Naciones Unidas A/C.2/57/L.10/Rev.1

Asamblea General

Distr. limitada
10 de diciembre de 2002
Español
Original: inglés

Quincuagésimo séptimo período de sesiones
Segunda Comisión
Tema 84 c) del programa
Cuestiones de política macroeconómica: ciencia y tecnología para el desarrollo

Alemania, Argentina, Australia, Bulgaria, Canadá, Chile, Croacia, Dinamarca, Eslovaquia, Estados Unidos de América, Etiopía, Federación de Rusia, India, Italia, Japón, Noruega, Nueva Zelandia, Pakistán, Polonia, Reino Unido de Gran Bretaña e Irlanda del Norte, República Checa, República de Corea, Rumania, Sudáfrica, Suecia, Suiza, Túnez, Turquía: proyecto de resolución revisado

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 la tecnología de la información con fines delictivos,

Recordando también sus resoluciones 53/70, 54/49, 55/28, 56/19 y 57/53 sobre los avances en 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 además de que por sí sola la tecnología no puede garantizar la seguridad cibernética y que debe darse prioridad a la planificación y gestión de la seguridad cibernética en toda la sociedad,

02-73142 (S) 101202 101202

Reconociendo que, cada uno en su papel, los gobiernos, las empresas, las 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, asumir sus responsabilidades y tomar medidas para mejorar la seguridad de esas tecnologías de la información,

Reconociendo que las lagunas en el acceso y la utilización por los Estados de las tecnologías de la información 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 reconociendo también la necesidad de facilitar la transferencia de tecnologías de la información, en particular a los países en desarrollo,

Reconociendo 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 las mismas,

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 todas sus labores futuras en materia de seguridad cibernética tengan presentes, entre otras cosas, los elementos que figuran en el anexo referentes a la creación de una cultura mundial de seguridad cibernética;

3. *Invita* a los Estados Miembros a tener 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 en diciembre de 2003 y en Túnez en 2005, tengan en cuenta, entre otras cosas, estos elementos y la necesidad de una cultura mundial de seguridad cibernética;

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

Anexo
Elementos para la creación de una cultura mundial de seguridad cibernética

Los rápidos progresos de la tecnología 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 principios 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. También 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 esos incidentes. 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, incluida 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 apertura 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 con 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 revisar 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 nuevas y cambiantes.