

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

OEA/Ser.K/XXXIV  
CIBER-VI/doc.3/09  
17 noviembre 2009  
Original: inglés

Sexta Reunión del Grupo de Trabajo en Delito Cibernético  
21 y 22 de Enero de 2010  
Washington, D.C.

**CUESTIONARIO PREPARATORIO  
DE LA SEXTA 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, 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 tres áreas temáticas: (1) Legislación; (2) Órganos Unidades Especializadas; y (3) Cooperación Internacional.

Teniendo en cuenta lo anterior, sírvanse remitir la respuesta de su Estado al presente cuestionario, a más tardar el **10 de diciembre de 2009**, a la Secretaría General de la OEA (Departamento de Cooperación Jurídica de la Secretaría de Asuntos Jurídicos), al correo electrónico [LegalCooperation@oas.org](mailto: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 adoptado su país legislación para prevenir, investigar y sancionar el delito cibernético?  
Sí ( X ) No ( )

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

***Ley 11.179, Ley 11.723, Ley 23.984, Ley 25.326, Ley 26.388***

***Como anexo al presente cuestionario se adjuntan, en un CD, los textos correspondientes a las citadas leyes.***

- 1.2. ¿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 (sírvese enumerarlas): _____                        | Sí ( X ) | No ( ) |

En aquellos casos afirmativos, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjunte copia, de preferencia electrónica, de las mismas:

***Las normas y medidas fueron citadas en el punto 1.1 y adjuntadas como Anexo del presente cuestionario.***

Si su país ha tipificado alguna de las anteriores conductas, mencione brevemente los resultados que se han obtenido al respecto, tales como procesos judiciales en curso y sus resultados:

***Debido a la que la normativa ha sido recientemente sancionada se desconoce el resultado de las actuaciones judiciales, pero se han dictado sentencias condenatorias en casos de distribución de pornografía infantil por Internet iniciadas con anterioridad a la modificación actual.***

En caso de que su país no haya tipificado alguna de las anteriores conductas, indique si está desarrollando algunas acciones para hacerlo:

- 1.3. ¿Ha adoptado su país la legislación sustantiva y procesal u otras medidas necesarias para asegurar la obtención y conservación de pruebas electrónicas de cualquier delito? Sí ( X )  
No ( )

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

***La obtención y conservación de pruebas se realiza acorde a lo estipulado en la Ley 23.984 (Código Procesal Penal de la Nación) y se establece mediante protocolos de especialistas en la materia***

- 1.4. ¿Ha adoptado su país la legislación sustantiva y procesal u otras medidas necesarias para permitir la admisibilidad en los procesos y juicios penales de pruebas electrónicas? Sí ( X )  
No ( )

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

***La admisibilidad de prueba se establece de acuerdo a lo estipulado en la Ley 23.984 (Código Procesal Penal de la Nación) y la Ley 11.179 (Código Penal Nacional)***

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

- a) Requerir a una persona en su territorio a proporcionar información en su poder o control almacenada en un sistema o dispositivo informático? Sí ( X ) No ( )
- b) Requerir a un proveedor (p. ej. de Internet) que ofrezca sus servicios en su territorio a proporcionar información en su poder o control relativos a sus abonados o clientes en relación con tales servicios? Sí ( X ) No ( )

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

***La obtención de esta información se concreta a través de la autoridad judicial que posee amplias facultades para requerir los datos necesarios, y en su caso la potestad de ordenar allanamientos, secuestros y pericias forenses pertinentes en caso de ser necesario, conforme a la normativa existente en el Código Procesal Penal de la Nación (en el ámbito Federal) y de los respectivos Códigos Procesales de las Provincias que integran el territorio Argentino.***

- 1.6. ¿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 ( )
- c) Preservar la integridad de los datos informáticos almacenados? Sí ( X ) No ( )
- d) Hacer inaccesibles o suprimir los datos del sistema consultado? Sí ( X ) No ( )

En aquellos casos afirmativos, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjunte copia, de preferencia electrónica, de las mismas:

***La normativa que rige en estos casos es la ley 23984 (Código Penal Procesal de la Nación) que se adjunta como Anexo al presente cuestionario.***

- 1.7. ¿Ha adoptado su país la legislación sustantiva y procesal u otras medidas necesarias que permitan a sus autoridades competentes obtener e interceptar información relativa al tráfico y contenido de comunicaciones específicas transmitidas en su territorio a través de sistemas informáticos? Sí ( X ) No ( )

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

***Conforme a lo dispuesto por la Ley N° 23984. La misma se adjunta como Anexo al presente cuestionario***

## II. UNIDADES ESPECIALIZADAS

- 2.1. ¿Ha establecido su país unidades o entidades encargadas específicamente de investigar y perseguir delitos cibernéticos? Sí ( X ) No ( )

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: *División Delitos en Tecnologías y Análisis Criminal*
- Institución de la que depende: *Policía Federal Argentina*
- Información de contacto:
  - o Nombre del Titular: *Subcomisario Carlos Gregorio SAVARO*
  - o Domicilio: *Cavia 3350, Piso 1ro., Ciudad Autónoma de Buenos Aires, Argentina*
  - o Teléfono(s): *54 (011) 4800-1120* Fax: *54 (011) 4370-5899*
  - o Correo electrónico: *delitosentecnologias@policiafederal.gov.ar*

- 2.2. ¿Ha establecido su país unidades o entidades encargadas 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. ¿Qué medidas ha adoptado su país para fomentar las relaciones entre las autoridades responsables de la investigación y persecución de delitos cibernéticos y el sector privado, especialmente con aquellas empresas proveedoras de servicios de tecnología de la información y las comunicaciones, en particular de servicios de Internet?

***Las áreas especializada en la materia, comprende entre sus funciones la realización de Seminarios, Cursos, Charlas dirigidas a miembros del Poder Judicial de la Nación, como así también a agentes de las Fuerzas de Seguridad, conjuntamente con los referentes del sector privado(Microsoft, Terra, Telefonica de Argentina, TELECOM, Fibertel, etc). Estas capacitaciones se realizan con el objeto de articular estos ámbitos, estrechar sus vínculos y proponer medidas consensuadas y coordinadas de acción.***

***Asimismo, ante requisitorias judiciales, las fuerzas especializadas solicitan información a la ISP para investigar crímenes de esta naturaleza.***

### 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 ( )

En caso afirmativo, sírvase desarrollar en qué ha consistido dicha consideración:

***Entre otras consideración, cabe mencionar que Argentina ha asumido la Presidencia del Grupo de Trabajo Latinoamericano sobre delito tecnológico de INTERPOL***

- 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 (X ) No ( )

En caso negativo, ¿ha tomado su país alguna(s) medida(s) para vincularse? Sí ( ) No ( )

En caso afirmativo, sírvase desarrollar en qué ha(n) consistido tal(es) medida(s):

***La Red de Emergencia de Contactos sobre Delitos de Alta Tecnología 24 horas/7 días, del G-8, se encuentra a cargo del Departamento de INTERPOL dependiente en Argentina, de Policía Federal.***

¿Cuenta su país con legislación u otras medidas que permitan dar trámite a las solicitudes de asistencia mutua de otros Estados, que de acuerdo con su derecho interno, tengan facultades para la investigación o juzgamiento de delitos cibernéticos? Sí (X ) No ( )

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

***Surgen de los Tratados de Extradición, Tratados Internacionales en Materia Penal y cooperación Judicial recíproca existente con cada país.***

- 3.3. ¿Cuenta su país con legislación u otras medidas que permitan dar trámite a las solicitudes de asistencia mutua de otros Estados para la obtención de pruebas electrónicas y la realización de otros actos necesarios para facilitar la investigación o juzgamiento de delitos cibernéticos? Sí (X ) No ( )

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

***Surge de la facultad que tienen los Jueces Nacionales, tal como ya se ha dejado constancia en los puntos 1.5 y 3.2, y también conforme a los Tratados de asistencia mutua celebrados entre Argentina y otros países***

- 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 ( )

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

***Se tiene conocimiento de requerimientos por medio de exhortos o rogatorias internacionales.***

#### 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:

***La capacitación consiste en Seminarios, Charlas y Cursos que se dictan al interior del país, asimismo los funcionarios responsables en la materia, reciben formación en el exterior (en Alemania, España, Estados Unidos)***

- 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 fiscales capacitados:

***A los fiscales que abordan los delitos cibernéticos, entre otros, se les brinda capacitación tal como se ha planteado anteriormente.***

- 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:

***Continuar con las capacitaciones en las distintas áreas involucradas, fortalecer la articulación entre los distintos ámbitos competentes (Poder Judicial, Poder Ejecutivo, Fuerzas de Seguridad).***

- 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:

***Las delegaciones Argentinas han sido tradicionalmente compuestas por funcionarios de diversos sectores gubernamentales, responsables en la materia. Los principios acordados en los sucesivos encuentros han sido considerados en el diagrama de la política nacional.***

- 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:

***Protocolos de actuación en referencia al decomiso, investigación, conservación de la información en relación a las áreas específicas de informática forenses.***

***Incorporar inventario de las conductas y modalidades de delito cibernético más frecuentes en los Estados Miembros***

- 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:

***-Elaborar Guías de buenas prácticas en materia de delitos cibernéticos por parte de los Estados Miembros.***

***-Fomentar el Intercambio de experiencias identificar los desafíos y avances en la materia***

***-Solicitar a la OEA la confección de Informe anuales con el reporte de los casos y los procedimientos derivados de las mismas.***

**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.: Carlos Gregorio Savaro

( ) Sra.: \_\_\_\_\_

Título/cargo: Subcomisario

Organismo/oficina: Policía Federal Argentina, División Delitos en Tecnologías y Análisis Criminal

Domicilio: Cavia 3350, piso 1º, Ciudad Autónoma de Buenos Aires, Argentina

Número de teléfono: 54 (011) 48001120

Número de fax: 54(011) 43705899

Correo electrónico: [delitosentecnologias@policiafederal.gov.ar](mailto:delitosentecnologias@policiafederal.gov.ar)