REUNIÓN DE MINISTROS DE JUSTICIA U
OTROS MINISTROS, PROCURADORES O FISCALES
GENERALES DE LAS AMÉRICAS

OEA/Ser.K/XXXIV
CIBER-VI/doc.3/09
17 noviembre 2009
Original: inglés

Sexta Reunión del Grupo de Trabajo en Delito Cibernético
21 y 22 de Enero de 2010
Washington, D.C.

CUESTIONARIO PREPARATORIO DE LA SEXTA REUNIÓN DEL GRUPO DE TRABAJO EN DELITO CIBERNÉTICO

INTRODUCCIÓN

El presente cuestionario busca recolectar información útil para los propósitos de la Sexta Reunión del Grupo de Trabajo en Delito Cibernético, en relación con las recomendaciones que han sido formuladas en las reuniones precedentes y las que han sido adoptadas en el marco del proceso de las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA), concordantes con las mismas.

Para estos efectos, el cuestionario se divide en cuatro áreas temáticas: (1) Legislación; (2) Órganos Unidades Especializadas; (3) Cooperación Internacional; y (4) Capacitación.

Teniendo en cuenta lo anterior, sírvanse remitir la respuesta de su Estado al presente cuestionario, a más tardar el **10 de diciembre de 2009**, a la Secretaría General de la OEA (Departamento de Cooperación Jurídica de la Secretaría de Asuntos Jurídicos), al correo electrónico LegalCooperation@oas.org o al número de fax: + (202) 458-3598.

Por favor adicionar el espacio que requiera en cada respuesta o anexar hojas, según lo estime necesario.

I. LEGISLACIÓN

1.1. ¿Ha adoptado su país legislación para prevenir, investigar y sancionar el delito cibernético?
Sí (X) No ( )

En caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica, de la legislación: Artículo 12 de la Ley Contra Actos de Terrorismo, Artículos 173, 184, 185, 186, 216, 222 y 230 del Código Penal (Se adjunta copia al final de los mismos).

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

a) Acceso ilícito Sí (X) No ( )

Acceso Ilícito: Este delito está previsto, pero sólo en el ámbito de las infracciones aduaneras penales, bajo el epígrafe "Delitos Informáticos", Artículo 24 Inc.1°. Letra a) de la Ley Especial para Sancionar Infracciones Aduaneras.

Delitos Informáticos

Art. 24 Inc.1°. Letra a).- Será sancionado con prisión de tres a cinco años, quien.

a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por la Dirección General;

b) Interceptación ilícita Sí (X) No ( )

Interceptación Ilícita: Los Artículos 184 y 185 del Código Penal, establecen la figura de Violación a las Comunicaciones Privadas, en soporte informático. También, se tipifica el delito de "Captación de Comunicaciones" de cualquier señal de comunicaciones, Art.186 del mismo Código.

DE LOS DELITOS RELATIVOS A LA INTIMIDAD

VIOLACIÓN DE COMUNICACIONES PRIVADAS

Art. 184.- El que con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido o se apodere de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivo o registro público o privado, será sancionado con multa de cincuenta a cien días multa.

Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de cien a doscientos días multa.

El tercero a quien se revelare el secreto y lo divulgare a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa.

VIOLACIÓN AGRAVADA DE COMUNICACIONES

Art. 185.- Si los hechos descritos en el artículo anterior se realizaren por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros, se impondrá, además de la pena de multa, inhabilitación del respectivo cargo o empleo público de seis meses a dos años.

CAPTACIÓN DE COMUNICACIONES

Art. 186.- El que con el fin de vulnerar la intimidad de otro, interceptare, impidiere o interrumpiere una comunicación telegráfica o telefónica o utilizare instrumentos o artificios técnicos de escucha, transmisión o grabación del sonido, la imagen o de

cualquier otra señal de comunicación, será sancionado con prisión de seis meses a un año y multa de cincuenta a cien días multa.

Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de prisión de seis meses a un año y multa de cien a ciento cincuenta días multa.

El tercero a quien se revelare el secreto y lo divulgare, a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa.

El que realizare los actos señalados en el primer inciso del presente artículo para preparar la comisión de un delito grave será sancionado con la pena de dos a seis años. (9)

c) Ataques a la Integridad de Datos Sí (X) No ( )

d) Ataques a la Integridad de Sistemas Sí (X) No ( )

La Ley Especial para Sancionar Infracciones Aduaneras, como se ha señalado, contempla la figura de "Delitos Informáticos" que recoge las diferentes conductas que lesionan o ponen en peligro bienes jurídicos relacionados con la renta de Aduanas; el Art.24 letra b) regula el delito de "Ataques a la Integridad de Datos" y las letras c) y e) recogen la figura de "Ataques a la Integridad de Sistemas", como sigue:

Delitos Informáticos

Art. 24.- Será sancionado con prisión de tres a cinco años, quien.

b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación diseñado por o para tal autoridad o sus bases de datos, que de manera exclusiva y en el ejercicio de sus controles y servicios utilizare la Dirección General;

c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos o de comunicaciones, diseñados para las operaciones de la Dirección General, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra personal;

e) Manipule el sistema informático o de comunicaciones a fin de imposibilitar cualquier control que con base en dicho sistema exista la posibilidad de realizar.

e) Abuso de dispositivos Sí ( ) No (X)

f) Falsificación informática Sí (X) No ( )

Falsificación Informática: Esta figura se encuentra prevista sólo para los casos constitutivos de infracciones aduaneras que consisten en hacer total o parcialmente falso o alterar información de trascendencia tributaria, Art.23 de la Ley Especial para Sancionar Infracciones Aduaneras.

Ocultamiento, falsificación o Destrucción de Información.

Art. 23.- Será sancionado con prisión de tres a seis años quien haya creado, ocultado, haga total o parcialmente falso o altere información de trascendencia tributaria a la autoridad aduanera o destruya libros de contabilidad o de control tributario, sus registro auxiliares, estados financieros y sus anexos, archivos, registros, mercancías, documentos; así como sistemas y programas computarizados o soportes magnéticos que respaldan o contengan la anterior información. Se considerará incurso en este delito, tanto la persona que participe directamente en la creación, ocultación, alteración o destrucción expresada, como la que hubiere decidido y dado la orden para la ejecución de las mismas

g) Fraude informático Sí (X) No ( )

El Capítulo III del Código Penal. Regula las defraudaciones contra el Patrimonio y en su Art.216 No.5, recoge, como circunstancia agravatoria, cometer el delito de Estafa mediante manipulación informática. Por otra parte, en los delitos relativos al Orden Socioeconómico, el Art.238-A del mismo Código, contempla la figura del "fraude de Comunicaciones", la que también prevé que su realización se lleve a cabo en sistema informático inclusive.

ESTAFA AGRAVADA

Art. 216.- El delito de estafa será sancionado con prisión de cinco a ocho años, en los casos siguientes:

5) Cuando se realizare manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos.

FRAUDE DE COMUNICACIONES

Art. 238-A.- El que interfiere, alterare, modificare o interviniere cualquier elemento del sistema de una compañía que provee servicios de comunicaciones con el fin de obtener una ventaja o beneficio ilegal, será sancionado con prisión de tres a seis años. (15)

Asimismo, el que activare o configurare ilegalmente teléfonos celulares u otros aparatos de comunicación robados, hurtados, extraviados provenientes de acciones ilícitas se aplicará una sanción de cuatro a ocho años de prisión y además una multa de ciento cincuenta a doscientos días multa. (15)(34)

Cuando se determinare que el uso de comunicaciones, a que se refiere el presente artículo, esté relacionado con los delitos de crimen organizado, la pena se aumentará hasta en una tercera parte del máximo. (15)

h) Pornografía infantil Sí (X) No ( )

Pornografía Infantil: De forma limitada se regula el delito de Pornografía Infantil; el Art.172 del Código Penal establece su comisión por medios electrónicos en personas menores de 18 años. También se contempla la figura de utilización de personas menores con fines pornográficos por medios informáticos prevista en el Art.173 del Código Penal; además, se penaliza la simple posesión de ese material, en el Art.173-A del mismo cuerpo legal.

PORNOGRAFIA

Art. 172.- El que por cualquier medio directo, inclusive a través de medios electrónicos, fabricare, transfiriere, difundiere, distribuyere, alquilare, vendiere, ofreciere, produjere, ejecutare, exhibiere o mostrare, películas, revistas, pasquines o cualquier otro material pornográfico entre menores de dieciocho años de edad o deficientes mentales, será sancionado con prisión de tres a cinco años. (19)

En la misma sanción incurrirá el que no advirtiere, de forma visible, sobre el contenido de las películas, revistas, pasquines o cualquier otro material, inclusive el que se pueda trasmitir a través de medios electrónicos, cuando éste fuere inadecuado para menores de dieciocho años de edad o deficientes mentales. (19)

UTILIZACIÓN DE PERSONAS MENORES DE DIECIOCHO AÑOS E INCAPACES O DEFICIENTES MENTALES EN PORNOGRAFIA

Art. 173.- El que produzca, reproduzca, distribuya, publique, importe, exporte, ofrezca, financie, venda, comercie o difunda de cualquier forma, imágenes, utilice la vos de una persona menor de dieciocho años, incapaz o deficiente mental, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en el que exhiban, en actividades sexuales, eróticas o inequívocas de naturaleza sexual, explícitas o no, reales o simuladas, será sancionado con prisión de seis a doce años. (19)

Igual sanción se impondrá a quien organizare o participare en espectáculos, públicos o privados, en los que se hace participar a las personas señaladas en el inciso anterior, en acciones pornográficas o eróticas. (19)

POSESION DE PORNOGRAFIA.

Art. 173-A.- El que posea material pornográfico en el que se utilice la imagen de personas menores de dieciocho años, incapaces o deficientes mentales, en actividades pornográficas o eróticas, será sancionado con pena de dos a cuatro años. (19)

i) Delitos contra la propiedad intelectual y derechos afines Sí (X) No ( )

Delitos contra la propiedad intelectual y derechos afines: Esta figura recoge la modalidad de Violación a Derechos de Autor en cualquier soporte, y aunque no menciona el informático, se entiende comprendido en el Art.226 del Código Penal. Otra modalidad que se regula en los delitos contra la propiedad intelectual, se encuentra en el Art.227-A letra a)

del mismo Código, y es la relativa a tener acceso a dicha propiedad, evadiendo las medidas tecnológicas previstas para controlar su acceso. Asimismo, el Art.227-C del Código Penal, recoge la figura de Violación a Medidas Tecnológicas Efectivas, siempre en el marco de los delitos contra la propiedad intelectual, en la que aparecen elementos del tipo relacionado con afectación de medidas informáticas o tecnológicas.

DE LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL

VIOLACION DE DERECHOS DE AUTOR Y DERECHOS CONEXOS

Art. 226.- El que a escala comercial reprodujere, plagiare, distribuyere al mayoreo o comunicare públicamente, en todo o en parte, una obra literaria o artística o su transformación o una interpretación o ejecución artística fijada en cualquier tipo de soporte o fuere comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios, será sancionado con prisión de dos a cuatro años. (30)

En la misma sanción incurrirá, el que a escala comercial importare, exportare o almacenare ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización. (30)

Escala comercial incluye la infracción dolosa significativa de derecho de autor y derechos conexos, con el fin de obtener una ventaja comercial o ganancia económica privada, así como la infracción dolosa que no tenga una motivación directo o indirecta de ganancia económica, siempre que se cause un daño económico mayor a una infracción de poco valor. (30)

VIOLACION A MEDIDAS TECNOLÓGICAS EFECTIVAS (30)

Art. 227-A.- Será sancionado con prisión de dos a cuatro años, el que con fines de lograr una ventaja comercial o ganancia financiera privada: (30)

a) Evadiere, sin autorización del titular del derecho, cualquier medida tecnológica efectiva que controle el acceso a una obra, interpretación, ejecución o fonograma protegido u otra materia objeto de protección; (30)

VIOLACION AL DERECHO SOBRE SEÑALES DE SATÉLITE (30)

Art. 227-C.- Será sancionado con prisión de dos a cuatro años, el que: (30)

a) Fabricare, ensamblare, modificare, importare, exportare, vendiere, arrendare o distribuyere por cualquier medio, un dispositivo o sistema tangible o intangible, sabiendo o teniendo razones para saber que el dispositivo o sistema sirve primordialmente para descodificar una señal de satélite codificada portadora de programas, sin la autorización del distribuidor legítimo de dicha señal; o (30)

b) Recibiere y subsiguientemente distribuyere una señal portadora de programas que se haya originado como una señal de satélite codificada, teniendo conocimiento que ha sido descodificada sin la autorización del distribuidor legítimo de dicha señal. (30)

j) Otras (sírvase enumerarlas): _____ 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: En El Salvador no existe un norma especial de delitos informáticos, sólo las enumeradas en la respuesta a la pregunta 1, pero que son de gran importancia por ser un primer acercamiento al delito cibernético.

1) Daño informático. En los delitos contra el patrimonio, Art.222 No.2 del Código Penal, se contempla la figura de Daños Agravados, cuando la conducta fuere ejecutada mediante manipulación informática. Asimismo, encontramos esta figura en el Art.23 de la Ley Especial para Sancionar Infracciones Aduaneras, en los casos de destrucción de información, de trascendencia tributaria.

DAÑOS AGRAVADOS

Art. 222.- Se impondrá prisión de dos a cuatro años; (10)

2) Si el daño se realizare mediante manipulación informática; (10)

Ocultamiento, falsificación o Destrucción de Información.

Art. 23.- Será sancionado con prisión de tres a seis años quien haya creado, ocultado, haga total o parcialmente falso o altere información de trascendencia tributaria a la autoridad aduanera o destruya libros de contabilidad o de control tributario, sus registro auxiliares, estados financieros y sus anexos, archivos, registros, mercancías, documentos; así como sistemas y programas computarizados o soportes magnéticos que respaldan o contengan la anterior información. Se considerará incurso en este delito, tanto la persona que participe directamente en la creación. ocultación, alteración o destrucción expresada, como la que hubiere decidido y dado la orden para la ejecución de las mismas

2) Los delitos relativos al honor y a la intimidad específicamente, los de Calumnia, Difamación e Injuria, cuando sean ejecutados con publicidad, Art.181 del Código Penal, son susceptibles de ser cometidos por medios informáticos inclusive; lo anterior se desprende del Art.191 del mismo código, que regula la inexistencia de delitos.

CONCEPTO DE PUBLICIDAD

Art. 181.- Se entenderá que la injuria y la calumnia han sido realizadas con publicidad cuando se propaguen por medio de papeles impresos, litografiados o gravados, por carteles o pasquines fijados en sitios públicos o ante un número indeterminado de personas o por expresiones en reuniones públicas o por radiodifusión o televisión o por medios análogos.

DISPOSICIÓN COMUN

EXCLUSION DE DELITOS

Art. 191.- No son punibles los juicios desfavorables de la crítica política, literaria, artística, histórica, científica, religiosa o profesional, ni los conceptos desfavorables expresados por cualquier medio por particulares en el ejercicio del derecho de la Libertad de Expresión, siempre que en el modo de proceder no demuestren un propósito calumnioso, injurioso o de ataque a la intimidad o a la propia imagen de una persona. (26)

De igual manera, no son punibles los juicios desfavorables de la crítica política, literaria, artística, histórica, científica, religiosa o profesional ni los conceptos desfavorables expresados o difundidos por quienes ejerzan el periodismo mediante noticias, reportajes, investigaciones periodísticas, artículos, opiniones, editoriales, caricaturas y notas periodísticas en general, publicados en medios periodísticos escritos, radiales, televisivos e informáticos, en cumplimiento del deber de informar, en virtud del derecho de información o en ejercicio de su cargo o función. (26)

En cualquiera de las situaciones reguladas en los dos incisos anteriores, no incurrirán en ningún tipo de responsabilidad penal, los medios escritos, radiales, televisivos e informáticos en que se publiquen los juicios o conceptos antes expresados, ni los propietarios, directores, editores, gerentes del medio de comunicación social o encargados del programa en su caso. (26)

3) En la Ley Especial Contra Actos de Terrorismo de 2006, se contempla un tipo penal denominado Delito Informático, Art.12 de la citada ley, el cual establece que cualquiera de los delitos que prevé la expresada ley, serán susceptibles de ser cometidos por medios electrónicos (Equipos, programas o cualquier aplicación informática), así como la creación, distribución, comercio o tenencia de programas electrónicos para conectar o producir los efectos previstos en el literal a) del artículo en referencia.

DELITO INFORMATICO

Art. 12.- Será sancionado con pena de prisión de diez a quince años, el que para facilitar la comisión de cualquiera de los delitos previstos en esta Ley:

a) Utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, información, documentos electrónicos, soportes informáticos, programas o sistemas de información y de comunicaciones o telemáticos, de servicios públicos, sociales, administrativos, de emergencia o de seguridad nacional, de entidades nacionales, internacionales o de otro país;

b) Creare, distribuyere, comerciare o tuviere en su poder programas capaces de producir los efectos a que se refiere el literal a, de este artículo.

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: Son muy pocos los casos que la justicia penal ha conocido respecto de este tipo de delincuencia, y los que han sido objeto de persecución son casos relacionados a delitos contra la propiedad intelectual y de pornografía infantil.

En caso de que su país no haya tipificado alguna de las anteriores conductas, indique si está desarrollando algunas acciones para hacerlo: La instancia del Estado encargada de esta materia (Ministerio de Seguridad Pública y Justicia) ha participado, los últimos años, en jornadas de capacitación y talleres sobre el delito cibernético, como pasos previos para proponer, oportunamente, a la Asamblea Legislativa las reformas legales pertinentes.

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? Si (X) No ( )

En caso afirmativo, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjunte copia, de preferencia electrónica, de las mismas: El Código Procesal Penal que entrará en vigencia en enero de 2010 (NCPP), contempla expresamente una sección sobre la prueba electrónica, que regula bajo el epígrafe, Obtención y Resguardo de Información Electrónica en su Art.201 NCPP. También, los Arts.186 y 282 letra e) del mismo código, establecen disposiciones sobre la prueba electrónica. Asimismo, la Ley Contra el Lavado de Dinero y Activos, en su Art.14, regula medidas a efecto de resguardar la prueba electrónica. También se faculta a la UIF de la Fiscalía General de la República, tener acceso en forma electrónica a la base de datos de los organismos e instituciones del Estado que manejan información útil a la investigación del delito de Lavado de Activos.

INFORMACIÓN ELECTRÓNICA

Obtención y resguardo de información electrónica

Art. 201.- Cuando se tengan razones fundadas para inferir que una persona posee información constitutiva de delito o útil para la investigación, almacenada en equipos o instrumentos tecnológicos de su propiedad o posesión, el fiscal solicitará la autorización judicial para adoptar las medidas que garanticen la obtención, resguardo o almacenamiento de la información; sin perjuicio que se ordene el secuestro respectivo.

Operaciones técnicas

Art. 186.- Para mayor eficacia de las inspecciones y reconstrucciones, y en cualquier caso cuando sea conveniente, se podrán ordenar operaciones técnicas y científicas, tales como exámenes serológicos, químicos, microscópicos, microfotografía, macrofotografía, pruebas ópticas, biogenéticas, antropométricas, fonográficas, grafoscópicas, electrónicas, acústicas, de rayos X, perfiles genéticos y las demás disponibles por la ciencia y la técnica.

Técnicas de investigación policial

Art. 282.- Cuando la fiscalía tuviere razones fundadas, para inferir que una persona está participando en la comisión de un hecho delictivo de gravedad o pudiere conducirlo a obtener información útil para la investigación, podrá disponer:

e) Que se realicen cotejo de bases de datos de acceso público o cruce de información.

Art. 14.- Las instituciones, designarán funcionarios encargados de velar por el mantenimiento y actualización de registros y formularios indicados en esta ley. Todos los registros e informes requeridos por esta ley pueden ser guardados y transmitidos en papel o en forma electrónica

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: En el apartado reservado para la prueba documental, Art.244 NCPP., se consigna, como prueba de esta naturaleza, cualquier soporte en que consten datos o información para probar un hecho determinado. Asimismo se prevé su incorporación en el debate, si fuese necesario, con la ayuda de un experto técnico, Art.248 NCPP. También el Art.42 letra a) de la Ley Especial Contra Actos de Terrorismo, dispone que se tendrán como pruebas, la información contenida en discos compactos, digitales y otros dispositivos de almacenamiento.

PRUEBA DOCUMENTAL

Documentos públicos, auténticos y privados

Art. 244.- Los documentos públicos, auténticos y privados, de conformidad con las leyes de la materia, serán admisibles como prueba siempre que no sean falsos o presenten alteraciones o deterioro; salvo que los hechos investigados estén relacionados a cualquiera de estas circunstancias. En caso de deterioro, si es posible acreditar que el contenido del documento es inteligible y su sentido no se ve afectado por tales circunstancias, será admitido para ser presentado como prueba. Para los efectos de este Código también se entenderá como documento cualquier soporte en que consten datos o información susceptibles de ser empleados para probar un hecho determinado.

Incorporación

Art. 248.- Los documentos serán leídos y exhibidos en la audiencia, con indicación de su origen. Los soportes de sonido, voz o imagen y el almacenamiento de información deberán reproducirse en audiencia mediante los medios idóneos y, si fuere necesario, con la ayuda de un experto técnico. Las partes y el juez podrán acordar la lectura, exhibición o reproducción parcial de esos medios de prueba.

REGIMEN DE LAS PRUEBAS

Art. 42. Se tendrán como medios de prueba, además de los contemplados en el Código Procesal Penal, los siguientes:

a) La información contenida en filmaciones, grabaciones, fotocopias, videocintas, discos compactos, digitales y otros dispositivos de almacenamiento, telefax, comunicaciones escritas, telegráficas y electrónicas, en los términos a que se refiere el

Art. 302, inciso segundo del Código Penal, cuando se tratare de los delitos previstos por esta Ley;

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: En el capítulo referido a la Fiscalía General de la República, Art.77 NCPP, se regula la facultad para los fiscales de requerir la colaboración de funcionarios públicos, autoridades o personas naturales o jurídicas de carácter público o privado, quienes están obligadas a expedir la información que se solicite sin demora alguna. Igual facultad tienen los fiscales en caso de investigación por delitos de droga, Art.62 de la Ley Reguladora de las Actividades Relativas a las Drogas. Finalmente, el Art.17 de la Ley de Lavado de Dinero y de Activos recoge la misma facultad.

Poder coercitivo
Art. 77.- En el ejercicio de sus funciones, los fiscales tendrán el poder de solicitar informaciones, requerir la colaboración de los funcionarios públicos, autoridades o personas naturales o jurídicas de carácter público o privado, quienes tendrán la obligación de prestar la colaboración y expedir la información que se les solicite sin demora alguna, cuando sea procedente. También podrán citar a testigos y víctimas, practicar todas las diligencias que consideren pertinentes para la investigación y, ordenar las medidas cautelares que sean de su competencia, todo de conformidad con la Constitución de la República, este Código y demás leyes. Para esos efectos, podrán requerir la intervención de la policía y disponer de todas las medidas que consideren necesarias y conformes con su competencia.

REQUERIMIENTO DE INFORMACION.

Art. 62.- La Fiscalía General de la República, podrá solicitar información a cualquier ente estatal, autónomo, privado o personas naturales para la investigación de delitos contemplados en la presente Ley, estando éstos obligados a proporcionar la información solicitada.

Art. 17.- El Fiscal General de la República, podrá solicitar información a cualquier ente estatal, autónomo, privado o personas naturales para la investigación del delito de lavado de dinero y de activos estando estos obligados a proporcionar la información solicitada.

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

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

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: Para cada uno de los casos señalados, salvo confiscar puesto que está prohibido por el artículo 106 de la Constitución, el nuevo Código Procesal Penal, establece normas que facultan a los fiscales para decomisar y en su caso, secuestrar equipos o instrumentos tecnológicos que almacenen información constitutiva de delito o útil para la investigación, así como para almacenar y resguardar la información electrónica, todo bajo control y orden judicial, Art.201, 283 y 284 NCPP.

ARTÍCULO 106 DE LA CONSTITUCIÓN DE LA REPÚBLICA

Art. 106.- Inciso Último. "Se prohíbe la confiscación ya sea como pena o en cualquier otro concepto. Las autoridades que contravengan este precepto responderán en todo tiempo con sus personas y bienes del daño inferido. Los bienes confiscados son imprescriptibles."

INFORMACIÓN ELECTRÓNICA

Obtención y resguardo de información electrónica

Art. 201.- Cuando se tengan razones fundadas para inferir que una persona posee información constitutiva de delito o útil para la investigación, almacenada en equipos o instrumentos tecnológicos de su propiedad o posesión, el fiscal solicitará la autorización judicial para adoptar las medidas que garanticen la obtención, resguardo o almacenamiento de la información; sin perjuicio que se ordene el secuestro respectivo.

Incautación y decomiso

Art. 283.- El fiscal durante el desarrollo de las diligencias de investigación, dispondrá que sean incautados o recolectados y conservados los objetos o documentos relacionados con la comisión de un hecho delictivo y aquellos que puedan servir como medios de prueba.

El fiscal ordenará el decomiso de aquellos objetos que sean nocivos a la salud, de tenencia prohibida o peligrosa, de comercio no autorizado o de ilícita procedencia, así también sobre los demás objetos y documentos respecto a los cuales no existan o no sea posible ejercer derechos patrimoniales. La incautación o recolección de objetos o documentos podrá ser dispuesta en casos urgentes por la policía, quien deberá dar cuenta en el plazo de ocho horas al fiscal, para ordenar su decomiso, solicitar el secuestro u ordenar su devolución.

Secuestro
Art. 284.- En los casos de los objetos y documentos mencionados en el artículo anterior, cuando se puedan afectar derechos patrimoniales, el fiscal solicitará el secuestro al juez competente, dentro de las cuarenta y ocho horas siguientes de su incautación.

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: Los fiscales están facultados en el nuevo código para ordenar, con el consentimiento de la víctima, la grabación, por cualquier medio electrónico, de las comunicaciones que utilicen el espectro electromagnético, Art.281 NCPP.

Comunicaciones electromagnéticas de las víctimas
Art. 281.- En el marco de una investigación, si existen razones fundadas, el fiscal podrá ordenar, con el consentimiento de la víctima o de su representante, la grabación magnetofónica o por otro medio electrónico, de las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético. Esta orden seguirá vigente mientras se desarrolle el proceso de investigación y se cuente con el consentimiento de la víctima.

II. UNIDADES ESPECIALIZADAS

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

Resulta imposible completar esta unidad debido a no contar, nuestra institución, esta clase de información.

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: _____

2.2. ¿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? No existe una política de prevención y persecución del delito cibernético, pero tenemos la voluntad de hacerla efectiva, previo estudio de la realidad cibernética salvadoreña y mundial, con el apoyo de organismos como la OEA, para capacitar al personal técnico y jurídico y además se está trabajando en la creación de una Política Criminal Cibernética.

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 ( ) No (X)

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

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

En caso negativo, ¿ha tomado su país alguna(s) medida(s) para vincularse? Sí ( ) No (X)

En caso afirmativo, sírvase desarrollar en qué ha(n) consistido tal(es) medida(s): _____
_____
_____

¿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: El actual Código Procesal Penal contiene una disposición que permite dar trámite a solicitudes de esta naturaleza. Art.140 CPP.

Comisión Rogatoria del Extranjero
Art. 140.- La Comisión Rogatoria de Tribunales Extranjeros serán diligenciados en los casos y formas establecidas por los tratados o costumbres internacionales y por las leyes del país y la respuesta se enviará a través del Ministerio de Relaciones Exteriores.

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

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

_____

_____

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: _____

_____

_____

IV. CAPACITACIÓN

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

En caso afirmativo, sírvase describir brevemente el tipo de capacitación y el número de funcionarios capacitados: Los cursos de capacitación impartidos hasta la fecha, son de tipo expositivo en los que se realizó un amplio análisis de los diferentes problemas que suscitan los delitos informáticos, tanto en el plano procesal-probatorio, así como los de figuras delictivas, susceptibles de ser cometidas a través de medios cibernéticos y en particular Internet. La capacitación estuvo dirigida a un total de ochenta funcionarios judiciales entre los que se destaca la presencia de treinta y nueve jueces de sentencia y los demás beneficiados con dicha capacitación, fueron Magistrados de Cámara y Colaboradores Jurídicos de la Sala de lo Penal de la Corte Suprema de Justicia.

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

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

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: Generalmente, estos talleres han contado con la participación de representantes de las instituciones involucradas en la investigación y procesamiento de personas por delitos informáticos; para el caso se puede mencionar la presencia, en los referidos talleres, de fiscales, representantes de la Superintendencia del Sistema Financiero, del Ministerio de Seguridad Pública y Justicia y de la Corte Suprema de Justicia, así como de la Policía Nacional Civil.

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: Se recomiendan como temas a desarrollar en futuras capacitaciones: problemas relacionados con la obtención, resguardo y admisibilidad de la prueba electrónica, así como el análisis de los diferentes tipos penales realizados por medios informáticos; finalmente, sería necesario una capacitación orientada a la adopción de una legislación especial para prevenir, investigar y sancionar el delito cibernético.

4.6. En el marco de las REMJA, sírvase proporcionar recomendaciones acerca de cómo el Grupo de Trabajo en Delito Cibernético puede ayudar mejor a su país en el desarrollo o mejoramiento de su capacidad para enfrentar los delitos relacionados con las computadoras y el Internet: Realizando jornadas de conferencias y capacitaciones periódicas a nivel nacional por medio de sus expertos, dirigidas a funcionarios encargados de la persecución del delito informático, que tengan como resultado la elaboración de un plan nacional de combate contra la Ciberdelincuencia, y de mecanismos anuales de evaluación con base a matrices previamente establecidas.

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: República de El Salvador en la América Central
(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:
() Sr.: Licenciado Carlos Alfredo Castaneda Magaña.
Titulo/cargo: Viceministro de Integración y Promoción Económica
Organismo/oficina: Ministerio de Relaciones Exteriores
Domicilio: Calle El Pedregal, Boulevard Cancillería, 500 metros al poniente del Campus II de la Universidad "José Matías Delgado". Ciudad Merliot, Antiguo Cuscatlán, El Salvador, Centroamérica.
Número de teléfono: (503) 2231-2905
Número de fax: (503) 2289-8990

(a) Estado: República de El Salvador en la América Central
(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:
( ) Sr.: Doctor José Belarmino Jaime
Título/cargo: Presidente del Órgano Judicial
Organismo/oficina: Corte Suprema de Justicia de El Salvador
Domicilio: 9a. Calle Poniente y 15a. Avenida Norte, Centro de Gobierno, San Salvador, El Salvador, Centro América.
Número de teléfono: (503) 2271-8748
Número de fax: (503) 2271-8758

(a) Estado: República de El Salvador en la América Central
(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:
( ) Sr.: Licenciado Romeo Benjamín Barahona Meléndez
Título/cargo: Fiscal General de la República de El Salvador
Organismo/oficina: Fiscalía General de la República
Domicilio: Final Cuarta Calle Oriente y 19 Avenida Sur, Residencial Primavera, Santa Tecla, La Libertad, El Salvador.
Número de teléfono: (503) 2523-7000 y (503) 2528-6000
Número de fax: (503) 2523-7402

(a) Estado: República de El Salvador en la América Central
(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:
() Sr.: Licenciado Álvaro Henry Campos Solórzano
Titulo/cargo: Viceministro
Organismo/oficina: Ministerio de Justicia y Seguridad Pública
Domicilio: 9a. Calle Poniente y 15a. Avenida Norte, Centro de Gobierno, San Salvador, El Salvador, Centro América.
Número de teléfono: (503) 2526-3093
Número de fax: (503) 2271-2484
Correo electrónico: vice.ministerio@seguridad.gob.sv

RECOPILACIÓN DE TODAS LAS NORMAS RELACIONADAS CON DELITOS INFORMÁTICOS EN EL SALVADOR

LEY CONTRA ACTOS DE TERRORISMO

DELITO INFORMATICO

Art. 12.- Será sancionado con pena de prisión de diez a quince años, el que para facilitar la comisión de cualquiera de los delitos previstos en esta Ley:

a) Utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, información, documentos electrónicos, soportes informáticos, programas o sistemas de información y de comunicaciones o telemáticos, de servicios públicos, sociales, administrativos, de emergencia o de seguridad nacional, de entidades nacionales, internacionales o de otro país;

b) Creare, distribuyere, comerciare o tuviere en su poder programas capaces de producir los efectos a que se refiere el literal a, de este artículo.

CODIGO PENAL

CAPITULO II

DE LOS DELITOS RELATIVOS A LA INTIMIDAD

UTILIZACIÓN DE PERSONAS MENORES DE DIECIOCHO AÑOS E INCAPACES O DEFICIENTES MENTALES EN PORNOGRAFIA

Art. 173.- El que produzca, reproduzca, distribuya, publique, importe, exporte, ofrezca, financie, venda, comercie o difunda de cualquier forma, imágenes, utilice la vos de una persona menor de dieciocho años, incapaz o deficiente mental, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en el que exhiban, en actividades sexuales, eróticas o inequívocas de naturaleza sexual, explícitas o no, reales o simuladas, será sancionado con prisión de seis a doce años. (19)

Igual sanción se impondrá a quien organizare o participare en espectáculos, públicos o privados, en los que se hace participar a las personas señaladas en el inciso anterior, en acciones pornográficas o eróticas. (19)

VIOLACIÓN DE COMUNICACIONES PRIVADAS

Art. 184.- El que con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido o se apodere de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivo o registro público o privado, será sancionado con multa de cincuenta a cien días multa.

Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de cien a doscientos días multa.

El tercero a quien se revelare el secreto y lo divulgare a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa.

VIOLACIÓN AGRAVADA DE COMUNICACIONES

Art. 185.- Si los hechos descritos en el artículo anterior se realizaren por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros, se impondrá, además de la pena de multa, inhabilitación del respectivo cargo o empleo público de seis meses a dos años.

CAPTACIÓN DE COMUNICACIONES

Art. 186.- El que con el fin de vulnerar la intimidad de otro, interceptare, impidiere o interrumpiere una comunicación telegráfica o telefónica o utilizare instrumentos o artificios técnicos de escucha, transmisión o grabación del sonido, la imagen o de cualquier otra señal de comunicación, será sancionado con prisión de seis meses a un año y multa de cincuenta a cien días multa.

Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de prisión de seis meses a un año y multa de cien a ciento cincuenta días multa.

El tercero a quien se revelare el secreto y lo divulgare, a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa.

El que realizare los actos señalados en el primer inciso del presente artículo para preparar la comisión de un delito grave será sancionado con la pena de dos a seis años. (9)

ESTAFA AGRAVADA

Art. 216.- El delito de estafa será sancionado con prisión de cinco a ocho años, en los casos siguientes:

1) Si recayere sobre artículos de primera necesidad, viviendas o terrenos destinados a la construcción de viviendas;

2) Cuando se colocare a la víctima o su familia en grave situación económica, o se realizare con abuso de las condiciones personales de la víctima o aprovechándose el autor de su credibilidad empresarial o profesional;

3) Cuando se realizare mediante cheque, medios cambiarios o con abuso de firma en blanco;

4) Cuando se obrare con el propósito de lograr para sí o para otro el cobro indebido de un seguro; y,

5) Cuando se realizare manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos.

DAÑOS AGRAVADOS

Art. 222.- Se impondrá prisión de dos a cuatro años; (10)

1) Cuando el daño se ejecutare con violencia en las personas; (10)

2) Si el daño se realizare mediante manipulación informática; (10)

3) Si el daño se ejecutare en objetos que forman parte del patrimonio cultural; y, (10)

4) Cuando el daño recaiga en la morada de la víctima, (10)

5) Cuando el daño fuere ejecutado por dos o más personas. (18)(21)

INFIDELIDAD COMERCIAL

Art. 230.- El que se apoderare de documentos, soporte informático u otros objetos, para descubrir o revelar un secreto evaluable económicamente, perteneciente a una empresa y que implique ventajas económicas, será castigado con prisión de seis meses a dos años.