



**ORGANIZACION DE LOS ESTADOS AMERICANOS  
ORGANIZATION OF AMERICAN STATES**

**Comisión Interamericana de Telecomunicaciones  
Inter-American Telecommunication Commission**

**XVII REUNIÓN DEL COMITÉ CONSULTIVO  
PERMANENTE I: TELECOMUNICACIONES/  
TECNOLOGIAS DE LA INFORMACION Y LA  
COMUNICACION**

**Del 2 al 5 de noviembre de 2010  
Salta, Argentina**

**OEA/Ser.L/XVII.4.1  
CCP.I-TIC/doc. 2013/10 rev. 1  
1 noviembre 2010  
Original: inglés**

**PROYECTO DE PROGRAMA  
TALLER REGIONAL PARA LAS AMÉRICAS DE DESARROLLO  
DE CAPACIDADES DE CIBERSEGURIDAD DE LA UIT Y LA  
CITEL  
“COOPERACIÓN INTERNACIONAL PARA LA CREACIÓN DE  
UNA CULTURA DE CIBERSEGURIDAD HEMISFÉRICA”  
(1 de noviembre de 2010, Salta, Argentina)  
(Punto del temario: 4.3)  
(Documento presentado por la UIT)**

## PROYECTO DE PROGRAMA

### TALLER REGIONAL PARA LAS AMÉRICAS DE DESARROLLO DE CAPACIDADES DE CIBERSEGURIDAD DE LA UIT Y LA CITEL

#### “COOPERACIÓN INTERNACIONAL PARA LA CREACIÓN DE UNA CULTURA DE CIBERSEGURIDAD HEMISFÉRICA”

1 de noviembre de 2010, Salta, Argentina

08:00–09:00	Inscripción a la reunión y entrega de las tarjetas de identificación (Se requiere una inscripción previa en línea)
09:00–09:20	Apertura de la reunión y palabras de bienvenida
	<i>Palabras de apertura:</i> Héctor Carril, Secretaría de Comunicaciones, Argentina <i>Palabras de apertura:</i> Clovis Baptista, Comisión Interamericana de Telecomunicaciones <i>Palabras de apertura:</i> Mario Maniewicz, Unión Internacional de Telecomunicaciones
09:20–11:00	Sesión 1: Entender la situación global y hemisférica de las amenazas cibernéticas
	<p><b>Descripción de la sesión:</b> La confianza y la seguridad en el uso de tecnologías de la información y la comunicación son fundamentales para construir una Sociedad de Información abarcadora, segura y global. Generalmente se reconoce la necesidad de promover la ciberseguridad y proteger las infraestructuras críticas a nivel nacional, regional e internacional. Esta sesión comparte una visión general acerca del panorama actual de las amenazas cibernéticas remarcando las principales amenazas y tendencias y ofrece una descripción de los desafíos que enfrentan los países, las empresas y los ciudadanos en el manejo de sus rutinas en este ambiente nuevo y en constante cambio. También explora cómo los países del hemisferio pueden evaluar los riesgos relacionados con posibles ataques si se conocen cuáles son los activos críticos para su contexto nacional y cuáles son las diferentes partes interesadas que deben estar involucrados. También detalla las actividades regionales que llevan a cabo las entidades de la OEA - CITEL, CICTE y REMJA.</p> <ul style="list-style-type: none"><li>- Mario Maniewicz, UIT, Políticas y Estrategias,</li><li>- Wayne Zeuch, CITEL, por la Rapporteur for Cybersecurity and Vulnerability Assesment</li><li>- Belisario Contreras, CICTE</li><li>- Albert Rees, REMJA, Presidente del Grupo de Trabajo sobre Crímenes de Ciberseguridad (presentación remota)</li></ul>
11:00–11:30	Pausa

<b>11:30–13:00</b>	<b>Sesión 2: Normas técnicas e intercambio de información confiable para mejorar la ciberseguridad del hemisferio y construir una cultura de ciberseguridad hemisférica</b>
	<p><b>Descripción de la sesión:</b> Cada país y Región tiene sus propios requisitos y necesidades que deben ser abordados teniendo en cuenta el contexto nacional y regional específico. Una parte de esta sesión presenta algunas de las actividades principales de las organizaciones de desarrollo de normas (SDO), que se concentran en temas tales como arquitecturas de seguridad, ciberseguridad, gestión de seguridad, gestión de identidad, base de seguridad para los operadores de red, Marco Global de Intercambio de Información de Ciberseguridad (CYBEX) y las Guías Básicas de las Normas de Seguridad de las TIC iniciadas por la Comisión de Estudio 17 del UIT-T.</p> <p>Dado que los actores del sector público y privado nacional aportan su propia perspectiva acerca de la importancia de los asuntos, el rol de los organismos de desarrollo de normas regionales e internacionales se vuelve cada vez más importante. La segunda parte de esta sesión analiza las asociaciones y considera el rol de las actividades nacionales, regionales e internacionales en este contexto. Al permitir el conocimiento de los roles y responsabilidades de cada parte con respecto a la ciberseguridad y al participar en el intercambio recíproco de información, las asociaciones especializadas y funcionales pueden mitigar y reducir los riesgos e implementar un enfoque integral a la ciberseguridad.</p> <ul style="list-style-type: none"> <li>- William McCrum, Consultor, TSB ITU</li> <li>- Antonio Guimaraes (Anatel), Vicepresidente ITU-T Comisión de Estudio 17</li> <li>- Wayne Zeuch, CITELE, PCC.I Rapporteur for Standards, Conformity and Interoperability</li> </ul>
<b>13:00–14:15</b>	<b>Pausa</b>
<b>14:15–16:00</b>	<b>Sesión 3: Definición de Estructuras de Organización Válidas y Desarrollo de Capacidades de Gestión de Incidentes para facilitar la Ciberseguridad Hemisférica</b>
	<p><b>Descripción de la sesión:</b> Una actividad fundamental para abordar la ciberseguridad hemisférica requiere el establecimiento de capacidades de vigilancia, alerta y respuesta a incidentes a fin de prepararse para, detectar, manejar y responder en caso de incidentes cibernéticos. El manejo eficaz de incidentes requiere la consideración de financiamiento, recursos humanos, capacitación, capacidades tecnológicas, colaboración del gobierno y del sector privado y requisitos legales. Esta sesión analiza las mejores prácticas, estructuras de organización y normas relacionadas a los aspectos técnicos, de gestión y financieros para establecer capacidades de vigilancia, alerta y respuesta a incidentes.</p> <p>La primera parte de esta sesión se referirá a los requisitos para establecer capacidades de vigilancia, alerta y respuesta a incidentes a fin de responder a incidentes cibernéticos. Esto incluirá una demostración de cómo un país puede intentar defender sus redes contra ataques hostiles. Qué tipo de indicaciones experimentarán en sus redes, qué herramientas pueden utilizar para detectar la intrusión, qué herramientas son útiles en el manejo y en la respuesta a un ataque y con qué procesos y procedimientos debería contar el país de antemano.</p>

	<p>La segunda parte de esta sesión destacará el trabajo que está realizando la OEA para promover una cultura hemisférica de ciberseguridad, particularmente a través del desarrollo de “Equipos de Respuesta a Incidentes de Seguridad en Computadoras” (CSIRT) y de capacidades humanas.</p> <ul style="list-style-type: none"> <li>- Emiliano Colina, Jefe de Telecomunicaciones, Ministerio de Defensa, Uruguay</li> <li>- Jorge J. Uya, Information Security Specialist (remote presentation)</li> <li>- David Probert, Experto UIT – Estrategia Nacional de Ciberseguridad</li> <li>- Belisario Contreras – CICTE</li> </ul>
<b>16:00–16:15</b>	<b>Pausa</b>
<b>16:15–17:45</b>	<b>Sesión 4: Desarrollo de capacidades y cooperación internacional y hemisférica</b>
	<p><b>Descripción de la sesión:</b> Las realidades del espacio cibernético dejan en claro que todos tienen que trabajar en conjunto. Responder de manera efectiva a las amenazas cibernéticas requiere recursos, know-how e inversiones fuertes en desarrollos de capacidades. Un elemento clave es reunir a todas las partes interesadas para abordar los desafíos comunes de ciberseguridad y desarrollar planes sólidos de creación de capacidades. Esta sesión examina los posibles mecanismos para crear capacidades de manera efectiva, a través de la colaboración y cooperación entre todas las partes interesadas a nivel nacional, regional e internacional, para lograr una mejor ciberseguridad hemisférica e incluye un enfoque en el importante papel del sector privado.</p> <p>También incluye un enfoque sobre los estudios comparativos/ejercicios de evaluación para proporcionar información a los Estados Miembros de las Américas que les permita contrastar y comparar diversas políticas actuales que se están implementando en todo el hemisferio y que se incluyen en la Resolución de la Asamblea General de las Naciones Unidas 64-211.</p> <p>Para cada país es fundamental promover una cultura de ciberseguridad. Es necesaria una colaboración estrecha entre todas las partes interesadas relevantes. El trabajo realizado en la Comisión de Estudio 2 del UIT-D, Cuestión 22/1 ha sido fundamental para educar a las partes interesadas en este sentido. La tercera parte de esta sesión proporcionará una visión general del trabajo que se ha realizado en la Cuestión 22 y la interacción entre las partes de la Región.</p> <ul style="list-style-type: none"> <li>- ITU-D Q22-Ciberseguridad, James Ennis, Departamento de Estado, EEUU</li> <li>- ITU Esfuerzos para crear capacidad en Ciberseguridad, Dr. David Probert</li> <li>- Proyecto Amparo, Eduardo Carozo, Director</li> <li>- OAS/CICTE Experto, Belisario Contreras</li> </ul>
<b>17:45–18:00</b>	<b>Cierre del taller y conclusiones</b> <b>1. UIT, Sergio Scarabino</b>

	<b>2. CITEL, Clovis Baptista</b>