REUNIONES DE MINISTROS DE JUSTICIA U
OTROS MINISTROS, PROCURADORES O FISCALES
GENERALES DE LAS AMÉRICAS

OEA/Ser.K/XXXIV
CIBER-VII/doc.1/11
14 noviembre 2011
Original: inglés

Séptima Reunión del Grupo de Trabajo en Delito Cibernético

CUESTIONARIO PREPARATORIO
DE LA SÉPTIMA REUNIÓN DEL GRUPO DE TRABAJO EN DELITO CIBERNÉTICO

INTRODUCCIÓN

El presente cuestionario busca recolectar información útil para los propósitos de la Sexta Reunión del Grupo de Trabajo en Delito Cibernético, la cual se celebrará el 6 y 7 de febrero de 2012, en relación con las recomendaciones que han sido formuladas en las reuniones precedentes y las que han sido adoptadas en el marco del proceso de las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA), concordantes con las mismas.

Para estos efectos, el cuestionario se divide en cuatro áreas temáticas: (1) Legislación; (2) Unidades Especializadas y Esfuerzos Nacionales; (3) Cooperación Internacional; y (4) Capacitación.

Teniendo en cuenta lo anterior, sírvanse remitir la respuesta de su Estado al presente cuestionario, a más tardar el **viernes, 16 de diciembre de 2011**, a la Secretaría General de la OEA (Departamento de Cooperación Jurídica de la Secretaría de Asuntos Jurídicos), al correo electrónico LegalCooperation@oas.org o al número de fax: + (202) 458-3598.

Por favor adicionar el espacio que requiera en cada respuesta o anexar hojas, según lo estime necesario.

I. LEGISLACIÓN

1.1. ¿Ha tipificado su país las siguientes modalidades de delito cibernético?

a)	Acceso ilícito	Sí (X)	No ( )
b)	Interceptación ilícita	Sí (X)	No ( )
c)	Ataques a la integridad de datos	Sí (X)	No ( )
d)	Ataques a la integridad de sistemas	Sí (X)	No ( )
e)	Abuso de dispositivos	Sí (X)	No ( )
f)	Falsificación informática	Sí (X)	No ( )
g)	Fraude informático	Sí (X)	No ( )
h)	Pornografía infantil	Sí (X)	No ( )
i)	Delitos contra la propiedad intelectual y derechos afines	Sí (X)	No ( )
j)	Otras (sírvase enumerarlas): _____	Sí (X)	No ( )

En caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica, de la legislación: Suplantación de sitios web para capturar datos personales

http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html

1.2. En caso de que su país no haya tipificado alguna de las anteriores conductas, indique si está desarrollando algunas acciones para hacerlo: Sí ( ) No ( )

En caso afirmativo, sírvase describir esos esfuerzos: _____
_____

1.3. ¿Permite le legislación de emergencia de su país, por parte los investigadores criminales, requerir a los Proveedores de Servicios de Internet a preservar pruebas electrónicas sin la necesidad de una orden judicial? Sí ( ) No (X)

En caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica, de la legislación: _____
_____

1.4. ¿Ha adoptado su país la legislación sustantiva y procesal u otras medidas necesarias que permitan a sus autoridades competentes?

a) Confiscar, decomisar o secuestrar sistemas o dispositivos de almacenamiento informáticos. Sí (X) No ( )

b) Copiar y conservar los datos informáticos consultados. Sí (X) No ( )

En caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica, de la legislación: LEY 906 DE 2004 – código procedimiento penal - Artículos 236, 237 y 244
http://www.secretariasenado.gov.co/senado/basedoc/ley/2004/ley_09060_204a.html

1.5. ¿Permite la legislación procesal de su país la interceptación legal de comunicaciones electrónicas trasmitidas en su territorio a través de sistemas de computación? Sí (X) No ( )

En caso afirmativo, sírvase describir brevemente y adjuntar copias, de preferencia electrónica, de esa legislación: LEY 906 DE 2004 – código procedimiento penal - Artículo 235
http://www.secretariasenado.gov.co/senado/basedoc/ley/2004/ley_09060_204a.html

II. UNIDADES ESPECIALIZADAS Y ESFUERZOS NACIONALES

2.1. ¿Hay en su país una unidad o entidad encargada específicamente de investigar los delitos cibernéticos? (autoridad de policía) Sí (X) No ( )

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: GRUPO INVESTIGACIONES TECNOLÓGICAS
- Institución de la que depende: POLICÍA NACIONAL – DIRECCIÓN DE INVESTIGACIÓN CRIMINAL
- Información de contacto:
    - Nombre del Titular: Teniente Coronel FREDY BAUTISTA GARCIA
    - Domicilio: *AV EL DORADO No. 75 25 BARRIO MODELIA BOGOTÀ D.C.*

- Teléfono(s):
- Correo electrónico: dijin.adepe-gridi@policia.gov.co

2.2. ¿Hay en su país una unidad o entidad encargada específicamente de procesar jurídicamente la comisión de delitos cibernéticos? Sí ( ) No (X)

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: _____
- Institución de la que depende: _____
- Información de contacto:
  - Nombre del Titular: _____
  - Domicilio: _____
  - Teléfono(s): _____ Fax: _____
  - Correo electrónico: _____

2.3. ¿Ha establecido su país páginas en Internet para facilitar que los ciudadanos cuenten con información para prevenir ser víctimas de delitos cibernéticos y para detectarlos y denunciarlos ante las autoridades competentes cuando ellos ocurran? Sí (X) No ( )

En caso afirmativo, sírvase proveer las direcciones en Internet respectivas, y una descripción breve de las mismas:

www.internetsano.gov.co/
Es un espacio virtual que permite a los navegantes en internet tener una hoja de ruta que minimiza los riesgos existentes en la red
www.delitosinformaticos.gov.co/
Espacio virtual que permite la interacción de la Policía Nacional con la ciudadanía generando un ambiente virtual que facilita la interpretación de conductas reprochables y la orientación para tener el acceso a la administración de justicia para la respectiva investigación penal.

2.4. ¿Ha desarrollado y/o implementado su país una estrategia nacional de seguridad cibernética? Sí (X) No ( )
En caso afirmativo, sírvase describir brevemente en que consiste esa estrategia:

El documento busca generar lineamientos de política en ciberseguridad1 y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

[1] Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

III. COOPERACIÓN INTERNACIONAL

3.1. ¿Se ha adherido su país a la Convención del Consejo de Europa sobre Delincuencia Cibernética? Sí ( ) No (X)

En caso negativo, ¿ha considerado su país la aplicación de los principios contenidos en dicha Convención? Sí (X) No ( ) No Conozco ( )

En caso afirmativo, sírvase expresar en qué ha consistido dicha consideración: LA ADECUACIÓN DE LAS NORMAS SUSTANTIVAS O LA TIPIFICACIÓN DE CONDUCTAS CON EL REFERENTE DE LAS NORMAS MÍNIMAS ESTABLECIDAS EN EL CONVENIO SOBRE CIBERSEGURIDAD.

3.2. ¿Se ha vinculado su país a la Red de Emergencia de Contactos sobre Delitos de Alta Tecnología 24 horas/7 días" del G-8? Sí ( ) No (X)

En caso negativo, ¿ha tomado su país alguna(s) medida(s) para vincularse?

Sí ( ) No (X) No Conozco ( )

En caso afirmativo, sírvase expresar en qué han consistido esas medidas: _____
_____

3.3. ¿Cuenta su país con legislación que permita dar trámite a las solicitudes de asistencia mutua de otros Estados para la obtención de pruebas electrónicas?

Sí (X) No ( ) No Conozco ( )

En caso afirmativo, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjuntar copia, de preferencia electrónica, de las mismas:

LEY 906 DE 2004 – código procedimiento penal - Artículo 484 al 489
http://www.secretariasenado.gov.co/senado/basedoc/ley/2004/ley_09060_204a.html

3.4. ¿Ha formulado o recibido su país solicitudes de asistencia mutua para la investigación o juzgamiento de delitos cibernéticos o bien para la obtención de pruebas electrónicas y la realización de otros actos necesarios para facilitar la investigación o juzgamiento de estos delitos? Sí (X) No ( ) No Conozco ( )

En caso afirmativo, sírvase indicar el número de solicitudes que ha formulado y/o recibido y el estado en que se encuentran dichas solicitudes: _____
_____

IV. CAPACITACIÓN

4.1. ¿Ofrece su país capacitación a los funcionarios responsables de la aplicación de la legislación contra el delito cibernético y para la obtención de pruebas electrónicas?

Sí (X) No ( )

En caso afirmativo, sírvase describir brevemente el tipo de capacitación y el número de funcionarios capacitados:

- Bajo la coordinación de la Dirección de Investigación Criminal e INTERPOL se ha desarrollado el curso denominado "ATENCION A INCIDENTES INFORMATICOS" donde se han capacitado a 90 funcionario de la policía nacional en la investigación de conductas que afectan la información y los datos y en mejores y prácticas para la recolección, identificación y procesamiento de evidencia digital.

- Bajo la coordinación del programa ICITAP se ha desarrollado el curso "Delitos Informáticos" donde se capacitan funcionarios de policía judicial de la Policía Nacional y Cuerpo técnico de investigación y está enfocado al ámbito legislativo y manejo de evidencia digital.

4.2. ¿Ofrece su país capacitación a los fiscales en delito cibernético y para la obtención de pruebas electrónicas? Sí (x) No ( )

- En coordinación con la ICITAP, se realizan los cursos denominado "DELITOS INFORMÁTICOS" y "ACTOS DE INVESTIGACION" donde se han capacitan fiscales y funcionarios de Policía Judicial.

4.3. De acuerdo con los esfuerzos de su país para ofrecer capacitación en la investigación y persecución de los delitos que involucren el uso de computadoras e Internet, sírvase describir las metas de su país para los próximos dos años y las condiciones necesarias para alcanzar esas metas:

La iniciativa de ciberseguridad consiste en el diseño de una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan al país.

Se desarrollará a través de tres ejes de trabajo. El primero consiste en la creación de las instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional. El segundo, es el fortalecimiento de la legislación relativa a la materia y la cooperación internacional asociada y el tercero es el que busca el fomento de programas de capacitación especializada en la materia.

Dos de los ejes de trabajo mencionados, todos ellos recogidos en el documento CONPES 3701 de 2011, estarán liderados por el Ministerio de Defensa Nacional.

En cuanto al primero, estamos creando y organizando las siguientes instancias:

1. Grupo de Respuesta a Emergencias Cibernéticas de Colombia-colCERT. Este es un grupo interdisciplinario cuya misión central será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad. Este grupo estará compuesto por personal militar, funcionarios civiles del Ministerio de Defensa y de otras entidades como el Ministerio de las Tecnologías de la información y las Comunicaciones.

2. El Comando Conjunto Cibernético – CCOC. Es el organismo que deberá prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales.

3. El Centro Cibernético Policial – CCP, el cual estará encargado de la ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos. Desarrollará labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país. Recibirá y atenderá los lineamientos nacionales en ciberseguridad y trabajará de forma coordinada con el colCERT.

En lo que hace a los programas de capacitación, se iniciarán en el 2012 un proyecto piloto con el Comité Interamericano Contra el Terrorismo de la Organización de Estados Americanos – CICTE en temas de seguridad de la información para funcionarios del Estado. Igualmente, se adelantarán otras capacitaciones que se enfocarán al sector privado.

Este plan piloto se ha ido planeando durante los últimos meses e involucrará funcionarios del Ministerio de Defensa y la Policía Nacional, así como de la Presidencia de la República, Ministerio de Relaciones Exteriores, de la Fiscalía General de la Nación, del Ministerio de Tecnologías de la Información y las Comunicaciones, de la Comisión de Regulación de Comunicaciones, del Departamento Nacional de Planeación, del Departamento Administrativo Seguridad – D.A.S y de la nueva agencia de inteligencia.

Vale la pena mencionar que el Ministerio de Defensa Nacional ha designado para esta iniciativa la suma de $16.428.444.328.oo para el cuatrienio, suma que no incluye el personal destinado para el efecto. Esta suma se dividirá de la siguiente manera:

2011	2012	2013	2014
$ 1.428.444.328	$ 5.400.000.000	$ 5.000.000.000	$4.600.000.000

4.4. ¿Ha participado su país en los talleres de capacitación celebrados en el marco del Grupo de Trabajo en Delito Cibernético? Sí (x) No ( )

En caso afirmativo, sírvase describir brevemente las personas que han participado; si estos talleres han ofrecido capacitación útil, y cómo los participantes han aplicado esta capacitación en el ejercicio de sus funciones: Se han capacitado funcionarios de la policía Judicial de la Policía Nacional, Cuerpo Técnico de Investigación y ministerio interior y de justicia y la capacitación ha sido en el marco del desarrollo de las investigaciones relacionadas con delitos informáticos relacionadas con Terrorismo, fraude bancario, pornografía infantil, trata de personas, hurto entre otras y reformas que se han realizado a la legislación Colombiana con referencia a la protección de la información y de los datos como la ley 1273 de 2009.

4.5. Sírvanse proporcionar recomendaciones sobre los temas que debieran incorporarse en los talleres de capacitación del Grupo de Trabajo para los próximos dos años relacionados con el delito cibernético y las pruebas electrónicas:

- Diseñar estrategias que permitan desarrollar a las universidades de nuestro país programas de capacitación contra la lucha del delito cibernético.

- Se deberían incorporar capacitaciones enfocadas al análisis forense en dispositivos de almacenamiento digital.

4.6. En el marco de las REMJA, sírvase proporcionar recomendaciones acerca de cómo el Grupo de Trabajo en Delito Cibernético puede ayudar mejor a su país en el desarrollo o mejoramiento de su capacidad para enfrentar los delitos relacionados con las computadoras y el Internet:

- Coordinar mecanismos que permitan establecer canales de cooperación que permitan reducir los tiempos de respuesta ante los proveedores de servicios en Estados Unidos.

- Implementar Programas de Capacitación para Jueces y fiscales del país, con el objetivo de fortalecer el soporte jurídico de las investigaciones que se adelantan en el país.

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: COLOMBIA
(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:
( ) Sr.: JUAN MIGUEL GÓMEZ VALENCIA
( ) Sra.:_____
Título/cargo: COORDINACIÓN DE LUCHA CONTRA LOS ILÍCITOS TRANSNACIONALES Y AMAENAZAS A LA SEGURIDAD
Organismo/oficina: DIRECCIÓN DE ASUNSTOS POLÍTICOS MULTILATERALES
MINISTERIO DE RELACIONES EXTERIORES
Domicilio: CALLE 10 No. 5-51
Número de teléfono: 57 (1) 3814285
MJ00585S01

Número de fax:
Correo electrónico: juanmiguel.gomez@cancilleria.gov.co