

**CUESTIONARIO PREPARATORIO  
DE LA SEPTIMA REUNION DEL GRUPO DE TRABAJO EN DELITO CIBERNETICO**

**I. LEGISLACION**

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

- |  |                 |
|--|-----------------|
| a) Acceso ilícito                          | Si ( X ) No ( ) |
| b) Interceptación telefónica               | Si ( X ) No ( ) |
| c) Ataques a la integridad de datos        | Si ( X ) No ( ) |
| d) Ataques a la integridad de sistemas     | Si ( X ) No ( ) |
| e) Abuso de dispositivos                   | Si ( ) No ( X ) |
| f) Falsificación informática               | Si ( ) No ( X ) |
| g) Fraude informático                      | Si ( X ) No ( ) |
| h) Pornografía infantil                    | Si ( X ) No ( ) |
| i) Delitos contra la propiedad intelectual | Si ( X ) No ( ) |
| j) Otras (sírvese enumerarlas) _____       | Si ( ) No ( X ) |

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

**Código Penal Peruano:**

**Violación del secreto de las comunicaciones Art 162°.- Interferencia telefónica**

**Pornografía Infantil Art. 183°A**

**Hurto Agravado Art 186° Inc. 3 transferencia electrónica de fondos.**

**Delitos Informáticos Art. 207°A, 207°B y 207°C.**

**Delitos contra la Propiedad Intelectual del Art 216° al Art. 221°.**

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

En caso afirmativo, sírvase describir los esfuerzos:

**El Congreso de la Republica se encuentra tramitando dos proyectos de ley**

**a. Proyecto de Ley 034/2011-CR “Ley de los delitos Informáticos”.**

**b. Proyecto de Ley 307/2011-CR “Ley Especial sobre los delitos cometidos con el uso de las TIC”.**

**Ambos proyectos de ley se encuentran en la Comisión de Justicia y Derechos Humanos.**

1.3 ¿Permite la legislación de emergencia de su país, por parte de los investigadores criminales, requerir a los proveedores de Servicios de Internet a preservar pruebas electrónicas sin la necesidad de una orden judicial?

**No, existe legislación al respecto.**

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

1.4 ¿Ha adoptado su país la legislación sustantiva y procesal y otras medidas necesarias que permitan a sus autoridades competentes?

a) Confiscar, decomisar o secuestrar sistemas o dispositivos de almacenamiento informáticos. Si ( ) No ( X )

b) Copiar o conservar los datos informáticos consultados Si ( ) No ( X )

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

1.5 Permite la legislación procesal de su país la interceptación legal de comunicaciones electrónicas transmitidas en su territorio a través de sistemas de computación?

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

**La Ley N° 27697 y su modificatoria el Decreto Legislativo N° 991 Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional, sin embargo, solo se podrá hacer uso de la facultad en algunos delitos.**

## II. UNIDADES ESPECIALIZADAS Y ESFUERZOS NACIONALES.

2.1 ¿Hay en su país una unidad o entidad encargada específicamente de investigar los delitos cibernéticos? (autoridad de policía) Si ( ) No ( )

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la Unidad o instancia.  
**División de Investigación de Delitos de Alta Tecnología (DIVINDAT)**
- Institución de la que depende  
**Dirección de Investigación Criminal de la Policía Nacional del Perú.**
- Información de Contacto.
  - o Nombre del Titular.  
**Jefe de la DIVINDAT**
  - o Domicilio.  
**Central Operativa de Investigación Policial (COIP) “Alcides Vigo Hurtado”, Av. España N° 323 Mezannine – Cercado de Lima.**
  - o Teléfono(s) **051 4318898** Fax:
  - o Correo Electrónico  
**jefatura@policiainformatica.gob.pe**

2.2 ¿Hay en su país una unidad o entidad encargada específicamente de procesar jurídicamente la comisión de delitos cibernéticos Si ( ) No ( X )

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la Unidad o instancia.
- Institución de la que depende
- Información de Contacto.
  - o Nombre del Titular.
  - o Domicilio.
  - o Teléfono(s) Fax:

○ Correo Electrónico

- 2.3 ¿Ha establecido su país páginas de internet para facilitar que los ciudadanos, cuenten con información para prevenir ser víctimas de delitos cibernéticos y para detectarlos y denunciarlos ante las autoridades competentes cuando ellos ocurran?  
Si ( X ) No ( )

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

**www.policiainformatica.gob.pe; página implementada por la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) órgano executor de la Dirección de Investigación Criminal de la Policía Nacional del Perú, que contiene su misión, visión, funciones organigrama, así como información sobre las principales modalidades delictivas cometidas con el uso de herramientas informáticas, recomendaciones, estrategias así como links de contactos.**

- 2.4 ¿Ha desarrollado y/o implementado su país una estrategia nacional de seguridad cibernética  
Si ( ) No ( X )

En caso afirmativo, sírvase describir brevemente en que consiste esa estrategia:

III. COOPERACION INTERNACIONAL.

- 3.1 ¿Se ha adherido su país a la convención del consejo de Europa sobre Delincuencia Cibernética?  
Si ( ) No ( X )

En casi negativo ¿ha considerado su país la aplicación de los principios contenidos en dicha Convención?  
Si ( ) No ( ) No Conozco ( X )

**Sin embargo, en el año 2007 se formulo un informe comparativo entre nuestra legislación y las normas del Convenio de Budapest suscrito el año 2001, documento cursado al Ministerio del Interior a fin de que sea remitido a la Oficina nacional de gobierno Electrónico e Informática de la PCM y al Ministerio de Relaciones Exteriores para su evaluación**

- 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?  
Si ( ) No ( X )

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

Si ( ) No ( ) No Conozco ( )

En caso afirmativo, sírvase expresar en que han consistido esas medidas.

- 3.2 ¿Cuenta su país con legislación que permita dar tramite a las solicitudes de asistencia mutua de otros Estados para la obtención de prueba electrónicas?

Si ( ) No ( ) No Conozco ( 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:

- 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?

Si ( ) No ( X ) No conozco ( )

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

#### IV. CAPACITACION.

- 4.1 ¿Ofrece su país capacitación a los funcionarios responsables de la aplicación de la legislación contar el delito cibernético y para la obtención de pruebas electrónicas?

Si ( ) No ( X )

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 delitos cibernéticos y para la obtención de pruebas electrónicas?

Si ( ) No ( X )

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

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

- 4.4 ¿Ha participado su país en los talleres de capacitación celebrados en el marco del grupo de Trabajo en Delito Cibernético: Si ( ) No ( X )

En caso afirmativo, sírvase describir brevemente las personas que han participado; si estos talleres han ofrecido capacitación útil, y como los participantes han aplicado esta capacitación en el ejercicio de sus funciones:

- 4.5. Sírvanse proporcionar recomendaciones sobre los temas que debieran incorporarse en los talleres de capacitación del Grupo de Trabajo para los próximos dos años relacionados con el delito cibernético y las pruebas electrónicas:

**Publicación en la página Web de eventos de capacitación sobre delitos cibernéticos, contactos de los miembros de la REMJA, en otros países.**

- 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:

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO:

Por favor, complete la siguiente información:

(a) Estado: **Perú**

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

( ) Sr.: **Manuel F. Guerrero Zerpa**

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

Título/cargo: Jefe de Departamento de Investigaciones Especiales

Organismo/oficina: División de Investigación de Delitos de Alta Tecnología – DIVINDAT – DIRINCRI PNP.

Domicilio: Av. España N° 323 Mezanine – Cercado de Lima

Número de teléfono: 051 997904862

Número de fax:

Correo electrónico: mafaguez2010@gmail.com

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

**I. LEGISLACIÓN**

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

- |  |        |        |
|--|--------|--------|
| a) Acceso ilícito  | SI (✓) | NO ( ) |
| b) Interceptación ilícita                                    | SI (✓) | NO ( ) |
| c) Ataques a la integridad de datos                          | SI (✓) | NO ( ) |
| d) Ataques a la integridad de sistemas                       | SI (✓) | NO ( ) |
| e) Abuso de dispositivos                                     | SI (✓) | NO ( ) |
| f) Falsificación informática                                 | SI (✓) | NO ( ) |
| g) Fraude informático  | SI (✓) | NO ( ) |
| h) Pornografía infantil                                      | SI (✓) | NO ( ) |
| i) Delitos contra la propiedad intelectual y derechos afines | SI (✓) | NO ( ) |
| j) Otras (sírvase enumerarlas): <u>VER ANEXO I</u>           | SI (✓) | NO ( ) |

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

VER ANEXO I

1.2. En caso de que su país no haya tipificado alguna de las anteriores conductas, indique si está desarrollando algunas acciones para hacerlo: SI ( ) NO (✓)

En caso afirmativo, sírvase describir esos esfuerzos:

1.3. ¿Permite la legislación de emergencia 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?

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

VER ANEXO I

1.4. ¿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. | SI (✓) | NO ( ) |
| b) Copiar y conservar los datos informáticos consultados.                                    | SI (✓) | NO ( ) |

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

VER ANEXO I

1.5. ¿Permite la legislación procesal de su país la interceptación legal de comunicaciones electrónicas transmitidas en su territorio a través de sistemas de computación?

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

VER ANEXO I

**II. UNIDADES ESPECIALIZADAS Y ESFUERZOS NACIONALES**

2.1. ¿Hay en su país una unidad o entidad encargada específicamente de investigar los delitos cibernéticos? (autoridad de policía) SI (✓) NO ( )

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: VER ANEXO II
- Institución de la que depende:
- Información de contacto:
  - o Nombre del Titular:
  - o Domicilio:
  - o Teléfono(s):
  - o Correo electrónico:

2.2. ¿Hay en su país una unidad o entidad encargada específicamente de procesar jurídicamente la comisión de delitos cibernéticos? SI ( ) NO (✓)

En caso afirmativo, sírvase proporcionar la siguiente información:

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

2.3. ¿Ha establecido su país páginas en Internet para facilitar que los ciudadanos cuenten con información para prevenir ser víctimas de delitos cibernéticos y para detectarlos y denunciarlos ante las autoridades competentes cuando ellos ocurran? SI ( ) NO (✓)

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

- 2.4. ¿Ha desarrollado y/o implementado su país una estrategia nacional de seguridad cibernética? SI ( ) No (✓)  
En caso afirmativo, sírvase describir brevemente en que consiste esa estrategia: \_\_\_\_\_

### III. COOPERACIÓN INTERNACIONAL

- 3.1. ¿Se ha adherido su país a la Convención del Consejo de Europa sobre Delincuencia Cibernética? SI ( ) No (✓)

En caso negativo, ¿ha considerado su país la aplicación de los principios contenidos en dicha Convención? SI (✓) No ( ) No Conozco ( )

En caso afirmativo, sírvase expresar en qué ha consistido dicha consideración: \_\_\_\_\_

VER ANEXO III

- 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? SI ( ) No (✓)

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

SI ( ) No ( ) No Conozco (✓)

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

- 3.3. ¿Cuenta su país con legislación que permita dar trámite a las solicitudes de asistencia mutua de otros Estados para la obtención de pruebas electrónicas?

SI (✓) No ( ) No Conozco ( )

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

VER ANEXO III

- 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? SI ( ) No ( ) No Conozco (✓)

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

### 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?

SI ( ) 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? SI ( ) No (✓)

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

- 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: \_\_\_\_\_

VER ANEXO IV

- 4.4. ¿Ha participado su país en los talleres de capacitación celebrados en el marco del Grupo de Trabajo en Delito Cibernético? SI ( ) No ( ) No Conozco (✓)

En caso afirmativo, sírvase describir brevemente las personas que han participado; si estos talleres han ofrecido capacitación útil, y cómo los participantes han aplicado esta capacitación en el ejercicio de sus funciones: \_\_\_\_\_

- 4.5. Sirvanse 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: \_\_\_\_\_

ver Anexo IV

- 4.6. En el marco de las REMJA, sirvase 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: \_\_\_\_\_

ver Anexo IV

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: