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.

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: Codigo Penal y Procesal Penal

LEGISLACION PENAL DEL PARAGUAY

CODIGO PENAL

Artículo N° 174 - Alteración de datos
1º El que lesionando el derecho de disposición de otro sobre datos los borrara, suprimiera, inutilizara o cambiara, será castigado con pena privativa de libertad de hasta dos años o con multa.

2º En estos casos, será castigada también la tentativa.

3º Como **datos, en el sentido del inciso 1º, se entenderán sólo aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible**.

Artículo N° 146 - Violación del secreto de la comunicación
1º El que, sin consentimiento del titular:

1. abriera una **carta cerrada** no destinada a su conocimiento;

2. abriera una **publicación (escrito, cinta portadora de sonido e imágenes, reproducciones y demás medio de registros)**, en los términos del artículo 14, inciso 3º, que se encontrara cerrada o depositada en un recipiente cerrado destinado especialmente a guardar de su conocimiento dicha publicación, o que procurara, para sí o para un tercero, el conocimiento del contenido de la publicación;

3. lograra mediante medios técnicos, **sin apertura del cierre**, conocimiento del contenido de tal publicación para sí o para un tercero, será castigado con pena privativa de libertad de hasta un año o con multa.

2º La persecución penal dependerá de la instancia de la víctima. Se aplicará lo dispuesto en el artículo 144, inciso 5º, última parte.

Artículo 144: Lesión del Derechos de la comunicación e imagen. El que sin consentimiento del afectado **escuchara mediante instrumentos técnicos** o **grabara o almacenara** técnicamente o hiciera mediante **instalaciones técnicas inmediatamente accesible a un tercero**. Produjera o transmitiera imágenes dentro de su recinto privado.

Artículo N° 174 - Alteración de datos (interferencia)
1º El que lesionando el derecho de disposición de otro sobre datos los **borrara, suprimiera, inutilizara o cambiara**, será castigado con pena privativa de libertad de hasta dos años o con multa.

2º En estos casos, será castigada también la tentativa.

3º Como datos, en el sentido del inciso 1º, se entenderán sólo aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible.

Artículo N° 175 - Sabotaje de computadoras
1º El que **obstaculizara un procesamiento de datos** de importancia vital para una empresa o establecimiento ajenos, o una entidad de la administración pública mediante:

1. un hecho punible según el artículo 174, inciso 1º; o

2. la **destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra parte accesoria vital**, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2º En estos casos, será castigada también la tentativa.

Artículo N° 248 - Alteración de datos relevantes para la prueba
1º El que con la intención de inducir al error en las relaciones jurídicas, almacenara o adulterara datos en los términos del artículo 174, inciso 3º, relevantes para la prueba de tal manera que, en caso de percibirlos se presenten como un documento no auténtico, será castigado con pena privativa de libertad de hasta cinco años o con multa.
2º En estos casos, será castigada también la tentativa.
3º En lo pertinente se aplicará también lo dispuesto en el artículo 246, inciso 4º

Artículo N° 249 - Equiparación para el procesamiento de datos
La manipulación que perturbe un procesamiento de datos conforme al artículo 174, inciso 3º, será equiparada a la inducción al error en las relaciones jurídicas

Artículo N° 253 - Destrucción o daño a documentos o señales
1º El que con la intención de perjudicar a otro:

1. destruyera, dañara, ocultara o de otra forma suprimiera un documento o una graficación técnica, en contra del derecho de otro a usarlo como prueba;

2. borrara, suprimiera, inutilizara o alterara, en contra del derecho de disposición de otro, datos conforme al artículo 174, inciso 3º, con relevancia para la prueba; o

3. destruyera o de otra forma suprimiera mojones u otras señales destinadas a indicar un límite o la altura de las aguas, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2º En estos casos, será castigada también la tentativa.

Artículo N° 188 - Operaciones fraudulentas por computadora
1º El que con la intención de obtener para sí o para otro un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante:

1. **programación falsa**;

2. utilización de datos falsos o incompletos;

3. utilización indebida de datos; o

4. otras influencias **indebidas sobre el procesamiento**, y con ello, perjudicara el patrimonio de otro, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2º En estos casos, se aplicará también lo dispuesto en el artículo 187, incisos 2º al 4º.

Ley 3440/07 - Pornografía relativa a niños y adolescentes. "**Art. 140**: El que por **cualquier medio produjere publicaciones** que contengan como temática actos sexuales…"

Art. 143: Lesión a la intimidad de las personas. : El que **mediante publicación expusiera la intimidad de otro…..**

PROPIEDAD INTELECTUAL

ART. 184a: Violación del Derecho del Autor y hechos conexos

ART. 184b: Violación de los Derechos de Marca

ART. 184c: Violación sobre los Derechos de Dibujos y Diseños Industriales

CODIGO PROCESAL PENAL

Artículo N° 200 - INTERVENCIÓN DE COMUNICACIONES
El juez podrá ordenar por resolución fundada, bajo pena de nulidad, la intervención de las comunicaciones del imputado, cualquiera sea el medio técnico utilizado para conocerlas.

El resultado sólo podrá ser entregado al juez que lo ordenó, quien procederá según lo indicado en el artículo anterior; podrá ordenar la versión escrita de la grabación o de aquellas partes que considere útiles y ordenará la destrucción de toda la grabación o de las partes que no tengan relación con el procedimiento, previo acceso a ellas del Ministerio Público, del imputado y su defensor.

La intervención de comunicaciones será excepcional.

Artículo N° 199 - APERTURA Y EXAMEN DE CORRESPONDENCIA
Recibida la correspondencia o los objetos interceptados, el juez procederá a su apertura haciéndolo constar

en acta.

Examinará los objetos y leerá para sí el contenido de la correspondencia. Si guardan relación con el procedimiento ordenará el secuestro; en caso contrario, mantendrá en reserva su contenido y dispondrá la entrega al destinatario.

Artículo N° 198 - INTERCEPCIÓN Y SECUESTRO DE CORRESPONDENCIA Siempre que sea útil para la averiguación de la verdad, el juez ordenará, por resolución fundada, bajo pena de nulidad, la intercepción o el secuestro de la correspondencia epistolar, telegráfica o de cualquier otra clase, remitida por el imputado o destinada a él, aunque sea bajo nombre supuesto.

Artículo N° 192 - OPERACIONES TÉCNICAS
Las restricciones establecidas para el allanamiento de domicilios o habitaciones no regirán para las oficinas administrativas o edificios públicos, templos o lugares religiosos, establecimientos militares, lugares comerciales de reunión o de esparcimiento, abiertos al público y que no estén destinados a habitación familiar. En estos casos se podrá prescindir de la orden de allanamiento con el consentimiento expreso y libre de las personas a cuyo cargo estén los locales. En caso de negativa o imposibilidad material de conseguir el consentimiento, se requerirá la orden de allanamiento y se podrá hacer uso de la fuerza policial para su cumplimiento.

Quien prestó el consentimiento será invitado a presenciar el registro.

Para el ingreso y registro de oficinas dependientes de un poder del Estado se necesitará autorización del funcionario competente.

Si durante el desarrollo del procedimiento, quien dio la autorización, la niega o expresa haberla consentido por coacción, la prueba de la libertad del consentimiento corresponderá a quien lo alega.

En el acta respectiva se consignarán los requisitos previstos por este código y el consentimiento otorgado.

Artículo N° 183 - REGISTRO

Cuando haya motivo suficiente que permita suponer que en un lugar público existen indicios del hecho punible investigado o la presencia de alguna persona fugada o sospechosa, si no es necesaria una orden de allanamiento, la policía realizará directamente el registro del lugar.

Cuando sea necesario realizar una inspección personal o el registro de un mueble o compartimento cerrado destinado al uso personal, en lugar público, regirán análogamente los artículos que regulan el procedimiento de la inspección de vehículos y personas.

Artículo N° 173 - LIBERTAD PROBATORIA
Los hechos y circunstancias relacionados con el objeto del procedimiento podrán ser admitidos por cualquier medio de prueba, salvo las excepciones previstas por las leyes.

Un medio de prueba será admitido si se refiere, directa o indirectamente, al objeto de la investigación y es útil para el descubrimiento de la verdad. El juez o tribunal limitará los medios de prueba ofrecidos cuando ellos resulten manifiestamente excesivos.

Artículo N° 192 OPERACIONES TECNICAS y

Artículo N° 193 - ENTREGA DE COSAS Y DOCUMENTOS. Secuestros. Los objetos y documentos relacionados con el hecho punible y los sujetos a comiso, que puedan ser importantes para la investigacion, seran tomadas en deposito o asegurados y conservados del mejor modo posible. Aquel que tenga en su poder objetos o documentos de los senalados, estara obligado a presentarlos y entregarlos cuando le sea requerido...Si los objetos requeridos no son entregados se dispondra su secuestro.

Para mayor eficacia y calidad de los registros e inspecciones**, se podrán ordenar operaciones técnicas o científicas, reconocimientos y reconstrucciones**.

Artículo N° 228 - INFORMES

El juez y el Ministerio Público podrán requerir informes a cualquier persona o entidad pública o privada.

Los informes se solicitarán verbalmente o por escrito, indicando el procedimiento en el cual se requieren, el nombre del imputado, el lugar donde debe ser entregado el informe, el plazo para su presentación y las consecuencias previstas para el incumplimiento del deber de informar.

Resolución 1134/2006 " Reglamento del Servicio de Acceso Internet"

Art. 17: " El Prestador instalará en el país, un **sistema de gestión**, cuyo propósito es la gestión técnica y administrativa del servicio. El sistema deberá registrar al menos:

1 Habitación/deshabilitación, de estaciones del usuario, velocidad de transmisión, volumen de tráfico, datos de facturación. Se deberá **mantener archivos históricos** de los registros.

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

2	Acceso ilícito	Sí ( )	No (x)
3	Interceptación ilícita	Sí (x)	No ( )
4	Ataques a la integridad de datos	Sí (x)	No ( )
5	Ataques a la integridad de sistemas	Sí (x)	No ( )
6	Abuso de dispositivos	Sí ( )	No (X)
7	Falsificación informática	Sí (X)	No ( )
8	Fraude informático	Sí (X)	No ( )
9	Pornografía infantil	Sí (X)	No ( )
10	Delitos contra la propiedad intelectual y derechos afines	Sí (X)	No ( )
11	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: Interceptacion ilicita, art. 146 y 144; Atentados contra la integridad de los datos art. 174; Atentado contra la integridad del sistema art. 175 y 249; Falsedad informatica art. 248, 249 y 253; Estafa informatica art.188; Pornografia infantil Ley 3440, art. 140; Delitos contra la propiedad intelectual ley 3440 art. 184.

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: Se han obtenido resultados positivos con la persecusion y condena de los imputados, en especial en los casos de Pornografia infantil y los hechos punibles contra la propiedad intelectual, que son los mas frecuentes, en menor grado se dieron casos de alteracion de datos y sabotaje en computadoras.

En caso de que su país no haya tipificado alguna de las anteriores conductas, indique si está desarrollando algunas acciones para hacerlo: Actualmente se encuentra en el Parlamento Nacional para su estudio un Proyecto de Ley presentado recientemente, que amplia el Codigo Penal y tipifica ciertas conductas como: Acceso ilicito, Falsificacion de tarjetas de credito y debito, Abuso de dispositivos y se amplian otros articulos ya previstos como el de Pornografia Infantil, Interceptacion indebida de datos.

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:
Codigo Procesal Penal.

Artículo N° 200 - INTERVENCIÓN DE COMUNICACIONES
El juez podrá ordenar por resolución fundada, bajo pena de nulidad, la intervención de las comunicaciones del imputado, cualquiera sea el medio técnico utilizado para conocerlas.

El resultado sólo podrá ser entregado al juez que lo ordenó, quien procederá según lo indicado en el artículo anterior; podrá ordenar la versión escrita de la grabación o de aquellas partes que considere útiles y ordenará la destrucción de toda la grabación o de las partes que no tengan relación con el procedimiento, previo acceso a ellas del Ministerio Público, del imputado y su defensor.

La intervención de comunicaciones será excepcional.

Artículo N° 199 - APERTURA Y EXAMEN DE CORRESPONDENCIA
Recibida la correspondencia o los objetos interceptados, el juez procederá a su apertura haciéndolo constar en acta.

Examinará los objetos y leerá para sí el contenido de la correspondencia. Si guardan relación con el procedimiento ordenará el secuestro; en caso contrario, mantendrá en reserva su contenido y dispondrá la entrega al destinatario.

Artículo N° 198 - INTERCEPCIÓN Y SECUESTRO DE CORRESPONDENCIA Siempre que sea útil para la averiguación de la verdad, el juez ordenará, por resolución fundada, bajo pena de nulidad, la intercepción o el secuestro de la correspondencia epistolar, telegráfica o de cualquier otra clase, remitida por el imputado o destinada a él, aunque sea bajo nombre supuesto.

Artículo N° 192 - OPERACIONES TÉCNICAS
Las restricciones establecidas para el allanamiento de domicilios o habitaciones no regirán para las oficinas administrativas o edificios públicos, templos o lugares religiosos, establecimientos militares, lugares comerciales de reunión o de esparcimiento, abiertos al público y que no estén destinados a habitación familiar. En estos casos se podrá prescindir de la orden de allanamiento con el consentimiento expreso y libre de las personas a cuyo cargo estén los locales. En caso de negativa o imposibilidad material de conseguir el consentimiento, se requerirá la orden de allanamiento y se podrá hacer uso de la fuerza policial para su cumplimiento.

Quien prestó el consentimiento será invitado a presenciar el registro.

Para el ingreso y registro de oficinas dependientes de un poder del Estado se necesitará autorización del funcionario competente.

Si durante el desarrollo del procedimiento, quien dio la autorización, la niega o expresa haberla consentido por coacción, la prueba de la libertad del consentimiento corresponderá a quien lo alega.

En el acta respectiva se consignarán los requisitos previstos por este código y el consentimiento otorgado.

Artículo N° 183 - REGISTRO

Cuando haya motivo suficiente que permita suponer que en un lugar público existen indicios del hecho punible investigado o la presencia de alguna persona fugada o sospechosa, si no es necesaria una orden de allanamiento, la policía realizará directamente el registro del lugar.

Cuando sea necesario realizar una inspección personal o el registro de un mueble o compartimento cerrado destinado al uso personal, en lugar público, regirán análogamente los artículos que regulan el procedimiento de la inspección de vehículos y personas.

Artículo N° 192 OPERACIONES TECNICAS y

Artículo N° 193 - ENTREGA DE COSAS Y DOCUMENTOS. Secuestros. Los objetos y documentos relacionados con el hecho punible y los sujetos a comiso, que puedan ser importantes para la investigacion, seran tomadas en deposito o asegurados y conservados del mejor modo posible. Aquel que tenga en su poder objetos o documentos de los senalados, estara obligado a presentarlos y entregarlos cuando le sea requerido...Si los objetos requeridos no son entregados se dispondra su secuestro.

Para mayor eficacia y calidad de los registros e inspecciones**, se podrán ordenar operaciones técnicas o científicas, reconocimientos y reconstrucciones**.

Artículo N° 228 - INFORMES
El juez y el Ministerio Público podrán requerir informes a cualquier persona o entidad pública o privada.

Los informes se solicitarán verbalmente o por escrito, indicando el procedimiento en el cual se requieren, el nombre del imputado, el lugar donde debe ser entregado el informe, el plazo para su presentación y las consecuencias previstas para el incumplimiento del deber de informar.

Resolución 1134/2006 " Reglamento del Servicio de Acceso Internet"

Art. 17: " El Prestador instalará en el país, un **sistema de gestión**, cuyo propósito es la gestión técnica y administrativa del servicio. El sistema deberá registrar al menos:

1 Habitación/deshabilitación, de estaciones del usuario, velocidad de transmisión, volumen de tráfico, datos de facturación. Se deberá **mantener archivos históricos** de los registros.

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: Ya mencionado, e igualmente el Art, 173 del CPP hace referencia a la LIBERTAD PROBATORIA, expresando que cualquier medio de prueba sera admitido si se refiere directa o indirectament, al objeto de la investigacion y es util para el descubrimiento de la verdad, siempre que no vulneren garantias procesales consagrados en la Constitucion Nacional, en el Derecho Internacional vigente y las leyes.

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

12 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 ( )

13 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: El reglamento del 2006, "

Reglamento del Servicio de Acceso Internet"

Art. 17: " El Prestador instalará en el país, un **sistema de gestión**, cuyo propósito es la gestión técnica y administrativa del servicio. El sistema deberá registrar al menos:
Habitación/deshabilitación, de estaciones del usuario, velocidad de transmisión, volumen de tráfico, datos de facturación. Se deberá **mantener archivos históricos** de los registros. Ley por la que se le obliga a las empresas prestadoras de servicios de telefonia movil al registro de datos del usuario, a la guarda de datos de trafico por el termino de seis meses.; Codigo Procesal Penal, por la que las empresas publicas y privadas tienen la obligacion de proporcionar los datos que les sean solicitados por el Juez y Fiscal, dentro de una investigacion penal, art. 228 del Codigo de Procedimientos Penales **- INFORMES:** El juez y el Ministerio Público podrán requerir informes a cualquier persona o entidad pública o privada. Los informes se solicitarán verbalmente o por escrito, indicando el procedimiento en el cual se requieren, el nombre del imputado, el lugar donde debe ser entregado el informe, el plazo para su presentación y las consecuencias previstas para el incumplimiento del deber de informar.

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 ( ) No (x)

14 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: Especificamente la legislacion procesal no hace referencia al secuestro de sistemas o dispositivos de almacenamieno informatico, sin embargo se menciona en el **Artículo 193 CPP Los objetos y documentos relacionados al hecho punible y sujetos a comiso que puedan ser importantes para la investigacion seran tomados en deposito o asegurados y conservados del mejor modo posible,Art. 195, art. 183 Registros , Art. 196 Operaciones tecnicas para registros.** Las empresas de telefonia movil, tienen la obligacion legal de guarda de datos de trafico por el termino de 6 meses, asi como tambien el registro de datos del usuario.

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: **art. 198 INTERCEPCIÓN Y SECUESTRO DE CORRESPONDENCIA** Siempre que sea útil para la averiguación de la verdad, el juez ordenará, por resolución fundada, bajo pena de nulidad, la intercepción o el secuestro de la correspondencia epistolar, telegráfica **o de cualquier otra clase,** remitida por el imputado o destinada a él, aunque sea bajo nombre supuesto

II. UNIDADES ESPECIALIZADAS

2.1. ¿Ha establecido su país unidades o entidades encargadas específicamente de investigar

y perseguir delitos cibernéticos? Sí ( ) No (x) Sin embargo si existen en el Ministerio Publico de Paraguay, Unidades especializadas de delitos contra menores, entre los que se encuentra Pornografia Infantil, y tambien de Delitos Marcarios y Derechos Intelectuales, esta por concretarse el proyecto la creacion de una Unidad especializada en Delitos Informaticos, tambien en el Ministerio Publico.

En caso afirmativo, sírvase proporcionar la siguiente información:

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

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:

18 Nombre de la unidad o instancia: _____
19 Institución de la que depende: _____
20 Información de contacto:
- Nombre del Titular: _____
- Domicilio: _____
- Teléfono(s): _____ Fax: _____
- 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? Se dieron acuerdos entre las telefonias moviles y el Ministerio Publico. Se han firmado acuerdos con las empreas de Telefonia movil, que en la mayoria tambien prestan servicios de Internet. Sin embargo, es necesario fomentar acuerdos mas efectivos.

II. 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: Los

equipos de trabajo que participaron de los cursos del REMJA, han recomendado a la institucion que representan la necesidad de formar parte del mismo. Igualmente se han realizado paralelismos de la legislacion paraguaya con la Convencion, y en el Proyecto en estudio en el Parlamento se tiene como modelo dicho convenio.

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 ( )

En caso afirmativo, sírvase desarrollar en qué ha(n) consistido tal(es) medida(s): Actualmente el Paraguay ya cuenta con un CSIRT Nacional que se encuentra en el Ministerio Publico, con la intervencion de varias instituciones del Estado, e igualmente se tiene en proyecto coordinar el trabajo tambien en el Ministerio Publico, para formar parte de la red, a traves de la creacion de la Unidad Especializada en Delitos informaticos.

¿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 ( ) No (x) Sin embargo si existen tratados bilaterales y multilaterales firmados entre varios paises que promueven la cooperacion internacional, dejando abierto los tipos penales y no limitando especificamente a delitos ciberneticos, existen acuerdos en otras areas donde tambien pueden guardar relacion con la obtencion de evidencia electronica como por ejemplo terrorismo, crimen organizado, narcotrafico, tratados de extradición donde se dejan abiertos los tipos penales por los cuales se puede extraditar a personas.

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

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 ( ) No (x)

En caso afirmativo, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjunte copia, de preferencia electrónica, de las mismas: Sin embargo, se han firmando tratados y convenios, que dejan abierto tipos penales, y tambien en los cuales se pueden obtener evidencia electronica, como el tratado contra terrorismo, crimen organizado, narcotrafico.

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: Solicitudes a Colombia, las que se encuentran finiquitadas como en el caso del secuestro de la señorita Cecilia Cubas (se han realizado video conferencia con varios paises entre ellos Espana y Chile), se han realizado procesos de extradicion por casos de pornografia infantil,

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 ( )

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

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: Han sido capacitados funcionarios del Ministerio Publico de Paraguay, a traves del Remja, en el exterior y tambien en Paraguay. Igualmente es importante mencionar que son capacitados en la Unidad de Trata de Personas y Pornografia infantil, asi como en el de Derechos Intelectuales, a traves del Centro de Entrenamiento del Ministerio Publico, que capacita fiscales desde su designacion pasando por mallas curriculares, a traves de modulos de capacitacion en diversas areas. Tambien, han sido capacitados funcionarios del Ministerio Publico a traves del Centro de entrenamiento, sobre clonacion de tarjetas, igualmente se está preparando en el Centro de Entrenamiento del MP un modulo especial sobre delitos ciberneticos y evidencia electronica (en proyecto), a los efectos de capacitar a fiscales y demas funcionarios de la fiscalia de Paraguay.-

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: Promover desde el Ministerio Publico de Paraguay, que es el organismo constitucional encargado de la investigacion y persecusion de hecho punibles, la sancion de leyes armonizadas y acordes con los standares mencionados en los acuerdos internacionales, para asi lograr una efectiva cooperacion internacional, evitando tambien asi la doble incriminacion. Promover la Creacion de una Unidad Especializada en Delitos informaticos. Lograr la capacitacion de la mayor cantidad posible de fiscales a traves del Centro de Entrenamiento y la ayuda de organismos

internacionales, apoyando tambien la capacitacion de funcionarios de la policia. (en lo que respecta en tipificacion y adecuacion de conducta, socializacion de los acuerdos internacionales en esta materia, obtencion de evidencia electronica, digital, presentacion en juicio), trabajo coordinado del CSIRT Py con la Unidad Especializada cuando la magnitud del evento suscitado asi lo requiera.

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: Fiscal Maria Teresa Aguirre, Diputado Nacional Sebastian Acha, Licenciada Maria Ines Lippman, Ingeniero Santiago Vazquez, Abogada Sandra Otazu (asesora parlamentaria), Abogado Pablo Cuevas (asesor del Ministerio del Interior).

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: Intensificar la parte procesal, asi como los diferentes tipos de evidencias que pueden obtenerse, forma de obtencion de las evidencias y pruebas, (relaciones con el sector privado, google, gmail, hotmail, yahoo etc.,) Relaciones con otras redes de cooperacion internacional. Efectuar ejercicios practicos.

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: Realizando constantes capacitaciones y facilitando la cooperacion para la obtencion de evidencias de empresas que se encuentran en el extranjero.

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado:
_Paraguay_____
(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:
( ) Sr.:_____
(x) Sra.:_____
Título/cargo: _____
Organismo/oficina: _____
Domicilio: _____
_____
Número de teléfono: _____
Número de fax: _____

Correo electrónico: _____