Asamblea General

Distr. general
17 de marzo de 2010

Sexagésimo cuarto período de sesiones
Tema 55 *c*) del programa

Resolución aprobada por la Asamblea General el 21 de diciembre de 2009

[*sobre la base del informe de la Segunda Comisión (A/64/422/Add.3)*]

64/211. Creación de una cultura mundial de seguridad cibernética y balance 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 1° 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 con respecto a las tecnologías de la información 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],

Reconociendo 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 información, y que es necesario alentar, fomentar, desarrollar y poner en práctica resueltamente una cultura global sólida de seguridad cibernética,

Reconociendo también la contribución cada vez mayor de las tecnologías de la información en red a muchas de las funciones esenciales de la vida cotidiana, el comercio y la prestación de bienes y servicios, la investigación, la innovación y la actividad empresarial, y a la libre circulación de información entre individuos y organizaciones, gobiernos, empresas y la sociedad civil,

[1] Véanse A/C.2/59/3 y A/60/687.

Reconociendo además 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 asumir sus responsabilidades y adoptar medidas para mejorar la seguridad de esas tecnologías de la información,

Reconociendo la importancia del mandato del Foro para la Gobernanza de Internet, como un diálogo entre múltiples interesados sobre diversos asuntos, entre ellos cuestiones de política pública relativas a elementos clave de la gobernanza de Internet a fin de fomentar la sostenibilidad, la solidez, la seguridad, la estabilidad y el desarrollo de Internet, y reiterando que todos los gobiernos deben tener igual cometido y responsabilidad respecto de la gobernanza de Internet y de la estabilidad, la seguridad y la continuidad de Internet,

Reafirmando la necesidad constante de una mayor cooperación que permita a los gobiernos cumplir en igualdad de condiciones su papel y responsabilidades en cuestiones de política pública internacional relativas a Internet, pero no en los asuntos técnicos y operacionales cotidianos que no repercuten en las cuestiones de política pública internacional,

Reconociendo que cada país determinará sus propias infraestructuras de información esenciales,

Reafirmando la necesidad de aprovechar el potencial de las tecnologías de la información y las comunicaciones para promover el logro de los objetivos de desarrollo internacionalmente convenidos, entre ellos los Objetivos de Desarrollo del Milenio, reconociendo que las lagunas en el acceso a las tecnologías de la información y su uso por los Estados pueden disminuir su prosperidad económica, y reafirmando también la eficacia de la cooperación para combatir la utilización de la tecnología de la información con fines delictivos y crear una cultura mundial de seguridad cibernética,

Destacando la necesidad de que se desplieguen mayores esfuerzos para cerrar la brecha digital con el fin de lograr el acceso universal a las tecnologías de la información y las comunicaciones y proteger las infraestructuras de información esenciales facilitando la transferencia de tecnología de la información y fomentando la capacidad de los países en desarrollo, en especial los países menos adelantados, en los ámbitos de las mejores prácticas y la capacitación en materia de seguridad cibernética,

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

Afirmando que la seguridad de las infraestructuras de información esenciales es una responsabilidad que los gobiernos deben asumir de manera sistemática y una esfera en la que deben desempeñar 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 internacional a fin de afrontar de manera efectiva el carácter cada vez más transnacional de esas amenazas,

Observando la labor realizada por las organizaciones regionales e internacionales competentes para mejorar la seguridad cibernética, y reiterando su función de alentar los esfuerzos nacionales y fomentar la cooperación internacional,

Observando también el informe de la Unión Internacional de Telecomunicaciones publicado en 2009 sobre la seguridad de las redes de información y comunicación y las prácticas óptimas para el desarrollo de una cultura de ciberseguridad, que se centra en un enfoque nacional amplio de 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 utilizar, siempre y cuando lo consideren procedente, el instrumento de autoevaluación voluntaria de las medidas nacionales para proteger las infraestructuras de información esenciales que figura en el anexo a fin de contribuir a la evaluación de sus esfuerzos en este sentido y fortalecer su seguridad cibernética de manera que se resalten los ámbitos en que se necesiten medidas adicionales con el objetivo de ampliar la cultura mundial de seguridad cibernética;

2. *Alienta* a los Estados Miembros y a las organizaciones regionales e internacionales pertinentes que hayan elaborado estrategias de seguridad cibernética y de protección de las infraestructuras de información esenciales a que compartan las mejores prácticas y las medidas que puedan ayudar a otros Estados Miembros en sus esfuerzos por facilitar el logro de la seguridad cibernética proporcionando esa información al Secretario General para que la recopile y la difunda entre los Estados Miembros.

66ª sesión plenaria
21 de diciembre de 2009

Anexo

Instrumento de autoevaluación voluntaria de las medidas nacionales para proteger las infraestructuras de información esenciales[2]

Balance 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 y la seguridad nacionales, 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.

2. Determinar los riesgos para la economía y la seguridad nacionales, las infraestructuras esenciales y la sociedad civil que deban gestionarse en el ámbito de 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 riesgo a que se enfrenta cada sector en la actualidad y el plan de gestión en vigor, 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.

[2] Instrumento voluntario que los Estados Miembros pueden utilizar, en parte o íntegramente, siempre y cuando consideren procedente, como contribución a sus esfuerzos por proteger sus infraestructuras de información esenciales y fortalecer su seguridad cibernética.

4. Determinar los objetivos de la 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 política 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;
- Los particulares, señalando si el usuario medio de Internet tiene acceso a capacitación básica para evitar los riesgos 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 para el logro de los objetivos pertinentes en materia de seguridad cibernética y protección de las infraestructuras de información esenciales.

7. Determinar otros foros o estructuras que podrían necesitarse 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 el 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 enfrentar 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 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, incluidos 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 los 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 de 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. Determinar si el país ha elaborado la legislación necesaria para la investigación y el enjuiciamiento de la delincuencia cibernética, indicando los marcos existentes, por ejemplo, las resoluciones de la Asamblea General 55/63 y 56/121 relativas a la lucha contra la utilización de la tecnología de la información con fines delictivos e iniciativas regionales como el Convenio del Consejo de Europa sobre la Ciberdelincuencia.

14. Determinar la situación actual de las autoridades y procedimientos nacionales que se ocupan de la delincuencia cibernética, incluidas las competencias legales y las dependencias nacionales encargadas de las cuestiones relativas a la delincuencia cibernética, y el nivel de comprensión de esas cuestiones 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 la participación nacional en las iniciativas internacionales para luchar contra la delincuencia cibernética, como la Red permanente de puntos de contacto.

17. Determinar los requisitos para que los 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 o los autores del delito se encuentren en el territorio nacional 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 la cultura nacional de seguridad cibernética a que se hace referencia en las resoluciones de la Asamblea General 57/239 y 58/199, incluida la ejecución de un plan de seguridad cibernética para los sistemas operados por el gobierno, de programas nacionales de concienciación y divulgación dirigidos, entre otros, a los niños y los usuarios individuales, y de actividades nacionales de capacitación en materia de seguridad cibernética y protección de las infraestructuras de información esenciales.