Foro Regional de la UIT para las Américas sobre Ciberseguridad 2009

"Conectar el mundo responsablemente"

23-25 de noviembre de 2009
Santo Domingo, República Dominicana[1]

Programa del Foro

Descripción: Las tecnologías de la información y la comunicación (TIC) pueden desempeñar un papel decisivo en el proceso de desarrollo de un país. Ahora bien, el rápido crecimiento en la utilización de las TIC también ha abierto nuevas oportunidades para los delincuentes, quienes aprovechan las vulnerabilidades en línea y lanzan ataques contra las infraestructuras esenciales de los países. Una función esencial de la UIT, tras la Cumbre Mundial sobre la Sociedad de la Información y la Conferencia de Plenipotenciarios de 2006, es la creación de confianza y seguridad en la utilización de las TIC. Los Jefes de Estado y de Gobierno, otros líderes que participan en la CMSI y los Estados Miembros de la UIT encargaron a la Unión que tomara medidas concretas para frenar las amenazas y la inseguridad relacionadas con la sociedad de la información. Por ese motivo, en su calidad de facilitador para la Línea de Acción C5 de la CMSI, el 17 de mayo de 2007 la UIT lanzó la Agenda sobre Ciberseguridad Global (ACG) con el fin de crear un marco para coordinar y abordar la respuesta internacional a los crecientes problemas de ciberseguridad. En su reciente reunión de 2009, el Consejo de la UIT ha refrendado las actividades de la Unión relativas a la creación de confianza y seguridad en la utilización de las TIC.

En el marco general de la ACG, el Foro Regional de la UIT de 2009 sobre ciberseguridad para las Américas gira en torno al tema "Conectar el mundo responsablemente", y tiene por objeto identificar algunos de los principales problemas que afrontan los países de la región a la hora de mejorar la ciberseguridad y proteger las infraestructuras esenciales de la información, examinar las prácticas idóneas, y compartir información relativa a las actividades de desarrollo de la ciberseguridad que realiza la UIT y otras entidades para crear capacidades de ciberseguridad. En el foro también se examinarán iniciativas regionales e internacionales destinadas a aumentar la cooperación y la coordinación entre las distintas partes interesadas.

LUNES 23 DE NOVIEMBRE DE 2009	
08:30–09:30	**Registro y entrega de tarjetas de identificación (preinscripción en línea obligatoria)**
09:30–10:00	**Apertura de la reunión y discurso de bienvenida**
	Bienvenida: Dario Cordero, Instituto Dominicano de las Telecomunicaciones (INDOTEL), República Dominicana *Discurso:* Dr. José Rafael Vargas, Secretario de Estado y Presidente del Instituto Dominicano de las Telecomunicaciones (INDOTEL), República Dominicana *Discurso:* Juan Zavattiero, Juan Zavattiero, Jefe de la Oficina Regional de la UIT para las Américas, Unión Internacional de las Telecomunicaciones (UIT)

[1] Véase Foro Regional de la UIT para las Américas sobre Ciberseguridad/ITU Regional Cybersecurity Forum for Americas en el sitio web: www.itu.int/ITU-D/cyb/events/2009/santo-domingo/.

10:00–11:45	**Sesión 1: Preparando el escenario — Hacia un enfoque integrado para la ciberseguridad y la protección de la infraestructura esencial de la información (PIEI)**
	Descripción: La confianza y la seguridad al utilizar las tecnologías de la información y la comunicación son esenciales para crear una sociedad de la información integradora, segura y de alcance mundial. Los continuos cambios en la utilización de las TIC, los sistemas y las redes presentan ventajas considerables, pero a su vez hacen necesario que los gobiernos, las empresas, las organizaciones y los usuarios particulares -que desarrollan, poseen, proporcionan, gestionan los servicios y utilizan estas redes- presten mayor atención a la ciberseguridad y la protección de la información esencial. La necesidad de instaurar la confianza y la seguridad en la utilización de las TIC, promover la ciberseguridad y proteger la infraestructura esencial a nivel nacional son asuntos generalmente reconocidos. La Agenda de la UIT sobre Ciberseguridad Global constituye un marco general para la ciberseguridad, en el que todas las partes pertinentes pueden debatir y colaborar para reaccionar lo mejor posible y de manera coordinada ante los crecientes problemas de ciberseguridad. En esta sesión se describe el panorama general de las ciberamenazas y se exponen los problemas que han de afrontar los países, las empresas y los ciudadanos en su vida cotidiana en este nuevo entorno que cambia constantemente. *Moderador:* Souheil Marine, Jefe, División de Aplicaciones de las TIC y Ciberseguridad, Sector de Desarrollo de las Telecomunicaciones (UIT-D) *Presentación:* Souheil Marine, Jefe, División de Aplicaciones de las TIC y Ciberseguridad, Sector de Desarrollo de las Telecomunicaciones (UIT-D) *Presentación:* Graciela Piedras, Especialista Senior en Telecomunicaciones, Comisión Interamericana de Telecomunicaciones (CITEL), Organización de los Estados Americanos (OEA) *Presentación:* Alberto Bolaña Wittenberger, Consultor Senior, Oficina de Programa Regional, Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) *Presentación:* Jaime Ansieta, Oficial de Inteligencia Criminal, Subdirección de Delincuencia de Crimen Financiero y de Alta Tecnología, Interpol
11:45–12:00	**Pausa para el café/té**
12:00–13:30	**Sesión 2: Ciberseguridad en la agenda nacional y medidas que se han de tomar en consideración al crear una estrategia nacional de ciberseguridad**
	Descripción: Cada país y región tiene unas necesidades y requisitos específicos, que se han de abortar teniendo en cuenta el contexto nacional y regional. A medida que los actores nacionales de los sectores público y privado ofrecen su propia perspectiva respecto a los problemas importantes, algunos países han creado estrategias en materia de ciberseguridad/protección de la infraestructura esencial de la información (PIEI) con el fin de adoptar un enfoque coherente, mientras que otros han enfocado el asunto de una manera menos estricta y no institucional. ¿Qué asuntos es necesario tener en cuenta en la estrategia nacional para la ciberseguridad y la protección de la infraestructura esencial de la información? ¿Qué actores deben participar? Habida cuenta del carácter mundial de los problemas encontrados, ¿cómo encajan estas iniciativas y enfoques nacionales en un marco global? En esta sesión se debatirá acerca de algunos elementos necesarios para crear y organizar actividades nacionales en materia de ciberseguridad /PIEI. En la sesión se presentará la herramienta de la UIT para la autoevaluación nacional de la ciberseguridad/PIEI, que está concebida para prestar asistencia a los gobiernos nacionales en la preparación de un enfoque nacional para la ciberseguridad.

	Moderador: José A. Rizek, Asesor de Telecomunicaciones del Poder Ejecutivo, Presidencia de la República, República Dominicana *Presentación:* Cesar Augusto Torres López, Director de Acceso y Desarrollo Social, Ministerio de Tecnologías de la Información y las Comunicaciones, Colombia *Presentación:* César Moliné Rodríguez, Asesor Legal en las áreas de Comercio Electrónico, Firma Digital, y Sociedad de la Información, Instituto Dominicano de las Telecomunicaciones (INDOTEL), República Dominicana *Presentación:* Belisario Contreras, Assistante, Gestión de Proyecto - Ciberseguridad, Comité Interamericano contra el Terrorismo (CICTE), Organización de los Estados Americanos (OEA) *Presentación:* Joseph Richardson, Consultor de la UIT.
13:30–14:30	**Almuerzo**
14:30–15:45	**Sesión 3: Estructuras organizativas y capacidades para la gestión de incidentes**
	Descripción: Una de las principales actividades relativas a la ciberseguridad consiste en la creación de capacidades de vigilancia, alerta y gestión de incidentes con el fin de estar preparados, detectar, gestionar ciberincidentes y reaccionar cuando se producen. La gestión eficiente de incidentes requiere el examen de la financiación, los recursos humanos, la formación, la capacidad tecnológica, la colaboración entre el gobierno y el sector privado y los requisitos jurídicos. En esta sesión se examinan las prácticas idóneas, las estructuras organizativas y las normas afines en lo que respecta a los aspectos técnicos, administrativos y financieros de la creación de capacidades nacionales, regionales e internacionales para la vigilancia, alerta y gestión de incidentes. *Moderador:* Juan Antonio Delgado, Instituto Dominicano de las Telecomunicaciones (INDOTEL), República Dominicana *Presentación:* Michael Lewis, Consultor de la UIT *Presentación:* Georges Sebek, Consejero del Grupo de Estudio 17 del UIT-T, Sector de Normalización de las Telecomunicaciones (UIT-T) *Presentación:* Anuj Singh, Director, Centro de Respuesta Global (GRC), IMPACT
15:45–16:00	**Pausa para el café/té**
16:00–17:15	**Sesión 4: Creación de capacidades y la cooperación internacional**
	Descripción: La realidad del ciberespacio hace que sea necesaria la colaboración de todo el mundo. Para responder con eficacia a las ciberamenazas se requieren recursos, conocimientos prácticos y una gran inversión en el desarrollo de capacidades. Un elemento esencial es lograr la colaboración de todas las partes interesadas para resolver los problemas comunes de ciberseguridad y crear un plan de creación de capacidades eficiente. Los desafíos que plantean los ciberataques y la ciberdelincuencia son de carácter mundial y de gran alcance, y sólo pueden resolverse mediante una estrategia coherente en el marco de la cooperación internacional, habida cuenta de los diferentes papeles que desempeñan cada una de las partes interesadas y de las iniciativas existentes. Los líderes mundiales que participaron en la CMSI destacaron la importancia de la seguridad, que constituye uno de los pilares sobre los que reposa la sociedad de la información global y encargaron a la UIT que coordinara una acción mundial para resolver los problemas de ciberseguridad. Habida cuenta de los numerosos actores que intervienen y el creciente número de amenazas, ¿cuál es la forma más eficaz de colaborar para adoptar una estrategia global? En esta sesión se examinan con detenimiento los posibles mecanismos para crear capacidades de manera eficaz, gracias a la colaboración y cooperación entre todas las partes interesadas a escala nacional, regional e internacional, para mejorar la ciberseguridad y proteger a los menores en línea. *Moderador:* Souheil Marine, Jefe, División de Aplicaciones de las TIC y Ciberseguridad, Sector de Desarrollo de las Telecomunicaciones (UIT-D) *Presentación:* Jorge Navarro, Consultor, Mexico *Presentación:* Souheil Marine, Jefe, División de Aplicaciones de las TIC y Ciberseguridad, Sector de Desarrollo de las Telecomunicaciones (UIT-D) *Presentación:* María José Cantarino de Frías, Responsabilidad Corporativa, Telefónica

	Presentación: Altagracia Chapman, Miembro de la Linea de Ayuda Internacional para los niños *Presentación:* Anuj Singh, Director, Centro de Respuesta Global Response Center (GRC), IMPACT , y Elina Noor, Analista Senior, IMPACT
17:15–17:30	**Resumen del día y anuncios**
19:00–	**Recepción**

MARTES 24 DE NOVIEMBRE DE 2009	
09:30–10:45	**Sesión 1 del Grupo de Trabajo: Creación de una estrategia nacional de ciberseguridad**
	Descripción: Cada país necesita una estrategia nacional exhaustiva y un plan de acción para resolver los problemas técnicos, jurídicos y de política, además de la cooperación regional e internacional. ¿Qué asuntos deben tenerse en cuenta en la estrategia nacional de ciberseguridad? ¿Qué actores deben participar? En esta sesión del Grupo de Trabajo se examinarán con detenimiento los componentes necesarios de una estrategia nacional y se expondrá en qué podría consistir una estrategia de este tipo.
10:45–11:00	**Pausa para el café/té**
11:00–12:45	**Sesión 1 del Grupo de Trabajo: Creación de una estrategia nacional de ciberseguridad (continuación)**
12:45–14:00	**Almuerzo**
14:00–15:30	**Sesión 2 del Grupo de Trabajo: Medidas jurídicas en materia de ciberseguridad**
	Descripción: Los ciberdelincuentes son una amenaza constante en cada país conectado a Internet. El crimen organizado ha crecido debido a que Internet permite realizar actividades lucrativas de bajo riesgo, ya que siguen habiendo lagunas en las legislaciones nacionales y regionales, lo que hace difícil seguirle la pista a los delincuentes. El principal problema estriba en la carencia de una armonización internacional de la legislación sobre la ciberdelincuencia. Se han desplegado esfuerzos para resolver este problema y, pese a que han sido valiosos, siguen siendo insuficientes. Internet es una herramienta de comunicación internacional y, por consiguiente, toda solución relativa a la seguridad debe encontrarse a nivel mundial. La finalidad de esta sesión es proporcionar a los países de la región una explicación práctica y pormenorizada de los distintos componentes que debe tener una legislación exhaustiva y eficaz para disuadir la ciberdelincuencia y penalizar la utilización indebida de las TIC. La UIT ha elaborado un conjunto exhaustivo de recursos jurídicos que sirven para facilitar las deliberaciones y la elaboración de legislación en materia de ciberseguridad.
15:30–15:45	**Pausa para el café/té**
15:45–17:30	**Sesión 2 del Grupo de Trabajo: Medidas jurídicas en materia de ciberseguridad (continuación)**
17:30–17:45	**Resumen del día y anuncios**

MIÉRCOLES 25 DE NOVIEMBRE DE 2009	
09:30–10:30	**Sesión 3 del Grupo de Trabajo: Creación de estructuras organizativas y capacidades de gestión de incidentes**
	Descripción: La finalidad de esta sesión del Grupo de Trabajo es definir los requisitos para crear capacidades de vigilancia, alerta y gestión de incidentes con el fin de detectar, gestionar y reaccionar a los ciberincidentes. Se debatirá acerca del Centro de Respuesta Global UIT-IMPACT y la asistencia conexa para crear capacidades nacionales de vigilancia, alerta y gestión de incidentes. Este Centro puede ofrecer a la comunidad global un sistema de alerta inmediata combinado y en tiempo real. Este "Sistema de alerta inmediata en Red" (NEWS) puede ayudar a los Estados Miembros a identificar ciberamenazas en cuanto se producen y proporciona orientación esencial sobre las medidas que se han de tomar para mitigar sus efectos. Si bien los miembros de este Centro pueden obtener acceso a herramientas y sistemas especializados, en particular la "Plataforma de aplicaciones electrónicas de colaboración segura para expertos" (ESCAPE).
10:30–10:45	**Pausa para café/té**
10:45–11:45	**Sesión 3 del Grupo de Trabajo: Creación de estructuras organizativas y capacidades de gestión de incidentes (continuación) (SÓLO PARA REPRESENTANTES DE ADMINISTRACIONES DE LOS ESTADOS MIEMBROS)**
11:45–12:30	**Resumen del Foro, Recomendaciones y trabajo futuro**
	Descripción: En esta última sesión del foro se resumirán las principales conclusiones del evento y se tratará de elaborar recomendaciones sobre las futuras actividades con el fin de mejorar la ciberseguridad y aumentar la protección de la infraestructura esencial de la información en la región. *Observaciones de clausura:* Joelle Exarhakos, Directora Ejecutiva, Instituto Dominicano de las Telecomunicaciones (INDOTEL), República Dominicana *Observaciones de clausura:* Juan Zavattiero, Jefe de la Oficina Regional de la UIT para las Américas, Unión Internacional de las Telecomunicaciones (UIT)