Naciones Unidas A/C.2/64/L.8

Asamblea General

Distr. limitada
22 de octubre de 2009
Español
Original: inglés

Sexagésimo cuarto período de sesiones
Segunda Comisión
Tema 55 c) del programa
Globalización e interdependencia: ciencia y tecnología para el desarrollo

Australia, Canadá, Estados Unidos de América, Islas Marshall, Israel y Japón: proyecto de resolución

Creación de una cultura mundial de seguridad cibernética y examen de las medidas nacionales para proteger las infraestructuras de información esenciales

La Asamblea General,

Recordando sus resoluciones 55/63, de 4 de diciembre de 2000, y 56/121, de 19 de diciembre de 2001, relativas a la lucha contra la utilización de la tecnología de la información con fines delictivos, 57/239, de 20 de diciembre de 2002, relativa a la creación de una cultura mundial de seguridad cibernética, y 58/199, de 23 de diciembre de 2003, relativa a la creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales,

Recordando también sus resoluciones 53/70, de 4 de diciembre de 1998, 54/49, de 1º de diciembre de 1999, 55/28, de 20 de noviembre de 2000, 56/19, de 29 de noviembre de 2001, 57/53, de 22 de noviembre de 2002, 58/32, de 8 de diciembre de 2003, 59/61, de 3 de diciembre de 2004, 60/45, de 8 de diciembre de 2005, 61/54, de 6 de diciembre de 2006, 62/17, de 5 de diciembre de 2007, y 63/37, de 2 de diciembre de 2008, relativas a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional,

Recordando además los documentos finales de la Cumbre Mundial sobre la Sociedad de la Información, celebrada en Ginebra del 10 al 12 de diciembre de 2003 (primera fase) y en Túnez del 16 al 18 de noviembre de 2005 (segunda fase)[1], en que los Estados reconocieron que la libertad de expresión y la libre circulación de información, las ideas y los conocimientos son esenciales para la sociedad de la información de hoy y benéficos para el desarrollo, y que, dado que la confianza y la seguridad en la utilización de las tecnologías de la información y las comunicaciones son unos de los pilares más importantes de la sociedad de la

[1] Véanse A/C.2/59/3 y A/60/687.

información, es necesario fomentar, desarrollar y poner en práctica una firme cultura global de seguridad cibernética,

Reconociendo que la contribución de las tecnologías de la información en red es cada vez más indispensable para la mayoría de las funciones esenciales de la vida cotidiana, el comercio y la prestación de bienes y servicios, la investigación, la innovación y el espíritu empresarial, y para la libre circulación de información entre individuos, organizaciones y gobiernos,

Observando que los gobiernos, las empresas, la sociedad civil y las personas dependen cada vez más de una red mundial de infraestructuras de información, y que esa dependencia aumentará,

Observando también que las lagunas en el acceso a las tecnologías de la información y su uso por los Estados pueden disminuir su prosperidad social y económica, y observando en especial las necesidades de los países menos adelantados en los ámbitos de las mejores prácticas y la capacitación en materia de seguridad cibernética,

Expresando preocupación por que las amenazas para el funcionamiento fiable de las infraestructuras de información esenciales y la integridad de la información transportada por esas redes están aumentando en complejidad y gravedad y afectando el bienestar interno, nacional e internacional,

Afirmando que la seguridad de las infraestructuras de información esenciales es una responsabilidad que los gobiernos deben abordar de manera sistemática y es una esfera en la que deben asumir un papel rector a nivel nacional, en coordinación con los interesados competentes, quienes a su vez deben ser conscientes de los riesgos correspondientes, las medidas de prevención y las respuestas efectivas de manera acorde con sus respectivas funciones,

Reconociendo que las medidas nacionales deben ir apoyadas por el intercambio de información y la colaboración a nivel nacional, regional e internacional a fin de afrontar efectivamente la naturaleza cada vez más transnacional de esas amenazas,

Observando la labor de las organizaciones regionales e internacionales competentes para mejorar la seguridad cibernética, especialmente las que han alentado los esfuerzos nacionales y fomentado la cooperación internacional,

Observando también el informe de la Unión Internacional de Telecomunicaciones publicado en 2009, titulado “Seguridad de la información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad”, centrado en un enfoque nacional amplio para la seguridad cibernética compatible con la libertad de expresión, la libre circulación de información y las debidas garantías procesales,

Reconociendo que es beneficioso evaluar periódicamente los progresos en las medidas nacionales para proteger las infraestructuras de información esenciales,

1. *Invita* a los Estados Miembros a que presenten voluntariamente resúmenes de sus principales iniciativas en materia de seguridad cibernética y protección de las infraestructuras de información esenciales, a fin de resaltar los avances y las mejores prácticas nacionales, las experiencias adquiridas y las esferas en las que se deberían adoptar medidas adicionales;

2. *Ofrece* a los Estados Miembros, a este respecto, la encuesta de autoevaluación sobre la seguridad cibernética nacional que se adjunta como posible instrumento para ayudarlos, cuando proceda, a examinar las medidas nacionales relativas a la seguridad cibernética y la protección de infraestructuras de información esenciales;

3. *Invita* a todos los Estados Miembros que hayan elaborado estrategias relativas a la seguridad cibernética y la protección de las infraestructuras de información esenciales a que informen al Secretario General, para el sexagésimo quinto período de sesiones de la Asamblea General, acerca de las mejores prácticas y las medidas que podrían ayudar a otros Estados Miembros, a las organizaciones regionales e internacionales, al sector privado y los interesados de la sociedad civil, en sus iniciativas por crear una cultura mundial de seguridad cibernética.

Anexo

Instrumento de autoevaluación de las medidas nacionales para proteger las infraestructuras de información esenciales

Examen de las necesidades y estrategias en materia de seguridad cibernética

1. Evaluar el papel de las tecnologías de la información y las comunicaciones en la economía, la seguridad nacional, las infraestructuras esenciales (como el transporte, el suministro de agua y alimentos, la salud pública, la energía, las finanzas y los servicios de emergencia) y la sociedad civil de su país.

2. Determinar los riesgos para la economía, la seguridad nacional, las infraestructuras esenciales y la sociedad civil de su país que deban gestionarse en relación con la seguridad cibernética y la protección de las infraestructuras de información esenciales.

3. Comprender las vulnerabilidades de las redes en uso, los niveles relativos de las amenazas a que se enfrenta cada sector en la actualidad y el plan de gestión en curso, y señalar la manera en que los cambios en el entorno económico, las prioridades de seguridad nacional y las necesidades de la sociedad civil afectan a esos cálculos.

4. Determinar los objetivos de su estrategia nacional en materia de seguridad cibernética y protección de las infraestructuras de información esenciales, describir sus objetivos, el nivel de ejecución actual, las medidas existentes para medir los progresos, su relación con otros objetivos de políticas nacionales y la manera en que esa estrategia concuerda con las iniciativas regionales e internacionales.

Funciones y responsabilidades de los interesados

5. Determinar los principales interesados que participen en la seguridad cibernética y la protección de las infraestructuras de información esenciales y describir la función de cada uno de ellos en la elaboración de las políticas y operaciones pertinentes, incluidos:

- Los ministerios u organismos gubernamentales nacionales, señalando los principales puntos de contacto y las responsabilidades de cada uno;
- Otros participantes gubernamentales (locales y regionales);
- Los agentes no gubernamentales, entre ellos la industria, la sociedad civil y los estamentos académicos;
- Las personas a título individual, señalando si los usuarios normales de Internet tienen acceso a capacitación básica para evitar las amenazas en línea y si existe una campaña nacional de concienciación sobre la seguridad cibernética.

Procesos políticos y participación

6. Determinar los medios oficiales y oficiosos que existan en la actualidad para la colaboración entre el gobierno y la industria en la elaboración de políticas y operaciones en materia de seguridad cibernética y protección de las infraestructuras de información esenciales; determinar los participantes, sus funciones y objetivos, los métodos para obtener y utilizar las aportaciones y su idoneidad en el logro de los

objetivos pertinentes en materia de seguridad cibernética y protección de las infraestructuras de información esenciales.

7. Determinar los foros o estructuras que podrían ser necesarios además para integrar las perspectivas y los conocimientos gubernamentales y no gubernamentales necesarios para lograr los objetivos nacionales en materia de seguridad cibernética y protección de las infraestructuras de información esenciales.

Cooperación entre el sector público y privado

8. Recopilar todas las medidas y planes adoptados para aumentar la cooperación entre el gobierno y el sector privado, incluyendo todo arreglo para intercambiar información y gestionar los incidentes.

9. Reunir todas las iniciativas actuales y previstas para promover intereses compartidos y abordar desafíos comunes entre los participantes encargados de las infraestructuras esenciales y los agentes del sector privado que dependan de las mismas infraestructuras esenciales interconectadas.

Gestión de los incidentes y recuperación

10. Determinar el organismo gubernamental que coordine la gestión de los incidentes, incluida la capacidad para ejercer funciones de observación, alerta, respuesta y recuperación, los organismos gubernamentales colaboradores, los participantes no gubernamentales colaboradores, incluida la industria y otros asociados, y todo arreglo existente para la cooperación y el intercambio de información confiable.

11. Determinar, separadamente, la capacidad nacional de respuesta ante incidentes informáticos, incluidos los equipos de respuesta ante incidentes informáticos con responsabilidades nacionales y sus funciones y atribuciones, incluidos los instrumentos y procedimientos existentes para la protección de las redes informáticas gubernamentales, y los instrumentos y procedimientos existentes para difundir información sobre la gestión de los incidentes.

12. Determinar las redes y procesos de cooperación internacional que puedan reforzar la respuesta ante los incidentes y la planificación para imprevistos, la identificación de los asociados y los arreglos para la cooperación bilateral y multilateral, cuando proceda.

Marcos jurídicos

13. Examinar y actualizar las autoridades jurídicas (incluidas las relacionadas con los delitos cibernéticos, la privacidad, la protección de los datos, el derecho comercial, las firmas digitales y el cifrado) que puedan estar anticuadas u obsoletas como resultado de la rápida incorporación de las nuevas tecnologías de la información y las comunicaciones y de la dependencia de esas tecnologías, y utilizar en esos exámenes los convenios, arreglos y precedentes regionales e internacionales. Señalar si su Estado es parte en el Convenio de Budapest sobre la Ciberdelincuencia o tiene previsto adherirse a él o aprobar leyes conmensurables.

14. Determinar el estado actual de las autoridades y procedimientos nacionales que se ocupan de la delincuencia cibernética, incluidas las autoridades jurídicas, las dependencias nacionales encargadas de la delincuencia cibernética y el

nivel de comprensión de las cuestiones relativas a la delincuencia cibernética entre los fiscales, jueces y legisladores.

15. Evaluar la idoneidad de los códigos jurídicos y las autoridades actuales para hacer frente a los desafíos presentes y futuros de la delincuencia cibernética y del ciberespacio de forma más general.

16. Examinar si su Estado participa en las medidas internacionales para luchar contra la delincuencia cibernética, como la Red 24/7 de puntos de contacto, y establecer en qué medida hacerlo promovería la consecución de los objetivos nacionales en materia de seguridad cibernética.

17. Determinar los requisitos para que sus organismos nacionales de imposición de la ley cooperen con sus homólogos internacionales a fin de investigar los delitos cibernéticos transnacionales en los casos en que la infraestructura esté situada en su territorio nacional o los culpables residan en él pero las víctimas residan en otros lugares.

Creación de una cultura mundial de seguridad cibernética

18. Resumir las medidas y los planes adoptados para crear una cultura nacional de seguridad cibernética a que se hace referencia en las resoluciones de la Asamblea General de las Naciones Unidas 57/239 y 58/199, incluida la ejecución de un plan de seguridad cibernética para los sistemas operados por el gobierno, la ejecución de programas nacionales de concienciación y divulgación dirigidos, entre otros, a los niños y los usuarios individuales, y las necesidades nacionales de capacitación en materia de seguridad cibernética y protección de las infraestructuras de información esenciales.