

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

OEA/Ser.K/XXXIV
CIBER-VII/doc.2/11
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 Séptima 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.

Este cuestionario es sustancialmente similar al documento que se envió en noviembre de 2009, con antelación a la Sexta Reunión del Grupo de Trabajo en Delito Cibernético, y a la cual su país respondió en su momento. Para facilitar la elaboración del presente cuestionario, la respuesta de su país al cuestionario anterior se anexa a este documento.

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 () No (x) |



En caso afirmativo, sírvase describir brevemente y adjuntar copias, de preferencia electrónica, de esa legislación:

Código Procesal Penal, artículo 236 ("El juez podrá ordenar, mediante auto fundado, la intervención de comunicaciones telefónicas o cualquier otro medio de comunicación del imputado, para impedir las o conocerlas. Bajo las mismas condiciones, el Juez podrá ordenar también la obtención de los registros que hubiere de las comunicaciones del imputado o de quienes se comunicaran con él...").

Código Procesal Penal de la Nación:

http://www.infojus.gov.ar/_pdf/codigos/grt_codigo_ppenal.pdf

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: **División Delitos en Tecnologías y Análisis Criminal de la Policía Federal Argentina**
- Institución de la que depende: **Ministerio de Seguridad, Presidencia de la Nación**
- Información de contacto:
 - o Nombre del Titular: **Comisario Carlos Savaro**
 - o Domicilio: **Cavia 3350, piso 1º, Ciudad Autónoma de Buenos Aires**
 - o Teléfono(s): **(54-11) 4370-5899**
 - o Correo electrónico: **análisis_criminal@policiafederal.gov.ar**

- 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:
 - o Nombre del Titular: _____
 - o Domicilio: _____
 - o Teléfono(s): _____ Fax: _____
 - o 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 ()** No **(x)**

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

- 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:

Instalación y funcionamiento del Arcert

Creación del Programa de Protección de Infraestructuras Críticas

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:

Se ha modificado el Código Penal de la Nación y se han incorporado los tipos penales contenidos en la Convención de Budapest (Ley 26.388, promulgada el 24 de junio de 2008). En febrero de 2010, en el marco de la *Octopus Interface Conference*, Argentina hizo entrega al Consejo de Europa de un requerimiento para ser invitada a acceder a la Convención de Budapest. Dicha invitación fue recibida en el mes de septiembre de 2010. Se ha confeccionado un ante proyecto de reforma del Código Procesal Penal de la Nación en el que se receptan las reglas contenidas en la Convención de Budapest.

- 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 (x) No () No Conozco ()

En caso afirmativo, sírvase expresar en qué han consistido esas medidas: **ver la respuesta a 3.1.**

- 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:

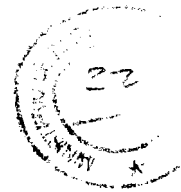
Ley 24.767 de Cooperación Internacional en Materia Penal.

http://www.infojus.gov.ar/index.php?kk_seccion=documento®istro=LEYNAC&docid=LEY%2520C%2520024767%25201996%252012%252018

- 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:

Argentina formula un promedio de diez (10) solicitudes anuales para la obtención de pruebas electrónicas para la investigación de todos los delitos previstos en el Código Penal. La Dirección de Asistencia Jurídica Internacional del Ministerio de Relaciones



Exteriores, Comercio Internacional y Culto (www.cooperación_penal.gov.ar - jgs@mrecic.gov.ar), es la autoridad de aplicación a través de la cual la autoridades judiciales formula sus solicitudes. Dicha Dirección no ha recibido solicitudes de asistencia mutua para la investigación o juzgamiento de delitos cibernéticos.

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:

En el marco del “Encuentro Internacional sobre Ciberdelito *Combate al Ciberdelito: Argentina y la Convención de Budapest*” se desarrolló la “Sesión Cerrada para Jueces y Fiscales *Delitos, ciberdelitos y prueba digital*”, el 14 de octubre de 2010, con la participación de Anthony Teelucksingh -Consejero Senior del Departamento de Justicia de EEUU-, Pedro Verdelho -Fiscal y Docente del Centro de Estudios Judiciales de Portugal y Cristina Schulman -Jefe de la Unidad de Ciberdelito del Consejo de Europa-.

Se desarrolló el “Seminario Iberoamericano sobre ciberdelito”, los días 6 y 7 de septiembre de 2011, organizado por la Conferencia de Ministros de justicia de los Países Iberoamericanos

- 4.2. ¿Ofrece su país capacitación a los fiscales en 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:

En el ámbito del Ministerio Público Fiscal de la Nación funciona una Fiscalía General encargada de la Capacitación de sus integrantes. Su titular y el Procurador General de la Nación forman parte del Consejo Directivo de la Carrera de Especialización en Ministerio Público que se dicta en la Facultad de Derecho de la Universidad de Buenos Aires, en el marco de la cual se dicta la materia “Delitos Informáticos”. Al margen, en el ámbito de la Procuración General de la Nación se dictan seminarios específicos sobre “Delitos Informáticos”

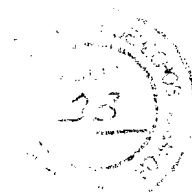
- 4.3. De acuerdo con los esfuerzos de su país para ofrecer capacitación en la investigación y persecución de los delitos que involucren el uso de computadoras e Internet, sírvase describir las metas de su país para los próximos dos años y las condiciones necesarias para alcanzar esas metas:

Argentina se plantea como meta para los próximos dos años

(a) acceder a la Convención de Budapest;

(b) vincularse a la Red de Emergencia de Contactos sobre Delitos de Alta Tecnología 24 horas/7 días” del G-8;

(c) crear un Centro de Orientación y Análisis sobre delitos Informáticos;



- 6 -

- (d) formular protocolos de actuación para las fuerzas de seguridad y operadores judiciales para la obtención, custodia y tratamiento de la evidencia o prueba digital; y
- (e) continuar con la capacitación de miembros de fuerzas de seguridad y operadores judiciales en la temática vinculada con el delito cibernético.

- 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 () No Conozco ()

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: **Desde enero 2010 a la fecha, Argentina ha participado en: (a) "Taller Regional sobre la Investigación de Delitos a través de Internet a Gran Escala", organizado por la Secretaría General de la Organización de Estados Americanos (OEA) y el Departamento de Justicia de Estados Unidos, 31 de agosto al 2 de septiembre de 2010, realizado en Lima, Perú, la delegación estuvo compuesta por Daniel Petrone -juez-; Ricardo Sáenz -fiscal-; y Norberto Frontini -asesor de la Subsecretaría de Política Criminal-; y (b) "Taller Hemisférico de Seguridad y Crimen Cibernético", realizado en Miami, EUA, entre los días 9 y 13 de mayo de 2011, la delegación argentina estuvo compuesta por Daniel Petrone -juez-; Hernán Báez, Técnico Coordinador de la Coordinación de Emergencias en Redes Teleinformáticas (ArCERT); y Eduardo Martínez, Director de Aplicaciones de la Oficina Nacional de las Tecnologías de la Información (ONTI) y Responsable de la ArCERT. Ambos talleres ofrecieron capacitación útil.**

- 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:

- (a) últimas modalidades delictivas en cibercrimen;
- (b) requerimientos para la obtención de prueba digital por parte de los operadores judiciales;
- (c) obtención de prueba digital por parte de las fuerzas de seguridad;
- (d) armonización de la ley de fondo y de forma sobre ciberdelito y cooperación internacional;
- (e) formación de miembros de fuerzas de seguridad y de operadores judiciales en la investigación de ciberdelitos y en investigación de delitos con prueba digital involucrada;
- (f) vinculación entre el sector público y privado a nivel regional respecto de la cuestión del ciberdelito y la obtención de evidencia 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:

Argentina considera de fundamental importancia la realización, a nivel regional, de talleres exclusivos sobre ciberdelito para fuerzas de seguridad; de talleres exclusivos para operadores judiciales -fiscales y jueces-; de talleres para la evaluación, la modernización y, en su caso, la proyección de legislación de fondo y de forma vinculada con el ciberdelito; y la confección de un manual de buenas prácticas o de un

protocolo de actuación para miembros de las fuerzas de seguridad -con intervención de expertos-.

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: Argentina

(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:

Sr.: Norberto Federico Frontini

Título/cargo: Asesor

Organismo/oficina: Subsecretaría de Política Criminal, Secretaría de Justicia, Ministerio de Justicia y Derechos Humanos

Domicilio: Sarmiento 329, Piso 4º (1041AAG) Buenos Aires, República Argentina

Número de teléfono: (54-11) 5300-4027

Número de fax: (54-11) 5300-4027

Correo electrónico: nfrontini@jus.gov.ar/nfrontini@fibertel.com.ar