridad celebrado simultáneamente con la AMNT-04 en Florianópolis (Brasil). En el simposio se llegaron a 11 conclusiones clave, la mayoría de la cuales siguen vigentes en la actualidad, por ejemplo que "La seguridad debe integrarse y no añadirse", o que "Las diferentes partes interesadas deberían intercambiar la información de que disponen", y que "la normalización es un componente esencial del enfoque mundial respecto a la ciberseguridad.

Con respecto a la situación actual, proporcionó algunas cifras relativas al número de ciberincidentes registrados en la infraestructura de red de la UIT. Afirmó que, a su parecer, la seguridad y la privacidad no son mutuamente exclusivas. También explicó que la UIT sigue trabajando para propiciar la confianza y la seguridad en las TIC, con objeto de que las infraestructuras, los servicios y las aplicaciones de red sean más seguros. Presentó los últimos trabajos de la UIT en relación con la seguridad y la confianza, incluido un informe en el que se resalta la importancia y la necesidad de la confianza en el contexto de las TIC y se presentan conceptos sobre ese asunto, así como características clave de la confianza. Una de las ideas expuestas en el informe es la de un "índice de confianza" que conjugue varios indicadores sobre confianza en una sola medida de referencia. Dicho índice podría utilizarse para comparar el grado de confianza entre las partes interesadas al establecer una nueva relación de confianza o una cadena de valor de confianza.

El Sr. Scholl señaló que los miembros han empezado a estudiar los requisitos, capacidades e hipótesis de servicio para la facilitación de confianza; el marco arquitectónico de las redes de comunicaciones fiables; las soluciones técnicas para la facilitación de confianza, incluso en el análisis de macrodatos; y la gestión de la confianza entre nubes a fin de elaborar Recomendaciones UIT-T al respecto. El UIT-T también se dedica a la normalización en materia de ciberseguridad, gestión de la seguridad, arquitecturas y marcos de seguridad, la lucha contra el spam, la gestión de identidades y la protección de información de identificación personal. El Sr. Scholl también recomendó que se estudiara la contribución que la comunidad de fuente abierta puede realizar en materia de normas sobre seguridad, privacidad y confianza en las infraestructuras y los servicios de las TIC. Afirmó que deberían desplegarse mayores esfuerzos para fomentar la colaboración entre las comunidades de fuente abierta y de normalización, a fin de garantizar normas de calidad y la aplicación de los soportes lógicos pertinentes.

Notas

1. Véase, por ejemplo, la Recomendación UIT-T X.1171 "Amenazas y requisitos para la protección de información de identificación personal en las aplicaciones que utilizan la identificación basada en las etiquetas". [↑](#endnote-ref-1)
2. Véase, por ejemplo, la Resolución 130 (Rev. Busán, 2014), sobre el fortalecimiento de la función de la UIT en la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación. [↑](#endnote-ref-2)
3. <http://www.un.org/en/universal-declaration-human-rights/> [↑](#endnote-ref-3)
4. <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> [↑](#endnote-ref-4)
5. <http://www.un.org/documents/ga/res/45/a45r095.htm>; UN Doc E/CN.4/1990/72 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement> [↑](#endnote-ref-5)
6. <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37> [↑](#endnote-ref-6)
7. <http://www.echr.coe.int/Documents/Convention_ENG.pdf> [↑](#endnote-ref-7)
8. <https://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm> [↑](#endnote-ref-8)
9. Véase, por ejemplo, el marco de privacidad de la APEC y la normativa de la UE sobre privacidad, que se han inspirado en cierta medida en las Directrices de la OCDE sobre la protección de la vida privada y la circulación transfronteriza de los datos de carácter personal; <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> [↑](#endnote-ref-9)
10. Declaración de Montreux de la Conferencia Internacional de Comisarios para la Protección de Datos y de la Privacidad, <https://icdppc.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf> [↑](#endnote-ref-10)
11. Resolución 68/167 de la AGNU, <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [↑](#endnote-ref-11)