**CCP.I/RES. 62 (V-04)**[1]

**ACTUALIZACION SOBRE SEGURIDAD CIBERNETICA EN LA CITEL**

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

**CONSIDERANDO:**

a) La reciente adopción por la XXXIV Reunión Ordinaria de la Asamblea General de la OEA, el 8 de junio de 2004, de la estrategia interamericana integral para combatir las amenazas a la seguridad cibernética; y

b) La continua importancia de fomentar una infraestructura de información y comunicación segura para todos los Estados miembros de la OEA, sus economías y sus sociedades,

**OBSERVANDO:**

1) Que el UIT-T realizará un simposio sobre seguridad cibernética para tratar inquietudes de normalización mundial acerca de seguridad en los sistemas de información y comunicación el 4 de octubre del 2004, un día antes del inicio de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT);

2) Que el CCP.I desea despertar el interés del Comité Interamericano contra el Terrorismo (CICTE) y de la Reunión de Ministros de Justicia o Procuradores Generales de las Américas (REMJA) sobre este simposio, el cual está abierto a todos. Información adicional puede encontrarse en la Página Web: itu.int/ITU-T/worksem/cybersecurity;

**OBSERVANDO ADEMAS:**

a) Que el CCP.I ha adoptado por la Resolución CCP.I/RES. 45 (IV-04) un documento coordinado de normas para la "Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo" (Recomendación X.805 del UIT-T) que define una arquitectura de seguridad de redes para proveer una seguridad de red extremo-a-extremo. La arquitectura considera asuntos de seguridad para la gestión, control y uso de la infraestructura de red, servicios y aplicaciones. Provee una perspectiva completa *top-dow*n, extremo a extremo de la seguridad de red y puede ser aplicada a elementos de red, servicios y aplicaciones para detectar, predecir y corregir vulnerabilidades de seguridad. La Recomendación X.805 divide en forma lógica un grupo complejo de características relacionadas a la seguridad de red extremo-a–extremo en componentes separados de arquitectura. Esta separación permite un enfoque sistemático para la seguridad extremo a extremo que puede ser utilizada para la planificación de nuevas soluciones de seguridad así como para evaluar la seguridad de las redes existentes; y

b) Que el CCP.I ha adoptado por la Resolución CCP.I/RES. 46 (IV-04) un Documento Coordinado de Normas para la "Arquitectura de seguridad para el protocolo de Internet" (IETF RFC 2401) que considera la seguridad al nivel de la capa IP a través del uso de mecanismos criptográficos y de protocolos de seguridad. Esta arquitectura de seguridad, referida como IPsec, provee servicios de seguridad para habilitar un sistema a seleccionar los protocolos de seguridad requeridos, determinar los algoritmos a usar para los servicios y poner cualquier clave criptográfica requerida para proveer los servicios requeridos. IPsec puede ser utilizada para proteger uno o más "caminos" entre un par de computadores centrales, entre un par de pasarelas (*gateway*) de seguridad, o entre una pasarela de seguridad y un computador central.

[1] CCP.I-TEL/doc.526/04 rev.1

IPsec no es una Arquitectura total de Seguridad para la Internet; trata sólo la capa IP, a través del uso de una combinación de mecanismos criptográficos y de protocolos de seguridad,

**RESUELVE:**

Continuar sus esfuerzos tendientes a identificar vulnerabilidades en las redes de telecomunicaciones, adoptar normas técnicas para mejorar la seguridad de las redes de telecomunicaciones de la región e investigar estrategias de mitigación y respuesta para asegurar la infraestructura regional crítica de telecomunicaciones. Esto será posible a través de una estrecha asociación de los sectores privado y público.

**INVITA AL PRESIDENTE DEL CCP.I:**

Enviar una carta al Presidente de la Comisión de Seguridad Hemisférica de la OEA que contenga al menos:

- Una copia de esta resolución
- El documento CCP.I-TEL/doc.511/04 sobre el invitación al Seminario de Ciberseguridad.
- Normas coordinadas adoptadas incluyendo una explicación de los objetivos de las mismas.
- Programa de trabajo del Grupo de Trabajo de Coordinación de Normas
- Programa de trabajo del Grupo Relator Cuestión de Estudio II del Grupo de Trabajo sobre Servicios y Tecnologías de Redes Avanzadas: Seguridad en el ciberespacio e infraestructura crítica.