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. Reafirmamos nuestro compromiso de desarrollar e implementar una estrategia integral

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

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

6. Anexo II.

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 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 comunicaciones, y que se asegure a los

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

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.

5. 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

ANEXO I

COMITÉ INTERAMERICANO CONTRA EL TERRORISMO (CICTE)

TALLER PARA PRACTICANTES EN MATERIA
DE SEGURIDAD CIBERNÉTICA
29-30 de marzo de 2004
Ottawa, Canadá

OEA/Ser.L/X.5
CICTE/REGVAC/doc.2/04
8 abril 2004
Original: inglés

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

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

I. OBJETIVOS

Crear una red hemisférica, que funcione 24 horas al día, 7 días a la semana, de puntos nacionales de contacto entre equipos de respuesta a incidentes de seguridad en computadoras (*Computer Security Incident Response Teams*: CSIRT) con responsabilidad nacional (CSIRT nacionales), en los Estados Miembros de la OEA, con el mandato y la capacidad de responder debida y rápidamente a las crisis, incidentes y peligros relacionados con la seguridad cibernética.

Estos equipos podrían comenzar simplemente como puntos de contacto oficiales en cada uno de los Estados y estarían a cargo de recibir información sobre seguridad cibernética. En el futuro se convertirían en un CSIRT.

Los intrusos ahora tienen medios cada vez más complejos para lanzar ataques muy automatizados que se desplazan rápidamente a través de Internet, empleando técnicas que tienen por fin encubrir el origen de tales ataques y dificultar su rastreo. Por tanto, reviste importancia creciente la colaboración mundial y la capacidad de respuesta en tiempo real entre los equipos. Dicha colaboración debe permitir lo siguiente:

1. El establecimiento de CSIRT en cada uno de los Estados Miembros;
2. El fortalecimiento de los CSIRT hemisféricos;
3. La identificación de los puntos de contacto nacionales;
4. La identificación de los servicios críticos;
5. El diagnóstico rápido y preciso del problema;
6. El establecimiento de protocolos y procedimientos para el intercambio de información;
7. La pronta diseminación regional de advertencias sobre ataques;
8. La pronta diseminación regional de advertencias sobre vulnerabilidades genéricas;
9. La difusión de un alerta regional sobre actividades sospechosas y la colaboración para analizar y diagnosticar tales actividades;
10. El suministro de información sobre medidas para mitigar y remediar los ataques y amenazas;
11. La reducción de duplicaciones de análisis entre los equipos;
12. El fortalecimiento de la cooperación técnica y la capacitación en materia de seguridad cibernética para establecer los CSIRTs nacionales;
13. La utilización de los mecanismos subregionales existentes.

La colaboración refuerza los conocimientos técnicos existentes entre los equipos para limitar mejor los perjuicios y permitir que continúen funcionando los servicios de importancia crítica.

II. PRINCIPIOS

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

2. Sistémicos – La red hemisférica debe ser una operación multifacética que requiera un personal consciente y especializado, la distribución periódica de información relativa a las amenazas y vulnerabilidades vigentes, una reevaluación e implementación constantes de mejores prácticas y una interacción adecuada con las autoridades públicas.

3. Permanentes – Debido a la evolución diaria inherente a la Internet, para que tenga buen resultado todo programa deberá actualizarse y mantenerse con regularidad, y el personal deberá ser capacitado periódicamente. La seguridad en la Internet no se logrará mediante una acción única.

4. Responsables – La "seguridad" en la "ciberseguridad". Deben entenderse y seguirse reglas establecidas respecto de 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 serán perjudicados e incluso serán contraproducentes.

5. Basados en disposiciones ya existentes – Hay un número de entidades que ya existen en el Hemisferio, entre ellas, CSIRT, compañías consultoras y redes de contactos, que proporcionan servicios de seguridad cibernética en mayor o menor medida. Un sistema nuevo deberá basarse en esas instituciones ya existentes y las relaciones de confianza que ya se han establecido dentro de cada región y entre regiones, a fin de evitar duplicaciones y promover una participación activa.

III. IDENTIFICACIÓN DE ORGANIZACIONES EXISTENTES, ESTABLECIMIENTO DE UN MODELO DE SERVICIO, CUESTIONES DE CONFIANZA, FINANCIAMIENTO, CONCIENCIA PÚBLICA Y EXTENSIÓN DE LA RED

1. Identificación de organizaciones existentes

En todo el mundo hay más de cien organizaciones que usan el nombre CERT (*Computer Emergency Response Team*: equipo de respuesta a emergencias de computación) o CSIRT (el término genérico de significado equivalente). El Foro de Equipos de Respuesta a Incidentes y de Seguridad (*Forum of Incident Response and Security Teams*: FIRST), una asociación mundial voluntaria de equipos CSIRT, cuenta con 79 miembros en los Estados Miembros de la OEA, sin embargo la gran mayoría de estos actualmente existen en un Estado Miembro solamente. Dadas las lagunas en la información, llevar a cabo un censo de los CSIRT es el primer paso fundamental para la creación de una red de seguridad cibernética.

2. Establecimiento de un modelo de servicio

Si bien no hay normas internacionales acordadas sobre qué es lo que constituye un CSIRT, hay una serie de documentos y actividades que pueden servir para definir un equipo CSIRT y para la certificación y autorización de tales equipos.

El CERT/CC ha publicado varios documentos que pueden servir de ayuda para la creación de un CSIRT, entre los que se cuentan los siguientes:

- *Handbook for Computer Security Incident Response Teams (CSIRTs)* (Manual para equipos de respuesta a incidentes de seguridad de computadoras [CSIRT]): guía actualizada sobre cuestiones genéricas que deben considerarse al formar un CSIRT;
- *State of the Practice of Computer Security Incident Response Teams* (Estado actual de las prácticas de los equipos de respuesta a incidentes de seguridad de computadoras). Este informe contiene información recogida mediante un estudio piloto de estos equipos, la experiencia propia del CERT/CC, discusiones con otros CSIRT y observaciones de éstos, e investigación y críticas de las publicaciones actuales sobre la respuesta a incidentes; y
- *Creating a Computer Security Incident Response Team: A Process for Getting Started* (Creación de un equipo de respuesta a incidentes de seguridad de computadoras: un método para su comienzo). Éste es un documento en el que se describen los requisitos básicos para crear un CSIRT.

Debería existir un sistema de certificación y autorización de CSIRT nacionales. Los Estados Miembros deberían considerar si la afiliación de sus CSIRT nacionales al FIRST satisfaría los requisitos de certificación y autorización.

Cuando se establece una red regional de CSIRT nacionales cooperantes, debe preverse un conjunto mínimo de normas para la cooperación y el intercambio de información entre los CSIRT, entre las que se contarían las siguientes:

i. designación del CSIRT nacional por el gobierno respectivo;

ii. convenio sobre los principios para compartir información entre los equipos cooperantes;

iii. responsabilidad por recibir información de otros CSIRT nacionales, y por diseminar dicha información entre las entidades idóneas dentro del país;

iv. participación en el intercambio de información entre los otros CSIRT nacionales en la red hemisférica;

v. autorización para diseminar información entre otros CSIRT nacionales; y

vi. prestación de asistencia a otros CSIRT nacionales para incidentes y amenazas.

3. Cuestiones de confianza

Gran parte de la información que tienen que intercambiar los CSIRT es de propiedad exclusiva, o es de carácter delicado por otros motivos, y hay pocos modelos buenos que sirvan para compartir uniformemente datos entre tales equipos. La confianza —el ingrediente esencial cuando se comparte información—, cuando existe, se desarrolla en la práctica entre individuos que se conocen y han trabajado juntos, más bien que institucionalmente entre organizaciones. Para establecer la confianza, todas las partes deben entender y seguir pautas claras sobre la forma en que la información intercambiada será usada o diseminada. Todos los CSIRT nacionales cooperantes deben convenir en las reglas para compartir información, que indiquen cómo tal información puede usarse o diseminarse.

Entre los atributos que los CSIRT requieren para promover la confianza en las comunicaciones y la cooperación respecto de asuntos delicados de seguridad figuran los siguientes:

i. una infraestructura segura para el manejo de información delicada;

ii. la capacidad para comunicarse sin riesgos con los interesados;

iii. la capacidad para reunir expertos y autoridades;

iv. una infraestructura que permita la notificación anticipada a determinadas audiencias;

v. procedimientos de protección contra fuga de información;

vi. una interfaz pública bien conocida para la diseminación de información crítica; y

vii. la capacidad para llegar rápidamente a una gran audiencia.

La creación de una capacidad CSIRT regional requiere la formación de un consenso sobre las reglas para el intercambio de información, incluso qué información puede compartirse, con quién, y cuándo.

4. Financiamiento

Los Estados Miembros considerarán los mecanismos de financiación para establecer y mantener un CSIRT nacional en cada país y participar en la red hemisférica.

5. Conciencia pública

Los Estados Miembros deben llevar a cabo, junto con la CITEL y el Grupo de Trabajo de la REMJA, un programa interamericano de concientización del público acerca de la seguridad y la ética cibernéticas en el que se destaquen:

i. las ventajas y responsabilidades del uso de redes de información;

ii. las mejores prácticas de seguridad y protección;
iii. las posibles consecuencias negativas del uso indebido de las redes;

iv. como reportar un incidente cibernético y a quien; y

v. información técnica y práctica relacionada con la seguridad cibernética.

El público incluye a los Estados Miembros, las entidades gubernamentales de todo nivel, el sector privado, el sector académico y la población general.

6. 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 planes concretos, la obtención de financiamiento y la creación de proyectos de desarrollo de capacidades.

IV. Plan de acción

A. Censo

Llevar a cabo un censo para identificar los CSIRT existentes, la diversidad de miembros y los servicios que proporcionan. Esto nos permitirá identificar las lagunas en la cobertura, tanto geográfica como sectorialmente, y establecerá las bases para fijar un conjunto consensual de servicios que ofrecerán los CSIRT miembros.

B. Reglas relativas al intercambio de información

Establecer reglas relativas al intercambio de información entre los CSIRT, incluido cómo debe protegerse y difundirse la información intercambiada.

C. Establecimiento de los CSIRT nacionales

Cada Estado miembro establecerá los CSIRT nacionales. Entre sus responsabilidades figurarán la implementación de las propuestas pertinentes contenidas 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" (REGVAC/doc.2/04).

D. Punto nacional de contacto

Designar un punto nacional de contacto con capacidad para intercambiar información acerca de amenazas, deficiencias e incidentes, informar sobre el estado de la seguridad cibernética en su jurisdicción y brindar información oportuna a las autoridades de ésta.

E. Compendio de mejores prácticas

Producir un compendio de mejores prácticas basado en las normas y prácticas CSIRT internacionales. Éstas podrían incluir normas y protocolos para llevar a cabo monitoreo en tiempo real y un subsiguiente intercambio de información en toda la red, y podría servir de base para protocolos posteriores de asistencia técnica y pruebas.

F. Asistencia para construir y mantener los CSIRT en los Estados Miembros

Identificar los recursos y capacidades que pueden utilizarse para ayudar a los Estados Miembros a construir y mantener la capacidad de los CSIRT o mejorar las infraestructuras de los CSIRT existentes a fin de participar con eficacia en la red hemisférica y cumplir las reglas de intercambio de información. Se incluirá la asistencia técnica y capacitación de personal necesarias.

G. Conciencia pública

El CICTE, la CITEL y el Grupo de Trabajo de Expertos Gubernamentales en materia de Delito Cibernético de la REMJA trabajarán juntos para llevar a cabo una campaña de concientización a fin de alertar al público en los Estados Miembros de las cuestiones relativas a la seguridad cibernética y la necesidad de proteger sus redes cibernéticas.

H. Seguimiento

Se recomienda que el CICTE convoque de nuevo la Reunión de Expertos en Materia de Seguridad Cibernética (Taller para Practicantes en Materia de Seguridad Cibernética) para elaborar e implementar las recomendaciones formuladas 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" (REGVAC/doc.2/04).

Asimismo, se recomienda que el Grupo de Trabajo encargado de la Elaboración de un Proyecto de Estrategia de Seguridad Cibernética para los Estados Miembros de la OEA, de la Comisión de Seguridad Hemisférica de la OEA, transmita este documento marco a la Asamblea General para su adopción.

ANEXO II

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 más 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 RESOLUCIÓN 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.

ANEXO III

REUNIÓN DE MINISTROS DE
JUSTICIA O DE MINISTROS O PROCURADORES
GENERALES DE LAS AMERICAS (REMJA)

OEA/Ser.K/XXXIV
CIBER-III/doc.4/03
24 junio de 2003
Original: español

Tercera Reunión del Grupo de Expertos Gubernamentales
en Materia de Delito Cibernético
23 y 24 de junio de 2003
Washington, D.C.

RECOMENDACIONES DE LA REUNIÓN INICIAL DEL GRUPO DE EXPERTOS GUBERNAMENTALES EN MATERIA DE DELITO CIBERNÉTICO*

Los expertos gubernamentales en materia de delito cibernético de los Estados Miembros de la OEA, se reunieron en la sede de esta Organización, en Washington D.C., Estados Unidos de América, durante los días 23 y 24 de junio de 2003, en cumplimiento de lo acordado en la Cuarta Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA-IV) y de la resolución de la Asamblea General de la OEA AG/RES. 1849 (XXXII-O/02).

Teniendo en cuenta el mandato que le fue asignado por la REMJA-IV, al finalizar sus deliberaciones en el marco de esta reunión inicial, el Grupo de Expertos Gubernamentales acordó formular las siguientes recomendaciones en relación con las áreas en las cuales se requieren mayores avances con el fin de fortalecer y consolidar la cooperación hemisférica en el combate contra el Delito Cibernético:

1. Que, de acuerdo con la recomendación formulada por este Grupo y adoptada por la REMJA-III, los Estados que aún no lo han hecho, en el menor plazo posible, identifiquen o, si fuere necesario, creen o establezcan unidades o entidades encargadas específicamente de dirigir y desarrollar la investigación y persecución de las diversas modalidades de delitos cibernéticos y les asignen los recursos humanos, financieros y técnicos necesarios para el cumplimiento de sus responsabilidades en forma eficaz, eficiente y oportuna.

2. Que los Estados que aún no lo hayan hecho, a la mayor brevedad posible, examinen sus sistemas jurídicos para determinar si éste se aplica en forma adecuada a los delitos cibernéticos y a la obtención y mantenimiento en custodia segura de indicios y/o pruebas electrónicas.

3. Que los Estados que aún no lo hayan hecho, adopten la legislación que específicamente se requiera para tipificar las diversas modalidades de delitos cibernéticos, así como para dictar las medidas procesales que aseguren la obtención y mantenimiento en custodia segura de indicios y/o pruebas electrónicas y la investigación y persecución de tales delitos en forma efectiva, eficaz y oportuna.

---

* El presente documento fue aprobado en su integridad por el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético, en la sesión celebrada el día 24 de junio de 2003.

4. Que, con el fin de asistir a los Estados en la elaboración o mejoramiento y adopción de la legislación en materia de delito cibernético, se realicen reuniones técnicas, en el marco de la OEA, sobre redacción de legislación en este campo, en las cuales se consideren los desarrollos específicos que se deben dar, entre otras, en las áreas substantiva, procesal y de asistencia judicial mutua, para facilitar la armonización de las legislaciones nacionales y contar con el marco jurídico que permita y garantice la efectiva, eficiente y oportuna cooperación hemisférica en el combate contra las diversas modalidades de delitos cibernéticos.

5. Que, con base en la información que le suministren los Estados, la Secretaría General de la OEA elabore y mantenga actualizado un directorio con los puntos de contacto de cada uno de los Estados que integran el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético, así como un directorio de las autoridades responsables de la investigación y persecución del Delito Cibernético.

6. Que los Estados que aún no lo han hecho, adopten todas las decisiones que se requieran con el fin de vincularse, a la mayor brevedad posible, a la "Red de Emergencia de 24 horas/7 días", habiendo tomado los pasos a que se refiere el párrafo 1, si fuere necesario.

7. Que, teniendo en cuenta los progresos dados a través de la página de la OEA en *Internet*, se avance en la consolidación de un sistema integral de información sobre los desarrollos dados en materia de combate contra el delito cibernético, con una parte pública y otra con acceso restringido para las autoridades gubernamentales con responsabilidades en este campo, en relación con información sensible. Asimismo que, con base en la información que provean los Estados, la Secretaría General compile y publique en la página en *Internet* de la OEA las legislaciones en la materia e identifique las áreas temáticas comunes entre estas.

8. Que los Estados incorporen la formación específica en materia de delito cibernético y el manejo de pruebas electrónicas como parte de los programas de capacitación dirigidos a jueces, fiscales y autoridades de policía judicial y que para el desarrollo de éstos, los Estados Miembros de la OEA y los Observadores Permanentes ante esta Organización se presten la más amplia asistencia y cooperación técnica mutua entre ellos.

9. Que se continúe fortaleciendo el intercambio de información y la cooperación con otras organizaciones e instancias internacionales en materia de delito cibernético como las Naciones Unidas, el Consejo de Europa, la Unión Europea, el Foro de Cooperación Económica del Pacífico Asiático, la OCDE, el G-8 y el Commonwealth, de manera que los Estados Miembros de la OEA puedan conocer y aprovechar los desarrollos dados en dichos ámbitos.

10. Que el Grupo de Expertos Gubernamentales en materia de Delito Cibernético se reúna por lo menos una vez al año, en el ámbito de la OEA, y que en el marco de las próximas reuniones:

    a. Examine los resultados de las reuniones técnicas a que se refiere el párrafo 4 y, teniendo en cuenta sus resultados, considere, si fuere el caso, los ajustes que se deben adoptar en futuros encuentros de esta naturaleza, así como otras acciones que se

deban realizar para facilitar la adopción y aplicación de la legislación antes mencionada.

b. Prepare recomendaciones para identificar y describir los diversos tipos de delitos cibernéticos.

c. Prepare recomendaciones para identificar y describir las facultades de investigación que los Estados deben poseer para investigar los delitos cibernéticos. Estas facultades de investigación deben:

   i. Aplicarse no sólo a las investigaciones de delitos cibernéticos, sino también a la recolección y custodia segura de indicios y/o pruebas en forma electrónica de cualquier otro delito.

   ii. Asegurar un adecuado equilibrio entre el ejercicio fundado y motivado de dichas facultades y la necesidad de garantizar las normas del debido proceso, en el marco del respeto de los derechos humanos y las libertades fundamentales.

   iii. Ser aplicables, en la forma permitida por la legislación nacional, tanto para responder a las solicitudes internacionales de cooperación como a las investigaciones nacionales.

   iv. Permitir el rastreo de comunicaciones de presuntos delincuentes, a través de redes electrónicas que comprendan a proveedores de servicios múltiples, para determinar el curso, origen o destino de las comunicaciones.

d. Recomiende medidas para evitar la creación de “paraísos de los delitos cibernéticos”, de conformidad con la ley de cada Estado y los tratados internacionales.

e. Los Estados informen sobre las medidas que han tomado entre una y otra reunión.

Washington D.C., Estados Unidos de América, 24 de junio de 2003.

ANEXO IV

QUINTA REUNIÓN DE MINISTROS DE JUSTICIA
O DE MINISTROS O PROCURADORES GENERALES
DE LAS AMÉRICAS
28 al 30 de abril de 2004
Washington, D.C.

OEA/Ser.K/XXXIV.5
REMJA-V/doc.7/04 rev. 4
30 abril 2004
Original: español

CONCLUSIONES Y RECOMENDACIONES DE LA REMJA-V *

* Las presentes "Conclusiones y Recomendaciones de la REMJA-V" fueron aprobadas por consenso en la sesión plenaria celebrada el día 30 de abril de 2004, en el marco de la Quinta Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA-V) celebrada en la sede de la OEA en Washington D.C., Estados Unidos de América.

CONCLUSIONES Y RECOMENDACIONES DE LA REMJA-V

Al finalizar los debates sobre los diferentes puntos comprendidos en su agenda, la Quinta Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA-V), convocada en el marco de la OEA, adoptó las siguientes conclusiones y recomendaciones para ser transmitidas, a través del Consejo Permanente, al trigésimo cuarto período ordinario de sesiones de la Asamblea General de la OEA.

I. COOPERACIÓN HEMISFÉRICA CONTRA LA DELINCUENCIA TRANSNACIONAL ORGANIZADA Y CONTRA EL TERRORISMO

La REMJA-V reafirma que el daño que infringen y la amenaza que representan las diversas manifestaciones de la criminalidad transnacional organizada y el terrorismo, para nuestros ciudadanos, para nuestras democracias y para el desarrollo económico y social de nuestros Estados, hacen necesario y urgente continuar fortaleciendo y perfeccionando la cooperación jurídica y judicial mutua a nivel hemisférico, así como, si no lo han hecho, adoptar legislación, procedimientos y mecanismos nuevos que les permitan combatir de manera eficaz estos delitos.

Al respecto, destaca que, de acuerdo con la "Declaración sobre la Seguridad en las Américas", aprobada en la ciudad de México, el 28 de octubre de 2003, el terrorismo y la delincuencia organizada transnacional hacen parte de las nuevas amenazas, preocupaciones y otros desafíos de naturaleza diversa que afectan la seguridad de los Estados del Hemisferio y que en ella se reafirma "que las Reuniones de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA) y otras reuniones de autoridades en materia de justicia penal son foros importantes y eficaces para la promoción y el fortalecimiento del entendimiento mutuo, la confianza, el diálogo y la cooperación en la formulación de políticas en materia de justicia penal y de respuestas para hacer frente a las nuevas amenazas a la seguridad".

Considerando que, si bien la comunidad internacional ha avanzado en la elaboración de normas para combatir estas formas de delincuencia, subsisten diferencias en la forma en que los Estados tipifican las conductas delictivas, lo cual puede crear impedimentos para una más efectiva cooperación internacional.

La REMJA-V reconoce la conveniencia de que el tema de la Delincuencia Organizada Transnacional continúe siendo tratado por las diferentes entidades de la OEA que lo han venido haciendo en el marco de sus respectivas competencias, tales como la CICAD, el Comité Consultivo de la CIFTA, la CIM, el Instituto Interamericano del Niño, la REMJA y el MESICIC.

La REMJA-V reafirma que las medidas realizadas por los Estados Parte para combatir el terrorismo deberán llevarse a cabo respetando plenamente el Estado de derecho, los derechos humanos y las libertades fundamentales, sin menoscabar los derechos y las obligaciones de los Estados y las personas conforme al Derecho Internacional, el Derecho Internacional de los Derechos Humanos y el Derecho Internacional de los Refugiados.

La REMJA-V expresa satisfacción ante el hecho de que en el período que siguió a la REMJA-IV, los Estados Miembros de la OEA hayan adoptado importantes medidas para reforzar la aplicación hemisférica de los instrumentos de las Naciones Unidas de lucha contra el terrorismo y la delincuencia transnacional organizada, de modo de hacer frente en forma eficaz a esos crímenes. En especial, en el intervalo comprendido entre la REMJA-IV y la REMJA-V, numerosos Estados Miembros de la OEA se convirtieron en Partes del Convenio para la Represión de la Financiación del

Terrorismo de 1999, así como de instrumentos universales anteriores de lucha contra el terrorismo. Análogamente, numerosos Estados Miembros de la OEA se convirtieron en Partes de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional de 2000 y sus tres Protocolos Complementarios o adoptaron importantes medidas encaminadas a adquirir esa condición. La REMJA-V reconoce este notable avance en la lucha contra el terrorismo y la delincuencia transnacional organizada.

La REMJA-V toma nota también con satisfacción de que se ha acelerado en gran medida la adhesión a instrumentos regionales de lucha contra el terrorismo y la delincuencia organizada. La Convención Interamericana contra el Terrorismo de 2002 entró en vigor el 10 de julio de 2003 y ha sido ratificada por ocho (8) Estados Miembros de la OEA; y la Convención Interamericana contra la Fabricación y el Tráfico Ilícitos de Armas de Fuego, Municiones, Explosivos y Otros Materiales Relacionados (CIFTA) ha sido ratificada por veintidós (22) Estados Miembros de la OEA.

La REMJA-V expresa asimismo su satisfacción por los avances registrados con el propósito de fortalecer y consolidar la cooperación entre los Estados de las Américas para combatir el terrorismo, a través del Trabajo del Comité Interamericano contra el Terrorismo (CICTE) y de sus puntos de contacto nacionales.

Al mismo tiempo quedan tareas por hacer en cuanto a determinación de mecanismos de eficaz aplicación de normas hemisféricas y mundiales de lucha contra el terrorismo y la delincuencia organizada, y tomamos nota con alarma del incremento de los ataques terroristas a nivel mundial y las actividades de otras organizaciones criminales. En consecuencia recomendamos:

A. COOPERACIÓN HEMISFÉRICA CONTRA LA DELINCUENCIA TRANSNACIONAL ORGANIZADA

1. Que con respecto a la lucha contra la delincuencia transnacional organizada, los Estados Miembros que aún no lo hayan hecho firmen y ratifiquen, ratifiquen, o adhieran, según sea el caso, e implementen, a la brevedad posible:

   a. La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, el Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, y el Protocolo contra el tráfico ilícito de migrantes por tierra, mar y aire. Instamos a los Estados Miembros a completar sus procesos internos para determinar si han de suscribir y ratificar el Protocolo contra la fabricación y el tráfico ilícitos de armas de fuego, sus piezas y componentes y municiones.

   b. La Convención Interamericana contra la Fabricación y el Tráfico Ilícitos de Armas de Fuego, Municiones, Explosivos y Otros Materiales Relacionados (CIFTA) que, entre otras cosas, establece un régimen eficaz de penalización del tráfico ilícito de armas de fuego que ayudará a la lucha contra la delincuencia transnacional organizada y contra el terrorismo y que, además, crea un mecanismo de seguimiento hasta la fuente de las armas de fuego que puedan ser objeto de tráfico ilícito.

2. Que los Estados Miembros que son Parte o signatarios de la Convención contra la Delincuencia Organizada Transnacional y sus dos protocolos en vigor trabajen conjuntamente en la Primera Conferencia de las Partes, que tendrá lugar entre el 28 de junio y el 9 de julio de 2003, para facilitar la aplicación de esos importantes instrumentos internacionales.

3. Recomendar a la Asamblea General de la OEA que convoque a un grupo de expertos que considere la posibilidad de la elaboración de un Plan de Acción Hemisférico contra la Delincuencia Transnacional Organizada, como un plan integrado que recoja el esfuerzo que cada área de la OEA viene desarrollando en los diferentes aspectos del problema, de conformidad con la Declaración sobre Seguridad en las Américas.

4. Que los Estados Miembros consideren –cuando sea apropiado– la armonización de sus respectivos ordenamientos jurídicos con las obligaciones asumidas en esta materia. A tal fin, se recomienda que la Asamblea General de la OEA encomiende al Comité Jurídico Interamericano la realización de un estudio sobre el punto antes mencionado, y que le informe a la entidad que la Asamblea General atribuya la responsabilidad de considerar la posibilidad de elaborar un Plan de Acción Hemisférico contra la Delincuencia Organizada Transnacional.

5. Que los Estados Miembros promuevan una mayor interrelación entre las autoridades de aplicación de la ley para que determinen líneas de acción comunes en la investigación y enjuiciamiento de estos delitos.

6. Instar a los Estados a la realización de seminarios y jornadas de capacitación tanto a nivel regional como nacional, referidos a los diferentes aspectos de la delincuencia transnacional organizada.

B. COOPERACIÓN HEMISFÉRICA CONTRA EL TERRORISMO

1. Que con respecto a la lucha contra el terrorismo, los Estados Miembros que aún no lo hayan hecho firmen y ratifiquen, ratifiquen, o adhieran, según sea el caso, e implementen, a la brevedad posible:

   a. Las doce convenciones de las Naciones Unidas contra el terrorismo.

   b. La Convención Interamericana contra el Terrorismo.

2. Que los Estados Miembros dispongan de capacidad suficiente para tomar acciones de aplicación de la ley con respecto a situaciones en las cuales aún no se ha realizado un ataque terrorista y en que una oportuna investigación y persecución pueda prevenir la realización de esos ataques, y adoptar medidas inmediatas que confieran capacidad suficiente para la persecución de dichas conductas y hacer efectiva la cooperación mutua al respecto.

3. Que cada Estado Miembro fortalezca su capacidad para facilitar el intercambio de información entre los servicios de seguridad y los organismos de aplicación de la ley para prevenir ataques y lograr el encauzamiento de terroristas, de conformidad con las leyes nacionales y los instrumentos internacionales aplicables.

4. Que, en aplicación del artículo 7 de la Convención Interamericana contra el Terrorismo, los Estados Miembros promuevan las más amplias medidas de cooperación, especialmente medidas que garanticen la eficaz colaboración entre los organismos de aplicación de la ley, los servicios de inmigración y entidades conexas y sometan a mejores controles a sus documentos de viaje y de identidad.

5. Tomar nota de la labor de la Comisión Interamericana de Derechos Humanos en la esfera del terrorismo y de los derechos humanos. Recomienda que las autoridades responsables de la elaboración de leyes contra el terrorismo sigan reuniéndose e intercambiando mutuamente prácticas modelo y experiencias nacionales sobre este tema.

6. Recomendar que la Red Hemisférica de Intercambio de Información para la Asistencia Judicial Mutua en Materia Penal comprenda información sobre legislación y, según sea apropiado, políticas antiterroristas vigentes en los Estados Miembros.

7. Recomendar que, para ayudar a la prevención de actos de terrorismo, deben tomarse medidas para evitar la discriminación contra miembros de la sociedad.

II. ASISTENCIA JUDICIAL MUTUA EN MATERIA PENAL Y EXTRADICIÓN

A. REUNIÓN DE AUTORIDADES CENTRALES Y OTROS EXPERTOS EN ASISTENCIA JUDICIAL MUTUA EN MATERIA PENAL

La REMJA-V recomienda:

1. Expresar su satisfacción por la realización de la “Reunión de Autoridades Centrales y Otros Expertos en Materia de Asistencia Judicial Mutua en Materia Penal”, celebrada en cumplimiento de las recomendaciones de la REMJA IV, en Ottawa, Canadá, entre los días 30 de abril y 2 de mayo de 2003, y adoptar en su integridad las recomendaciones formuladas, las cuales se encuentran publicadas en el documento OEA/Ser.K/XXXIV.5 REMJA-V/doc.4.

2. Respaldar, conforme a la recomendación 6 de esa reunión, la continua celebración de reuniones de las Autoridades Centrales y otros Expertos sobre asistencia judicial mutua en materia penal del Hemisferio, por lo menos una vez entre una REMJA y la siguiente, con el apoyo y la coordinación del Grupo de Trabajo sobre Asistencia Judicial Mutua, y la consideración, en su siguiente reunión, del avance logrado en cuanto a la aplicación de las recomendaciones de la reunión de Ottawa e, *inter alia*, los temas a los que se refiere la arriba mencionada recomendación 6, conforme al orden de prioridades que definan.

3. Decide que, en la próxima reunión de autoridades centrales y otros expertos, se inicie la consideración de acciones para fortalecer la cooperación jurídica hemisférica en materia de extradición, incluyendo la extradición temporal cuando proceda de acuerdo con la legislación nacional, y proceda a la preparación de las secciones relativas a la cooperación jurídica y judicial mutua de un plan de acción hemisférico para el combate contra la delincuencia transnacional organizada y contra el terrorismo, incluyendo medidas de administración de casos por el Estado requirente para no sobrecargar al Estado requerido.

4. Decide que la próxima reunión de autoridades centrales y otros expertos continúe fortaleciendo y haciendo más efectivos los mecanismos de asistencia judicial mutua en materia penal y la cooperación hemisférica en materia de extradición. A tal efecto la reunión de autoridades centrales y otros expertos, podrá solicitar insumos a las siguientes entidades en relación con las áreas de su competencia: CICTE, CICAD, Comité Consultivo de la CIFTA, CIM, MESICIC, Instituto Interamericano del Niño y al Comité Jurídico Interamericano.

B. RED HEMISFÉRICA DE INTERCAMBIO DE INFORMACIÓN PARA LA ASISTENCIA JUDICIAL MUTUA EN MATERIA PENAL

Considerando la utilidad e importancia de la *Red Hemisférica de Intercambio de Información para la Asistencia Judicial Mutua en Materia Penal,* la REMJA-V formula las siguientes recomendaciones:

1. Decide adoptar la Red Hemisférica de Intercambio de Información para la Asistencia Judicial Mutua en Materia Penal e insta a todos los Estados Miembros a implementar su componente público y darle difusión entre los usuarios más interesados.

2. Establece, que como la red, bajo la orientación de un grupo formado por Argentina, Bahamas, Canadá y El Salvador y administrado por la Secretaría General de la OEA, comprende datos referentes a todos los Estados Miembros de la OEA, en el sitio público en "Internet" debe seguir publicándose información referente a asistencia judicial mutua en materia penal.

3. Que los Estados que hasta ahora no lo hayan hecho, identifiquen a una persona de contacto para que proporcione y actualice la información que se proporciona a través de la red.

4. Expresar satisfacción con respecto a la elaboración del proyecto piloto de AJM de correo electrónico seguro, y recomienda que todos los Estados adopten las medidas apropiadas para evaluarlo y que el mismo siga funcionando y se amplíe de modo de abarcar a otros Estados.

5. Examinar la posibilidad de intercambiar información, en las áreas y metodologías de mutuo interés, con la "Fiscalía Virtual de Iberoamérica".

III. POLÍTICAS PENITENCIARIAS Y CARCELARIAS

Dada la importancia y conveniencia de continuar y consolidar el proceso de intercambio de información y de experiencias y de cooperación mutua en relación con las políticas penitenciarias y carcelarias de los Estados Miembros de la OEA, la REMJA-V recomienda:

1. Expresar su satisfacción por los resultados y adoptar el informe de la Primera Reunión de Autoridades Responsables de las Políticas Penitenciarias y Carcelarias de los Estados Miembros de la OEA (documento OEA/Ser.K/XXXIV.5 REMJA-V/doc.6/04), celebrada en la sede de la OEA, durante los días 16 y 17 de Octubre de 2003, en cumplimiento de lo acordado en la REMJA-IV.

2. Respaldar la realización de reuniones periódicas de las autoridades responsables de las políticas penitenciarias y carcelarias de los Estados Miembros de la OEA y la creación de un sistema de información a través de "Internet" en relación con dichas políticas, de acuerdo con las recomendaciones formuladas en la primera reunión de tales autoridades.

3. Que los Estados, a través de su participación en las reuniones de autoridades penitenciarias y carcelarias, promuevan estrategias y políticas penitenciarias, basadas en el respeto a los derechos humanos, que contribuyan al deshacinamiento carcelario. Con este fin, los Estados incentivarán la modernización de la infraestructura carcelaria y la profundización de las funciones de rehabilitación y reinserción social del individuo, a través del mejoramiento de las condiciones de privación de la libertad y el estudio de nuevos estándares penitenciarios.

IV. DELITO CIBERNÉTICO

En relación con esta materia, la REMJA-V recomienda:

1. Expresar su satisfacción por los resultados de la Reunión Inicial del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético, celebrada en la sede de la OEA, durante los días 23 y 24 de junio de 2003, en cumplimiento de lo acordado en la REMJA-IV.

2. Adoptar las recomendaciones formuladas por el Grupo de Expertos Gubernamentales (documento OEA/Ser.K/XXXIV.5 REMJA-V/doc.5/04) y solicitarle que, a través de su Presidencia, informe a la próxima REMJA sobre los avances dados en relación con las mismas.

3. Respaldar que las recomendaciones formuladas por el Grupo de Expertos Gubernamentales en su reunión inicial sirvan como la contribución de las REMJA para el desarrollo de la Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética a que se refiere la resolución de la Asamblea General de la OEA AG/RES. 1939 /XXXIII-O/03), así como solicitar al Grupo que, a través de su Presidencia, continúe apoyando el proceso de elaboración de dicha Estrategia.

4. Que se dispense capacitación internacional en relación con el delito cibernético a los Estados de la OEA que la soliciten, y que los Estados de la OEA en general consideren la posibilidad de asignar recursos que garanticen el suministro de esa capacitación.

5. Que los Estados Miembros participen en las reuniones técnicas del Grupo de Expertos Gubernamentales sobre Delito Cibernético, a fin de que a nivel hemisférico se logre una clara comprensión sobre los futuros desafíos.

6. Que los Estados Miembros, en el contexto del Grupo de Expertos, examinen mecanismos que faciliten una amplia y eficiente cooperación mutua para combatir el Delito Cibernético y estudien, según sea posible, el desarrollo de la capacidad técnica y jurídica para unirse a la red 24/7 establecida por el G-8 para ayudar a realizar las investigaciones sobre delitos cibernéticos.

7. Que en la medida de lo posible, los Estados Miembros dispongan lo necesario para que las diferencias en la descripción de los delitos no vayan en detrimento de la eficiencia de la cooperación a través de la asistencia jurídica y judicial mutua y la extradición.

8. Que los Estados Miembros evalúen la conveniencia de la aplicación de los principios de la Convención del Consejo de Europa sobre la Delincuencia Cibernética (2001) y que consideren la posibilidad de adherirse a dicha Convención.

9. Que los Estados Miembros examinen y, si corresponde, actualicen, la estructura y la labor de entidades u organismos internos encargados de hacer cumplir las leyes, de modo de adaptarse a las cambiantes características de los delitos cibernéticos, incluso examinando la relación entre los organismos que combaten ese tipo de delitos y los que proporcionan la asistencia policial o judicial mutua tradicional.

V. CORRUPCIÓN: SEGUIMIENTO DE LOS COMPROMISOS DE LA DECLARACIÓN DE NUEVO LEÓN

En las Declaraciones de Nuevo León y de la ciudad de Quebec, así como en anteriores REMJA, se reconoce la seriedad del problema de la corrupción en nuestras sociedades.

Tomamos nota con aprobación del hecho de que a partir de la REMJA-IV, la mayor parte de los Estados Miembros suscribieron la Convención de las Naciones Unidas contra la Corrupción y algunos Estados Miembros adicionales se convirtieron en Partes de la Convención Interamericana contra la Corrupción, pero hoy procuramos reforzar nuestros esfuerzos para promover eficazmente la lucha contra la corrupción.

En consecuencia, la REMJA-V recomienda que los Estados Miembros:

1. Que aún no lo hayan hecho, adopten a la brevedad posible las medidas necesarias para alcanzar los siguientes objetivos:

   a. Firmar y ratificar, ratificar, o adherir, según sea el caso, e implementar la Convención de las Naciones Unidas contra la Corrupción de 2003.

   b. Firmar y ratificar, ratificar, o adherir, según sea el caso, e implementar la Convención Interamericana contra la Corrupción de 1996.

2. Cooperen para reforzar el Mecanismo de Seguimiento de la Implementación de la Convención Interamericana contra la Corrupción, a través de medidas prácticas que lo hagan más eficaz, incluyendo lo relativo a la necesidad de incrementar los recursos económicos y perfeccionar los recursos humanos y la aceleración del proceso de evaluación en la Primera Ronda.

3. Antes de la realización de la REMJA-VI, cada Estado Miembro, con apego a su legislación nacional y a las normas internacionales aplicables, adoptará medidas legales internas que nieguen acogida a funcionarios corruptos, a quienes los corrompen y a sus bienes e intercambiarán información sobre las medidas que hayan adoptado.

4. Con apego a sus legislaciones nacionales y a las normas internacionales aplicables, revisen sus regímenes legales de extradición y suministro de asistencia judicial mutua en relación con delitos de corrupción, incluida su capacidad de disponer el decomiso o la confiscación de activos derivados de actividades criminales a pedido de otros países que tengan diferentes modalidades de realización del decomiso o confiscación, a fin de reforzarlos.

5. Adopten, conforme a los principios fundamentales de su legislación interna, las medidas legislativas y de otro género que sean necesarias para que sus autoridades competentes puedan devolver los bienes decomisados o confiscados al Estado requirente, en caso de apropiación fraudulenta de fondos públicos o lavado de fondos públicos que hayan sido objeto de apropiación fraudulenta.

6. Apoyen los trabajos de la reunión de los Estados Parte de la Convención Interamericana contra la Corrupción que tendrá lugar en Managua, Nicaragua, en julio de 2004, la cual deberá considerar “medidas concretas adicionales para aumentar la transparencia y combatir la corrupción”.

VI. TRATA DE PERSONAS, ESPECIALMENTE MUJERES Y NIÑOS

Teniendo en cuenta que la trata de personas es un grave delito, que debe ser tipificado, prevenido y combatido, que sus víctimas se encuentran en una condición de vulnerabilidad lo cual exige una mayor atención internacional y la debida asistencia y protección, amparando sus derechos humanos y que para lograr estos fines se requiere de la cooperación integral por parte de todos los Estados.

Reconociendo que existe un importante conjunto de instrumentos internacionales para garantizar la protección de las mujeres, niños, niñas y adolescentes, como son la Convención sobre los Derechos Humanos del Niño, la Convención sobre todas las formas de Discriminación contra la Mujer, la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer, la Convención No. 182 de la OIT sobre las peores formas de trabajo infantil, el Protocolo Opcional de la Convención sobre los Derechos del Niño en relación con la venta de niños, la prostitución y la pornografía infantiles, la Convención Interamericana sobre el Tráfico Internacional de Menores y el Protocolo para Prevenir, Reprimir y Sancionar la Trata de Personas, Especialmente Mujeres y Niños.

Teniendo presente que el Protocolo para Prevenir, Reprimir y Sancionar la Trata de Personas, Especialmente Mujeres y Niños, complementario de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, especifica las acciones que configuran el delito de trata de personas.

Decididos a superar los obstáculos en la lucha contra este delito transnacional.

La REMJA-V recomienda:

1. Que los Estados Miembros que aún no lo hayan hecho firmen y ratifiquen, ratifiquen, o adhieran, según sea el caso, e implementen, a la brevedad posible, el Protocolo para Prevenir, Reprimir y Sancionar la Trata de Personas, Especialmente Mujeres y Niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Trasnacional.

2. Instar a los Estados Miembros a completar sus procesos internos para determinar si han de suscribir y ratificar:

   a. El Protocolo contra el Tráfico Ilícito de Migrantes por Tierra, Mar y Aire, y
   b. La Convención Interamericana sobre el Tráfico Internacional de Menores.

3. La realización de una Reunión de autoridades nacionales en esta materia, incluyendo la participación, entre otros, de la CIM, el IIN, las Naciones Unidas, la OIM y otros organismos internacionales relacionados, con el propósito de estudiar mecanismos de cooperación integral entre los Estados para asegurar la protección y asistencia a las víctimas, la prevención del delito y la persecución a sus autores. Asimismo, la reunión facilitará el intercambio de información y experiencias, el diálogo político y la cooperación entre los países de origen, tránsito y destino de la trata de personas, así como el establecimiento o mejoramiento de registros estadísticos en la materia.

4. Mantener el tema de la Trata de Personas como punto del temario en futuros debates de la REMJA.

VII. VIOLENCIA CONTRA LA MUJER

La REMJA-V:

1. Insta a los Estados Miembros a completar sus procesos internos para determinar si han de suscribir y ratificar la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belem do Pará).

2. Alienta a los Estados Parte de la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belem do Pará) a analizar el modo más apropiado de crear un mecanismo de seguimiento de la Convención.

VIII. GÉNERO Y JUSTICIA

La REMJA-V, habiendo escuchado la presentación de la CIM (Comisión Interamericana de Mujeres), toma nota de las recomendaciones sobre genero y justicia formuladas a la REMJA-V por la Segunda Reunión de Ministras o Ministros o Autoridades al más alto nivel Responsables de las Políticas de las Mujeres en los Estados Miembros y las refiere a los Estados Miembros para mayor consideración.

IX. CENTRO DE ESTUDIOS DE JUSTICIA DE LAS AMÉRICAS (CEJA)

En cumplimiento de los mandatos de la Segunda y Tercera Cumbres de las Américas, de las resolución de la Asamblea General de la OEA AG/RES. 1 (XXVI-E/99) y de las conclusiones y recomendaciones de las REMJA II y III, que impulsaron la creación de un Centro de Estudios que contribuya al mejoramiento de las políticas de Justicia y al desarrollo institucional de los sistemas judiciales en la región.

Y habiendo oído el informe del Centro de Estudios de Justicia de las Américas, la REMJA-V decide:

1. Expresar su agradecimiento al Consejo Directivo y al Director Ejecutivo por la orientación e iniciativa que han puesto de manifiesto al guiar y elaborar los pasos iniciales del trabajo del Centro en la esfera de la justicia penal, y dar forma concreta a la visión de un centro regional de expertos en el sector de la justicia establecido por los Jefes de Estado y de Gobierno en Santiago de Chile.

2. Felicitar al Centro por la exitosa puesta en marcha de sitios y publicaciones en Internet que están siendo ampliamente consultados en la región, y por la elaboración de un importante estudio comparado de normas y prácticas de procedimiento penal en la región que contribuirán a mejorar el desempeño del sistema de justicia.

3. Expresar satisfacción por los esfuerzos realizados para hacer efectiva la participación de los Estados Miembros en programas y actividades del Centro, pese a la diversidad de intereses e instituciones que intervienen y la escasez de financiamiento.

4. Solicitar al Centro que, de conformidad con los objetivos establecidos en su Estatuto, incluya en sus planes de trabajo las conclusiones y recomendaciones de la REMJA. Para este fin, los Estados Miembros proveerán los recursos que sean necesarios.

5. Solicitar al Centro que organice un grupo o proceso de trabajo, incluyendo los Estados Miembros y otros donantes, a fin de elaborar, para que sea considerado por la REMJA-VI, un plan de financiamiento del Centro de acuerdo con el mandato de la Tercera Cumbre de las

Américas. Este proceso debe ser desarrollado sin perjuicio de las contribuciones voluntarias que con este objeto los Estados Miembros deban entregar, de acuerdo a lo establecido en el Estatuto del Centro, aprobado por la Asamblea General de la Organización de los Estados Americanos.

6. Aprobar la renovación del mandato del Director Ejecutivo del Centro acordada por su Consejo Directivo, de acuerdo con su Estatuto, en sesión ordinaria celebrada el 5 de enero de 2004, en Santiago de Chile.

7. Solicitar al Centro que siga apoyando los esfuerzos que se realizan para fortalecer los sistemas de Justicia internos con miras al mejoramiento de los marcos nacionales en el ámbito de la cooperación y asistencia judicial mutua en el Hemisferio.

X. PRÓXIMA REUNIÓN

La REMJA-V recomienda que la Sexta Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA-VI) se realice en el año 2006 y que la Asamblea General de la OEA encargue al Consejo Permanente de la Organización de fijar la fecha y sede de la misma.

ANEXO V

CUARTO PERÍODO ORDINARIO DE SESIONES
28-30 de enero de 2004
Montevideo, Uruguay

OEA/Ser.L/X.2.4
CICTE/INF.4/04
29 enero 2004
Original: inglés

MARCO PARA ESTABLECER UNA RED INTERAMERICANA CSIRT DE VIGILANCIA Y ALERTA

(Presentado por la Embajadora Margarita Escobar, Presidenta del Grupo de Trabajo de la Comisión de Seguridad Hemisférica de la OEA, en la tercera sesión plenaria celebrada el día 29 de enero de 2004)

MARCO PARA ESTABLECER UNA RED INTERAMERICANA CSIRT DE VIGILANCIA Y ALERTA

(Presentado por la Embajadora Margarita Escobar, Presidenta del Grupo de Trabajo de la Comisión de Seguridad Hemisférica de la OEA, en la tercera sesión plenaria celebrada el día 29 de enero de 2004)

Objetivo: Crear una red hemisférica, que funcione 24 horas al día, 7 días a la semana, de puntos nacionales de contacto entre equipos de respuesta a incidentes de seguridad en computadoras (*Computer Security Incident Response Teams*: CSIRT) con responsabilidad nacional (CSIRT nacionales), en los Estados Miembros de la OEA, con la capacidad y a cargo de responder debida y rápidamente a las crisis, incidentes y peligros relacionados con la seguridad cibernética.

Dado que los intrusos emplean instrumentos de ataque cada vez más sofisticados, lanzan ataques muy automatizados que se desplazan a la velocidad de la Internet, y emplean intencionalmente técnicas de ataque que hacen difícil entender la naturaleza y origen de tales ataques, la colaboración mundial en tiempo real entre los equipos de respuesta tiene una importancia creciente. Dicha colaboración permitiría lo siguiente:

- un diagnóstico rápido y preciso del problema;
- la pronta diseminación mundial de advertencias sobre ataques;
- la pronta diseminación mundial de advertencias sobre vulnerabilidades genéricas;
- un alerta mundial sobre actividades sospechosas, y la colaboración para investigar y diagnosticar tales actividades;
- el suministro de información sobre medidas para mitigar y remediar los ataques y amenazas; y
- una reducción de duplicaciones de análisis entre los equipos.

La colaboración refuerza los conocimientos técnicos existentes entre los equipos para limitar los perjuicios y permitir que continúen funcionando los servicios de importancia crítica.

Principios:

Locales – El programa debe ser manejado y controlado por entidades locales de cada país participante, designadas por su Gobierno.

Sistémicos – El sistema debe ser una operación multifacética que requiere un personal consciente y especializado, una distribución regular de la información relativa a las amenazas y vulnerabilidades vigentes, una reevaluación e implementación constantes de las mejores prácticas, y una interacción adecuada con las autoridades públicas.

Permanentes – Debido a la evolución diaria inherente de la Internet, para que tenga buen resultado un programa deberá actualizarse y mantenerse con regularidad. La seguridad en la Internet no se logrará mediante una acción única.

Responsables – La “seguridad” en la ciberseguridad. Deben entenderse y seguirse reglas estrictas respecto de cuestiones tales como el manejo de la información, ya que de otra manera los usuarios perderían la confianza, y los esfuerzos para proteger el sistema serán perjudicados e incluso serán contraproducentes.

Basados en disposiciones ya existentes – Hay un número de entidades preexistentes en el Hemisferio 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.

Identificación de organizaciones existentes

En todo el mundo, hay más de cien organizaciones que usan el nombre CERT (*Computer Emergency Response Team*: equipo de respuesta a emergencias de computación), o CSIRT (el término genérico de significado equivalente). Muchas de ellas, pero no todas, tienen una cierta relación con el Centro de Coordinación CERT (CERT/CC) en la Universidad de Carnegie Mellon, en donde se creó el primer "CERT". Incluso los CSIRT relacionados con el CERT/CC tienen diferentes métodos de respuesta a los incidentes, dependiendo de diversos factores tales como la uniformidad, cuestiones geográficas y técnicas, la autoridad, los servicios suministrados, y los recursos. En los Estados Unidos, el Departamento de Seguridad de la Patria, División de Ciberseguridad Nacional, ha creado el US-CERT, para que sea el "Equipo de emergencias informáticas", con responsabilidad nacional en los Estados Unidos. En el Canadá, la División de Ciberprotección, dentro de la organización de Seguridad Pública y Preparación para Emergencias-Canadá (PSEPC) cumple una función similar de responsabilidad nacional.

El Foro sobre Equipos de Respuesta a Incidentes (*Forum on Incident Response Teams*: FIRST), una asociación mundial voluntaria de equipos CSIRT, cuenta con 79 miembros en los Estados Miembros de la OEA, 68 de ellos en los EE.UU. De los restantes, seis son del Canadá, dos del Brasil, con sendos miembros en Chile, México y Perú. Además, algunas compañías, tales como ATT, Symantec, y Visa, ofrecen servicios CSIRT a sus clientes de todo el mundo, y puede haber otros CSIRT en la región, tales como Ar-CERT en la Argentina, que no forman parte de la red FIRST.

Dadas las lagunas en la información, llevar a cabo un censo de los CSIRT es el primer paso para la creación de una red de seguridad cibernética.

Establecimiento de un modelo de servicio

Si bien no hay normas internacionales acordadas sobre qué es lo que constituye un CSIRT, hay una serie de documentos y actividades que pueden servir para definir un equipo CSIRT, y que están relacionados con la certificación y autorización de tales equipos.

El CERT/CC ha publicado varios documentos que pueden servir de ayuda para la creación de un CSIRT, entre los que se cuentan los siguientes:

- *Handbook for Computer Security Incident Response Teams (CSIRTs)* (Manual para equipos de respuesta a incidentes de seguridad de computadoras [CSIRT]): guía actualizada sobre cuestiones genéricas que deben considerarse al formar un CSIRT;
- *State of the Practice of Computer Security Incident Response Teams* (Estado actual de las prácticas de los equipos de respuesta a incidentes de seguridad de computadoras). Este informe contiene información recogida mediante un estudio piloto de estos equipos, la experiencia propia del CERT/CC, discusiones con otros CSIRT y observaciones de éstos, e investigación y críticas de las publicaciones actuales sobre la respuesta a incidentes; y
- *Creating a Computer Security Incident Response Team: A Process for Getting Started* (Creación de un equipo de respuesta a incidentes de seguridad de computadoras: un método para su comienzo). Éste es un documento en el que se describen los requisitos básicos para crear un CSIRT.

Además, el Departamento de Defensa de los Estados Unidos (US DoD) ha creado un programa de certificación y autorización de proveedores de servicios de defensa de redes de computadoras dentro de dicho Departamento. Ese programa puede usarse de punto de partida para establecer criterios para la certificación de equipos CSIRT nacionales.

Cuando se establece una red regional de CSIRT nacionales cooperantes, debe preverse un conjunto mínimo de normas y servicios, entre los que se contarían los siguientes:

- designación de responsabilidad por el Gobierno del CSIRT nacional;
- convenio sobre los principios para compartir información entre los equipos cooperantes;
- responsabilidad por recibir información de otros CSIRT nacionales, y por diseminar dicha información entre las entidades idóneas dentro del país;
- autorización para diseminar información entre otros CSIRT nacionales; y
- proporcionar asistencia de coordinación a otros CSIRT nacionales para incidentes y amenazas.

Cuestiones de confianza

Gran parte de la información que tienen que intercambiar los CSIRT es de propiedad exclusiva, o es de carácter delicado por otros motivos, y hay pocos modelos buenos que sirvan para compartir uniformemente datos entre tales equipos. La confianza—el ingrediente esencial cuando se comparte información—, cuando existe, se desarrolla entre individuos que se conocen y han trabajado juntos, más bien que institucionalmente entre organizaciones. Para establecer la confianza, todas las partes deben entender y seguir pautas claras sobre la forma en que la información intercambiada será usada o diseminada. Todos los CSIRT nacionales cooperantes deben convenir en los principios para compartir información que indiquen cómo tal información puede usarse o diseminarse.

Las normas de divulgación de la vulnerabilidad describen las circunstancias en las cuales se disemina información sobre tal vulnerabilidad, y entre quiénes. En tales normas debe establecerse un equilibrio entre la necesidad de diseminar información procesable entre las audiencias debidas y la necesidad de minimizar las posibilidades de que un intruso pudiera obtener tal información antes de contar con parches o soluciones improvisadas.

Entre los atributos de los CSIRT necesarios para promover la confianza en las comunicaciones y la cooperación respecto de asuntos delicados de seguridad figuran los siguientes:

- una infraestructura segura para el manejo de información delicada;
- la capacidad para comunicarse sin riesgos con los interesados;
- la capacidad para reunir expertos y autoridades;
- una infraestructura que permita la notificación anticipada a determinadas audiencias;
- procedimientos de protección contra fugas de información;
- una interfaz pública bien conocida para la diseminación de información crítica; y
- la capacidad para llegar rápidamente a una gran audiencia.

La creación de una capacidad CSIRT regional requiere la formación de un consenso sobre los principios para el intercambio de información, incluso qué información puede compartirse, con quién, y cuándo.

Financiamiento

No es barato financiar los CSIRT. Además de suministrar equipos y personal especializado permanentemente, los administradores de dichos equipos tienen que proporcionar asistencia técnica periódica y organizar ejercicios regulares para mantener sus operaciones a punto. Los Estados Miembros y la Organización deberán considerar cuidadosamente los mecanismos de financiación de los CSIRT y probablemente tengan que establecer un orden de prioridades de su cobertura, o buscar fuentes estables de financiación externa.

Cabe señalar que en octubre de 2002 los líderes de la APEC pidieron la creación de una capacidad regional CSIRT 24/7 para octubre de 2003. Tanto la APEC como el Gobierno de Australia convinieron en financiar proyectos de creación de capacidad CSIRT en las economías de cuatro miembros. En su informe más reciente sobre el proyecto, funcionarios de la APEC admitieron que hay dificultades para atraer candidatos aceptables y para obtener fondos adecuados para cubrir el costo del proyecto.

Conciencia pública

El apoyo del Gobierno y la industria para los programas (y financiación) de los CSIRT está directamente relacionado con la conciencia que tiene el público del problema de la ciberseguridad y sus posibles repercusiones en objetivos sumamente deseables en materia de desarrollo. Si los sistemas de una economía interconectada no se protegen debidamente, las redes e infraestructuras de todas las economías interconectadas son vulnerables. Los participantes en una red, ya sea como creadores, propietarios, explotadores o usuarios individuales, deben tener conciencia de las amenazas a la red y de sus vulnerabilidades, y asumir la responsabilidad de su protección según la posición que ocupen y la función que cumplan. La Organización, trabajando con los Estados Miembros y los CSIRT, debe llevar a cabo un programa de concientización del público acerca de la seguridad y la ética cibernéticas en el que se destaquen (1) las ventajas y responsabilidades del uso de redes de información; (2) las mejores prácticas de seguridad y protección; y (3) las posibles consecuencias negativas del uso indebido de las redes. Existen varias organizaciones y sitios en línea con datos útiles para dicho fin, y la Organización debe hacer uso de ellos.

Extensión de la red

Si bien la conciencia del público es un elemento esencial de esta propuesta, establecer una capacidad regional de CSIRT requerirá compromisos políticos en donde éstos puedan no existir. El grupo de trabajo deberá proponer un proyecto de resolución sobre la seguridad cibernética para su aprobación por la Comisión de Seguridad Hemisférica y transmitirlo a la Asamblea General con el mismo fin, que comprometa a los Estados Miembros a establecer equipos CSIRT en sus países, y a implementar las recomendaciones que pudiera presentar el grupo y aprobar la Comisión. Así se aplicará la voluntad política de los Estados Miembros al logro de una cobertura regional de los CSIRT, y se proporcionará a la Organización el marco institucional necesario para proceder. Con esta resolución, el grupo de trabajo puede asistir a los Estados a formular planes concretos y, suponiendo una financiación adecuada, a organizar proyectos para crear capacidad en sus respectivos países. Hasta el momento, ningún Estado ha ofrecido financiar este proyecto.

Plan de acción

Acción 1: Llevar a cabo un censo para identificar los CSIRT existentes, su variedad de miembros y los servicios que proporcionan. Esto nos permitirá identificar las lagunas en la cobertura, tanto geográfica como sectorialmente, y establecerá las bases para fijar un conjunto consensual de servicios que ofrecerán los CSIRT miembros. Se adjunta un posible cuestionario de censo.

Acción 2: Establecer un consenso para un conjunto mínimo de servicios que ofrecerán todos los CSIRT miembros. Eso ayudará a formar una doctrina de operación hemisférica uniforme, y servirá de base para las actividades subsiguientes de asistencia técnica.

Acción 3: Redactar una resolución para presentarla a la Comisión de Seguridad Hemisférica y la Asamblea General, pidiendo a los Estados Miembros que creen equipos CSIRT y que implementen las otras propuestas que figuren en el informe del grupo de trabajo. De los 11 CSIRT no estadounidenses que son miembros de la red FIRST, seis son estatales, cuatro son privados, y uno es dirigido por una universidad.

Acción 4: Producir un compendio de mejores prácticas basado en los servicios y normas CSIRT consensuales, acordes con las prácticas similares en Europa y Asia. Incluiría normas y protocolos para llevar a cabo monitoreo en tiempo real y un subsiguiente intercambio de información en toda la red, y servirán de base para protocolos consiguientes de pruebas y asistencia técnica.

Acción 5: Establecer un sistema de asistencia técnica e intercambio de información permanente para los CSIRT. Algunos países necesitarán asistencia para crear capacidad, o asistencia técnica para crear una capacidad de coordinación de la protección informática, o mejorar las capacidades existentes a fin de cumplir con las normas requeridas. Será necesario obtener financiamiento.

Al finalizarse la acción 1, realizar una reunión interamericana de representantes de los CSIRT existentes, a fin de adelantar las acciones y las cuestiones de compartimiento de información, la identificación de lagunas en la cobertura y asistencia técnica, la capacidad de interfuncionamiento, y la intercomunicación. Podrían asistir representantes del Grupo de Trabajo de Seguridad Cibernética de la OEA a fin de proporcionar información normativa cuando ello sea necesario, y asegurarse de que se aborden las cuestiones descritas en el presente documento. Esa reunión también sería un paso importante para enfrentar la cuestión de la confianza y, como sería a nivel técnico, no dependería de las acciones de la Asamblea General.