|  |  |  |
| --- | --- | --- |
| 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 | **Documento 58-S** |
|  | **24 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. |

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** entro 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 integrante del Informe)

Un resumen detallado de las presentaciones efectuadas en el SMN‑16 figurarán en la Revisión 1 al presente Documento.

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)