

Octava Reunión del Grupo de Trabajo en Delito Cibernético

**CUESTIONARIO PREPARATORIO  
DE LA OCTAVA REUNIÓN DEL GRUPO DE TRABAJO EN DELITO CIBERNÉTICO**

INTRODUCCIÓN

El presente cuestionario busca recolectar información útil para los propósitos de la Octava Reunión del Grupo de Trabajo en Delito Cibernético, la cual se celebrará a principios de 2014, en relación con las recomendaciones que han sido formuladas en las reuniones anteriores 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 cinco áreas temáticas: (I) Legislación; (II) Cooperación internacional; (III) Unidades especializadas y esfuerzos nacionales; (IV) Resultados de investigaciones y enjuiciamientos en materia de delito cibernético; y (V) Capacitación.

Teniendo en cuenta lo anterior, sírvase remitir la respuesta de su Estado al presente cuestionario, a más tardar el **martes 10 de diciembre de 2013**, 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

A. LEGISLACIÓN SUSTANTIVA:

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

- |                                                              |               |
|--------------------------------------------------------------|---------------|
| a) Acceso ilícito                                            | Sí (X) No ( ) |
| b) Interceptación ilícita                                    | Sí ( ) No (X) |
| 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 (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 ( ) |

- Obtención y utilización no autorizada de información

En caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica, de la legislación: *Se adjunta legislación correspondiente.* \_\_\_\_\_

1.2. ¿Ha promulgado su país legislación que:

a) Tipifique la tentativa de comisión de cualquiera de las modalidades de delito cibernético enumeradas arriba? Sí (X) No ( )

En caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica, de la legislación: *Se adjunta legislación correspondiente.* \_\_\_\_\_

b) Tipifique la complicidad y la instigación en la comisión de cualquiera de las modalidades de delito cibernético enumeradas arriba? Sí (X) No ( )

En caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica, de la legislación: *Se adjunta legislación correspondiente.* \_\_\_\_\_

c) Contemple posibilidad de responsabilidad institucional por delitos cibernéticos, es decir, legislación según la cual puede hacerse responsables a personas morales por delitos penales de tipo cibernético? Sí ( ) No (X)

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

\_\_\_\_\_

#### B. LEGISLACIÓN PROCESAL:

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

En caso afirmativo, sírvase describir esos esfuerzos: *Se adjunta legislación correspondiente.* \_\_\_\_\_

1.4. ¿Permite la legislación 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 describir brevemente las normas y/u otras medidas existentes al respecto y adjuntar copia, de preferencia electrónica, de las mismas: \_\_\_\_\_

\_\_\_\_\_

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

a) Confiscar, decomisar o secuestrar sistemas o dispositivos de almacenamiento informático? Sí (X) No ( )

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

En caso afirmativo, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjuntar copia, de preferencia electrónica, de las mismas: *Se adjunta legislación correspondiente.* \_\_\_\_\_

## II. COOPERACIÓN INTERNACIONAL

2.1. ¿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 ( )

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

Sí ( ) No ( ) No lo sé ( )

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

2.2. ¿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 lo sé ( )

En caso afirmativo, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjuntar copia, de preferencia electrónica, de las mismas: *Se adjunta legislación correspondiente.* \_\_\_\_\_

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

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

## III. UNIDADES ESPECIALIZADAS Y ESFUERZOS NACIONALES

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: \_\_\_\_\_
- Institución de la que depende: \_\_\_\_\_

- Dirección en internet de la unidad o instancia: \_\_\_\_\_
- Información de contacto: \_\_\_\_\_
  - o Nombre del titular: \_\_\_\_\_
  - o Domicilio: \_\_\_\_\_
  - o Teléfono(s): \_\_\_\_\_ Fax: \_\_\_\_\_
  - o Correo electrónico: \_\_\_\_\_

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: \_\_\_\_\_
- Institución de la que depende: \_\_\_\_\_
- Dirección en internet de la unidad o instancia: \_\_\_\_\_
- Información de contacto: \_\_\_\_\_
  - o Nombre del titular: \_\_\_\_\_
  - o Domicilio: \_\_\_\_\_
  - o Teléfono(s): \_\_\_\_\_ Fax: \_\_\_\_\_
  - o Correo electrónico: \_\_\_\_\_

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

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

\_\_\_\_\_

3.4. ¿Ha implementado su país algún programa de probidad o creación de conciencia sobre los riesgos del delito cibernético, o ha producido manuales o guías para orientar y alertar a la ciudadanía sobre los riesgos del delito cibernético y formas para evitar convertirse en víctima del mismo? Sí ( ) No ( )

En caso afirmativo, sírvase proveer una descripción breve de dichos programas, manuales o guías: \_\_\_\_\_

\_\_\_\_\_

#### IV. RESULTADOS DE INVESTIGACIONES Y ENJUICIAMIENTOS EN MATERIA DE DELITO CIBERNÉTICO

4.1. Sírvase indicar el número de **investigaciones** que ha realizado su país con respecto a cada uno de los siguientes delitos cibernéticos o conductas desde enero de 2012 hasta la fecha:

- |                                        |                                  |
|----------------------------------------|----------------------------------|
| a) Acceso ilícito                      | Número de investigaciones: _____ |
| b) Interceptación ilícita              | Número de investigaciones: _____ |
| c) Ataques a la integridad de datos    | Número de investigaciones: _____ |
| d) Ataques a la integridad de sistemas | Número de investigaciones: _____ |



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

- 5.2. ¿Ofrece su país capacitación a los fiscales sobre delito cibernético y obtención de pruebas electrónicas? Sí ( ) No ( )

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

- 5.3. ¿Ofrece su país capacitación a los jueces sobre delito cibernético y obtención de pruebas electrónicas? Sí ( ) No ( )

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

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: \_\_\_\_\_

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

( ) Sr.: \_\_\_\_\_

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

Título/cargo: \_\_\_\_\_

Organismo/oficina: \_\_\_\_\_

Domicilio: \_\_\_\_\_  
\_\_\_\_\_

Número de teléfono: \_\_\_\_\_

Número de fax: \_\_\_\_\_

Correo electrónico: \_\_\_\_\_

Octava Reunión del Grupo de Trabajo en Delito Cibernético

**CUESTIONARIO PREPARATORIO  
DE LA OCTAVA REUNIÓN DEL GRUPO DE TRABAJO EN DELITO CIBERNÉTICO**

INTRODUCCIÓN

El presente cuestionario busca recolectar información útil para los propósitos de la Octava Reunión del Grupo de Trabajo en Delito Cibernético, la cual se celebrará a principios de 2014, en relación con las recomendaciones que han sido formuladas en las reuniones anteriores 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 cinco áreas temáticas: (I) Legislación; (II) Cooperación internacional; (III) Unidades especializadas y esfuerzos nacionales; (IV) Resultados de investigaciones y enjuiciamientos en materia de delito cibernético; y (V) Capacitación.

Teniendo en cuenta lo anterior, sírvase remitir la respuesta de su Estado al presente cuestionario, a más tardar el **martes 10 de diciembre de 2013**, 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

A. LEGISLACIÓN SUSTANTIVA:

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

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

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

---

1.2. ¿Ha promulgado su país legislación que:

a) Tipifique la tentativa de comisión de cualquiera de las modalidades de delito cibernético enumeradas arriba? Sí ( ) No ( )

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

\_\_\_\_\_

b) Tipifique la complicidad y la instigación en la comisión de cualquiera de las modalidades de delito cibernético enumeradas arriba? Sí ( ) No ( )

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

\_\_\_\_\_

c) Contemple posibilidad de responsabilidad institucional por delitos cibernéticos, es decir, legislación según la cual puede hacerse responsables a personas morales por delitos penales de tipo cibernético? Sí ( ) No ( )

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

\_\_\_\_\_

**B. LEGISLACIÓN PROCESAL:**

1.3. 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: \_\_\_\_\_

\_\_\_\_\_

1.4. ¿Permite la legislación 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 ( )

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

\_\_\_\_\_

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

a) Confiscar, decomisar o secuestrar sistemas o dispositivos de almacenamiento informático? Sí ( ) No ( )

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

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

\_\_\_\_\_

## II. COOPERACIÓN INTERNACIONAL

2.1. ¿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 lo sé ( )

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

*Nota: El anterior [punto de contacto](#) entre FISCALIA GENERAL DEL ESTADO y la OEA realizó un trámite para vincularnos a la red pero como dicho funcionario renunció no sabemos en que situación esta el trámite.*

2.2. ¿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 lo sé ( )

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

*1.- Convención Interamericana sobre Asistencia Mutua en Materia Penal (Nassau -1992).*

*2.- Convención de las Naciones Unidas contra la Delincuencia Organizada Transaccional – PALERMO 2000.*

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

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

Desde el año 2012 hasta noviembre 2013 se han recibido DOS solicitudes de asistencia mutua.

Año 2012 UN CASO - Contra la Propiedad Intelectual y Seguridad informática.  
Año 2013 UN CASO – Apropiación Ilicita por medios informáticos.

### III. UNIDADES ESPECIALIZADAS Y ESFUERZOS NACIONALES

- 3.1. ¿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: DIRECCION DE INVESTIGACIONES
- Institución de la que depende: FISCALIA GENERAL DEL ESTADO
- Dirección en internet de la unidad o instancia:
- Información de contacto: Ing. Javier Leon
  - o Nombre del titular: Coronel Alain Gonzalo Luna
  - o Domicilio: \_\_\_\_\_
  - o Teléfono(s): (593-2) 2985800 ext. 174159 Fax: \_\_\_\_\_
  - o Correo electrónico: luna@fiscalia.gob.ec --- leonj@fiscalia.gob.ec

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: \_\_\_\_\_
- Institución de la que depende: \_\_\_\_\_
- Dirección en internet de la unidad o instancia: \_\_\_\_\_
- Información de contacto: \_\_\_\_\_
  - o Nombre del titular: \_\_\_\_\_
  - o Domicilio: \_\_\_\_\_
  - o Teléfono(s): \_\_\_\_\_ Fax: \_\_\_\_\_
  - o Correo electrónico: \_\_\_\_\_

- 3.3. ¿Ha establecido su país páginas en internet para facilitar que los ciudadanos cuenten con información para evitar 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: \_\_\_\_\_

\_\_\_\_\_

- 3.4. ¿Ha implementado su país algún programa de probidad o creación de conciencia sobre los riesgos del delito cibernético, o ha producido manuales o guías para orientar y alertar a la ciudadanía sobre los riesgos del delito cibernético y formas para evitar convertirse en víctima del mismo? Sí ( ) No (X)

En caso afirmativo, sírvase proveer una descripción breve de dichos programas, manuales o guías: \_\_\_\_\_

Nota: En lo que se refiere a Delitos Informáticos relacionados con la BANCA (sustracción de dinero no autorizado) la Superintendencia de Bancos y la Asociación de Bancos Privados y la propia banca ha generado programas para crear conciencia sobre los riesgos de los delitos informáticos.

#### IV. RESULTADOS DE INVESTIGACIONES Y ENJUICIAMIENTOS EN MATERIA DE DELITO CIBERNÉTICO

4.1. Sírvase indicar el número de **investigaciones** que ha realizado su país con respecto a cada uno de los siguientes delitos cibernéticos o conductas desde enero de 2012 hasta la fecha:

- |                                                              |                                  |
|--------------------------------------------------------------|----------------------------------|
| a) Acceso ilícito                                            | Número de investigaciones: _____ |
| b) Interceptación ilícita                                    | Número de investigaciones: _____ |
| c) Ataques a la integridad de datos                          | Número de investigaciones: _____ |
| d) Ataques a la integridad de sistemas                       | Número de investigaciones: _____ |
| e) Abuso de dispositivos                                     | Número de investigaciones: 1.225 |
| f) Falsificación informática                                 | Número de investigaciones: _____ |
| g) Fraude informático                                        | Número de investigaciones: 1.210 |
| h) Pornografía infantil                                      | Número de investigaciones: 12    |
| i) Delitos contra la propiedad intelectual y derechos afines | Número de investigaciones: _____ |

La informaciónn enviada cubren solamente las investigaciones relacionadas a los items: e, f, g y h.

Las cifras corresponde al año 2012 y agosto 31 del 2013.

En las cifras del item g) se incluyen dos items: f y g.

Nota: Es importante indicar que a la fecha se esta discutiendo en la Asamblea Nacional un NUEVO CODIGO DE INTEGRACION PENAL en el cual ya se tipifica ciertas modalidades de Delitos Cibernéticos. Con esta nueva tipificación de los delitos cibernéticos se podra lograr una mejor colaboración e intercambio de informacion con los diferentes paises miembros de la OEA.

4.2. Si su país ha tipificado cualquiera de los delitos cibernéticos a que se refiere la pregunta 1.1 anterior, sírvase indicar el número de **enjuiciamientos** que ha realizado su país con respecto a cada uno de los delitos cibernéticos correspondientes, desde enero de 2012 hasta la fecha, así como el número de casos que dieron lugar a una **condena**:

- |                                     |                          |                |
|-------------------------------------|--------------------------|----------------|
| a) Acceso ilícito                   | Casos enjuiciados: _____ | Condenas _____ |
| b) Interceptación ilícita           | Casos enjuiciados: _____ | Condenas _____ |
| c) Ataques a la integridad de datos | Casos enjuiciados: _____ | Condenas _____ |

- |                                                              |                         |               |
|--------------------------------------------------------------|-------------------------|---------------|
| d) Ataques a la integridad de sistemas                       | Casos enjuiciados: ____ | Condenas ____ |
| e) Abuso de dispositivos                                     | Casos enjuiciados: ____ | Condenas ____ |
| f) Falsificación informática                                 | Casos enjuiciados: ____ | Condenas ____ |
| g) Fraude informático                                        | Casos enjuiciados: ____ | Condenas ____ |
| h) Pornografía infantil                                      | Casos enjuiciados: ____ | Condenas ____ |
| i) Delitos contra la propiedad intelectual y derechos afines | Casos enjuiciados: ____ | Condenas ____ |

- 4.3. ¿Han enfrentado alguna dificultad con respecto a la investigación o el enjuiciamiento de estos delitos? Sí () No ( )

En caso afirmativo, sírvase proveer una descripción detallada y específica del tipo de dificultades que se han enfrentado: [falta de colaboración internacional para obtener información. No hay una respuesta rápida y oportuna. Así como los delincuentes cibernéticos actúan sin fronteras así debemos actuar nosotros en la investigación de los delitos.](#)

- 4.4. ¿Existen ámbitos relativos al combate del delito cibernético en que su país podría beneficiarse de cooperación técnica suministrada por otros Estados miembros?

Sí () No ( )

En caso afirmativo, sírvase proveer una descripción detallada y específica del tipo de cooperación técnica que podría ser benéfica para su país:

- 1.- [Intercambio de información, con organismos internacionales que a la fecha luchan contra el delito cibernético.](#)
- 2.- [Buscar convenios internacional que permitan desarrollar un trabajo más eficiente durante la investigación de los delitos informáticos.](#)
- 3.- [Aprovechar la infraestructura de ciertos organismos ya establecidos que lucha contra el crimen cibernético.](#)
- 4.- [Buscar que la Fiscalía General del Estado tenga un mayor nivel participativo en las futuras Reuniones del Grupo de Trabajo en Delito Cibernético.](#)

## V. CAPACITACIÓN

- 5.1. ¿Ofrece su país capacitación sobre delito cibernético y sobre la obtención de pruebas electrónicas a los funcionarios responsables de la aplicación de la legislación?

Sí ( ) No ( )

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

\_\_\_\_\_

- 5.2. ¿Ofrece su país capacitación a los fiscales sobre delito cibernético y obtención de pruebas electrónicas? Sí () No ( )

En caso afirmativo, sírvase describir brevemente el tipo de capacitación y el número de funcionarios capacitados: La Fiscalía General del Estado organizó un Seminario relacionado a Ciber Espacio y sus Peligros al cual asistieron Fiscales a nivel nacional; sin embargo consideramos necesario y urgente capacitar a los Fiscales en temas que crecen y se expanden aceleradamente como son los DELITOS CIBERNETICOS y lo mas importante capacitar en COMO OBTENER LAS PRUEBAS O EVIDENCIAS DIGITALES. El Fiscal además de conocer el MARCO LEGAL debe estar capacitado en como obtener las evidencias y pruebas para poder desarrollar su trabajo.

- 5.3. ¿Ofrece su país capacitación a los jueces sobre delito cibernético y obtención de pruebas electrónicas? Sí ( ) No ( )

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

\_\_\_\_\_

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: ECUADOR

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

(x) Sr.: CESAR CUESTA

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

Título/cargo: Asistente Tecnologic – Delitos Informáticos

Organismo/oficina: FISCALIA GENERAL DEL ESTADO

Domicilio: Av. Patria y 12 de Octubre - QUITO

Número de teléfono: (593-2) 3985800 EXT. 173166

Número de fax: \_\_\_\_\_

Correo electrónico: [cuestac@fiscalia.gob.ec](mailto:cuestac@fiscalia.gob.ec)

Octava Reunión del Grupo de Trabajo en Delito Cibernético

**CUESTIONARIO PREPARATORIO  
DE LA OCTAVA REUNIÓN DEL GRUPO DE TRABAJO EN DELITO CIBERNÉTICO**

INTRODUCCIÓN

El presente cuestionario busca recolectar información útil para los propósitos de la Octava Reunión del Grupo de Trabajo en Delito Cibernético, la cual se celebrará a principios de 2014, en relación con las recomendaciones que han sido formuladas en las reuniones anteriores 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 cinco áreas temáticas: (I) Legislación; (II) Cooperación internacional; (III) Unidades especializadas y esfuerzos nacionales; (IV) Resultados de investigaciones y enjuiciamientos en materia de delito cibernético; y (V) Capacitación.

Teniendo en cuenta lo anterior, sírvase remitir la respuesta de su Estado al presente cuestionario, a más tardar el **martes 10 de diciembre de 2013**, 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

A. LEGISLACIÓN SUSTANTIVA:

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

- |                                                              |               |
|--------------------------------------------------------------|---------------|
| a) Acceso ilícito                                            | Sí ( ) No ( ) |
| b) Interceptación ilícita                                    | Sí ( ) 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 ( ) |
| f) Falsificación informática                                 | Sí (x) No ( ) |
| g) Fraude informático                                        | Sí ( ) 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 caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica, de la legislación: \_\_\_\_\_

---

1.2. ¿Ha promulgado su país legislación que:

a) Tipifique la tentativa de comisión de cualquiera de las modalidades de delito cibernético enumeradas arriba? Sí ( ) No ( )

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

b) Tipifique la complicidad y la instigación en la comisión de cualquiera de las modalidades de delito cibernético enumeradas arriba? Sí ( ) No ( )

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

c) Contemple posibilidad de responsabilidad institucional por delitos cibernéticos, es decir, legislación según la cual puede hacerse responsables a personas morales por delitos penales de tipo cibernético? Sí ( ) No ( )

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

**B. LEGISLACIÓN PROCESAL:**

1.3. 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: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

1.4. ¿Permite la legislación 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 ( )

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

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

a) Confiscar, decomisar o secuestrar sistemas o dispositivos de almacenamiento informático? Sí ( ) No ( )

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

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

\_\_\_\_\_

## II. COOPERACIÓN INTERNACIONAL

2.1. ¿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 lo sé ( )

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

\_\_\_\_\_

2.2. ¿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 ( ) No ( **X** ) No lo sé ( )

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

\_\_\_\_\_

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

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

\_\_\_\_\_

## III. UNIDADES ESPECIALIZADAS Y ESFUERZOS NACIONALES

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: \_\_\_\_\_
- Institución de la que depende: \_\_\_\_\_
- Dirección en internet de la unidad o instancia: \_\_\_\_\_
- Información de contacto: \_\_\_\_\_
  - o Nombre del titular: \_\_\_\_\_
  - o Domicilio: \_\_\_\_\_
  - o Teléfono(s): \_\_\_\_\_ Fax: \_\_\_\_\_
  - o Correo electrónico: \_\_\_\_\_

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: \_\_\_\_\_
- Institución de la que depende: \_\_\_\_\_
- Dirección en internet de la unidad o instancia: \_\_\_\_\_
- Información de contacto: \_\_\_\_\_
  - o Nombre del titular: \_\_\_\_\_
  - o Domicilio: \_\_\_\_\_
  - o Teléfono(s): \_\_\_\_\_ Fax: \_\_\_\_\_
  - o Correo electrónico: \_\_\_\_\_

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

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

3.4. ¿Ha implementado su país algún programa de probidad o creación de conciencia sobre los riesgos del delito cibernético, o ha producido manuales o guías para orientar y alertar a la ciudadanía sobre los riesgos del delito cibernético y formas para evitar convertirse en víctima del mismo? Sí ( ) No ( )

En caso afirmativo, sírvase proveer una descripción breve de dichos programas, manuales o guías: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

#### IV. RESULTADOS DE INVESTIGACIONES Y ENJUICIAMIENTOS EN MATERIA DE DELITO CIBERNÉTICO

4.1. Sírvase indicar el número de **investigaciones** que ha realizado su país con respecto a cada uno de los siguientes delitos cibernéticos o conductas desde enero de 2012 hasta la fecha:

- |                                                              |                                  |
|--------------------------------------------------------------|----------------------------------|
| a) Acceso ilícito                                            | Número de investigaciones: _____ |
| b) Interceptación ilícita                                    | Número de investigaciones: _____ |
| c) Ataques a la integridad de datos                          | Número de investigaciones: _____ |
| d) Ataques a la integridad de sistemas                       | Número de investigaciones: _____ |
| e) Abuso de dispositivos                                     | Número de investigaciones: _____ |
| f) Falsificación informática                                 | Número de investigaciones: _____ |
| g) Fraude informático                                        | Número de investigaciones: _____ |
| h) Pornografía infantil                                      | Número de investigaciones: _____ |
| i) Delitos contra la propiedad intelectual y derechos afines | Número de investigaciones: _____ |

4.2. Si su país ha tipificado cualquiera de los delitos cibernéticos a que se refiere la pregunta 1.1 anterior, sírvase indicar el número de **enjuiciamientos** que ha realizado su país con respecto a cada uno de los delitos cibernéticos correspondientes, desde enero de 2012 hasta la fecha, así como el número de casos que dieron lugar a una **condena**:

- |                                                              |                          |                |
|--------------------------------------------------------------|--------------------------|----------------|
| a) Acceso ilícito                                            | Casos enjuiciados: _____ | Condenas _____ |
| b) Interceptación ilícita                                    | Casos enjuiciados: _____ | Condenas _____ |
| c) Ataques a la integridad de datos                          | Casos enjuiciados: _____ | Condenas _____ |
| d) Ataques a la integridad de sistemas                       | Casos enjuiciados: _____ | Condenas _____ |
| e) Abuso de dispositivos                                     | Casos enjuiciados: _____ | Condenas _____ |
| f) Falsificación informática                                 | Casos enjuiciados: _____ | Condenas _____ |
| g) Fraude informático                                        | Casos enjuiciados: _____ | Condenas _____ |
| h) Pornografía infantil                                      | Casos enjuiciados: _____ | Condenas _____ |
| i) Delitos contra la propiedad intelectual y derechos afines | Casos enjuiciados: _____ | Condenas _____ |

*NOTA: En el Sistema SATJE de la Función Judicial los delitos informáticos se agrupan en un solo código, por lo cual no es posible definir la tipicidad en particular. De igual forma para solventar el requerimiento de “número de condenas”, según el departamento de Estadística del Consejo de la Judicatura, en la mayoría de los casos la información no ha sido registrada en el sistema SATJE. Sin embargo se anexa cuadro de causas ingresadas, resueltas y en trámite, según delitos informáticos, pornografía infantil y contra la propiedad intelectual.*

*( Fuente: Sistema de Automático de Trámites Judiciales del Ecuador SATJE Consejo de la Judicatura Dirección Nacional de Planificación- Subdirección Nacional de Estadística; Jefatura de Producción Estadística).*

4.3. ¿Han enfrentado alguna dificultad con respecto a la investigación o el enjuiciamiento de estos delitos? Sí ( ) No ( X ).

En caso afirmativo, sírvase proveer una descripción detallada y específica del tipo de dificultades que se han enfrentado: \_\_\_\_\_

4.4. ¿Existen ámbitos relativos al combate del delito cibernético en que su país podría beneficiarse de cooperación técnica suministrada por otros Estados miembros?

Sí ( ) No ( )

En caso afirmativo, sírvase proveer una descripción detallada y específica del tipo de cooperación técnica que podría ser benéfica para su país: \_\_\_\_\_  
\_\_\_\_\_

V. CAPACITACIÓN

- 5.1. ¿Ofrece su país capacitación sobre delito cibernético y sobre la obtención de pruebas electrónicas a los funcionarios responsables de la aplicación de la legislación?

Sí ( ) No ( X )

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

- 5.2. ¿Ofrece su país capacitación a los fiscales sobre delito cibernético y obtención de pruebas electrónicas? Sí ( ) No ( X )

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

- 5.3. ¿Ofrece su país capacitación a los jueces sobre delito cibernético y obtención de pruebas electrónicas? Sí ( ) No ( X )

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

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: República del Ecuador

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

( ) Sr.: Dr. Esteban Zavala Palacios

Título/cargo: Director Nacional de Asesoría Jurídica del Consejo de la Judicatura

Organismo/oficina: Consejo de la Judicatura

Domicilio: Jorge Washington E4-157 y Av. Amazonas

Número de teléfono: (02) 3953 600

Número de fax: (02) 3953 600

Correo electrónico: [www.función.judicial.gob.ec](http://www.función.judicial.gob.ec)

MJ00585E01

Consejo de la Judicatura de Ecuador

## I. LEGISLACIÓN

### A. LEGISLACIÓN SUSTANTIVA:

#### 1.1. Modalidades de delitos cibernéticos:

##### a) Acceso ilícito

Ley de Comercio Electrónico

**Art. 58.-** A continuación del artículo 202, inclúyanse los siguientes artículos innumerados:

**"Art. ..-** El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica. Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

##### c) y d) Ataques a la integridad de datos y ataques a la integridad de sistemas.

**Art. 61.-** A continuación del artículo 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

**"Art. ...-** Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

**Art. ...-** Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.

**Art. 62.-** A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos innumerados:

## **f) Falsificación informática**

**Art. 60.-** A continuación del artículo 353, agréguese el siguiente artículo innumerado:

**"Art. ...-** Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

- 1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
  - 2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
  - 3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.
- El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.

## **g) Fraude informático**

**"Art. ...-** Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

**Art. ...-** La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.

## **h) Pornografía infantil**

Código Penal

CAPITULO ...

DE LOS DELITOS DE EXPLOTACION SEXUAL

**(Artículo innumerado después del Art. 520) Art. ...-** Quien produjere, publicare o comercializare imágenes pornográficas, materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato, u organizare espectáculos en vivo, con escenas pornográficas en que participen los mayores de catorce y menores de dieciocho años, será reprimido con la pena de seis a nueve años de reclusión menor ordinaria, el comiso de los objetos y de los bienes producto del delito, la inhabilidad para el empleo, profesión u oficio.

Con la misma pena incurrirá quien distribuyere imágenes pornográficas, cuyas características externas hiciere manifiesto que en ellas sea grabado o fotografiado la exhibición de mayores de doce y menores de dieciocho años al momento de la creación de la imagen.

Con la misma pena será reprimido quien facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico en cuyas imágenes participen menores de edad.

Cuando en estas infracciones, la víctima sea un menor de doce años o discapacitado, o persona que adolece enfermedad grave incurable, la pena será de reclusión mayor extraordinaria de doce a dieciséis años, al pago de la indemnización, el comiso de los objetos y de los bienes producto del delito, a la inhabilidad del empleo, profesión u oficio; y, en caso de reincidencia, la pena será de veinticinco años de reclusión mayor especial.

Cuando el infractor de estos delitos sea el padre, la madre, los parientes hasta el cuarto grado de consanguinidad y segundo de afinidad, los tutores, los representantes legales, los curadores o cualquier persona del contorno íntimo de la familia, los ministros de culto, los maestros y profesores y, cualquier otra persona que por su profesión u oficio hayan abusado de la víctima, serán sancionados con la pena de dieciséis a veinticinco años de reclusión mayor extraordinaria, al pago de la indemnización, el comiso de los objetos y de los bienes producto del delito, a la inhabilidad del empleo, profesión u oficio.

Si la víctima fuere menor de doce años, se aplicará el máximo de la pena.

## **i) Delitos contra la Propiedad Intelectual**

### **LEY DE PROPIEDAD INTELECTUAL:**

#### Capítulo III

#### De los delitos y de las penas

**Art. 319.-** Será reprimido con prisión de tres meses a tres años y multa de mil trescientos catorce 45/100 (1.314,45) dólares de los Estados Unidos de América a trece mil ciento cuarenta y cuatro 50/100 (13.144,50) dólares de los Estados Unidos de América, tomando en consideración el valor de los perjuicios ocasionados, quien en violación de los derechos de propiedad intelectual, almacene, fabrique, utilice con fines comerciales, oferte en venta, venda, importe o exporte:

- a) Un producto amparado por una patente de invención o modelo de utilidad obtenido en el país; b) Un producto fabricado mediante la utilización de un procedimiento amparado por una patente de invención obtenida en el país;
- c) Un producto amparado por un dibujo o modelo industrial registrado en el país;
- d) Una obtención vegetal registrada en el país, así como su material de reproducción, propagación o multiplicación;
- e) Un esquema de trazado (topografía) registrado en el país, un circuito semiconductor que incorpore dicho esquema de trazado (topografía) o un artículo que incorpore tal circuito semiconductor;
- f) Un producto o servicio que utilice una marca no registrada idéntica o similar a una marca notoria o de alto renombre, registrada en el país o en el exterior;
- g) Un producto o servicio que utilice una marca no registrada idéntica o similar a una marca registrada en el país; y,
- h) Un producto o servicio que utilice una marca o indicación geográfica no registradas, idéntica o similar a una indicación geográfica registrada en el país.

En los casos de los literales g) y h) los productos o servicios que utilicen el signo no registrado, deberán ser idénticos o similares a los productos o servicios protegidos por las marcas o indicaciones geográficas registradas en el país.

**Art. 320.-** Serán reprimidos con igual pena que la señalada en el artículo anterior, quienes en violación de los derechos de propiedad intelectual:

1. Divulguen, adquieran o utilicen secretos comerciales, secretos industriales o información confidencial;
2. En productos o servicios o transacciones comerciales utilicen marcas o indicaciones geográficas no registradas en el país, que constituyan una imitación de signos distintivos notorios o de alto renombre, registrados en el país o en el exterior que pueden razonablemente confundirse con el original; y,
3. En productos o servicios o transacciones comerciales utilicen marcas o indicaciones geográficas que constituyan una imitación de signos distintivos registrados en el país, que pueden razonablemente confundirse con el original, para distinguir productos o servicios que puedan suplantar a los protegidos.

**Art. 321.-** Serán reprimidos con prisión de un mes a dos años y multa de seiscientos cincuenta y siete 22/100 (657,22) dólares de los Estados Unidos de América a seis mil quinientos setenta y dos 25/100 (6.572,25) dólares de los Estados Unidos de América, tomando en consideración el valor de los perjuicios ocasionados, quienes en violación de los derechos de propiedad intelectual utilicen nombres comerciales sobre los cuales no han adquirido derechos, que sean idénticos a nombres comerciales pública y notoriamente conocidos en el país o marcas registradas en el país, o a marcas notorias o de alto renombre registradas en el país o en el exterior.

También se reprimirá con la pena señalada en el inciso anterior, a quienes en violación de los derechos de propiedad intelectual utilicen apariencias distintivas, idénticas o similares a apariencias distintivas pública y notoriamente conocidas en el país.

**Art. 322.-** Serán reprimidos con prisión de un mes a dos años y multa de seiscientos cincuenta y siete 22/100 (657,22) dólares de los Estados Unidos de América a seis mil quinientos setenta y dos 25/100 (6.572,25) dólares de los Estados Unidos de América, tomando en consideración el valor de los perjuicios ocasionados, quienes en violación de los derechos de propiedad intelectual:

- a) Fabriquen, comercialicen o almacenen etiquetas, sellos o envases que contengan marcas de alto renombre o notorias, registradas en el país o en el exterior;
- b) Fabriquen, comercialicen o almacenen etiquetas, sellos o envases que contengan marcas o denominaciones de origen registradas en el país; y,
- c) Separen, arranquen, reemplacen o utilicen etiquetas, sellos o envases que contengan marcas legítimas, para utilizarlas en productos de distinto origen.

Con igual sanción serán reprimidos quienes almacenen, fabriquen, utilicen con fines comerciales, oferten en venta, vendan, importen o exporten artículos que contengan indicaciones falsas acerca de la naturaleza, procedencia, modo de fabricación, calidad, características o aptitud para el empleo de los productos o servicios de que se trate; o, contengan informaciones falsas acerca de premios u otras distinciones.

**Art. 323.-** Serán reprimidos con prisión de tres meses a tres años y multa de mil trescientos catorce 45/100 (1.314,45) dólares de los Estados Unidos de América a trece mil ciento cuarenta y cuatro 50/100 (13.144, 50) dólares de los Estados Unidos de América, tomando en consideración el valor de los perjuicios ocasionados, quienes almacenen, fabriquen, utilicen con fines comerciales, oferten en venta, vendan, importen o exporten productos falsificados identificados con marcas de alto renombre o notoriamente conocidas, registradas en el país o en el exterior, o con marcas registradas en el país.

También se reprimirá con la pena señalada en el inciso anterior a quienes rellenen con productos espurios envases identificados con marca ajena.

**Art. 324.-** Serán reprimidos con prisión de tres meses a tres años y multa de mil trescientos catorce 45/100 (1.314,45) dólares de los Estados Unidos de América a trece mil ciento cuarenta y cuatro 50/100 (13.144, 50) dólares de los Estados Unidos de América, tomando en consideración el valor de los perjuicios ocasionados, quienes en violación de los derechos de autor o derechos conexos:

- a) Alteren o mutilen una obra, inclusive a través de la remoción o alteración de información electrónica sobre el régimen de derechos aplicables;
- b) Inscriban, publiquen, distribuyan, comuniquen o reproduzcan, total o parcialmente, una obra ajena como si fuera propia;
- c) Reproduzcan una obra;
- d) Comuniquen públicamente obras, videogramas o fonogramas, total o parcialmente;
- e) Introduzcan al país, almacenen, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros reproducciones ilícitas de obras;
- f) Reproduzcan un fonograma o videograma y en general cualquier obra protegida, así como las actuaciones de intérpretes o ejecutantes, total o parcialmente, imitando o no las características externas del original, así como quienes introduzcan al país, almacenen, distribuyan, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros tales reproducciones ilícitas; y,
- g) Introduzcan al país, almacenen, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros reproducciones de obras, fonogramas o videogramas en las cuales se ha alterado o removido información sobre el régimen de derechos aplicables.

**Art. 325.-** Serán reprimidos con prisión de un mes a dos años y multa de seiscientos cincuenta y siete 22/100 (657,22) dólares de los Estados Unidos de América a seis mil quinientos setenta y dos 25/100 (6.572,25) dólares de los Estados Unidos de América, tomando en consideración el valor de los perjuicios ocasionados, quienes en violación de los derechos de autor o derechos conexos:

- a) Reproduzcan un número mayor de ejemplares de una obra que el autorizado por el titular;
- b) Introduzcan al país, almacenen, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros reproducciones de obras en número que exceda del autorizado por el titular;
- c) Retransmitan por cualquier medio las emisiones de los organismos de radiodifusión; y,
- d) Introduzcan al país, almacenen, ofrezcan en venta, vendan, arrienden o de cualquier otra manera pongan en circulación o a disposición de terceros aparatos u otros medios destinados a descifrar o decodificar las señales codificadas o de cualquier otra manera burlar o quebrantar los medios técnicos de protección aplicados por el titular del derecho.

**Art. 326.-** Serán reprimidos con prisión de un mes a dos años y multa de seiscientos cincuenta y siete 22/100 (657,22) dólares de los Estados Unidos de América, a seis mil quinientos setenta y dos 25/100 (6.572,25) dólares de los Estados Unidos de América, quienes ilícitamente obstaculicen, incumplan o impidan la ejecución de una providencia preventiva o cautelar.

## **j) Otros**

Ley de Comercio Electrónico

**Art. ..-** Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena

de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

**Art. 59.-** Sustitúyase el artículo 262 por el siguiente:

"**Art. ...- 262.-** Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo.

**Art. 63.-** Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.

## **1.2 Legislación**

### **a) Tentativa:**

**Art. 16.-** Quien practica actos idóneos conducentes de modo inequívoco a la realización de un delito, responde por tentativa si la acción no se consuma o el acontecimiento no se verifica.

Si el autor desiste voluntariamente de la acción está sujeto solamente a la pena por los actos ejecutados, siempre que éstos constituyan una infracción diversa, excepto cuando la Ley, en casos especiales, califica como delito la mera tentativa.

Si voluntariamente impide el acontecimiento, está sujeto a la pena establecida para la tentativa, disminuida de un tercio o la mitad.

Las contravenciones solo son punibles cuando han sido consumadas.

### **b) Complicidad e instigación:**

**Art. 47.-** Los cómplices serán reprimidos con la mitad de la pena que se les hubiere impuesto en caso de ser autores del delito.

**Art. 386.-** El que públicamente instigare a cometer un delito determinado contra una persona o institución, cuando el instigador no puede ser considerado legalmente como correo, será reprimido, por la instigación y aunque el delito no se hubiere perpetrado, con prisión de quince días a dos años, según la gravedad del delito instigado.

## **B. LEGISLACIÓN PROCESAL:**

### **1.3. Acciones para incluir en la legislación lo no contemplado:**

Interceptación ilícita

#### **Proyecto de Código Orgánico Integral Penal**

**Artículo 231(xxx).- Interceptación ilegal de datos.**

Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible,
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

#### **Artículo 52 (xxx).- Responsabilidad de las personas jurídicas.**

En los supuestos previstos en este Código, las personas jurídicas nacionales o extranjeras de derecho privado son penalmente responsables por los delitos cometidos para beneficio propio o de sus asociados, por la acción u omisión de quienes ejercen su propiedad o control, sus órganos de gobierno o administración, apoderadas o apoderados, mandatarias o mandatarios, representantes legales o convencionales, agentes, operadoras u operadores, factores, delegadas o delegados, por terceros que contractualmente o se inmiscuyen en una actividad de gestión, ejecutivos principales o quienes cumplan actividades de administración, dirección y supervisión, y en general por quienes actúen bajo órdenes o instrucciones de las personas naturales citadas.

La responsabilidad penal de la persona jurídica es independiente de la responsabilidad penal de las personas naturales que intervengan con sus acciones u omisiones en la comisión del delito.

No hay lugar a la determinación de la responsabilidad penal de la persona jurídica, cuando el delito se comete por cualquiera de las personas naturales indicadas en el inciso primero, en beneficio de un tercero ajeno a la persona jurídica.

#### **1.5 Medidas adoptadas.**

- a) Confiscar, decomisar o secuestrar sistemas o dispositivos de almacenamiento informático

**Art. 93.- Incautación.-** Si el Fiscal supiere o presumiere que en algún lugar hay armas, efectos, papeles u otros objetos relacionados con la infracción o sus posibles autores, solicitará al juez competente autorización para incautarlos, así como la orden de allanamiento, si fuere del caso.

Si se trata de documentos, el Fiscal procederá como lo dispone el Capítulo IV de este título, en cuanto fuere aplicable.

- b) Copiar y conservar datos informáticos consultados

**Art. 35.- Actos urgentes.-** En los casos de acción pública, el Fiscal podrá realizar los actos urgentes que impidan la consumación del delito o los necesarios para conservar los elementos de prueba pero sin afectar los derechos del ofendido. En los casos de acción privada será el juez de garantías penales quien podrá realizar tales actos, con notificación a la persona contra quien se presentará la diligencia.

## **II. COOPERACIÓN INTERNACIONAL**

### **2.2. Legislación para dar trámite a las solicitudes de asistencia mutua de otros Estados**

CONVENCION INTERAMERICANA SOBRE ASISTENCIA MUTUA EN MATERIA PENAL

Registro Oficial Suplemento 153

Fecha: 25-nov-2005

Art. 7.- AMBITO DE APLICACION.- La asistencia prevista en esta convención comprenderá, entre otros, los siguientes actos:

h. Remisión de documentos, informes, información y elementos de prueba.

Art. 25.- LIMITACION AL USO DE INFORMACION O PRUEBAS.- El Estado requirente no podrá divulgar o utilizar ninguna información o prueba obtenida en aplicación de la presente convención para propósitos diferentes a aquellos especificados en la solicitud de asistencia, sin previo consentimiento de la Autoridad Central del Estado requerido.

En casos excepcionales, si el Estado requirente necesitare divulgar y utilizar, total o parcialmente, la información o prueba para propósitos diferentes a los especificados, solicitará la autorización correspondiente del Estado requerido, el que, a su juicio, podrá acceder o negar, total o parcialmente, lo solicitado.

La información o prueba que deba ser divulgada y utilizada, en la medida necesaria para el apropiado cumplimiento del procedimiento o diligencias especificadas en la solicitud, no estarán sujetas al requerimiento de autorización a que se refiere este artículo.

Cuando resulte necesario, el Estado requerido podrá solicitar que la información o las pruebas suministradas se conserven en confidencialidad de conformidad con las condiciones que especifique la Autoridad Central. Si la Parte requirente no puede cumplir con tal solicitud, las autoridades centrales se consultarán para determinar las condiciones de confidencialidad que mutuamente resulten convenientes.