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 cuatro áreas temáticas: (1) Legislación; (2) Órganos Unidades Especializadas; (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 **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 o al número de fax: + (202) 458-3598.

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:
Código Penal:
Artículo 207-A.- Delito Informático
Artículo 207-B.- Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras.
Artículo 207-C.- Delito informático agravado.
Artículo 181-A.- Turismo sexual infantil
Artículo 183-A.- Pornografía infantil
Artículo 186.- delito de Hurto Agravado, específicamente el inciso 3): "Mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas".

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 ( )	No (X)
f) Falsificación informática	Sí ( )	No (X)
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 ( )

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:

En la legislación peruana dentro del Título V – Delitos contra el Patrimonio, en el Capítulo X del Código Penal, se desarrolla los delitos informáticos, que recogen en apenas 2 artículos las modalidades enunciadas en los items a, b, c y d, pero no se encuentran tipificados en tipos penales independientes, es un conglomerado de acciones que recogen estos dos artículos 207-A y 207-B mencionados en 1.1.

En caso de que su país no haya tipificado alguna de las anteriores conductas, indique si está desarrollando algunas acciones para hacerlo:
Como se comentó en el Taller Regional de Legislación Cibernética llevado a cabo en la ciudad de Asunción – Paraguay del 13 al 15 de octubre de 2009, a nivel del Congreso de la República del Perú existe un predictamen favorable, sin embargo, dado el cambio de legislatura en julio de 2009, la nueva comisión no ha vuelto a tocar el tema. En esta propuesta legislativa, se acogía las modalidades descritas en el Convenio de Budapest.

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 ( ) No (X).

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 () No (X)

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 ( ) No (X)
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 de ser afirmativo, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjunte copia, de preferencia electrónica, de las mismas:
Articulo 230° del Código Procesal Penal de 2004, aprobado mediante Decreto Legislativo N° 957, trata sobre la intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación.

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 informático? Sí ( ) No (X)
b) Copiar y conservar los datos informáticos consultados? Sí ( ) No (X)
c) Preservar la integridad de los datos informáticos almacenados? Sí ( ) No (X)
d) Hacer inaccesibles o suprimir los datos del sistema consultado? Sí ( ) No (X)

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: _____

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 ( ) No (X).

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

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 de Investigación de Delitos de Alta Tecnología
- Institución de la que depende: Dirección de Investigación Criminal y de Apoyo a la Justicia de la Policía Nacional del Perú
- Información de contacto:
  - Nombre del Titular: Jefe DIVINDAT – Coronel PNP – Oscar William Gonzales Rabanal.
  - Domicilio: AV. España N° 323 Mezanine-Edificio "Alcides Vigo Hurtado" – Cercado de Lima – Perú.
  - Teléfono (s): 511 – 4318898/ 511 – 980122062
  - Correo electrónico: www.policiainformatica.gob.pe
    delitosinformaticos@policiainformatica.gob.pe
    fraudes@policiainformatica.gob.pe
    pornografiainfantil@policiainformatica.gob.pe
    piratería@policiainformatica.gob.pe

2.2 ¿Ha establecido su país unidades o entidades encargadas específicamente de procesar jurídicamente la comisión de delitos cibernéticos? Sí ( ) No (X)

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?

Perú no ha adoptado medidas para fomentar las relaciones entre las autoridades responsables de la investigación y persecución de delitos cibernéticos y el sector privado.

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 ( )

3.2 ¿Se ha vinculado su país a la Red de Emergencia de Contactos sobre Delitos de Alta Tecnología 24 Horas/7días 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) medidas: la institución encargada de estas medidas es la Divindat.

¿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:
Artículo 511° del Código Procesal Penal de 2004, aprobado mediante Decreto Legislativo N° 957, que regula sobre los Actos de Cooperación Judicial Internacional que se pueden realizar vía asistencia mutua.

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/o otras medidas existentes al respecto y adjunte copia, de preferencia electrónica, de las mismas:
Sobre el tema de Asistencia Judicial Internacional nuestra legislación procesal – Código Procesal Penal de 2004, aprobado mediante Decreto Legislativo N° 957, prevé en el Libro Séptimo, Sección Tercera el desarrollo de todo el procedimiento de la asistencia mutua desde el artículo 528 al 539 de dicho cuerpo normativo.

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 ( ) No ( ).

Las solicitudes de asistencia mutua se canalizan a través del Ministerio Público, que es la autoridad central.

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 ( ) No (X)

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

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:

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:
La suscrita, Fernanda Ayasta Nassif ha participado en 2 talleres: el primero se realizó en la ciudad de Bogotá- Colombia en setiembre del 2008 y el segundo en la ciudad de Asunción-Paraguay en octubre de 2009. La capacitación recibida ha sido muy útil, tanto así que este año 2009 se realizó en la Comisión de Justicia y Derechos Humanos del Congreso de la República un predictamen modificando diversos artículos del Código Penal para adecuar nuestra legislación al ciber crimen.

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 la pruebas electrónicas:

- Incentivar la firma de convenios de asistencia mutua internacional específicamente para el tema del ciber crimen.
- El recojo y conservación de la pruebas para este tipo de delitos.

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:

Definitivamente el primer paso a dar es en materia legislativa, sea sustantiva y procesal, adecuarla a las conductas delictivas del ciber crimen, modificar la legislación procesal para prever de forma específica la forma de conservación de material informático o tecnológico o

virtual. Otra forma es que se fomente la suscripción de convenios entre países para el tema de la asistencia mutua internacional.

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: **Perú**
(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:
Sra.: **Fernanda Isabel Ayasta Nassif**
Título/cargo : **Asesora de la Alta Dirección**
Organismo/oficina : **Ministerio de Justicia**
Domicilio: **Calle Carlos Tenaud cuadra 3 – Miraflores – Lima – Perú.**
Número de teléfono: 511-4227517 / 511-990395538
Número de fax : 511-
Correo electrónico : **fayasta@minjus.gob.pe**