Asamblea General

Distr. general
31 de enero de 2003

Quincuagésimo séptimo período de sesiones
Tema 84 *c*) del programa

Resolución aprobada por la Asamblea General

[*sobre la base del informe de la Segunda Comisión (A/57/529/Add.3)*]

57/239. Creación de una cultura mundial de seguridad cibernética

La Asamblea General,

Observando que los gobiernos, las empresas, otras organizaciones y los usuarios individuales dependen cada vez más de las tecnologías de la información para el suministro de bienes y servicios esenciales, la gestión de sus asuntos y el intercambio de información,

Reconociendo que la necesidad de seguridad cibernética aumenta a medida que los países incrementan su participación en la sociedad de la información,

Recordando sus resoluciones 55/63, de 4 de diciembre de 2000, y 56/121, de 19 de diciembre de 2001, sobre el establecimiento de la base jurídica para luchar contra la utilización de las tecnologías de la información con fines delictivos,

Recordando también sus resoluciones 53/70, de 4 de diciembre de 1998, 54/49, de 1° de diciembre de 1999, 55/28, de 20 de noviembre de 2000, 56/19, de 29 de noviembre de 2001, y 57/53, de 22 de noviembre de 2002, sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional,

Consciente de que la seguridad cibernética no es sólo cuestión de prácticas de gobierno o de orden público, sino que debe alcanzarse por medio de la prevención y con el apoyo de toda la sociedad,

Consciente también de que la tecnología por sí sola no puede garantizar la seguridad cibernética y que debe darse prioridad a la planificación y gestión de la seguridad cibernética en toda la sociedad,

Reconociendo que, cada uno en su papel, los gobiernos, las empresas, otras organizaciones, y los propietarios y usuarios individuales de las tecnologías de la información deben tener conciencia de los riesgos que existen para la seguridad cibernética y de las medidas preventivas, deben asumir sus responsabilidades y tomar medidas para mejorar la seguridad de esas tecnologías de la información,

Reconociendo también que las disparidades entre los países en el acceso a las tecnologías de la información y en su utilización pueden reducir la eficacia de la cooperación internacional en la lucha contra la utilización de las tecnologías de la información con fines delictivos y en la creación de una cultura mundial de la

seguridad cibernética, y teniendo en cuenta la necesidad de facilitar la transferencia de las tecnologías de la información, en particular a los países en desarrollo,

Reconociendo además la importancia de la cooperación internacional para lograr la seguridad cibernética apoyando las iniciativas nacionales encaminadas a desarrollar la capacidad humana, aumentar las oportunidades de aprendizaje y empleo y mejorar los servicios públicos y la calidad de vida aprovechando las posibilidades que brindan las tecnologías y las redes de información y comunicaciones avanzadas, fiables y seguras y promoviendo el acceso universal a ellas,

Observando que, como resultado de la creciente interconectividad, los sistemas y redes de información están hoy expuestos a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades que plantean nuevos problemas de seguridad para todos los usuarios de computadoras,

Tomando conocimiento de la labor de las organizaciones internacionales y regionales pertinentes en relación con el mejoramiento de la seguridad cibernética y la seguridad de las tecnologías de la información,

1. *Toma nota* de los elementos que figuran en el anexo de la presente resolución, con miras a crear una cultura mundial de seguridad cibernética;

2. *Invita* a todas las organizaciones internacionales pertinentes a que en toda labor futura en materia de seguridad cibernética tengan presentes, entre otras cosas, esos elementos para la creación de una cultura mundial de seguridad cibernética;

3. *Invita* a los Estados Miembros a que tengan en cuenta esos elementos, entre otras cosas, en sus actividades para promover en todas sus sociedades una cultura de seguridad cibernética en la aplicación y utilización de las tecnologías de la información;

4. *Invita* a los Estados Miembros y a todas las organizaciones internacionales pertinentes a que en los preparativos de la Cumbre Mundial sobre la Sociedad de la Información, que se celebrará en Ginebra del 10 al 12 de diciembre de 2003 y en Túnez en 2005, tengan en cuenta, entre otras cosas, esos elementos y la necesidad de una cultura mundial de seguridad cibernética;

5. *Subraya* la necesidad de facilitar la transferencia de las tecnologías de la información y el fomento de la capacidad para ayudar a los países en desarrollo a adoptar medidas en materia de seguridad cibernética.

78ª sesión plenaria
20 de diciembre de 2002

Anexo

Elementos para la creación de una cultura mundial de seguridad cibernética

Los rápidos progresos de las tecnologías de la información han cambiado el modo en que los gobiernos, las empresas, otras organizaciones y los usuarios individuales que desarrollan, poseen, proporcionan, gestionan, mantienen y utilizan esos sistemas y redes de información (“participantes”) deben abordar la cuestión de la seguridad cibernética. Una cultura mundial de seguridad cibernética requerirá que

todos los participantes tomen en consideración los nueve elementos complementarios siguientes:

a) *Conciencia*. Los participantes deben tener conciencia de la necesidad de la seguridad de los sistemas y redes de información y de lo que pueden hacer por mejorar esa seguridad;

b) *Responsabilidad*. Los participantes son responsables de la seguridad de los sistemas y redes de información en cuanto corresponde a sus funciones individuales. Deben examinar periódicamente sus propias políticas, prácticas, medidas y procedimientos y evaluar si son las que convienen en su contexto;

c) *Respuesta*. Los participantes deben actuar de manera oportuna y cooperativa para prevenir y detectar los incidentes de seguridad y reaccionar ante ellos. Deben compartir la información sobre las amenazas y las vulnerabilidades, según convenga, y aplicar procedimientos para establecer una cooperación rápida y eficaz a fin de prevenir y detectar los incidentes de seguridad y reaccionar ante ellos. Para ello puede ser necesario compartir información y cooperar a través de las fronteras;

d) *Ética*. Dada la omnipresencia de los sistemas y redes de información en las sociedades modernas, los participantes deben respetar los legítimos intereses de los demás y reconocer que lo que hagan o dejen de hacer puede perjudicar a otros;

e) *Democracia*. Las medidas de seguridad deben aplicarse de manera compatible con los valores reconocidos de las sociedades democráticas, incluidos la libertad de intercambiar pensamientos e ideas, el libre flujo de la información, la confidencialidad de la información y las comunicaciones, la debida protección de la información personal, la franqueza y la transparencia;

f) *Evaluación de riesgos*. Todos los participantes deben realizar evaluaciones periódicas de los riesgos a fin de determinar las amenazas y vulnerabilidades; esas evaluaciones deben tener una base suficientemente amplia para abarcar los principales factores internos y externos, tales como la tecnología, los factores físicos y humanos, las políticas y los servicios de terceros que tengan consecuencias para la seguridad; permitir la determinación del nivel de riesgo aceptable; y ayudar a la selección de controles apropiados para gestionar el riesgo de posibles daños a los sistemas y redes de información, teniendo en cuenta la naturaleza y la importancia de la información que se debe proteger;

g) *Diseño y puesta en práctica de la seguridad*. Los participantes deben incorporar la seguridad como elemento esencial de la planificación y el diseño, el funcionamiento y el uso de los sistemas y redes de información;

h) *Gestión de la seguridad*. Los participantes deben adoptar un enfoque amplio de la gestión de la seguridad basado en una evaluación de los riesgos que sea dinámica e incluya todos los niveles de las actividades de los participantes y todos los aspectos de sus operaciones;

i) *Reevaluación*. Los participantes deben examinar y reevaluar la seguridad de los sistemas y redes de información e introducir las modificaciones apropiadas en las políticas, prácticas, medidas y procedimientos de seguridad que permitan hacer frente a las amenazas y vulnerabilidades a medida que se presentan o se transforman.