CCP.I/RES. 157 (XV-09) [1]

APOYO AL TALLER HEMISFÉRICO CONJUNTO DE LA OEA SOBRE EL DESARROLLO DE UN MARCO DE SEGURIDAD CIBERNÉTICA

La XV Reunión del Comité Consultivo Permanente I: Telecomunicaciones,

CONSIDERANDO:

a) Que el CCP.I de la CITEL ha reconocido el rol central que cumplen las telecomunicaciones en la seguridad cibernética y ha creado un programa de trabajo propio para centrarse en la normalización técnica y en su coordinación, y para destacar las cuestiones regulatorias relacionadas con el desarrollo de una cultura en seguridad cibernética para la región;

b) Que garantizar la seguridad de los sistemas de información constituye una prioridad para el hemisferio, ya que las redes de información desempeñan un papel vital en la infraestructura crítica de los países, en sus economías y sociedades;

a) Que la CITEL está trabajando, con el Comité Interamericano contra el terrorismo (CICTE) y los Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA) de la Organización de los Estados Americanos (OEA), de manera coordinada con miras a avanzar en los objetivos del hemisferio relacionados con estos asuntos importantes,

RECONOCIENDO:

a) Que la CITEL sostiene un enfoque activo y multidisciplinario en materia de seguridad cibernética que suma sus esfuerzos a los esfuerzos y la pericia del CICTE y los REMJA;

b) Que la Estrategia Interamericana Integral de Seguridad Cibernética tiene como base los esfuerzos y el conocimiento especializado de CITEL, CICTE y REMJA;

c) Que un taller hemisférico conjunto de la OEA conllevará un avance en el entendimiento de las cuestiones vitales inherentes a la seguridad cibernética para los gobiernos estaduales y nacionales, y constituirá un foro para compartir información, desarrollar capacidades y fomentar la colaboración continua entre los participantes,

RESUELVE:

1. Confirmar el apoyo por parte del CCP.I al próximo Taller Hemisférico Conjunto de la OEA sobre el desarrollo de un marco de seguridad cibernética a tener lugar del 16 al 18 de noviembre de 2009 en Río de Janeiro, Brasil.

2. Agradecer de antemano a los coordinadores del taller por organizar este importante evento.

3. Invitar a los miembros del CCP.I a participar de este taller.

[1] CCP.I-TEL/doc. 1879/08

ENCARGA AL SECRETARIO EJECUTIVO DE LA CITEL A:

Enviar esta Resolución a todos los miembros a fin de informar a las delegaciones sobre este importante taller e invitar a los Estados Miembros y Miembros Asociados de la CITEL a participar de este evento.

ANEXO A LA RESOLUCION CCP.I/RES. 157 (XV-09)

TALLER HEMISFÉRICO CONJUNTO DE LA OEA SOBRE EL DESARROLLO DE UN MARCO DE SEGURIDAD CIBERNÉTICA

Del 16 al 18 de noviembre de 2009
Río de Janeiro, Brasil

Organizado por:
Comisión Interamericana de Telecomunicaciones (CITEL), Comité Interamericano contra el Terrorismo (CICTE), Grupo de Expertos Gubernamentales sobre el Delito Cibernético de la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA), y el Gobierno del Brasil

Lunes – 17 de noviembre de 2009

9:00 Ceremonia de apertura
(Representantes del Gobierno del Brasil, CITEL, CICTE, REMJA)

9:30 Panel 1 – ¿Qué es la ciberseguridad? ¿Qué es la protección de la infraestructura esencial (CIP)?

11:00 Pausa para el café

11:30 Panel 2 – ¿Cuáles son las amenazas y vulnerabilidades?

- ¿Cuáles son las posibles consecuencias en el caso de que una amenaza identificada se convierta en realidad?
- ¿Qué partes tienen una función que desempeñar?
- ¿Qué medidas deben tomarse para reducir las vulnerabilidades identificadas, si las hubiere?
- ¿Qué nivel de riesgo es aceptable? - ¿Quién determina cuál es un nivel aceptable de riesgo? ¿Puede manejarse el riesgo?
- ¿Cuáles son las intervenciones (controles/contramedidas) con que se cuenta para manejar el riesgo? ¿Qué combinación de intervenciones tiene sentido en cuanto a las consideraciones económicas, sociales, políticas y jurídicas?

13:00 Almuerzo

14:00 Panel 3 – Implicaciones para el Estado y el Gobierno nacional

- ¿Qué es de importancia crítica en los países?
- ¿Sería eficaz un marco común para fortalecer la protección de la infraestructura crítica (CIP)? ¿Ayudaría un marco común a aclarar las responsabilidades de las partes afectadas? ¿En que medida debiera ese marco ser obligatorio, y en qué medida voluntario?
- ¿Qué métodos y modelos podrían usarse para analizar y evaluar el riesgo?

15:30 Pausa para el café

16:00 Discusiones – Ronda 1
Los participantes discuten sobre la seguridad cibernética en las Américas, los desafíos y amenazas, las respuestas de los gobiernos y otras mejores prácticas

17:00 Presentación de puntos destacados de la discusión de la ronda 1
Un representante de cada grupo de discusión presenta

18:00 Cierre

Martes – 17 de noviembre de 2009

9:00 Panel 4 – Cuestiones legales, reglamentarias y de políticas
- ¿Cuáles son las cuestiones legales, reglamentarias y de políticas, incluidas la privacidad y la información compartida, relacionadas con el uso de tecnologías de ciberseguridad para la protección de la infraestructura crítica?
- Si se necesita un marco legislativo para una estrategia CIP, ¿cuáles deberían ser sus elementos?
- ¿Cuáles son los temas posibles para las tareas de coordinación legal regionales o internacionales?

10:30 Pausa para el café

11:00 Panel 5 – Cuestiones de implementación técnica y de gestión para la capacidad de recuperación y adaptabilidad de las redes de información y comunicaciones
- ¿Qué tecnologías están actualmente en servicio o se ofrecen pero no se hallan todavía en servicio muy difundido?
- ¿Qué tecnologías se están investigando para la protección de infraestructura crítica, particularmente para la ciberseguridad?
- ¿Cómo está alterando la aplicación de nuevas tecnologías las necesidades de interoperabilidad entre redes de determinados organismos y/o de organismos múltiples?

12:30 Almuerzo

13:30 Panel 6 – Compartición de información y coordinación de interesados
- ¿Cómo debe estructurarse el diálogo con los gobiernos, las empresas operadoras, la academia y los usuarios de infraestructuras críticas?
- ¿Cómo se identifican los datos pertinentes?
- ¿Cómo se buscan?
- ¿Cómo se almacenan?
- ¿Cuáles son las reglas legales en materia de pruebas?
- ¿Cuáles son las funciones y responsabilidades de las agencias, las organizaciones y comunidades para intervenir en un proceso para gestionar riesgos?
- ¿Cómo definir estructuras sólidas de organización y crear una capacidad de controlar incidentes?
- ¿Cómo debe estructurarse el diálogo con los gobiernos, las empresas operadoras, la academia y los usuarios de CIP?

15:00 Pausa para el café

15:30 Discurso principal (OPTATIVO – Tema a definirse)

16:00 Discusiones – Ronda 2
Los participantes hablan sobre sus experiencias, desafíos y mejores prácticas en relación con los temas de los paneles 4, 5 y 6.

17:00 Presentación de puntos destacados de la discusión de la ronda 2
Un representante de cada grupo de discusión presenta

18:00 Cierre

Miércoles – 18 de noviembre de 2009

9:00 Panel 7 –Creación de un Marco Nacional para la ciberseguridad
- ¿Cuáles son los requisitos para implementar una estrategia integrada? ¿Cuál debiera ser el alcance del marco común?
- ¿Qué hipótesis son pertinentes para los gobiernos, sociedades y economías nacionales de las Américas?

10:30 Pausa para el café

11:00 Panel 8 –Imposicion e implementación
- ¿Cuál es el valor económico de la seguridad?
- ¿Qué puede ofrecer la seguridad a la organización que la implemente?
- En vista de la realidad cotidiana de los problemas relacionados con la seguridad para la mayoría de las infraestructuras, de la proliferación de soluciones propuestas, y de un mercado floreciente en materia de seguridad, ¿se ajustan a los requisitos las soluciones que se proponen?
- ¿Qué debe hacerse para fomentar la cooperación regional e internacional?

12:30 Almuerzo

13:30 Discusiones – Ronda 3
Las delegaciones nacionales identifican los elementos y un plan de acción para crear un marco nacional

15:00 Pausa para el café

15:30 Presentación de puntos destacados de la discusión de la ronda 3

16:30 Ceremonia de cierre

17:00 Cierre