Naciones Unidas A/67/167

Asamblea General

Distr. general
23 de julio de 2012
Español
Original: español/inglés/ruso

Sexagésimo séptimo período de sesiones
Tema 90 del programa provisional*
Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Informe del Secretario General

Índice

* A/67/150.

12-43417 (S) 090812 140812

I. Introducción

1. En el párrafo 3 de su resolución 66/24, la Asamblea General invitó a todos los Estados Miembros a que, teniendo en cuenta las evaluaciones y recomendaciones que figuran en el informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (A/65/201), siguieran comunicando al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes:

a) La evaluación general de los problemas de la seguridad de la información;

b) Las medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y contribuir a la cooperación internacional en esa esfera;

c) El contenido de los conceptos mencionados en el párrafo 2 de la resolución;

d) Las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial.

2. Atendiendo a esa petición, el 16 de febrero de 2012 se envió una nota verbal a los Estados Miembros invitándolos a proporcionar información sobre el tema. Las respuestas recibidas se recogen en la sección II. Las respuestas que se reciban posteriormente se publicarán como adiciones al presente informe.

II. Respuestas recibidas de los Gobiernos

Colombia

[Original: español]
[21 de mayo de 2012]

Sin lugar a dudas, el uso de las tecnologías de la información y las comunicaciones ha traído consigo importantes cambios y beneficios a nuestros países. No obstante, y de manera simultánea, el avance de estas tecnologías ha incrementado el uso de medios tecnológicos con fines delictivos alrededor del mundo que ponen de manifiesto la necesidad de adoptar urgentes medidas y controles que permitan proteger al Estado ante estas nuevas amenazas.

El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado, incluyendo a la sociedad civil, lo que pone de manifiesto la necesidad de aplicar de forma estricta los protocolos y políticas de seguridad necesarias para establecer controles que permitan proteger al Estado y sus infraestructuras críticas ante estas nuevas amenazas.

En este marco, en el año 2005 Colombia elaboró la denominada norma ISO 27001, concebida como un sistema de gestión que comprende la política, estructura organizativa, procedimientos, procesos y recursos necesarios para implementar la gestión de la seguridad de la información, la cual propende por la aplicación de

estándares de calidad, como el código de buenas prácticas y objetivos de control (norma ISO 17799), la cual se centra en la preservación de las características de confidencialidad, integridad y disponibilidad, tal como se relaciona a continuación:

- Confidencialidad: evitar que la información sea utilizada por individuos o procesos no autorizados.
- Integridad: proteger la precisión y completitud de cualquier cosa que posee valor para una organización.
- Disponibilidad: información accesible y utilizable bajo petición de las entidades autorizadas.

Los beneficios de la norma ISO 27001 se plasman en:

a) El establecimiento de una metodología de gestión de la seguridad de la información clara y bien estructurada;

b) Reducción de riesgos de pérdida o robo de la información;

c) Acceso a información de manera segura por parte de usuarios;

d) Los riesgos a la información y los respectivos controles a la seguridad de la misma son revisados de forma constante;

e) Posibilidad de ejecutar auditorías externas e internas que permitan identificar posibles debilidades en los sistemas de seguridad de la información;

f) Garantiza el cumplimiento de leyes y regulaciones establecidas en materia de gestión de la información;

g) Incremento del nivel de concientización de personas con respecto a los tópicos de seguridad informática.

Como complemento y búsqueda de mejores marcos legales y operativos para la seguridad de la información, el 5 de enero del año 2009, el Congreso de la República de Colombia promulgó la Ley 1273, "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —denominado 'de la protección de la información y de los datos'— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

La importante Ley se divide en dos capítulos: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones".

El capítulo primero determina:

- *Acceso abusivo a un sistema informático*: el que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
- *Obstaculización ilegítima de sistema informático o red de telecomunicación*: el que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí

contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- *Interceptación de datos informáticos*: el que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
- *Daño informático*: el que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
- *Uso de software malicioso*: el que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
- *Violación de datos personales*: el que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
- *Suplantación de sitios web para capturar datos personales*: el que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

El capítulo segundo señala:

- *Hurto por medios informáticos y semejantes*: el que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.
- *Transferencia no consentida de activos*: el que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120)

meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Sin duda alguna, la Ley 1273 de 2009 fue un avance supremamente importante en la lucha contra los delitos informáticos en Colombia; no obstante, el avance de las diferentes formas y manifestaciones de la criminalidad organizada, y en especial del delito cibernético, obligó a Colombia a desarrollar una estrategia integral para la lucha contra la ciberdelincuencia enfocándose en la ciberdefensa y la ciberseguridad en donde el trabajo interagencial fuera el factor predominante para el logro de los objetivos a que apunta el concepto de seguridad de la información.

En este marco el pasado mes de julio del año 2011, el Gobierno de Colombia puso en marcha su política nacional de ciberdefensa y ciberseguridad basada en tres pilares esenciales:

- La adopción de un marco interinstitucional apropiado para prevenir, coordinar, controlar y generar recomendaciones para afrontar las amenazas y los riesgos que se presenten.
- Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad.
- Fortalecer la legislación en estas materias, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales.

Con el objetivo de desarrollar de manera integral las precitadas líneas estratégicas, Colombia diseñó y puso en marcha cuatro (4) instancias:

a) En primer orden se encuentra la denominada Comisión Intersectorial, encargada de fijar la visión estratégica de la gestión de la información, así como de establecer los lineamientos de política respecto de la gestión de la infraestructura tecnológica, información pública y ciberseguridad y ciberdefensa;

b) La segunda instancia es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia quien es el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa;

c) Tercero, se cuenta con el Comando Conjunto Cibernético de las Fuerzas Militares que tiene la función de prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales;

d) Finalmente, se implementó el Centro Cibernético Policial, encargado de la ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos.

Esta institucionalidad le permitirá a Colombia cumplir y desarrollar los mandatos de la política nacional en ciberdefensa y ciberseguridad y enfrentar de una manera integral y efectiva esta nueva forma de criminalidad que hoy evoluciona en el mundo con gran rapidez.

Sin embargo, Colombia no se ha quedado en el desarrollo de su política de ciberdefensa y ciberseguridad; a través de ella se han venido implementado una serie de importantes iniciativas sectorizadas que responden a la generación de

políticas efectivas de seguridad de la información. A continuación se relacionan las más importantes.

Iniciativa	*Entidad líder*	*Alcance*
Modelo de seguridad de la información para la estrategia de Gobierno en línea	Programa Gobierno en línea-Ministerio de las Tecnologías de Información y las Comunicaciones	Este modelo de seguridad hace referencia al conjunto de políticas estratégicas que soportan objetivos de Gobierno en línea como la protección de información del individuo y la credibilidad y confianza en el Gobierno en línea. Establece como elementos fundamentales de la seguridad de la información para los organismos gubernamentales: a) la disponibilidad de la información y los servicios; b) la integridad de la información y los datos; y c) la confidencialidad de la información.
Recomendaciones al Gobierno nacional para la implementación de una estrategia nacional de ciberseguridad	Comisión de Regulación de Telecomunicaciones	Mediante este documento, la Comisión de Regulación de Comunicaciones da al Gobierno nacional recomendaciones para la creación de una estrategia nacional de ciberseguridad y a su vez proporciona instrumentos idóneos para la colaboración y cooperación entre el Gobierno y todos los niveles del sector privado; identifica caminos para la disuasión del crimen cibernético; recomienda la implementación y desarrollo de marcos jurídicos relacionados con la ciberseguridad que sean consistentes con los parámetros internacionales; da recomendaciones para la elaboración de sistemas de respuesta ante incidentes de seguridad en la red, incluyendo la vigilancia, análisis y respuesta a estos incidentes, y propone lineamientos para la implementación de una cultura nacional de ciberseguridad que mejore los niveles de protección de la infraestructura crítica de la información en Colombia.

Iniciativa	*Entidad líder*	*Alcance*
Centro de coordinación de atención a incidentes de seguridad informática colombiano para proveedores de servicios de Internet	Cámara Colombiana de Informática y Telecomunicaciones	Centro de coordinación de atención a incidentes de seguridad informática colombiano, el cual está en contacto directo con los centros de seguridad de sus empresas afiliadas (las más grandes empresas proveedoras de Internet en Colombia). Está en capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas.

Ahora bien, dejando a un lado el tema de capacidades nacionales de seguridad de la información, es importante hacer mención a una serie de medidas que Colombia estima pertinente tomar a nivel internacional para fortalecer la seguridad de la información:

- Fortalecer los canales de comunicación entre los países que integran la Organización de las Naciones Unidas, con el fin de articular esfuerzos en la lucha transnacional contra los delitos que afectan la información y los datos.
- Definir instrumentos internacionales y regionales enfocados en la tipificación de las conductas punibles que atenten contra la ciberseguridad y ciberdefensa en cada Estado.
- Definir y estructurar los protocolos de atención a incidentes informáticos, generando políticas globales sobre la seguridad de la información.
- Fortalecer las actividades en el ámbito preventivo y el marco de la legalidad en lo referente a los grupos “hacktivistas”, especialmente en las universidades y colegios con el fin de reducir la participación de jóvenes en estas organizaciones que ponen en peligro el normal desarrollo de la infraestructura digital de los Estados.
- Legislación estandarizada en énfasis a la prevención, atención y seguimiento de las actividades que rodean la seguridad de la información.
- Convergencia e implementación tecnológica enfocada en la adopción de mejores prácticas en el manejo de la seguridad de la información. En este tema es importante indicar que deben existir unos planes de inversión en tecnología de punta así como del apoyo de los gobiernos a los proyectos de desarrollo tecnológico.
- Generar espacios de intercambio de información y conocimiento frente a los estándares universales que regulan la materia.

Normatividad de la República de Colombia en materia de Seguridad de la información

Ley/resolución	*Tema*
Ley 527 de 1999 (Comercio electrónico)	Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 599 de 2000	Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra, de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el acceso abusivo a un sistema informático (art. 195). El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.
Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Se prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
Ley 1150 de 2007	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual se prevé el desarrollo del sistema electrónico para la contratación pública.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —denominado "de la protección de la información y de los datos"— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley/resolución	*Tema*
Resolución de la Comisión de Regulación de Comunicación 2258 de 2009	Sobre la seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrecen acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la Unión Internacional de Telecomunicaciones, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Asimismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información.
Circular 052 de 2007 (Superintendencia Financiera de Colombia)	Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.

Cuba

[Original: español]
[21 de mayo de 2012]

El uso hostil de las telecomunicaciones, con el propósito declarado o encubierto de subvertir el ordenamiento jurídico y político de los Estados, es una violación de las normas internacionalmente reconocidas en esta materia, cuyos efectos pueden generar tensiones y situaciones desfavorables para la paz y la seguridad internacionales.

Cuba comparte plenamente la preocupación que se expresa en la resolución 66/24 de la Asamblea General, respecto al empleo de las tecnologías y medios de información con propósitos incompatibles con la estabilidad y la seguridad internacionales, que afecten negativamente la integridad de los Estados, en detrimento de su seguridad en las esferas civil y militar. Igualmente, esa resolución enfatiza adecuadamente en la necesidad de impedir la utilización de los recursos y las tecnologías de la información con fines delictivos o terroristas.

En este contexto, Cuba reitera su condena a la escalada agresiva del Gobierno de los Estados Unidos en su guerra radial y televisiva contra Cuba, que viola las normativas internacionales vigentes en materia de regulación del espectro radioeléctrico. Esta agresión se realiza sin reparar en el daño que pudieran causar a la paz y seguridad internacionales, creando situaciones de peligro, incluso utilizando

un avión militar para transmitir señales de televisión hacia el país, sin el consentimiento de la República de Cuba.

Durante el año 2011, se trasmitieron contra Cuba desde el territorio de los Estados Unidos un promedio de 2.193 horas de transmisiones semanales ilegales, emitidas por 30 frecuencias. Varias de estas emisoras pertenecen o prestan sus servicios a organizaciones vinculadas con conocidos elementos terroristas que residen y actúan contra Cuba en territorio estadounidense, quienes transmiten programas en que se incita al sabotaje, los atentados políticos, el magnicidio y otros temas propios del radio-terrorismo.

Estas transmisiones provocadoras contra Cuba constituyen violaciones de los siguientes preceptos internacionales:

- Principios fundamentales de la Unión Internacional de Telecomunicaciones, expresados en el preámbulo de su constitución. El contenido de la programación televisiva que se transmite por el Gobierno de los Estados Unidos contra Cuba tiene un carácter subversivo, desestabilizador y engañoso, que entra en contradicción con estos principios.
- Disposiciones CS 197 y CS 198 de la constitución de la Unión Internacional de Telecomunicaciones, que establecen que todas las estaciones, cualquiera que sea su objeto, deberán ser instaladas y explotadas de tal manera que no puedan causar interferencias perjudiciales a las comunicaciones o servicios radioeléctricos de otros Estados miembros.
- Acuerdo de la novena sesión plenaria de la Conferencia Mundial de Radiocomunicaciones, celebrada en noviembre de 2007, que estableció en el párrafo 6.1, inciso g) “que toda estación de radiodifusión que funcione a bordo de una aeronave y transmita exclusivamente en el territorio de otra administración sin su consentimiento, no puede considerarse que funcione de conformidad con el Reglamento de Radiocomunicaciones”.
- Artículo 8, numeral 8.3, del Reglamento de Radiocomunicaciones, que establece que las frecuencias asignadas e inscritas, con reconocimiento internacional, deberán ser tenidas en cuenta por las otras administraciones cuando efectúen sus propias asignaciones a fin de evitar una interferencia perjudicial.
- Artículo 42, numeral 42.4, del Reglamento de Radiocomunicaciones, que prohíbe a las estaciones de aeronaves en el mar o por encima del mar efectuar servicio alguno de radiodifusión.
- Dictamen de la Junta del Reglamento de Radiocomunicaciones, que en su 35ª reunión en diciembre de 2004, estableció la interferencia perjudicial a los servicios cubanos que esas transmisiones causaban en los 213 MHz y reclamó a la administración de los Estados Unidos de América tomar las medidas pertinentes para su eliminación. Además, desde septiembre de 2006, la Junta del Reglamento de Radiocomunicaciones ha estado reclamando a la Administración de los Estados Unidos las medidas adoptadas para eliminar la interferencia en los 509 MHz, sin que haya dado respuesta hasta el momento. El 20 de marzo de 2009 concluyó la 50ª Reunión de la Junta y en su resumen de decisiones (documento RRB09-1/5) se reitera, una vez más, la ilegalidad de las transmisiones y solicita a la Administración de los Estados Unidos de

América que adopte todas las medidas necesarias con miras a eliminar estos dos casos de interferencia a los servicios de televisión de Cuba.

- Artículo 23, numeral 23.3, del Reglamento de Radiocomunicaciones, que limita las transmisiones televisivas fuera de las fronteras nacionales. Un informe emitido en enero de 2009 por la Oficina de Auditoría del Gobierno de los Estados Unidos reconoce las violaciones de las normas internacionales y la legislación interna en que incurre el programa de transmisiones radiales y televisivas del Gobierno estadounidense contra Cuba.

La Conferencia Mundial de Radiocomunicaciones, que sesionó en Ginebra en 2007, aprobó un texto de conclusiones que califica de no conformes con el Reglamento de Radiocomunicaciones las transmisiones desde aeronaves desde los Estados Unidos hacia Cuba. Las conclusiones refrendadas por el plenario establecieron textualmente que: "una estación de radiodifusión que funcione a bordo de una aeronave y transmita únicamente hacia el territorio de otra Administración sin su acuerdo, no puede considerarse que esté de conformidad con el Reglamento de Radiocomunicaciones".

Estas conclusiones tienen valor legal para el trabajo de la Unión Internacional de Telecomunicaciones. De esta forma, la Conferencia Mundial de Radiocomunicaciones refrendó el pronunciamiento realizado en 1990 por la entonces Junta Internacional de Registro de Frecuencia, según el cual la transmisión de televisión a bordo de un aerostato con programación dirigida hacia territorio nacional cubano contraviene la regulación del Reglamento.

En la 54ª reunión de la Junta del Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones, celebrada en julio de 2010, se adoptó la siguiente decisión:

> Tras estudiar de manera pormenorizada el informe del Director y la comunicación de la Administración de Cuba (documento RRB10-2/3 (Add.1)), la Junta lamentó el hecho de que continúe la interferencia a las estaciones de radiodifusión de Cuba por emisiones de los Estados Unidos y decidió mantener sus decisiones a este respecto.
>
> La Junta tomó asimismo nota de la solicitud de "la Oficina, en su calidad de Secretaría Ejecutiva de la Junta" para que planteara la cuestión de la interferencia perjudicial a las estaciones de radiodifusión en ondas métricas y disimétricas de Cuba antes de la próxima Conferencia de Plenipotenciarios. Tras reconocer el derecho soberano de cada administración a plantear cualquier cuestión ante la Conferencia de Plenipotenciarios, la Junta confirmó que los dos representantes de la Junta del Reglamento de Radiocomunicaciones ante la Conferencia de Plenipotenciarios 2010 y su Secretario Ejecutivo estarían dispuestos a facilitar toda la información y el asesoramiento pertinentes que pudiera requerirse de ellos en la próxima Conferencia de Plenipotenciarios.

Más recientemente, en febrero de 2012, la Conferencia Mundial de Radiocomunicaciones confirió el mandato al Director de la Oficina de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones, de brindar seguimiento e informar a la próxima Conferencia, a celebrarse en el año 2015, respecto a las interferencias que causa el Gobierno de los Estados Unidos a los servicios radiales y televisivos cubanos, en sus acciones de agresión radioeléctrica.

La Conferencia confirmó así la vigencia de la conclusión adoptada en su edición anterior, en la que se reconoció la ilegalidad de las transmisiones radiotelevisivas anticubanas que realizan las autoridades estadounidenses mediante la utilización de aeronaves.

La hostilidad del Gobierno de los Estados Unidos contra Cuba también se ha puesto de manifiesto a través del bloqueo económico, comercial y financiero impuesto por más de 50 años, que incluye la esfera de la información y las telecomunicaciones:

- EI sector de la informática y las comunicaciones se ha visto severamente afectado por el bloqueo. De 2010 a 2011, el monto de las afectaciones se calcula en 7.396.394 dólares.
- Cuba continúa sin tener derecho a acceder a los servicios que ofrecen gran número de sitios en la web, negación que se produce al reconocerse que el enlace se establece desde una dirección de Internet (IP) otorgada al dominio cubano .cu.
- Con total cinismo e hipocresía los Estados Unidos continúan acusando a Cuba con la mentira de impedir el acceso de sus ciudadanos a la red global, cuando la realidad bien diferente es que Cuba no puede, por las leyes del bloqueo que le aplica el Gobierno de los Estados Unidos, conectarse a los cables de fibra óptica que rodean el archipiélago cubano, obligándola a pagar caros servicios mediante satélites.
- EI 6 de octubre de 2010, la red social Twitter reconoció su total responsabilidad por haber bloqueado el envío de mensajes vía celular desde Cuba hacia su plataforma. De igual forma, en abril de 2011 se conoció que a Cuba se le está limitando el acceso a determinadas herramientas de Twitter con el argumento de que se está accediendo desde un país prohibido.
- A partir de febrero de 2011, la casa financiera Syniverse dejó de realizar los pagos a la Empresa de Telecomunicaciones de Cuba (ETECSA) por concepto de “roaming” para telefonía celular, aduciendo que su banco no podía realizar transacciones con Cuba, lo que implica que no se ha podido cobrar un monto ascendente a 2,6 millones de dólares, más las dificultades adicionales ocasionadas.

La discusión en la Asamblea General de las Naciones Unidas sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional es muy pertinente e importante. Actuaciones como las detalladas anteriormente del Gobierno de los Estados Unidos contra Cuba confirman la necesidad de ese debate y la urgencia de adoptar medidas para poner fin a tales acciones.

Cuba apoyó la resolución 66/24 de la Asamblea General y continuará contribuyendo al desarrollo global pacífico de las tecnologías de la información y las telecomunicaciones y su empleo en bien de toda la humanidad.

Panamá

[Original: español]
[10 de julio de 2012]

Las economías del siglo XXI están basadas, cada vez más, en el sector de servicios; esto es especialmente evidente en las economías del primer mundo. El comercio electrónico no es más que la expresión más reciente de este sector de la economía, facilitando las transacciones comerciales, reduciendo costos y tiempos de entrega de mercancías y servicios alrededor de todo el mundo. El gobierno electrónico es la versión estatal de comercio electrónico que permite a los Estados atender una gran cantidad de solicitudes de parte de los ciudadanos de un Estado, de manera rápida y eficiente a través de diferentes tecnologías (web y móvil).

Debido al amplio uso de las tecnologías de información y comunicación para soportar el comercio y gobierno electrónico, es necesario realizar esfuerzos para asegurar que dichas tecnologías provean los requisitos mínimos de confidencialidad, integridad y disponibilidad, requeridos por los clientes y ciudadanos de un Estado. Sin embargo, muchos de los esfuerzos realizados hoy día se concentran en soluciones técnicas a problemas globales, que requieren atacar el problema desde varios ángulos.

Creemos que el desarrollo de marcos legales, basados en referencias internacionales, previamente adoptadas por otros Estados y que cuenten con amplia aceptación, debe ser la tarea número uno de los Estados que quieran promover el comercio y gobierno electrónico, mientras se crea un ambiente hostil para los delincuentes y terroristas que utilicen estos medios para llevar a cabo sus actividades. Al proveer un ambiente amigable para el comercio y gobierno electrónico, solo se puede esperar obtener beneficios para las economías de los países que adopten medidas de protección legal y técnica a la problemática.

Al mismo tiempo, se deben continuar los esfuerzos para desarrollar técnicas y políticas de defensa del ciberespacio de los Estados, donde se encuentren los intereses de los diferentes países, mediante estrategias nacionales de ciberseguridad que puedan ser implementadas en tiempos definidos y realistas. Estas estrategias deben estar orientadas a la conservación de la seguridad nacional y estabilidad de los países, además de contribuir a la paz internacional.

Las medidas adoptadas a nivel nacional por parte de Panamá para fortalecer la seguridad de la información y contribuir con la cooperación internacional son:

a) Creación del Centro Nacional de Respuesta a Incidentes, mediante decreto ejecutivo No 709 de 26 de septiembre de 2011;

b) Revisión de la ley sustantiva (Código Penal) para la inclusión de nuevas conductas criminales relacionadas con el ciberdelito y su posterior remisión a la Asamblea Nacional de Diputados para su aprobación (Proyecto de Ley No. 377);

c) Discusión y revisión del Código Procesal Penal, para alinearlo con las nuevas conductas incluidas en el Código Penal;

d) Conformación del grupo de trabajo para la discusión de la responsabilidad de los proveedores de acceso a Internet en el ámbito de la seguridad de la información, dirigida por la Autoridad Nacional para la Innovación Gubernamental y Autoridad Nacional de los Servicios Públicos; también se discute

la aplicación de los resultados de este grupo de discusión a nivel regional (Comisión Técnica de Telecomunicaciones de Centroamérica/Unión Internacional de Telecomunicaciones) a través de los reguladores nacionales de la región de Centroamérica;

e) Grupo de trabajo sobre manejo de la evidencia digital liderado por el Ministerio Público y con la participación de la Autoridad Nacional para la Innovación Gubernamental;

f) Formalización de solicitud de asistencia técnica enviada a la Organización de Estados Americanos (OEA) para el desarrollo de la estrategia nacional de ciberseguridad;

g) Entrenamiento avanzado en el manejo de incidentes proporcionado por la OEA /CERT-CC, llevado a cabo en Panamá en el mes de abril;

h) Evaluación de la propuesta de la Oficina de las Naciones Unidas contra la Droga y el Delito para un programa de fortalecimiento de capacidades de Panamá de lucha contra del cibercrimen;

i) Participación recurrente en las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas y del Comité Interamericano contra el Terrorismo (OEA);

j) Solicitud formal de acceso al Convenio de Budapest sobre la ciberdelincuencia, mediante la nota de 31 de enero de 2012, enviada por el Ministro de Relaciones Exteriores a Carlos Arosemena, Embajador de Panamá en Bruselas.

En cuanto a las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial, creemos que las siguientes recomendaciones deben ser consideradas:

a) Adopción de un marco legal común que permita la colaboración entre Estados a través de asistencias legales mutuas de manera expedita, basados en procedimientos internacionales aceptados;

b) Desarrollo de estrategias nacionales y regionales de ciberseguridad;

c) Promocionar el intercambio de información entre Estados a través de los centros nacionales de respuestas a incidentes de manera normalizada, para que se facilite el flujo de información, especialmente aquella relacionada con persecución del crimen y terrorismo;

d) Desarrollo de programas de concienciación de las normas locales e internacionales aplicables a cada Estado.

Qatar

[Original: inglés]
[18 de mayo de 2012]

Las iniciativas nacionales del Estado de Qatar en el ámbito de la seguridad de la información se basan en la adopción de un enfoque holístico que abarca tanto los instrumentos para la seguridad de la información como la protección de las personas que utilizan dichos instrumentos. La estrategia está en consonancia con la Visión Nacional de Qatar 2030, asentada sobre los pilares básicos del desarrollo humano,

social y económico y reforzada por iniciativas internacionales como el Programa Mundial sobre la seguridad cibernética de la Unión Internacional de Telecomunicaciones (UIT) y las medidas para la protección de las infraestructuras de información esenciales adoptadas por el Grupo de los Ocho.

En la actualidad, el núcleo fundamental de la estructura de seguridad cibernética de Qatar está compuesto por el programa nacional de seguridad cibernética (el Equipo de respuesta a emergencias cibernéticas de Qatar, iniciativa del Centro de excelencia para la seguridad de la información), patrocinado por el Gobierno en el marco del Consejo Supremo de Tecnología de la Información y las Comunicaciones. En la estructura de seguridad cibernética nacional también se incluyen las subdivisiones de protección de las infraestructuras de información esenciales y de supervisión de las tecnologías de la información y las comunicaciones.

El Equipo de respuesta a emergencias cibernéticas de Qatar trabaja con organismos gubernamentales, con organizaciones de los sectores público y privado y con la ciudadanía de Qatar a fin de garantizar el control de las amenazas y los riesgos cibernéticos. Los protocolos que ha establecido para investigar las amenazas incluyen técnicas avanzadas de análisis forense digital, sistemas de estudio de *malware* y de supervisión de amenazas e instrumentos para mejorar la seguridad preventiva y la capacidad de respuesta mediante programas de capacitación que simulan situaciones reales. A continuación se presenta una breve descripción de sus funciones.

Unidades de inteligencia centradas en el análisis de amenazas

Centro de Operaciones de Seguridad. Los analistas de seguridad emplearán instrumentos elaborados internamente (sistemas de control de amenazas) para alertar de forma proactiva a los organismos gubernamentales y otras entidades fundamentales acerca de las amenazas relacionadas con los instrumentos de eliminación.

Sistema de control de amenazas. Este sistema es un mecanismo elaborado internamente que recopila y analiza información sobre amenazas procedente de diferentes fuentes para detectar computadoras o sitios web locales infectados y mitigar los daños que puedan causar.

Centro de análisis de *malware*

El objetivo de este centro consiste en fomentar la capacidad de determinar el nivel de las amenazas de *malware*, analizarlas y ofrecer protección frente a ellas a nivel nacional. En la actualidad, este centro elabora un informe detallado sobre el comportamiento del *malware* en las computadoras infectadas; los tipos de sistema a los que ataca; el país de origen del programa; y cualquier conexión realizada a través de Internet con el servidor de comando y control. También contribuye a medir la repercusión de cada programa de *malware* detectado para evaluar el riesgo asociado con cada amenaza en función de su volumen y para colaborar en la detección de *malware* mediante los programas antivirus del mercado.

Gestión de incidentes públicos

El Equipo de respuesta a emergencias cibernéticas de Qatar se propone reducir al mínimo el número de computadoras infectadas en el Estado de Qatar mediante la prestación de apoyo fundamental a los usuarios públicos y a los sectores esenciales. A fin de cumplir este objetivo y proporcionar una orientación adecuada, Qatar ha ampliado su servicio de respuesta a incidentes para incluir a los usuarios domésticos de la línea de conexión digital asimétrica (ADSL) a través del portal de gestión de incidentes públicos. La ayuda prestada incluye diversos recursos, directrices y programas informáticos básicos para detectar y eliminar infecciones de los sistemas domésticos que utilicen una conexión ADSL.

Capacitación en materia de seguridad cibernética

El Equipo de respuesta a emergencias cibernéticas de Qatar lleva a cabo actividades y talleres de capacitación en materia de seguridad cibernética para los profesionales de la tecnología de la información de los organismos gubernamentales de Qatar y de otros Estados del Consejo de Cooperación del Golfo.

Concienciación en materia de seguridad cibernética

El Equipo de respuesta a emergencias cibernéticas de Qatar busca asentar los conocimientos y las mejores prácticas en relación con la seguridad cibernética, con especial atención a los trabajadores del sector empresarial.

El Equipo de respuesta a emergencias cibernéticas de Qatar trabaja para proteger las infraestructuras esenciales, habida cuenta de que sectores como el financiero, el energético y el de las tecnologías de la información y las comunicaciones son cruciales para el mantenimiento de la economía de Qatar, de su población y de su Gobierno. Por ello, su cometido consiste en proteger los sistemas de información en que se asientan estos sectores fundamentales mediante las tareas siguientes:

- Elaborar estrategias de protección nacional, marcos sobre las mejores prácticas e instrumentos y sensibilizar a las partes interesadas;
- Prestar apoyo directo a los propietarios y los operadores de las infraestructura esenciales para mejorar las salvaguardias del sistema de control de supervisión y adquisición de datos (SCADA);
- Analizar las cuestiones que afectan al sector industrial y otras cuestiones que influyen en varios sectores y aplicar estrategias de protección específicas para cada sector;
- Colaborar con organizaciones internacionales que se ocupen de proteger infraestructuras de información esenciales para establecer soluciones transnacionales;
- Evaluar la preparación de las organizaciones que se ocupan de proteger infraestructuras de información esenciales de Qatar y los avances realizados.

Además, el programa nacional de seguridad cibernética del Consejo Supremo de Tecnología de la Información y las Comunicaciones sigue colaborando con el poder legislativo para elaborar varias leyes y reglamentos centrados en la mejora

permanente de las salvaguardias nacionales en materia de tecnologías de la información y las comunicaciones para hacer frente a nuevas amenazas.

El Consejo Supremo recomienda que la comunidad internacional adopte o aplique las siguientes medidas:

- Establecer, en un plazo de cinco años, marcos jurídicos internacionales armonizados a nivel regional en todos los países;
- Establecer, en un plazo de tres años, equipos encargados de los incidentes informáticos en todos los países que aún no dispongan de ellos;
- Desarrollar, en un plazo de cinco años, estrategias nacionales de seguridad cibernética conformes a los principios de la cooperación internacional y que incluyan la protección de las infraestructuras de información esenciales;
- Elaborar programas de estudios sobre la seguridad informática destinados a desarrollar la capacidad y a fomentar la concienciación en diversos sectores (como los gobiernos, las instituciones académicas, el sector privado o las escuelas);
- Hacer hincapié en la importancia de los programas de sensibilización sobre la seguridad en Internet dirigidos a niños y jóvenes.

Turquía

[Original: inglés]
[31 de mayo de 2012]

Las tecnologías de la información y las comunicaciones están penetrando rápidamente tanto en la vida cotidiana como en los procesos institucionales. Diversos datos esenciales para las personas, las instituciones o los gobiernos se almacenan digitalmente y se transmiten por el ciberespacio. A pesar de sus ventajas, estas tecnologías entrañan algunos riesgos, como la incapacidad de asegurar la confidencialidad e integridad de los datos almacenados en forma digital y la disponibilidad de los sistemas de información. Las vulnerabilidades de los sistemas de información y comunicaciones (derivadas de un diseño, una configuración y un funcionamiento defectuosos, así como de una capacidad técnica inadecuada y de la falta de capacitación y concienciación sobre la seguridad de los trabajadores y los usuarios) proporcionan un entorno adecuado para que esos riesgos se materialicen.

A fin de evitar o mitigar los riesgos y corregir las vulnerabilidades, es cada vez más importante que se realicen esfuerzos para fomentar la seguridad cibernética a nivel nacional e institucional. En este sentido, la creación de capacidad técnica y administrativa y la mayor sensibilización de los ejecutivos, los trabajadores y los usuarios de las instituciones públicas y privadas son aspectos esenciales de estos esfuerzos.

La sensibilización de los funcionarios de alto nivel del Gobierno turco sobre la necesidad de aumentar la seguridad de la información es inequívoca. Además, la Dirección de Información y Comunicaciones de Turquía se centra concretamente en estudiar las mejores prácticas y las nuevas amenazas en el ciberespacio, organizar y llevar a cabo ejercicios de seguridad cibernética nacional, aumentar la capacidad institucional y técnica de responder a las situaciones de emergencia y realizar

auditorías periódicas de los operadores de comunicaciones electrónicas a fin de garantizar que se estén aplicando las políticas, procesos, programas y controles pertinentes para responder adecuadamente a los incidentes de seguridad relacionados con las comunicaciones electrónicas.

La investigación de conceptos internacionales relacionados con las amenazas mundiales, las vulnerabilidades específicas de los sistemas de información y las mejores prácticas sobre los mecanismos de intercambio de información, así como el intercambio de conocimientos entre expertos con otras organizaciones internacionales, son actividades pertinentes para fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.

Las convenciones multilaterales sobre la cooperación y las técnicas forenses aplicadas a los incidentes de seguridad de la información y las comunicaciones en el ciberespacio, así como el intercambio de información sobre bases de datos de *malware*, podrían resultar instrumentos útiles para fortalecer la seguridad de la información a nivel mundial.

Ucrania

[Original: ruso]
[31 de mayo de 2012]

Evaluación general de los problemas de la seguridad de la información

La rápida introducción de las tecnologías de la información y las comunicaciones en todas las esferas de actividad y la globalización de los intercambios de comunicación han suscitado que las actividades ilícitas tiendan, a nivel mundial, a trasladarse al ámbito virtual. En la actualidad, la delincuencia cibernética, también conocida como ciberdelincuencia, no conoce fronteras estatales y entraña una amenaza tanto para los derechos y libertades civiles como para los intereses nacionales y la seguridad de los Estados.

En los últimos años ha tenido lugar un aumento constante de los ataques informáticos contra elementos fundamentales de las estructuras nacionales de los Estados, agresiones que han provocado daños a los países mediante acciones como la alteración de información crucial o el bloqueo de procesos productivos del sector industrial, los servicios públicos, el transporte y el suministro energético.

El balance de las actividades de ciberdelincuencia registradas en 2011 en varios Estados en los cuales sistemas de información de organismos e instituciones públicas fueron objeto de ataques informáticos que lograron interrumpir sus actividades refleja la magnitud de las amenazas que se ciernen sobre la sociedad y el carácter imprevisible de los efectos adversos de los ataques cibernéticos.

Medidas que se adoptan a nivel nacional para fortalecer la seguridad de la información y contribuir a la cooperación internacional en esa esfera

La experiencia de varios países desarrollados en la lucha contra estas amenazas apunta a la creación de sistemas a nivel de Estado para combatir la ciberdelincuencia, encabezados por un único organismo de coordinación. Con ello se asegura la acumulación estratégica de recursos y esfuerzos de los órganos

gubernamentales y no gubernamentales competentes con miras a combatir y eliminar las amenazas a la seguridad de la información.

Este fue uno de los aspectos fundamentales durante la revisión de los enfoques de evaluación de nuevas amenazas y desafíos, en especial en el ámbito de la información, y la aplicación de las medidas adoptadas por las altas instancias políticas del Estado con miras a crear un sistema estatal único de lucha contra la ciberdelincuencia, elaborar un proyecto de ley nacional sobre la seguridad cibernética y establecer y reforzar la cooperación con los servicios especiales y organismos encargados de hacer cumplir la ley de otros Estados.

En junio de 2011, el Servicio de Seguridad de Ucrania, en colaboración con otros organismos encargados de hacer cumplir la ley de 11 Estados (Alemania, Canadá, Chipre, Estados Unidos de América, Francia, Letonia, Lituania, Países Bajos, Reino Unido de Gran Bretaña e Irlanda del Norte, Rumania y Suecia), puso fin a las actividades delictivas de una agrupación internacional involucrada en actos de piratería cibernética que, mediante la difusión de *malware* en Internet, robó más de 72 millones de dólares de entidades bancarias extranjeras.

En octubre de 2011, el Servicio de Seguridad de Ucrania organizó y celebró en Yalta (Ucrania) la reunión anual de expertos de Ucrania y la Organización del Tratado del Atlántico Norte en materia de seguridad cibernética, cuyas conclusiones reforzaron la posición ucraniana relativa a la necesidad de seguir desarrollando un sistema de seguridad de la información que incluyera al sector público y al privado y que incorporara las experiencias de otros Estados.

A iniciativa del Servicio de Seguridad de Ucrania, está previsto que durante el 32º período de sesiones del Consejo de jefes de órganos de seguridad y servicios especiales de los Estados miembros de la Comunidad de Estados Independientes se estudie la posibilidad de crear una comisión específica sobre la seguridad de la información.

Contenido de los conceptos mencionados en el párrafo 2 de la resolución 66/24 de la Asamblea General

Con arreglo a la legislación ucraniana, las siguientes actividades se consideran amenazas fundamentales a la seguridad nacional, incluido en el ámbito de la información:

- El menoscabo de la libertad de expresión y del acceso de los ciudadanos a la información;
- La delincuencia informática y el terrorismo informático;
- La difusión de información que haya sido calificada como secreta por el Estado o por ley, así como de información confidencial que sea propiedad del Estado o haya sido calificada como esencial para garantizar las necesidades nacionales y los intereses de la sociedad y del Estado;
- Los intentos de manipular la conciencia colectiva, en particular mediante la difusión de información falsa, incompleta o prejuiciosa.

Medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial

La base de la seguridad de la información de la comunidad internacional consiste en establecer las condiciones para garantizar la seguridad de la información de los Estados por separado y en fomentar una cooperación eficaz entre ellos en dicho ámbito.

Los mecanismos para combatir eficazmente las amenazas reales y potenciales a la seguridad de la información incluyen la aplicación de las siguientes medidas de cooperación internacional:

- La puesta en práctica de mecanismos consultivos de cooperación en el ámbito de la seguridad cibernética para fomentar el intercambio de experiencias en materia de procedimientos legislativos y de regulación en dicho ámbito;
- El establecimiento de un sistema de intercambio de información sobre las actividades de supervisión del ciberespacio y de un sistema que incluya la alerta temprana de ataques cibernéticos, el intercambio de información sobre los aspectos técnicos de esas agresiones, la detección de sus fuentes y la elección de los métodos efectivos para combatirlas;
- La colaboración para contrarrestar los efectos adversos de los ataques cibernéticos y extraer enseñanzas de experiencias previas, así como el fomento de decisiones técnicas y recomendaciones institucionales para evitar esos ataques;
- La elaboración de instrumentos jurídicos internacionales destinados a establecer una terminología y una regulación únicas, como un Código de conducta en Internet, entre otros.

En relación con la necesidad de combatir las amenazas citadas, los servicios especiales y los organismos encargados de hacer cumplir la ley deberían fomentar su interacción respecto a las tareas siguientes:

- Configurar mecanismos para el intercambio oportuno entre servicios especiales de datos sobre las actividades de organizaciones delictivas, incluidas las de carácter terrorista, cuyo fin sea acceder sin autorización a las fuentes de información de los sectores nacionales de Internet y a los sistemas de información de organismos estatales y empresas;
- Intercambiar información sobre las actividades delictivas relacionadas con el acceso no autorizado a los sistemas informáticos de entidades financieras, en particular en lo que respecta a la falsificación de tarjetas bancarias y a la intromisión no autorizada en el funcionamiento de los sistemas informáticos bancarios con miras a bloquearlos o a sustraer información confidencial;
- Organizar la cooperación en la búsqueda de personas que hayan cometidos delitos informáticos en los sectores nacionales de Internet y documentar sus actividades ilícitas;
- Intercambiar experiencias y prácticas sobre los análisis de expertos técnicos e informáticos (incluidos los de carácter jurídico-cibernético) realizados en el contexto de las investigaciones de delitos informáticos, así como sobre los métodos y técnicas de investigación informática para documentar las actividades delictivas;

- Crear programas de capacitación comunes para la formación de personal cualificado y pasantías para los expertos de los servicios especiales;
- Participar en simposios, seminarios y conferencias sobre la lucha contra la delincuencia cibernética.

Una de las modalidades de cooperación en este sentido podría ser el establecimiento de un sistema de supervisión de los recursos de los sectores nacionales de Internet destinado a detectar de manera oportuna las amenazas y a identificar los medios óptimos para neutralizarlas.

Con el fin de coordinar las actividades centradas en la detección de infracciones informáticas en relación con los organismos públicos, los operadores de telecomunicaciones y otras entidades relacionadas con las infraestructuras de comunicaciones nacionales, otro de los mecanismos posibles podría consistir en el establecimiento de centros nacionales de respuesta para emergencias informáticas y el fomento de una colaboración estrecha entre ellos.

Las tareas fundamentales de estos centros nacionales podrían incluir:

- Obtener, analizar y almacenar en bases de datos específicas la información sobre las amenazas actuales a la seguridad informática;
- Asumir el control técnico y la detección de los mecanismos y recursos de Internet cuyo funcionamiento sea contrario a la normativa que regula las actividades de los usuarios de los sectores nacionales de Internet;
- Formular recomendaciones dirigidas a los usuarios de Internet en relación con la protección de los intereses individuales, sociales y estatales en el ámbito de la información y ofrecerles servicios de consulta y apoyo técnico;
- Recibir notificaciones y prestar ayuda de emergencia para detener los ataques cibernéticos e informar oportunamente a los usuarios de Internet y a otros sistemas de información, incluidos los locales y los empresariales, acerca de las amenazas a la seguridad informática que puedan surgir;
- Cooperar e intercambiar información con centros similares de otros países.