AG/RES. 2004
ESTRATEGIA DE SEGURIDAD CIBERNETICA
(RESOLUCION)

Organización de los Estados Americanos
Organização dos Estados Americanos
Organisation des États Américains
Organization of American States

Organización de los Estados Americanos

AG/RES. 2004 (XXXIV-O/04)

ADOPCIÓN DE UNA ESTRATEGIA INTERAMERICANA INTEGRAL
DE SEGURIDAD CIBERNÉTICA: UN ENFOQUE MULTIDIMENSIONAL
Y MULTIDISCIPLINARIO PARA LA CREACIÓN DE UNA CULTURA
DE SEGURIDAD CIBERNÉTICA

(Aprobada en la cuarta sesión plenaria, celebrada el 8 de junio de 2004)

LA ASAMBLEA GENERAL,

VISTO el informe anual del Consejo Permanente a la Asamblea General, en particular la sección sobre los temas encomendados a la Comisión de Seguridad Hemisférica (AG/doc.4265/04 add. 5 corr. 1), y específicamente las recomendaciones sobre una Estrategia Interamericana Integral para combatir las amenazas a la seguridad cibernética;

RECORDANDO su resolución AG/RES. 1939 (XXXIII-O/03), "Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética";

TENIENDO PRESENTE que el Comité Interamericano contra el Terrorismo (CICTE), en su cuarto período ordinario de sesiones, celebrado en Montevideo, Uruguay, del 28 al 30 de enero de 2004, adoptó la Declaración de Montevideo (CICTE/DEC. 1/04 rev. 3), en la que declara su compromiso de identificar y combatir las amenazas terroristas emergentes, independientemente de sus origen o motivación, tales como las amenazas a la seguridad cibernética;

OBSERVANDO CON SATISFACCIÓN:

Que la Conferencia de la OEA sobre Seguridad Cibernética, celebrada en Buenos Aires, Argentina, del 28 al 29 de julio de 2003, en cumplimiento de la resolución AG/RES. 1939 (XXXIII-O/03), demostró la gravedad de las amenazas en el ámbito de seguridad cibernética a los sistemas de información esenciales, las estructuras de información esenciales y las economías en todo el mundo y subrayó que una acción eficaz para abordar este problema debe contar con cooperación intersectorial y coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales;

Que el CICTE, en su cuarto período ordinario de sesiones, consideró el documento "Marco para el establecimiento de una Red Interamericana CSIRT de vigilancia y alerta" (CICTE/INF.4/04) y decidió celebrar una reunión de expertos gubernamentales en materia de seguridad cibernética en marzo de 2004 en Ottawa, Canadá, a fin de preparar sus recomendaciones para el proyecto de Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética, en cumplimiento de la citada resolución AG/RES. 1939 (XXXIII-O/03); y

Las recomendaciones formuladas por el CICTE (CICTE/REGVAC/doc.2/04), la CITEL (CPP.I-TEL/doc.427/04 rev. 2) y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA) y su Grupo de Expertos Gubernamentales en Materia de Delito Cibernético (CIBER-III/doc.4/03);

ACOGIENDO CON BENEPLÁCITO la Estrategia Interamericana Integral de Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para crear una cultura de seguridad cibernética, recomendada a la Asamblea General por el Consejo Permanente como un esfuerzo conjunto de los Estados Miembros y sus expertos, con los conocimientos técnicos especializados del CICTE, la CITEL y el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA (CP/doc.3901/04);

RECONOCIENDO:

La urgente necesidad de incrementar la seguridad de las redes y sistemas de información comúnmente denominados Internet, a fin de abordar las vulnerabilidades y proteger a los usuarios, la seguridad nacional y las infraestructuras esenciales frente a las graves y perjudiciales amenazas que representan aquellos que podrían llevar a cabo ataques en el espacio cibernético con fines maliciosos o delictivos;

La necesidad de crear una red interamericana de alerta y vigilancia para diseminar rápidamente información sobre seguridad cibernética y responder a crisis, incidentes y amenazas a la seguridad de las computadoras y recuperarse de los mismos;

La necesidad de desarrollar redes y sistemas de Internet dignos de confianza y fiables, mejorando de ese modo la confianza del usuario en dichas redes y sistemas;

REITERANDO la importancia de desarrollar una estrategia integral para la protección de la infraestructura de información que adopte un enfoque global, internacional y multidisciplinario;

CONSIDERANDO:

Las resoluciones 55/63 y 56/121 de la Asamblea General de las Naciones Unidas sobre la lucha contra la utilización de la tecnología de la información con fines delictivos, la resolución 57/239 relativa a la creación de una cultura mundial de seguridad cibernética y la resolución 58/199 sobre creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales; y

Que en su XII Reunión, el Comité Directivo Permanente de la Comisión Interamericana de Telecomunicaciones (COM/CITEL) señaló que “la creación de una cultura de ciberseguridad para proteger la infraestructura de las telecomunicaciones aumentando la conciencia entre todos los participantes de las Américas en las redes y sistemas de información relacionados con el riesgo de dichos sistemas y desarrollando las medidas necesarias para hacer frente a los riesgos de seguridad respondiendo rápidamente a los ciber-incidentes” es parte de los mandatos de la CITEL,

RESUELVE:

1. Adoptar la Estrategia Interamericana Integral de Seguridad Cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética, que se adjunta como anexo A.

2. Instar a los Estados Miembros a implementar dicha Estrategia.

3. Instar a los Estados Miembros a establecer o identificar grupos nacionales de "vigilancia y alerta", también conocidos como "Equipos de Respuesta a Incidentes de Seguridad en Computadoras" (CSIRT).

4. Dar renovado énfasis a la importancia de lograr sistemas seguros de información de Internet en todo el Hemisferio.

5. Solicitar al Consejo Permanente que, por medio de la Comisión de Seguridad Hemisférica, siga abordando esta cuestión y continúe facilitando las medidas de coordinación para implementar dicha Estrategia, en particular los esfuerzos de los expertos gubernamentales, el Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA) y otros órganos pertinentes de la OEA.

6. Instar a los Estados Miembros y a los órganos, organismos y entidades de la OEA a que coordinen sus esfuerzos para incrementar la seguridad cibernética.

7. Solicitar a las Secretarías del CICTE y la CITEL y al Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA que asistan a los Estados Miembros, cuando lo soliciten, en la implementación de las respectivas partes de la Estrategia y presenten un informe conjunto al Consejo Permanente, por medio de la Comisión de Seguridad Hemisférica, sobre el cumplimiento de esta resolución, antes del trigésimo quinto período ordinario de sesiones de la Asamblea General.

8. Respaldar la celebración de la segunda reunión de practicantes gubernamentales en materia de seguridad cibernética que convocará el CICTE para el seguimiento oportuno de las recomendaciones sobre el establecimiento de la Red Interamericana de Alerta y Vigilancia, que figuran en el documento CICTE/REGVAC/doc.2/04 y que forman parte de la Estrategia.

9. Estipular que esa reunión de practicantes gubernamentales en materia de seguridad cibernética se celebre de acuerdo con los recursos asignados en el programa-presupuesto de la Organización y otros recursos, y solicitar que la Secretaría General y la Secretaría del CICTE proporcionen el apoyo administrativo y técnico necesario para esta reunión.

10. Instar a los Estados Miembros a implementar, según corresponda, las recomendaciones de la Reunión Inicial del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA (REMJA-V/doc.5/04) y las recomendaciones relativas a seguridad cibernética de la Quinta Reuníón de la REMJA (REMJA-V/doc.7/04 rev. 4) como medio de crear un

marco para promulgar leyes que protejan los sistemas de información, impidan el uso de computadoras para facilitar actividades ilícitas y sancionen el delito cibernético.

11. Solicitar al Consejo Permanente que informe a la Asamblea General en su trigésimo quinto período ordinario de sesiones sobre la implementación de esta resolución.

ANEXO A

UNA ESTRATEGIA INTERAMERICANA INTEGRAL DE SEGURIDAD CIBERNÉTICA: UN ENFOQUE MULTIDIMENSIONAL Y MULTIDISCIPLINARIO PARA LA CREACIÓN DE UNA CULTURA DE SEGURIDAD CIBERNÉTICA

INTRODUCCIÓN

La Internet y las redes y tecnologías relacionadas se han convertido en instrumentos indispensables para los Estados Miembros de la OEA. La Internet ha impulsado un gran crecimiento en la economía mundial y ha aumentado la eficacia, productividad y creatividad en todo el Hemisferio. Individuos, empresas y gobiernos cada vez utilizan más las redes de información que integran la Internet para hacer negocios; organizar y planificar actividades personales, empresariales y gubernamentales; transmitir comunicaciones; y realizar investigaciones. Asimismo, en la Tercera Cumbre de las Américas, en la ciudad de Quebec, Canadá, en 2001, nuestros líderes se comprometieron a seguir aumento la conectividad en las Américas.

Lamentablemente, la Internet también ha generado nuevas amenazas que ponen en peligro a toda la comunidad mundial de usuarios de Internet. La información que transita por Internet puede ser malversada y manipulada para invadir la privacidad de los usuarios y estafar a los negocios. La destrucción de los datos que residen en las computadoras conectadas por Internet puede obstaculizar las funciones del gobierno e interrumpir el servicio público de telecomunicaciones y otras infraestructuras críticas. Estas amenazas a nuestros ciudadanos, economías y servicios esenciales, tales como las redes de electricidad, aeropuertos o suministro de agua, no pueden ser abordadas por un solo gobierno ni tampoco pueden combatirse utilizando una sola disciplina o práctica. Como reconoce la Asamblea General en la resolución AG/RES. 1939 (XXXIII-O/03) (Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética), es necesario desarrollar una estrategia integral para la protección de las infraestructuras de información que adopte un enfoque integral, internacional y multidisciplinario. La OEA está comprometida con el desarrollo e implementación de esta estrategia de seguridad cibernética y en respaldo a esto, celebró una Conferencia sobre Seguridad Cibernética (Buenos Aires, Argentina, del 28 al 29 de julio de 2003) que demostró la gravedad de las amenazas a la seguridad cibernética para la seguridad de los sistemas de información esenciales, las infraestructuras esenciales y las economías en todo el mundo, y que una acción eficaz para abordar este problema debe contar con la cooperación intersectorial y la coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales.[1/]

De forma similar, en la Conferencia Especial sobre Seguridad (ciudad de México, México, del 28 al 20 de octubre de 2003) los Estados Miembros consideraron el tema de la seguridad cibernética y acordaron lo siguiente:

"*Desarrollaremos* una cultura de seguridad cibernética en las Américas adoptando medidas de prevención eficaces para prever, tratar y responder a los ataques cibernéticos, cualquiera sea su origen, luchando contra las amenazas cibernéticas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas.

1. Informe de la Conferencia sobre Seguridad Cibernética, documento OEA/Ser.L/X.5/ CICTE/CS/doc.2/03.

Reafirmamos nuestro compromiso de desarrollar e implementar una estrategia integral de la OEA sobre seguridad cibernética, utilizando las contribuciones y recomendaciones elaboradas conjuntamente por los expertos de los Estados Miembros y por el Grupo de Expertos Gubernamentales de la REMJA en Materia de Delito Cibernético, el CICTE, la Comisión Interamericana de Telecomunicaciones (CITEL) y otros órganos apropiados, teniendo en cuenta el trabajo que desarrollan los Estados Miembros coordinado con la Comisión de Seguridad Hemisférica."[2/]

Los estados del Hemisferio, reunidos en el cuarto período ordinario de sesiones del Comité Interamericano contra el Terrorismo (CICTE) (Montevideo, Uruguay, del 28 al 30 de enero de 2004), una vez más declararon su compromiso de combatir el terrorismo, incluidas las amenazas a la seguridad cibernética, la cual identificaron como una de las amenazas terroristas emergentes.[3/] en esa ocasión, el CICTE también consideró el documento "Marco para establecer una Red Interamericana CSIRT de Vigilancia y Alerta".[4/] En esa ocasión el CICTE también decidió celebrar, en Ottawa, Canadá, en marzo de 2004, una reunión de expertos o practicantes gubernamentales para considerar ese Marco y elaborar recomendaciones, como aporte del CICTE a la Estrategia Interamericana Integral de Seguridad Cibernética.

La Estrategia Interamericana Integral de Seguridad Cibernética se basa en los esfuerzos y conocimientos especializados del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL), y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA). La Estrategia reconoce la necesidad de que todos los participantes en las redes y sistemas de información sean conscientes de sus funciones y responsabilidades con respecto a la seguridad a fin de crear una cultura de seguridad cibernética.

La Estrategia también reconoce que un marco eficaz para la protección de las redes y sistemas de información que integran la Internet y para responder a incidentes y recuperarse de los mismos dependerá en igual medida de que:

Se proporcione información a los usuarios y operadores para ayudarles a asegurar sus computadoras y redes contra amenazas y vulnerabilidades, y a responder ante incidentes y a recuperarse de los mismos;

Se fomenten asociaciones públicas y privadas con el objetivo de incrementar la educación y la concientización, y se trabaje con el sector privado –el cual posee y opera la mayoría de las infraestructuras de información de las que dependen las naciones—para asegurar esas infraestructuras;

Se identifiquen y evalúen normas técnicas y prácticas óptimas para asegurar la seguridad de la información transmitida por Internet y otras redes de comunicaciones, y se promueva la adopción de las mismas; y

Se promueva la adopción de políticas y legislación sobre delito cibernético que protejan a los usuarios de Internet y prevengan y disuadan el uso indebido e ilícito de computadoras y redes informáticas, respetando a su vez la privacidad de los derechos individuales de los usuarios de Internet.

---

2. Declaración sobre Seguridad en las Américas, documento CES/DEC.1/04 rev. 1.
3. Declaración de Montevideo, OEA/Ser.L/X.2.4, CICTE/DEC. 1/04 rev. 3.
4. Anexo V, documento OEA/Ser.L/X.2.4, CICTE/INF.4/04.

Los Estados Miembros de la OEA están comprometidos, en el marco de este proyecto de Estrategia Interamericana Integral de Seguridad Cibernética, a fomentar una cultura de seguridad cibernética que disuada el uso indebido de la Internet y los sistemas de información asociados e impulse el desarrollo de redes de información que sean de confianza y fiables. Este compromiso se llevará a cabo por medio de las acciones de los Estados Miembros y las iniciativas que emprenderán el CICTE, la CITEL, y el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA que se describen a continuación.

CICTE: Formación de una Red Interamericana de Vigilancia y Alerta para la rápida divulgación de información sobre seguridad cibernética y la respuesta a crisis, incidentes y amenazas a la seguridad informática

Dada la rápidamente cambiante naturaleza de la tecnología, el descubrimiento diario de nuevas vulnerabilidades en el software y hardware, y el creciente número de incidentes de seguridad, la seguridad cibernética es imposible sin un suministro constante y fiable de información sobre amenazas y vulnerabilidades y sobre cómo responder ante estos incidentes y recuperarse de los mismos. Por lo tanto, en respaldo a la Estrategia Interamericana Integral de Seguridad Cibernética, el CICTE formulará planes para la creación de una red hemisférica que funcione 24 horas al día, 7 días a la semana, de Equipos de Respuesta a Incidentes de Seguridad en Computadoras (CSIRT) con la capacidad y el mandato de divulgar correcta y rápidamente información relacionada con la seguridad cibernética y proporcionar orientación y apoyo técnico en el caso de un incidente cibernético. Estos equipos podrían empezar simplemente como puntos nacionales de contacto ubicados en cada Estado encargados de recibir información relacionada con la seguridad informática que se transformarían en CSIRT en el futuro. Las características principales de la iniciativa para crear esta red hemisférica se esbozan más abajo y se describen en detalle en el documento "Recomendaciones del Taller para Practicantes en Materia de Seguridad Cibernética del CICTE sobre la Estrategia Integral de Seguridad Cibernética de la OEA: Marco para establecer una Red Interamericana CSIRT de Vigilancia y Alerta" (CICTE/REGVAC/doc.2/04).[5/] El CICTE creará, junto con los Estados Miembros, esta red hemisférica utilizando el plan de acción que se presenta en ese documento (CICTE/REGVAC/ doc.2/04, Sección IV, páginas 4-6).

Principios

Los grupos de "vigilancia y alerta" que participarán en la iniciativa del CICTE compartirán los siguientes principios comunes:

Locales – La red hemisférica debe ser manejada y controlada por los puntos nacionales de contacto en cada país participante nombrados por los gobiernos.

Sistémicos – La red hemisférica requiere un personal capacitado, la distribución periódica de información relativa a las amenazas y vulnerabilidades vigentes, una reevaluación constante, la implementación de las mejores prácticas y la apropiada interacción con las personas encargadas de formular políticas.
Permanentes – Debido a la evolución diaria inherente a la Internet, el programa deberá actualizarse y mantenerse con regularidad, y el personal deberá ser capacitado periódicamente.

5. Anexo I.

Responsables – Deben entenderse y seguirse las reglas establecidas con respecto a cuestiones tales como el manejo y el suministro de la información, ya que de otra manera los usuarios perderían la confianza y los esfuerzos para proteger el sistema se verán perjudicados e incluso serán contraproducentes.

Basados en disposiciones ya existentes – Hay un número de entidades que ya existen en el Hemisferio y que proporcionan servicios de seguridad cibernética en mayor o menor medida. Un sistema nuevo deberá basarse en esas instituciones ya existentes, a fin de evitar duplicaciones y promover una participación activa.

Creación de la red hemisférica

La creación de una red hemisférica de CSIRT requerirá una serie de medidas progresivas que dependerán de la participación activa de los Estados Miembros:

Identificación de organizaciones CSIRT existentes – Debe realizarse un censo de CSIRT en el Hemisferio a fin de identificar lagunas en la cobertura de los CSIRT que actualmente existen en el Hemisferio y prevenir la duplicación de esfuerzos.

Establecimiento de un modelo de servicio – Los CSIRT nacionales deberán ser designados por sus gobiernos respectivos y será certificados y autorizados de acuerdo con las normas internacionales de la comunidad de servicios informáticos. También deberá establecerse un conjunto mínimo de normas para la cooperación y el intercambio de información entre los CSIRT, como las que se enumeran en el documento CICTE/REGVAC/doc.2/04.

Cuestiones de confianza – Dado que gran parte de la información que tienen que intercambiar los CSIRT es de propiedad exclusiva, o es de carácter delicado por otros motivos, debe crearse confianza entre los participantes como un elemento esencial de la red hemisférica. Para establecer relaciones de confianza, los CSIRT deberán contar con los atributos y capacidades que se describen en el documento CICTE/REGVAC/doc.2/04, los cuales incluyen una infraestructura segura para el manejo de información delicada; la capacidad para comunicarse sin riesgos con los interesados; y procedimientos de protección contra la fuga de información. Los Estados Miembros mantendrán en todo momento el derecho a determinar el tipo de información que intercambiarían a través de sus CSIRT designados.

Creación de conciencia pública – Los CSIRT nacionales deberán asegurar que el público sabe cómo notificar un incidente cibernético y a quién notificarlo.

Extensión de la red – Los Estados Miembros considerarán, cuando proceda, extender las capacidades de la red hemisférica, a fin de ayudar a los Estados que así lo soliciten en la elaboración de sus planes concretos, la obtención de financiamiento y la creación de proyectos de desarrollo de capacidades.

Mantenimiento de la red – El Grupo de Practicantes Gubernamentales en Materia de Seguridad Cibernética se reunirá periódicamente, en la medida necesaria y cuando lo convoque el CICTE, teniendo en cuenta los recursos disponibles.

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

La IV Reunión del Comité Consultivo Permanente I: Normalización de las Telecomunicaciones, celebrada en Quito, Ecuador, del 16 al 19 de marzo de 2004, adoptó la Resolución adjunta CCP.I/RES.49

(IV-04)[6/] "Seguridad cibernética", tras llevar a cabo un taller conjunto con la Unión Internacional de Telecomunicaciones (UIT) que abordó cuestiones clave de seguridad cibernética en lo que concierne a la CITEL. Dicha resolución, que incluye la contribución de la CITEL a la Estrategia Interamericana Integral sobre Seguridad Cibernética, se reproduce más adelante y proporciona orientación para la futura labor de la CITEL en esa área:

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 con 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. 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, el alcance, la pericia, los marcos técnicos y los 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

6. Anexo II.

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 Interamericana Integral 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.

REMJA: Asegurar que los Estados Miembros de la OEA cuentan con los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información

Los delincuentes, como los “piratas informáticos”, los grupos delictivos organizados y los terroristas cada vez explotan más la Internet para fines ilícitos e ingenian nuevos métodos para utilizar la Internet como un medio para cometer y facilitar delitos. Estas actividades ilícitas, a las que normalmente nos referimos como “delitos cibernéticos,” impiden el crecimiento y desarrollo de la Internet, fomentando el temor de que la Internet no es un medio seguro ni de confianza para realizar transacciones personales, gubernamentales o de negocios. Por consiguiente, la contribución de la REMJA a la Estrategia Interamericana Integral de Seguridad Cibernética, por medio de las iniciativas del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético (el Grupo de Expertos), se centrará en asistir a los Estados Miembros a combatir el delito cibernético, asegurando que las autoridades policiales y judiciales cuenten con los instrumentos jurídicos necesarios para investigar y

enjuiciar dichos delitos. Esta decisión fue adoptada por la REMJA en su reunión celebrada del 28 al 30 de abril de 2004 en Washington, D.C., Estados Unidos.[7/]

Redacción y promulgación de legislación en materia de delito cibernético y mejoramiento de la cooperación internacional en asuntos relacionados con delitos cibernéticos

Si no cuentan con leyes y reglamentos adecuados, los Estados Miembros no pueden proteger a sus ciudadanos de los delitos cibernéticos. Además, los Estados Miembros que carecen de leyes y mecanismos de cooperación internacional en materia de delito cibernético corren el riesgo de convertirse en refugios para los delincuentes que cometen estos delitos. Por consiguiente, el Grupo de Expertos proporcionará asistencia técnica a los Estados Miembros para la redacción y promulgación de leyes que tipifiquen el delito cibernético, protejan los sistemas de información y eviten el uso de las computadoras para facilitar actividades delictivas. El Grupo de Expertos también promoverá mecanismos jurídicos que fomenten la cooperación en asuntos relacionados con delitos cibernéticos entre los investigadores y las autoridades policiales y judiciales que investigan y procesan casos de delitos cibernéticos. Estas iniciativas de respaldo a la Estrategia Interamericana Integral de Seguridad Cibernética se emprenderán en el marco de las recomendaciones formuladas por el Grupo de Expertos (Tercera Reunión del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético, OEA/Ser.K/XXXIV, CIBER-III/doc.4/03).[8/]

Para llevar a cabo esta iniciativa, el Grupo de Expertos creará material de capacitación, proporcionará asistencia técnica y llevará a cabo talleres regionales para asistir en la formulación de políticas gubernamentales y leyes que ayuden a generar confianza en los sistemas de información y en la Internet, mediante la tipificación como delito del uso indebido de computadoras y redes informáticas. La capacitación en colaboración que proporcionará el Grupo de Expertos a los Estados Miembros se centrará en la modernización de las leyes y reglamentos para hacer frente al desafío que representa la lucha contra el delito cibernético. Uno de los objetivos principales de estas sesiones de capacitación será el esbozo de las leyes penales y protecciones de la privacidad que sean necesarias para ayudar a hacer más seguros sus sistemas de información y promover la confianza entre los usuarios de esos sistemas. Específicamente, los talleres se concentrarán en la promulgación de distintas categorías de leyes:

- Leyes substantivas sobre delitos cibernéticos – Todos los Estados Miembros deberán establecer prohibiciones de carácter penal y jurídico a los ataques contra la confidencialidad, integridad y seguridad de los sistemas informáticos. Comportamientos tales como el acceso a computadoras sin autorización, la intercepción ilícita de datos, la interferencia con la disponibilidad de sistemas informáticos, y el robo y sabotaje de datos deberán considerarse ilícitos de conformidad con la ley de cada Estado Miembro de la OEA.

- Leyes procesales para la recopilación de pruebas electrónicas – Además, todos los países deberán contar con procedimientos claros acordes con las normas internacionales para el acceso del gobierno a las comunicaciones y los datos almacenados cuando sea necesario para la investigación de un delito. Es igualmente importante que se asegure a las empresas y consumidores que el gobierno no va a vigilar de forma injustificada sus

7. Anexo IV, documento OEA/Ser.K/XXXIV.5/REMJA-V/doc.7/04 rev. 4.
8. Anexo III.

comunicaciones, y que se asegure a los consumidores que los datos que suministran a los comerciantes no van a ser utilizados indebidamente.

Los talleres se centrarán en la necesidad de redactar dichas leyes de un manera que sea “neutral con respecto a la tecnología” (por ejemplo, dichas leyes deberán contemplar tipos de delitos o tipos de comportamiento en vez de ser redactadas solamente para contemplar un tipo particular de tecnología) para prevenir que las leyes recién promulgadas se vuelvan rápidamente obsoletas o irrelevantes.

La naturaleza sin fronteras de las redes mundiales significa que un único acto delictivo relacionado con una computadora puede afectar o dirigirse a computadoras en varios países. Durante sus talleres regionales, el Grupo de Expertos también proporcionará capacitación sobre cómo responder a estos desafíos en el marco de la cooperación internacional y facilitar el intercambio de información relativa a las investigaciones sobre casos de delitos cibernéticos. Se pondrá especial énfasis en el establecimiento de relaciones entre los expertos en materia de delito cibernético en el Hemisferio a fin de facilitar la cooperación internacional y proporcionar un acceso fácil a los conocimientos especializados y recursos de la región para combatir el delito cibernético.

Tras la celebración de los talleres, el Grupo de Expertos asistirá nuevamente a los Estados Miembros proporcionando consultas jurídicas para respaldar a los ministerios del gobierno y legislaturas en la redacción de leyes, reglamentos y políticas. Puede requerirse asistencia de los expertos a nivel bilateral para respaldar a los gobiernos en la formulación de leyes y políticas que consagren los conceptos centrales de las leyes en materia de delito cibernético, autoridades de investigación y privacidad.

CONCLUSIONES Y ESTRATEGIA DE SEGUIMIENTO

Cada una de las iniciativas del CICTE, la CITEL y la REMJA que se describen arriba representa un pilar de este proyecto de Estrategia Interamericana Integral de Seguridad Cibernética. De forma conjunta, los esfuerzos multidisciplinarios concertados de estos órganos apoyarán el crecimiento, desarrollo y protección de la Internet y los sistemas de información relacionados, y protegerán a los usuarios de esas redes de información. Estas iniciativas pueden ir cambiando con el paso del tiempo y requerir nuevos enfoques, pero su objetivo seguirá siendo el mismo: la creación y apoyo de una cultura de seguridad cibernética. Considerando que la Estrategia es dinámica, debe emprenderse un examen periódico a fin de asegurar su continua aplicabilidad y eficacia. Esto puede lograrse a través de las siguientes acciones:

1. Coordinación y cooperación permanentes entre las Secretarías del CICTE, la CITEL y el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA.

2. Fortalecimiento de la coordinación entre las autoridades y entidades nacionales, incluidos los CSIRT nacionales, que trabajan en cuestiones relacionadas con la seguridad cibernética.

3. Establecimiento de una sitio Web conjunto en el que pueda introducirse la información pertinente sobre seguridad cibernética generada por el CICTE, la CITEL y el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA, a fin de permitir un fecundo intercambio de ideas y facilitar el intercambio de información.

4. Los Estados Miembros deberán llevar a cabo, junto con el CICTE, la CITEL y el Grupo de Expertos Gubernamentales de la REMJA en Materia de Delito Cibernético, un programa interamericano de concientización del público acerca de la seguridad y la ética cibernéticas en el que se destaquen: las ventajas y responsabilidades del uso de redes de información; las mejores prácticas de seguridad y protección; las posibles consecuencias negativas del uso indebido de las redes; cómo reportar un incidente cibernético y a quién; e información técnica y práctica relacionada con la seguridad cibernética.

Exámenes periódicos de las iniciativas y programas en materia de seguridad cibernética del CICTE, la CITEL y el Grupo de Expertos Gubernamentales de la REMJA en Materia de Delito Cibernético, y sobre la implementación de la Estrategia, que realizarán estos tres órganos, con un informe conjunto de progreso para la Asamblea General