

ANEXO VIII

RECOMENDACIONES DE LA TERCERA REUNIÓN 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.
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 sustantiva, 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.