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 ( ) No (**X**)

Actualmente México no cuenta con una legislación que tipifique los Delitos Cibernéticos como tal, sin embargo, la Constitución Política de los Estados Unidos Mexicanos, el Código Penal Federal, el Código de Procedimientos Penales, la Ley Federal de Derechos de Autor, la Ley Federal de Telecomunicaciones, la Ley General del Sistema Nacional de Seguridad Pública, la Ley Orgánica de la Procuraduría General de la República, la Ley de la Policía Federal, la Ley de la Propiedad Industrial y otros Ordenamiento Legales, dejan abierta la posibilidad de ofrecer cualquier tipo de prueba que acredite la comisión de un delito.

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

a) Acceso ilícito Sí (X) No ( )

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

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

Derecho Penal	
Acceso ilícito	**Se cumple parcialmente con los artículos 211 Bis 3 y 211 Bis 5 del Código Penal Federal.** **Artículo 211 bis 3**.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública. **Artículo 211 bis 5**.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

	Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.
Intercepción ilícita	**El artículo 173 del CPF cumple parcialmente.** **Artículo 173**.- Se aplicarán de tres a ciento ochenta jornadas de trabajo en favor de la comunidad: **I.-** Al que abra indebidamente una comunicación escrita que no esté dirigida a él, y **II.-** Al que indebidamente intercepte una comunicación escrita que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido. Los delitos previstos en este artículo se perseguirán por querella **En la Ley Federal de Telecomunicaciones (Art. 71 fr. V) se contempla como una infracción administrativa en relación a "comunicaciones".** **Artículo 71.** Las infracciones a lo dispuesto en esta Ley, se sancionarán por la Secretaría de conformidad con lo siguiente: **A.** Con multa de 10,000 a 100,000 salarios mínimos por: **V.** Interceptar información que se transmita por las redes públicas de telecomunicaciones, y *Fracción reformada DOF 09-02-2009*
Atentados contra la integridad de datos	**Se cumple con los artículos 211 bis 1 a 7 del CPF.** **Artículo 211 bis 1**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. **Artículo 211 bis 2**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

	Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. **Artículo 211 bis 3**.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública. **Artículo 211 bis 4**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

	Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero. **Artículo 211 bis 6**.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código. **Artículo 211 bis 7**.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.
Atentados contra la integridad del sistema	Esta conducta no se encuentra legislada, en lo relativo a la obstaculización grave a través de transmisión, toda vez que un sistema se puede obstaculizar en su funcionamiento sin accesar a él. La normativa mexicana se refiere a datos y no a sistemas informáticos.
Abuso de equipos	**Parcialmente se cumple con el artículo 424 Bis, fracción II del CPF.** **Artículo 424 bis**.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa: **II.-** A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación. **La Ley Federal del Derecho de Autor, prevé algunas de estas conductas como infracciones en los artículos 112 y 231 fracciones V y VII.** **Artículo 112.-** Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

	Artículo 231.- Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto: **V.** Importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de Computación. **VII.** Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular.
Falsedad informática	No está previsto en legislación mexicana.
Estafa informática	La legislación tipifica robo y fraude genéricos, en el Artículo 386 de la CPF. **Artículo 386**.- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido. El delito de fraude se castigará con las penas siguientes: **I.-** Con prisión de 3 días a 6 meses o de 30 a 180 días multa, cuando el valor de lo defraudado no exceda de diez veces el salario. **II.-** Con prisión de 6 meses a 3 años y multa de 10 a 100 veces el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario. **III.-** Con prisión de tres a doce años y multa hasta de ciento veinte veces el salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario.
Infracciones relativas a la pornografía infantil	**Los artículos 202 y 202 bis del CPF.** **Artículo 202.-** Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa.

	A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito. La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores. **Artículo 202 BIS.-** Quien almacene, compre, arriende, el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa. Asimismo, estará sujeto a tratamiento psiquiátrico especializado.
Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines	**Se da cumplimiento parcial con los artículos 424 al 429 del CPF, en particular los artículos 424 bis, 426 y 428.** **Artículo 424**.- Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa: **I.** Al que especule en cualquier forma con los libros de texto gratuitos que distribuye la Secretaría de Educación Pública. **II.** Al editor, productor o grabador que a sabiendas produzca más números de ejemplares de una obra protegida por la Ley Federal del Derecho de Autor, que los autorizados por el titular de los derechos. **III.** A quien use en forma dolosa, con fin de lucro y sin la autorización correspondiente obras protegidas por la Ley Federal del Derecho de Autor. **Artículo 424 bis**.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa: **I.-** A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

	Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior. **II.-** A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación. **Artículo 424 ter**.- Se impondrá prisión de seis meses a seis años y de cinco mil a treinta mil días multa, a quien venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa, con fines de especulación comercial, copias de obras, fonogramas, videogramas o libros, a que se refiere la fracción I del artículo anterior. Si la venta se realiza en establecimientos comerciales, o de manera organizada o permanente, se estará a lo dispuesto en el artículo 424 Bis de este Código. **Artículo 425**.- Se impondrá prisión de seis meses a dos años o de trescientos a tres mil días multa, al que a sabiendas y sin derecho explote con fines de lucro una interpretación o una ejecución. **Artículo 426**.- Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes: **I.-** A quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal. **II.-** A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal. **Artículo 427.-** Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa, a quien publique a sabiendas una obra substituyendo el nombre del autor por otro nombre. **Artículo 428**.- Las sanciones pecuniarias previstas en el presente título se aplicarán sin perjuicio de la reparación del daño, cuyo monto no podrá ser menor al cuarenta por ciento del precio de venta al público de cada producto o de la prestación de servicios que impliquen violación a alguno o algunos de los derechos tutelados por la Ley Federal del Derecho de Autor. **Artículo 429**.- Los delitos previstos en este título se perseguirán por querella de parte ofendida, salvo el caso previsto en el artículo 424, fracción I, que será perseguido de oficio. En el caso de que los

	derechos de autor hayan entrado al dominio público, la querella la formulará la Secretaría de Educación Pública, considerándose como parte ofendida.

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:

Uno de los resultados que se ha obtenido con relación a una de las tipificaciones más sancionadas, es la de Pornografía Infantil.

Derivado de la Averiguación Previa PGR/SIEDO/UEITMIO/7/2008 instruida en contra de **Domingo Abarca Ramírez, por el probable delito de pornografía infantil,** se inició la causa penal 10/2008, por **el delito de Pornografía de Menores de dieciocho años de edad, en las modalidades de Comprar y Almacenar Imágenes Lascivas y Sexuales de Niños y Niñas cuyas edades oscilan entre los seis y los doce años.**

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:

Con base al Código Federal de Procedimientos Penales, Artículo 123 Cuarto Articulo 123 Quinto.

Articulo 123 Cuarto. El Ministerio Público se cerciorará de que se han seguido los procedimientos para preservar los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito.

Tratándose de los indicios, huellas o vestigios del hecho delictuoso, el Ministerio Público ordenará la práctica de las pruebas periciales que resulten procedentes. Respecto de los instrumentos, objetos o productos del delito ordenará su aseguramiento de conformidad con lo dispuesto en el artículo 181 de este Código, previos los dictámenes periciales a los que hubiere lugar.

En caso de que la recolección levantamiento y traslado de los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito no se haya hecho como lo señala el artículo anterior, el Ministerio Público lo asentará en la averiguación previa y, en su caso, dará vista a las autoridades que resulten competentes para efectos de las responsabilidades a las que haya lugar.

Artículo 123 Quinto. Los peritos se cerciorarán del correcto manejo de los indicios, huellas o vestigios del hecho delictuoso, así como de los instrumentos, objetos o productos del delito y realizarán los peritajes que se le instruyan. Los dictámenes respectivos serán enviados al Ministerio

Público para efectos de la averiguación. La evidencia restante será devuelta al Ministerio Público, quien ordenará su resguardo para posteriores diligencias o su destrucción, si resulta procedente.

Los peritos darán cuenta por escrito al Ministerio Público cuando los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito no hayan sido debidamente resguardados, de conformidad con lo dispuesto en los artículos anteriores y demás aplicables, sin perjuicio de la práctica de los peritajes que se les hubiere instruido.

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:

Con base al Código Federal de Procedimientos Penales.

La ley mexicana no específica que los medios electrónicos se puedan ofrecer como pruebas ante los procesos y juicios penales, sin embargo, deja abierta la posibilidad de ofrecer cualquier tipo de prueba que acredite la comisión de un delito.

Capitulo VIII Bis, Articulo 278 Bis, en los párrafos I, II, III, IV, V.

Las comunicaciones entre particulares podrán ser aportadas voluntariamente a la averiguación previa o al proceso penal, cuando hayan sido obtenidas directamente por alguno de los participantes en la misma.

El tribunal recibirá las grabaciones o video filmaciones presentadas como prueba por las partes y las agregará al expediente.

Las comunicaciones que obtenga alguno de los participantes con el apoyo de la autoridad, también podrán ser aportadas a la averiguación o al proceso, siempre que conste de manera fehaciente la solicitud previa de apoyo del particular a la autoridad. De ser necesario, la prueba se perfeccionará con las testimoniales o periciales conducentes.

En ningún caso el Ministerio Público o el juez admitirán comunicaciones que violen el deber de confidencialidad que establezca la Ley, ni la autoridad prestará el apoyo a que se refiere el párrafo anterior cuando se viole dicho deber.

No se viola el deber de confidencialidad cuando se cuente con el consentimiento expreso de la persona con quien se guarda dicho deber.

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

a) Requerir a una persona en su territorio a proporcionar información en su poder o control almacenada en un sistema o dispositivo informático? Sí (X) No ( )

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

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

Con base al Código Federal de Procedimientos Penales en el Capitulo VIII Bis, Articulo 278 Bis, en los párrafos VI, VII.

Las empresas concesionarias y permisionarias del servicio de telecomunicaciones o de Internet, estarán obligadas a colaborar con las autoridades para la obtención de dichas pruebas cuando así lo soliciten. Cualquier omisión o desacato a esta disposición será sancionada por la autoridad, en los términos del artículo 178 del Código Penal Federal.

Carecen de todo valor las comunicaciones que sean obtenidas y aportadas en contravención a las disposiciones señaladas en este Código.

Código Penal Federal Artículo 178. Al que, sin causa legítima, rehusare a prestar un servicio de interés público a que la ley le obligue, o desobedeciere un mandato legítimo de la autoridad, se le aplicarán de quince a doscientas jornadas de trabajo en favor de la comunidad.

Al que desobedeciere el mandato de arraigo domiciliario o la prohibición de abandonar una demarcación geográfica, dictados por autoridad judicial competente, se le impondrán de seis meses a dos años de prisión y de diez a doscientos días multa.

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

a) Confiscar, decomisar o secuestrar sistemas o dispositivos de almacenamiento informáticos? Sí (X) No ( )
b) Copiar y conservar los datos informáticos consultados? Sí (X) No ( )
c) Preservar la integridad de los datos informáticos almacenados? Sí (X) No ( )
d) Hacer inaccesibles o suprimir los datos del sistema consultado? Sí (X) No ( )

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

Con base al Código Federal de Procedimientos Penales, Articulo 61, párrafos I, II.

Cuando en la averiguación previa el Ministerio Público estime necesaria la práctica de un cateo, acudirá a la autoridad judicial competente, o si no la hubiere a la del orden común, a solicitar por cualquier medio la diligencia, dejando constancia de dicha solicitud, expresando su objeto y necesidad, así como la ubicación del lugar a inspeccionar y persona o personas que han de localizarse o de aprehenderse, y los objetos que se buscan o han de asegurarse a lo que únicamente debe limitarse la diligencia.

Al inicio de la diligencia el Ministerio Público designará a los servidores públicos que le auxiliarán en la práctica de la misma.

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:

En base al Código Federal de Procedimientos Penales, Artículo 278 Tercero.

Cuando la solicitud de intervención de comunicaciones privadas sea formulada por el Procurador General de la República o los servidores públicos en quienes delegue la facultad, la autoridad judicial otorgará la autorización cuando se constate la existencia de indicios suficientes que acrediten la probable responsabilidad en la comisión de delitos graves.

El Ministerio Público será responsable de que la intervención se realice en los términos de la autorización judicial. La solicitud de autorización deberá contener los preceptos legales que la funda, el razonamiento por el que se considera procedente, el tipo de comunicaciones, los sujetos y los lugares que serán intervenidos, así como el periodo durante el cual se llevarán a cabo las intervenciones, el cual podrá ser prorrogado, sin que el periodo de intervención, incluyendo sus prórrogas, pueda exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.

En la autorización, el juez determinará las características de la intervención, sus modalidades, límites y, en su caso, ordenará a instituciones públicas o privadas, modos específicos de colaboración.

En la autorización que otorgue el juez deberá ordenar que, cuando en la misma práctica sea necesario ampliar a otros sujetos o lugares la intervención, se deberá presentar ante el propio juez, una nueva solicitud; también ordenará que al concluir cada intervención se levante un acta que contendrá un inventario pormenorizado de las cintas de audio y video que contengan los sonidos o imágenes captadas durante la intervención, así como que se le entregue un informe sobre sus resultados, a efecto de constatar el debido cumplimiento de la autorización otorgada.

El juez podrá, en cualquier momento, verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total.

En caso de no ejercicio de la acción penal y una vez transcurrido el plazo legal para impugnarlo, sin que ello suceda, el juez que autorizó la intervención, ordenará que se pongan a su disposición las cintas resultado de las investigaciones, los originales y sus copias, y ordenará su destrucción en presencia del Ministerio Público.

II. UNIDADES ESPECIALIZADAS

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

- Nombre de la unidad o instancia: **UNAM-CERT**
- Institución de la que depende: **Universidad Nacional Autónoma de México (UNAM)**
    - Nombre del Titular: **Ing. Rubén Aquino Luna**
    - Domicilio: **En el Departamento de Seguridad en Cómputo (DSC) de la Dirección General de Servicios de Cómputo Académico (DGSCA), de la UNAM. Ubicado Colonia Copilco Universidad, CP 04360 Delegación Coyoacán México, D. F.**
    - Teléfono(s): **56 22 81 69** Fax: **56 22 80 47**
    - Correo electrónico: raquino@seguridad.unam.mx

- Nombre de la unidad o instancia: **Dirección General de Delitos Cibernéticos**
- Institución de la que depende: **Secretaría de Seguridad Pública (SSP)**
    - Nombre del Titular: **Lic**. **Juan Carlos Guel López**
    - Domicilio: **Av. Constituyentes 947, Col. Belén de las Flores, Del. Álvaro Obregón, C.P. 01110**
    - Teléfono(s): **11036000 Ext. 22022**
    - Correo electrónico: carlos.guell@ssp.gob.mx

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: _____
- Institución de la que depende: _____
- Información de contacto:
    - 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 han llevado a cabo foros celebrados entre las autoridades del gobierno federal y el sector privado, en los que se han establecido mecanismos de intercambio de información en materia cibernética, sin embargo, se ha recalcado la necesidad de legislar en materia de Delitos Cibernéticos, ya que actualmente existen vacíos legales que no entorpecen la debida investigación y persecución del delito.

III. COOPERACIÓN INTERNACIONAL

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

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

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

México ha participado únicamente como observador desde 1 de diciembre de 1999.

Además, de fomentar una cultura cibernética en el ámbito gubernamental y en la sociedad civil, se consideró como prioridad la tarea de armonización legislativa, para estar en capacidad de aplicar una política penal común contra los delitos cibernéticos tomando en cuenta los preceptos del Convenio sobre Cibercriminalidad del Consejo de Europa.

3.2. ¿Se ha vinculado su país a la Red de Emergencia de Contactos sobre Delitos de Alta Tecnología 24 horas/7 días" del G-8? Sí (X) No ( )

En caso afirmativo, sírvase desarrollar en que han consistido tales medidas:

Las áreas responsables de la investigación en casos relacionados con redes informáticas deben reaccionar con prontitud solicitando el apoyo a los Proveedores de Servicio de Internet, a fin de conservar la información electrónica y ubicar sospechosos.

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

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

Las partes aplicarán los instrumentos internacionales en materia de cooperación internacional penal vigentes:

- Extradición
- Asistencia jurídica mutua
- Medidas provisionales para asegurar la conservación rápida de datos almacenados
- Países que están en esta cooperación, los cuales han desarrollado diversas iniciativas para aumentar la toma de conciencia y promover la cooperación internacional en la lucha contra la delincuencia informática, incluidas las medidas tomadas por el Consejo de Europa, la Unión Europea, el Grupo de los Ocho, la Organización de Cooperación y Desarrollo Económicos y las Naciones Unidas.

En base al **Reglamento de la Ley Orgánica de la PGR, Articulo 25, fracciones I, II, III, VII, VIII Y IX, se señala que:**

Artículo 25. Al frente de la Coordinación de Asuntos Internacionales y Agregadurías habrá un Titular, quien tendrá las facultades siguientes:
I. Coordinar el ejercicio de las atribuciones del Ministerio Público de la Federación en materia internacional;
II. Coordinar las Agregadurías, Subagregadurías y Oficinas de Enlace de la Procuraduría en el extranjero, así como a las unidades administrativas que le estén adscritas;
III. Vigilar que las Agregadurías, Subagregadurías y Oficinas de Enlace de la Procuraduría en el extranjero, establezcan mecanismos eficientes de coordinación y colaboración con las autoridades de los países en cuya circunscripción territorial ejerciten sus funciones;
VII. Organizar la participación de la Procuraduría en foros y reuniones internacionales, en coordinación con la Secretaría de Relaciones Exteriores, y promover la cooperación internacional en materia de procuración de justicia;
VIII. Someter a consideración de su superior jerárquico, previa consulta con las unidades administrativas competentes, la posición que deba asumir la Institución en foros y organismos internacionales, así como las necesidades de asistencia técnica internacional;
IX. Realizar estudios de carácter internacional y promover la celebración de instrumentos internacionales en el ámbito de competencia de la Procuraduría;

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

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

En base al **Reglamento de la Ley Orgánica de la PGR, Artículos 25 Fracción VIII, 27 Fracciones I y X, 35 Fracción VII y 36 Fracciones I, II, V y VI.**

Artículo 25. Al frente de la Coordinación de Asuntos Internacionales y Agregadurías habrá un Titular, quien tendrá las facultades siguientes:
VIII. Someter a consideración de su superior jerárquico, previa consulta con las unidades administrativas competentes, la posición que deba asumir la Institución en foros y organismos internacionales, así como las necesidades de asistencia técnica internacional.

Artículo 27. Al frente de cada una de las unidades especializadas habrá un Titular, quien tendrá las facultades siguientes:
I. Ejercer las atribuciones previstas en el artículo 4 de la Ley Orgánica, respecto de los delitos materia de su competencia, en coordinación con las unidades administrativas y órganos competentes;
IX. Participar, en coordinación con las unidades administrativas competentes de la Institución, en los organismos y grupos internacionales encargados o que tengan relación con la investigación y represión de los delitos materia de sus respectivas competencias.

Artículo 35. Al frente de la Dirección General de Extradiciones y Asistencia Jurídica habrá un Director General, quien tendrá las facultades siguientes:

VII. Auxiliar en la práctica de diligencias y obtención de información en el extranjero, a las distintas unidades administrativas de la Procuraduría, así como a las procuradurías generales de justicia de los Estados y del Distrito Federal.

Artículo 36. Al frente de la Dirección General de Cooperación Internacional habrá un Director General, quien tendrá las facultades siguientes:
I. Promover en coordinación con las autoridades competentes, la celebración de tratados y acuerdos internacionales en materia de procuración de justicia, extradición, asistencia jurídica mutua, ejecución de sentencias penales, devolución internacional de bienes, cooperación en el combate a la delincuencia y otras que sean de la competencia de la Procuraduría;
II. Participar en coordinación con las unidades administrativas competentes, en reuniones internacionales en las que se traten temas relacionados con las funciones de la Procuraduría;
V. Desahogar las consultas jurídicas internacionales que le sean formuladas por las unidades administrativas de la Institución, así como por otras autoridades federales, del Distrito Federal y de los Estados de la República, relacionadas con el ámbito de sus funciones;
VI. Establecer en coordinación con las autoridades competentes, canales de comunicación y mecanismos de concertación con autoridades de otros países, para realizar actividades de cooperación internacional, así como darles seguimiento.

Tratados y Convenios Internacionales suscritos entre nuestro país y otros Estados en materia de asistencia jurídica, se puede lograr la obtención de pruebas electrónicas y la realización de otros actos necesarios para facilitar la investigación o juzgamiento de delitos cibernéticos, así como el principio de reciprocidad internacional tratándose de países con los que no existe un tratado internacional vigente en materia de asistencia jurídica.

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

4. CAPACITACIÓN

4.1 ¿Ofrece su país capacitación a los funcionarios responsables de la aplicación de la legislación contra el delito cibernético y para la obtención de pruebas electrónicas? Sí ( ) No (X)

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:

ACTIVIDAD ACADÉMICA	FECHA INICIO	FECHA TERMINO	IMPARTIÓ	TOTAL PARTICIPANTES
INVESTIGACIÓN DE DELITOS CIBERNÉTICOS	17/7/2006	21/07/2006	DIRECCIÓN GENERAL DE PLANEACIÓN POLICIAL	8
CIBERCRIMINALIDAD II	28/6/2007	01/06/2007	INACIPE	33
CIBERCRIMINALIDAD	6/11/2006	10/11/2006	INACIPE	4
CIBERCRIMINALIDAD	7/8/2006	11/08/2006	INACIPE	20
SEMINARIO DE DELITOS INFORMÁTICOS	3/3/2008	04/03/2008	INACIPE	3
TEMÁTICA ESPECIALIZADA DE DELITOS INFORMÁTICOS	3/3/2008	07/03/2008	INACIPE	2
INVESTIGACIÓN DE DELITOS CIBERNÉTICOS	17/07/2006	21/07/2006	DIRECCIÓN GENERAL DE PLANEACIÓN POLICIAL	8

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:

- En materia legislativa elaborar un instrumento jurídico que atienda y regule el uso de computadoras e Internet, con base en un estándar internacional, a fin de armonizar tipos penales y técnicas forenses, con el propósito de adoptar mejores prácticas en seguridad de la información.

- Retroalimentación constante entre autoridades de gobierno y proveedores del servicio de Telefonía e Internet, a fin de que emitan recomendaciones de seguridad de acuerdo a las necesidades que vayan surgiendo.

- La creación de un CSIRT nacional.

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:

Estos talleres han servido para resaltar la posición que tiene México en materia de Legislación en Delitos Cibernéticos, ya que se puede observar coincidencia con otros países de la problemática que existe en este tema, como es la falta de legislación armonizada, técnicas forenses similares, de conceptos y conductas tipificadas. Además de la participación del sector privado para enfrentar la amenaza del cibercrimen.

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:

- Seguridad Informática
- Legislación en Contra de los Delitos Cibernéticos
- Análisis Forense en equipos de Cómputo y Telecomunicaciones
- Direccionamiento IP (Rastreo de direcciones)
- Rastreo de correos electrónicos
- Procesos de Investigación, enfocado a la búsqueda de sitios Web.
- Ciberterrorismo

4.6. En el marco de las REMJA, sírvase proporcionar recomendaciones acerca de cómo el Grupo de Trabajo en Delito Cibernético puede ayudar mejor a su país en el desarrollo o mejoramiento de su capacidad para enfrentar los delitos relacionados con las computadoras y el Internet:

- Elaborar exclusivamente una legislación contra los Delitos Cibernéticos
- Es necesario rehacer una regulación relativa a la coordinación que se debe tener con los organismos privados
- Es necesario fomentar el diálogo constante de personal que conoce las leyes y operadores técnicos de los sistemas informáticos
- Identificar mecanismos y necesidades para establecer un CSIRT nacional
- Adherirse a convenios y tratados para el combate a los Delitos Cibernéticos

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: México, Distrito Federal
(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:
Ing. Javier Téllez García
Título/cargo: Subcoordinador de Servicios
Organismo/oficina: Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia (CENAPI) de la Procuraduría General de la República (PGR)
Domicilio: Calle Xóchitl S/N, Colonia El Reloj, delegación Coyoacán, CP: 04640
Número de teléfono: 55-51-69-65-60
Correo electrónico: javiertellezgarcia@prodigy.net.mx

(a) Estado: México
(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:
Lic. Yessica De Lamadrid Téllez
Título/cargo: Directora General de Cooperación Internacional
Organismo/oficina: Procuraduría General de la República
Domicilio: Av. Paseo de la Reforma No. 211-213, piso 14, Colonia Cuauthémoc, Deleg. Cuauthémoc, C.P. 06500
Número de teléfono: 53-46-02-06
Correo electrónico: yess@pgr.gob.mx