CCP.I/RES. 49 (IV-04)[1]

SEGURIDAD CIBERNÉTICA

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

RECONOCIENDO:

a) Que garantizar la 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 desempeñan un papel importante en la infraestructura crítica de todos los Estados miembros de la OEA, sus economías y sus sociedades; y

c) Que las redes de próxima generación (NGN) que actualmente se están diseñando y normalizando podrán tomar en cuenta tecnologías y técnicas para asegurar su solidez y fortalecer su resistencia contra los ataques cibernéticos,

TENIENDO EN CONSIDERACION:

a) Que la operación segura y eficiente de la infraestructura global de telecomunicaciones es crucial para el bienestar y desarrollo de todos los sectores de la economía y, en consecuencia, de interés vital tanto para los gobiernos como para el sector privado; y

b) El número cada vez mas frecuente y la naturaleza insidiosa de los ataques cibernéticos sobre las redes, instituciones y usuarios, que están produciendo todo tipo de daño, especialmente morales, económicos y financieros,

CONSIDERANDO:

a) Que la CITEL, CICTE (el Comité Interamericano contra el Terrorismo de la OEA) y REMJA (la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas) están trabajando para desarrollar una estrategia a nivel hemisférico para la seguridad cibernética, como lo determinó la Asamblea General de la OEA en la Resolución AG/RES.1939 (XXXIII-O/03);

b) El taller realizado conjuntamente por el Grupo de Trabajo sobre Servicios y Tecnologías de Redes Avanzadas y el Grupo de Trabajo sobre Coordinación de Normas acerca de la seguridad cibernética, en la IV Reunión del CCP.1 en Quito, Ecuador, trató los asuntos claves de la seguridad cibernética vinculados a la CITEL; y

c) Los importantes compromisos realizados por los Jefes del Estado y de Gobierno de la Región, planteados en la Declaración de Nuevo León, incluyendo incentivos para un acceso asequible para todos a las tecnologías de información y comunicaciones,

[1] CCP.I-TEL/doc.427/04 rev.2

CONSIDERANDO ADEMÁS:

Que la CITEL, a través de sus alianzas con el sector privado sobre asuntos en sus áreas de responsabilidad, y a través de su Plan de Trabajo para temas de redes avanzadas, y en particular la seguridad cibernética y las NGN, podrá realizar un aporte importante tanto para una mayor concienciación acerca de los temas críticos que puedan tener un impacto potencial en la Región, como para perfeccionar sus planes de trabajo en dichas áreas facilitando discusiones enfocadas y la compartición de información,

RESUELVE:

1. Aprobar el aporte adjunto de la CITEL sobre la Estrategia de Seguridad Cibernética de la OEA y enviarlo al Comité sobre Seguridad Hemisférica de la OEA para su revisión y entrega a la Asamblea General de la OEA en junio de 2004.

2. Solicitar al Relator de la CITEL sobre asuntos de Seguridad Cibernética e Infraestructura Crítica que envíe una copia de esta Resolución al Grupo de Trabajo Conjunto de CICTE/CITEL/REMJA sobre la Seguridad Cibernética.

INVITA:

a) Al Grupo de Trabajo sobre los Servicios y Tecnologías de Redes Avanzadas y al Grupo de Trabajo sobre Coordinación de Normas a que sigan trabajando en el tema de la seguridad cibernética y que informen al CCP.I acerca de sus logros en dicho tema específico.

b) Al Presidente del CCP.I a enviar una carta al Presidente del Comité sobre Seguridad Hemisférica de la OEA adjuntando una copia de esta Resolución.

ANEXO A LA RESOLUCION CCP.I/RES. 49 (IV-04)

CITEL: La identificación y adopción de normas técnicas para una arquitectura segura de Internet

Una estrategia eficaz de seguridad cibernética deberá reconocer que la seguridad de la red de los sistemas de información que comprenden la Internet requiere una alianza entre el gobierno y la industria. Tanto las industrias de telecomunicaciones y de tecnología de la información como los gobiernos de los Estados miembros de la OEA están buscando soluciones integrales de seguridad cibernética eficaces en función de costos. Las capacidades de seguridad en los productos de computación son imprescindibles como elementos de la seguridad global de la red. Sin embargo, a medida de que se produzcan más tecnologías y se las integren en las redes existentes, su compatibilidad e interoperabilidad – o la falta de estas – determinarán su eficacia. La seguridad deberá desarrollarse de una manera tal que promueva la integración de capacidades de seguridad aceptables en la arquitectura general de la red. Para lograr semejantes soluciones integradas de seguridad cibernética con base en la tecnología, deberá diseñarse la seguridad de la red alrededor de normas internacionales desarrolladas en un proceso abierto.

El desarrollo de normas para la arquitectura de seguridad en Internet requerirá un proceso de múltiples pasos para asegurar que se logre un nivel adecuado de consenso, planificación y aceptación entre las diferentes entidades gubernamentales y privadas que deberán cumplir un papel en la promulgación de semejantes normas. Aprovechando el trabajo de organizaciones de normalización como el Sector de Normalización de la Unión Internacional de Telecomunicaciones (UIT-T), la CITEL está identificando y evaluando las normas técnicas para poder recomendar su aplicabilidad a la región de las Américas, teniendo presente que el desarrollo de las redes en algunos de los Estados miembros de la OEA ha sufrido algunos retrasos, lo que implica que, para tales países, el logro de un cierto grado de calidad para sus redes será importante para poder llevar a cabo plenamente sistemas para intercambio de información adecuadamente seguros. Para agilizar su trabajo, la CITEL y el UIT-T organizaron un taller conjunto sobre Seguridad Cibernética en marzo del 2004. La CITEL está estableciendo enlaces, además, con otras entidades de normalización y foros de la industria para obtener la participación y los aportes de dichas partes.

La identificación de las normas de seguridad cibernética será un proceso de múltiples pasos. Una vez que la evaluación por la CITEL de las normas técnicas vigentes se complete, recomendará la adopción de normas especialmente importantes para la región. Además, en forma oportuna y permanente, identificará los obstáculos que impidan la aplicación de dichas normas de seguridad en las redes de la región, y la posible acción apropiada que puedan considerar los Estados miembros.

El desarrollo de las normas técnicas no es un emprendimiento que sea igual para todos. La CITEL evaluará los enfoques regionales a la seguridad de redes, las estrategias de despliegue, el intercambio de información y la difusión a los sectores público y privado. Como parte de este esfuerzo, la CITEL identificará los recursos para las mejores prácticas en la comunicación en redes y la protección de la infraestructura con base en las tecnologías. Este proceso requerirá que la CITEL revise los objetivos, alcances, pericia, marcos técnicos y lineamientos asociados con los recursos disponibles, para poder determinar su aplicabilidad dentro de la región de las Américas, con el fin de decidir cuáles serán los más apropiados. La CITEL continuará trabajando con los Estados miembros para asistirles para la aplicación más apropiada y eficaz.

La contribución de la CITEL a la estrategia de seguridad cibernética adoptará un enfoque prospectivo y buscará fomentar el intercambio de información entre los Estados miembros para así promover las redes seguras. Identificará y evaluará los asuntos técnicos relativos a las normas requeridas para la seguridad de las redes futuras de comunicaciones en la región, así como las existentes. Esta función aprovechará primordialmente del trabajo del UIT-T. Otras entidades de normalización existentes, a través de la CITEL, serán consideradas según sean apropiadas. En último término, la CITEL resaltará las normas

de seguridad de especial importancia y recomendará que los Estados miembros adopten dichas normas. También es importante enfatizar el papel crucial de la CITEL en la promoción de programas de aumento de la capacidad y capacitación, con el fin de llevar adelante el proceso de propagación de información técnica y práctica relacionada con los asuntos de la seguridad cibernética.

La CITEL reconoce que, aunque la primera prioridad deberá enfocarse en las políticas públicas que llevarán los beneficios de las tecnologías de las telecomunicaciones y la información a todos los ciudadanos de los Estados miembros de la OEA, el fortalecimiento de la alianza privada / pública que redundará en la adopción amplia de un marco de normas técnicas que ayudarán a asegurar la Internet, requerirá de la comunicación y cooperación entre y dentro de las comunidades involucradas en esta asociación. La CITEL fomentará la cooperación entre los Estados miembros en los aspectos relativos a la seguridad de redes, mediante la asistencia a las Administraciones a que adopten políticas y prácticas que incentiven a los proveedores de servicios y redes a aplicar las normas técnicas para la seguridad de sus redes. La nueva edición del Libro Azul "Políticas de Telecomunicaciones para las Américas", publicación conjunta de la CITEL y la UIT, incluirá un capítulo sobre la seguridad cibernética. La CITEL también fomentará un diálogo dentro de las comunidades técnicas y gubernamentales pertinentes con relación al trabajo sobre la seguridad cibernética y de redes mediante seminarios conjuntos con la UIT sobre normas de seguridad. Las acciones de la CITEL podrán también incluir materias relativas a las políticas de telecomunicaciones, prácticas, regulaciones, aspectos económicos y responsabilidades de los usuarios, todo ello en el marco jurídico dentro del cual operan los servicios de telecomunicaciones, y dentro de las funciones y responsabilidades de la CITEL.