

SEGURIDAD CIBERNETICA

La III Reunión del Comité Consultivo Permanente I: Normalización de Telecomunicaciones,

RECONOCIENDO:

- a) Que el garantizar la protección y seguridad de los sistemas de información en red (seguridad cibernética) es un asunto de prioridad para nuestro hemisferio;
- b) Que las redes de información ubicuas y seguras juegan un papel importante para la infraestructura esencial de todos los Estados miembros de la OEA, sus economías y sus sociedades, y,
- c) Que el Comité Directivo Permanente de la Comisión Interamericana de Telecomunicaciones (COM/CITEL) ha identificado la creación de una cultura de seguridad cibernética como un objetivo importante para la CITEL (COM/CITEL/ Res. 151 (XII-02);

RECONOCIENDO ADEMÁS:

- a) Que la seguridad no puede ser una responsabilidad que sólo compete a los gobiernos; por el contrario, se requiere una amplia colaboración entre los gobiernos y el sector privado de las Américas, y
- b) Que el tema de la seguridad de las telecomunicaciones tiene efectos importantes en sectores críticos de infraestructura, tales como energía eléctrica, servicios públicos, comunicaciones, instituciones financieras, transporte y servicios de emergencia,

CONSIDERANDO:

- a) Que la Asamblea General de la OEA, en la Resolución AG/RES 1939 (XXXIII-O/03), "Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética", resuelve lo siguiente:

1. Encomendar al Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Expertos Gubernamentales sobre Delito Cibernético de la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA) que se aseguren de que la Conferencia de la Organización de los Estados Americanos (OEA) sobre Seguridad Cibernética, propuesta por la Argentina, empiece a trabajar en el desarrollo de un proyecto de estrategia integral de la OEA sobre seguridad cibernética que aborde los aspectos multidimensional y multidisciplinario de la seguridad cibernética, y que informen sobre los resultados de la reunión, y sobre el

¹ CCP.I-TEL/doc.262/03rev.2

trabajo de seguimiento que se considere apropiado, a la Comisión de Seguridad Hemisférica para su consideración.

2. Encomendar al Consejo Permanente que, a través de la Comisión de Seguridad Hemisférica, desarrolle un proyecto de estrategia de seguridad cibernética para los Estados miembros en coordinación y colaboración con la CITEL, el CICTE, el Grupo de Expertos Gubernamentales sobre Delito Cibernético de la REMJA y cualquier otro órgano de la OEA que se considere apropiado, sin perjuicio de sus respectivos mandatos, misiones y requerimientos existentes sobre presentación de informes, teniendo en consideración cualquier actividad pertinente en los Estados miembros relativa a la protección de infraestructura crítica, y que presente este proyecto de estrategia sobre seguridad cibernética al Consejo Permanente para su consideración.
3. Solicitar al Consejo Permanente que informe a la Asamblea General en su trigésimo cuarto período ordinario de sesiones sobre la implementación de esta resolución.

b) Que el CICTE (Comité Interamericano contra el Terrorismo de la OEA) solicitó y recibió la cooperación de la CITEL en la planeación de la Conferencia Hemisférica de la OEA sobre Seguridad cibernética en julio del 2003;

c) Que la Conferencia Hemisférica de la OEA sobre Seguridad cibernética se reunió el 28 y 29 de Julio en Buenos Aires para fortalecer el diálogo entre los Estados miembros de la OEA con objeto de desarrollar una estrategia hemisférica de seguridad cibernética; y,

d) Que como resultado de la Conferencia Hemisférica de la OEA sobre Seguridad cibernética, se insta a la CITEL, CICTE, y a los Ministros de Justicia o Procurador General de las Américas (REMJA), en conjunto con los expertos de los Estados miembros, a continuar sus esfuerzos para el desarrollo de una estrategia integral de seguridad cibernética de la OEA,

CONSIDERANDO ADEMÁS:

a) Que la CITEL, a través de su función como socio del sector privado en asuntos relativos a sus áreas de responsabilidad, y a través de su Plan de Trabajo para temas de red avanzada, incluyendo la seguridad cibernética, puede ofrecer una importante contribución para la creación de una cultura de seguridad cibernética en las Américas, y

b) Que el memorando enviado por la CICTE a la CITEL (documento CCP.I-TEL/doc.302/03), “Seguridad cibernética-Informe sobre la conferencia especial”, detalla un plan de trabajo para CITEL, CICTE y REMJA con el fin de redactar una estrategia de seguridad cibernética en respuesta a la Resolución AG/RES1939 (XXXIII-O/03) de la OEA.

RESUELVE:

1. Adoptar el plan de trabajo para la CITEL que se adjunta, en respuesta a los anteriores mandatos de la OEA.

2. Solicitar que el Coordinador de Seguridad Cibernética y de Infraestructura Crítica en colaboración con el Presidente del CCP.I, contribuya con aportaciones apropiadas para el Grupo de Trabajo Conjunto CICTE/CITEL/REMJA.

INVITA:

Al Presidente del CCP.I a transmitir esta Resolución a la XIII Reunión del COM/CITEL con propósitos informativos.

ENCARGA AL SECRETARIO EJECUTIVO:

A enviar esta Resolución al CICTE, en nombre del Presidente del CCP.I, e informar acerca del progreso de la CITEL en el área de seguridad cibernética.

ANEXO A CCP.I/RES. 35 (III-03)
PLAN DE TRABAJO SOBRE SEGURIDAD CIBERNÉTICA

1. Apoyar el trabajo de seguimiento de la Conferencia Especial sobre Seguridad Cibernética dirigido por el Comité sobre Seguridad Hemisférica (CHS) de la OEA:
 - a. Proporcionar comentarios a la CICTE sobre el borrador del informe de la Conferencia Especial sobre Seguridad Cibernética de Buenos Aires.
 - b. Enviar informes y resoluciones sobre Seguridad Cibernética al Comité sobre Seguridad Hemisférica para su incorporación en la Estrategia de Seguridad Cibernética de la OEA.
 - c. Revisar el proyecto de Estrategia de Seguridad Cibernética de la CHS.
2. Desarrollar enfoques nacionales y regionales de seguridad de redes, estrategias de despliegue, intercambio de información, y alcance a los sectores público y privado:
 - a. Reunir las mejores prácticas regionales para la protección de comunicación e infraestructura de redes.
 - b. Revisar los diferentes marcos de referencia y lineamientos sobre redes y seguridad cibernética y su aplicabilidad dentro de la región de las Américas.
3. Fomentar la cooperación entre los Estados miembros sobre aspectos relacionados con la seguridad de redes:
 - a. Ayudar a las administraciones a fomentar en los proveedores de servicios y redes la implementación de estándares técnicos para redes seguras.
4. Alentar el diálogo sobre el trabajo de la UIT (por ejemplo, Comisión de Estudio 17) y de otros foros relevantes sobre Seguridad Cibernética y de Redes:
 - a. Organizar un seminario conjunto sobre normas de seguridad con la UIT
5. Identificar y evaluar temas técnicos relativos a normas necesarios para la seguridad de redes de comunicaciones existentes y futuras (alámbricas e inalámbricas) en toda la región. Esta actividad se basará, principalmente, en el trabajo del UIT-T (en especial, SG 17). Se tomará en cuenta a otros organismos existentes que fijan normas, incluyendo el IETF y las SDOs regionales, según convenga:
 - a. Recomendar a los Estados miembros la adopción de normas de seguridad de particular importancia.
6. Identificar de manera oportuna y continua obstáculos en la implementación de medidas de seguridad en las redes de la región. Esto requerirá cooperación continua entre el Grupo de Trabajo sobre Coordinación de Normas y el Grupo de Trabajo sobre Tecnologías y Servicios de Redes Avanzadas.
7. Establecer enlaces con otros organismos de normas y foros de la Industria, según sea necesario, para avanzar el trabajo sobre los mandatos de la OEA.