

Octava Reunión del Grupo de Trabajo en Delito Cibernético

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

INTRODUCCIÓN

El presente cuestionario busca recolectar información útil para los propósitos de la Octava Reunión del Grupo de Trabajo en Delito Cibernético, la cual se celebrará a principios de 2014, en relación con las recomendaciones que han sido formuladas en las reuniones anteriores y las que han sido adoptadas en el marco del proceso de las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA), concordantes con las mismas.

Para estos efectos, el cuestionario se divide en cinco áreas temáticas: (I) Legislación; (II) Cooperación internacional; (III) Unidades especializadas y esfuerzos nacionales; (IV) Resultados de investigaciones y enjuiciamientos en materia de delito cibernético; y (V) Capacitación.

Teniendo en cuenta lo anterior, sírvase remitir la respuesta de su Estado al presente cuestionario, a más tardar el **martes 10 de diciembre de 2013**, a la Secretaría General de la OEA (Departamento de Cooperación Jurídica de la Secretaría de Asuntos Jurídicos) al correo electrónico LegalCooperation@oas.org o al número de fax: + (202) 458-3598.

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

I. LEGISLACIÓN

A. LEGISLACIÓN SUSTANTIVA:

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

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

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

En Colombia, la Ley 1273 de 2009, por medio de la cual se modificó el Código Penal - Ley 599 de 2000, creó un nuevo bien jurídico tutelado denominado “*de la Protección de la información y de los datos*” y buscó la preservación integral de los sistemas que utilizan las tecnologías de la información y las comunicaciones.

Dado, lo anterior, las modalidades de delito cibernético contenidas en los numerales a) al g) e i) se encuentran tipificados en el Título VII Bis – *De la Protección de la Información y de los Datos*, del Código Penal Colombiano, Ley 599 del 2000, así como en la Ley 1273 de 2009, de la siguiente manera:

a) Acceso ilícito:

Artículo 269A. Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

b) Interceptación ilícita:

Artículo 269C. Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

c) Ataques a la integridad de datos:

Artículo 269D. Daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

d) Ataques a la integridad de sistemas:

Artículo 269D. Daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

e) Abuso de dispositivos:

Artículo 269A. Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E. Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

f) Falsificación informática:

Artículo 269F. Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G. Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

g) Fraude informático

Artículo 269I. Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J. *Transferencia no consentida de activos.* El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

i) Delitos contra la propiedad intelectual y derechos afines:

Artículo 270. *Violación a los derechos morales de autor.* Incurrirá en prisión de treinta y dos (32) a noventa (90) meses y multa de veinte seis punto sesenta y seis (26.66) a trescientos (300) salarios mínimos legales mensuales vigentes quien:

1. Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico.

2. Inscriba en el registro de autor con nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado, modificado o mutilado, o mencionando falsamente el nombre del editor o productor de una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

3. Por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

PARAGRAFO. Si en el soporte material, carátula o presentación de una obra de carácter literario, artístico, científico, fonograma, videograma, programa de ordenador o soporte lógico, u obra cinematográfica se emplea el nombre, razón social, logotipo o distintivo del titular legítimo del derecho, en los casos de cambio, supresión, alteración, modificación o mutilación del título o del texto de la obra, las penas anteriores se aumentarán hasta en la mitad.

Artículo 271. *Violación a los derechos patrimoniales de autor y derechos conexos.* Incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis punto sesenta y seis (26.66) a mil (1.000) salarios mínimos legales mensuales vigentes quien, salvo las excepciones previstas en la ley, sin autorización previa y expresa del titular de los derechos correspondientes:

1. Por cualquier medio o procedimiento, reproduzca una obra de carácter literario, científico, artístico o cinematográfico, fonograma, videograma, soporte lógico o programa de ordenador, o, quien transporte, almacene, conserve, distribuya, importe, venda, ofrezca, adquiera para la venta o distribución, o suministre a cualquier título dichas reproducciones.

2. Represente, ejecute o exhiba públicamente obras teatrales, musicales, fonogramas, videogramas, obras cinematográficas, o cualquier otra obra de carácter literario o artístico.

3. Alquile o, de cualquier otro modo, comercialice fonogramas, videogramas, programas de ordenador o soportes lógicos u obras cinematográficas.
4. Fije, reproduzca o comercialice las representaciones públicas de obras teatrales o musicales.
5. Disponga, realice o utilice, por cualquier medio o procedimiento, la comunicación, fijación, ejecución, exhibición, comercialización, difusión o distribución y representación de una obra de las protegidas en este título.
6. Retransmita, fije, reproduzca o, por cualquier medio sonoro o audiovisual, divulgue las emisiones de los organismos de radiodifusión.
7. Recepcione, difunda o distribuya por cualquier medio las emisiones de la televisión por suscripción.

Artículo 272. *Violación a los mecanismos de protección de derecho de autor y derechos conexos, y otras defraudaciones.* Incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis punto sesenta y seis (26.66) a mil (1.000) salarios mínimos legales mensuales vigentes, quien:

1. Supere o eluda las medidas tecnológicas adoptadas para restringir los usos no autorizados.
2. Suprima o altere la información esencial para la gestión electrónica de derechos, o importe, distribuya o comunique ejemplares con la información suprimida o alterada.
3. Fabrique, importe, venda, arriende o de cualquier forma distribuya al público un dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal; o, de cualquier forma, eluda, evada, inutilice o suprima un dispositivo o sistema, que permita a los titulares del derecho controlar la utilización de sus obras o fonogramas, o les posibilite impedir o restringir cualquier uso no autorizado de estos.
4. Presente declaraciones o informaciones destinadas directa o indirectamente al pago, recaudación, liquidación o distribución de derechos económicos de autor o derechos conexos, alterando o falseando, por cualquier medio o procedimiento, los datos necesarios para estos efectos.

Ahora bien, el Código Penal Colombiano, Ley 599 de 2000, en su capítulo IV establece todo lo relacionado con la explotación sexual, estableciendo delitos como: inducción a la prostitución, proxenetismo con menor de edad, constreñimiento a la prostitución, trata de personas¹ entre otros, decretando como circunstancias de agravación punitiva respecto de estos delitos, situaciones como pornografía con personas menores de 18 años y utilización o facilitación de medios de comunicación para ofrecer actividades sexuales con personas menores de 18 años.

En esta perspectiva, el tema de pornografía infantil se tipifica de la siguiente manera:

¹ Artículos 213 al 214, Código Penal Colombiano.

Artículo 218. Pornografía con personas menores de 18 años. El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, transmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, incurrirá en prisión de 10 a 20 años y multa de 150 a 1.500 salarios mínimos legales mensuales vigentes.

Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro.

La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima.

Artículo 219-A. Utilización o facilitación de medios de comunicación para ofrecer actividades sexuales con personas menores de 18 años. El que utilice o facilite el correo tradicional, las redes globales de información, telefonía o cualquier medio de comunicación, para obtener, solicitar, ofrecer o facilitar contacto o actividad con fines sexuales con personas menores de 18 años de edad, incurrirá en pena de prisión de diez (10) a catorce (14) años y multa de sesenta y siete (67) a (750) salarios mínimos legales mensuales vigentes.

Las penas señaladas en el inciso anterior se aumentarán hasta en la mitad (1/2) cuando las conductas se realizaren con menores de catorce (14) años.

1.2. ¿Ha promulgado su país legislación que:

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

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

En el ordenamiento penal colombiano se tiene establecido como dispositivo amplificador del tipo penal la figura de la *tentativa*, contemplada en el artículo 27 del Código Penal (Ley 599 de 2000), de la siguiente forma:

Ley 599 de 2000. Artículo 27. Tentativa. El que iniciare la ejecución de una conducta punible mediante actos idóneos e inequívocamente dirigidos a su consumación, y ésta no se produjere por circunstancias ajenas a su voluntad, incurrirá en pena no menor de la mitad del mínimo ni mayor de las tres cuartas partes del máximo de la señalada para la conducta punible consumada.

Cuando la conducta punible no se consuma por circunstancias ajenas a la voluntad del autor o partícipe, incurrirá en pena no menor de la tercera parte del mínimo ni mayor de las dos terceras partes del máximo de la señalada para su consumación, si voluntariamente ha realizado todos los esfuerzos necesarios para impedirla.

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

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

Ley 599 de 2000. Artículo 28. Concurso de personas en la conducta punible. Concurren en la realización de la conducta punible los autores y los partícipes.

Ley 599 de 2000. Artículo 29. Autores. Es autor quien realice la conducta punible por sí mismo o utilizando a otro como instrumento.

Son coautores los que, mediando un acuerdo común, actúan con división del trabajo criminal atendiendo la importancia del aporte.

También es autor quien actúa como miembro u órgano de representación autorizado o de hecho de una persona jurídica, de un ente colectivo sin tal atributo, o de una persona natural cuya representación voluntaria se detente, y realiza la conducta punible, aunque los elementos especiales que fundamentan la penalidad de la figura punible respectiva no concurran en él, pero sí en la persona o ente colectivo representado.

El autor en sus diversas modalidades incurrirá en la pena prevista para la conducta punible.

Ley 599 de 2000. Artículo 30. Partícipes. Son partícipes el determinador y el cómplice.

Quien determine a otro a realizar la conducta antijurídica incurrirá en la pena prevista para la infracción.

Quien contribuya a la realización de la conducta antijurídica o preste una ayuda posterior, por concierto previo o concomitante a la misma, incurrirá en la pena prevista para la correspondiente infracción disminuida de una sexta parte a la mitad.

Al interviniente que no teniendo las calidades especiales exigidas en el tipo penal concurra en su realización, se le rebajará la pena en una cuarta parte.

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

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

Código Penal. Ley 599 de 2000. Artículo 29. Autores. (...) También es autor quien actúa como miembro u órgano de representación autorizado o de hecho de una persona jurídica, de un ente colectivo sin tal atributo, o de una persona natural cuya representación voluntaria se detente, y realiza la conducta punible, aunque los elementos especiales que fundamentan la penalidad de la figura punible respectiva no concurran en él, pero sí en la persona o ente colectivo representado.

Código Penal. Ley 599 de 2000. Artículo 269H. Circunstancias de agravación punitiva. Las penas imponibles de acuerdo con los artículos descritos en este título (Título VII Bis – De la Protección de la Información y de los Datos), se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Código de Procedimiento Penal. Ley 906 de 2004. Artículo 91. Suspensión y cancelación de la personería jurídica. En cualquier momento y antes de presentarse la acusación, a petición de la Fiscalía, el juez de control de garantías ordenará a la autoridad competente que, previo el cumplimiento de los requisitos legales establecidos para ello, proceda a la suspensión de la personería jurídica o al cierre temporal de los locales o establecimientos abiertos al público, de personas jurídicas o naturales, cuando existan motivos fundados que permitan inferir que se han dedicado total o parcialmente al desarrollo de actividades delictivas. (...)

Código de comercio. Artículo 200. Responsabilidad de administradores. Los administradores responderán solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros. (...)

B. LEGISLACIÓN PROCESAL:

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

En caso afirmativo, sírvase describir esos esfuerzos: NO APLICA

- 1.4. ¿Permite la legislación de su país, por parte los investigadores criminales, requerir a los Proveedores de Servicios de Internet a preservar pruebas electrónicas sin la necesidad de una orden judicial?

Sí (**X**) No ()

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

Código de Procedimiento Penal colombiano. Ley 906 de 2004

Artículo 236. Recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes. Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado ha estado transmitiendo información útil para la investigación que se adelanta, durante su navegación por internet u otros medios tecnológicos que produzcan efectos equivalentes, ordenará la aprehensión del computador, computadores y servidores que pueda haber utilizado, disquetes y demás medios de almacenamiento físico, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen.

En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos.

La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados.

Artículo 205. Actividad de policía judicial en la indagación e investigación. Los servidores públicos que, en ejercicio de sus funciones de policía judicial, reciban denuncias, querellas o informes de otra clase, de los cuales se infiera la posible comisión de un delito, realizarán de inmediato todos los actos urgentes, tales como inspección en el lugar del hecho, inspección de cadáver, entrevistas e interrogatorios. Además, identificarán, recogerán, embalarán técnicamente los elementos materiales probatorios y evidencia física y registrarán por escrito, grabación magnetofónica o fonográfica las entrevistas e interrogatorios y se someterán a cadena de custodia.

Cuando deba practicarse examen médico-legal a la víctima, en lo posible, la acompañará al centro médico respectivo. Si se trata de un cadáver, este será trasladado a la respectiva dependencia del Instituto Nacional de Medicina Legal y Ciencias Forenses o, en su defecto, a un centro médico oficial para que se realice la necropsia médico-legal.

Sobre esos actos urgentes y sus resultados la policía judicial deberá presentar, dentro de las treinta y seis (36) horas siguientes, un informe ejecutivo al fiscal competente para que asuma la dirección, coordinación y control de la investigación.

En cualquier caso, las autoridades de policía judicial harán un reporte de iniciación de su actividad para que la Fiscalía General de la Nación asuma inmediatamente esa dirección, coordinación y control.

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

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

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

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

Código de Procedimiento Penal colombiano. Ley 906 de 2004.

Artículo 82. Procedencia. El comiso procederá sobre los bienes y recursos del penalmente responsable que provengan o sean producto directo o indirecto del delito, o sobre aquellos utilizados o destinados a ser utilizados en los delitos dolosos como medio o instrumentos para la ejecución del mismo, sin perjuicio de los derechos que tengan sobre ellos los sujetos pasivos o los terceros de buena fe.

Cuando los bienes o recursos producto directo o indirecto del delito sean mezclados o encubiertos con bienes de lícita procedencia, el comiso procederá hasta el valor estimado del producto ilícito, salvo que con tal conducta se configure otro delito, pues en este último evento procederá sobre la totalidad de los bienes comprometidos en ella.

Sin perjuicio también de los derechos de las víctimas y terceros de buena fe, el comiso procederá sobre los bienes del penalmente responsable cuyo valor corresponda o sea equivalente al de bienes producto directo o indirecto del delito, cuando de estos no sea posible su localización, identificación o afectación material, o no resulte procedente el comiso en los términos previstos en los incisos precedentes.

Decretado el comiso, los bienes pasarán en forma definitiva a la Fiscalía General de la Nación a través del Fondo Especial para la Administración de Bienes, a menos que la ley disponga su destrucción o destinación diferente.

PARÁGRAFO. Para los efectos del comiso se entenderán por bienes todos los que sean susceptibles de valoración económica o sobre los cuales pueda recaer derecho de dominio, corporales o incorporeales, muebles o inmuebles, tangibles o intangibles, así como los documentos o instrumentos que pongan de manifiesto el derecho sobre los mismos.

Artículo 83. Medidas cautelares sobre bienes susceptibles de comiso. Se tendrán como medidas materiales con el fin de garantizar el comiso la incautación y ocupación, y como medida jurídica la suspensión del poder dispositivo.

Las anteriores medidas procederán cuando se tengan motivos fundados para inferir que los bienes o recursos son producto directo o indirecto de un delito doloso, que su valor equivale a dicho producto, que han sido utilizados o estén destinados a ser utilizados como medio o instrumento de un delito doloso, o que constituyen el objeto material del mismo, salvo que deban ser devueltos al sujeto pasivo, a las víctimas o a terceros.

Artículo 92. Medidas cautelares sobre bienes. El juez de control de garantías, en la audiencia de formulación de la imputación o con posterioridad a ella, a petición del fiscal o de las víctimas directas podrá decretar sobre bienes del imputado o del acusado las medidas cautelares necesarias para proteger el derecho a la indemnización de los perjuicios causados con el delito.

La víctima directa acreditará sumariamente su condición de tal, la naturaleza del daño recibido y la cuantía de su pretensión.

El embargo y secuestro de los bienes se ordenará en cuantía suficiente para garantizar el pago de los perjuicios que se hubieren ocasionado, previa caución que se debe prestar de acuerdo al régimen establecido en el Código de Procedimiento Civil, salvo que la solicitud sea formulada por el fiscal o que exista motivo fundado para eximir de ella al peticionante. El juez, una vez decretado el embargo y secuestro, designará secuestre y adelantará el trámite posterior conforme a las normas que regulan la materia en el Código de Procedimiento Civil.

Cuando las medidas afecten un bien inmueble que esté ocupado o habitado por el imputado o acusado, se dejará en su poder a título de depósito gratuito, con el compromiso de entregarlo a un secuestre o a quien el funcionario indique si se profiere sentencia condenatoria en su contra.

Artículo 236. Recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes. Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado ha estado transmitiendo información útil para la investigación que se adelanta, durante su navegación por internet u otros medios tecnológicos que produzcan efectos equivalentes, ordenará la aprehensión del computador, computadores y servidores que pueda haber utilizado, disquetes y demás medios de almacenamiento físico, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen.

En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos.

La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados.

Artículo 275. Elementos materiales probatorios y evidencia física. Para efectos de este código se entiende por elementos materiales probatorios y evidencia física, los siguientes: (...)

g) El mensaje de datos, como el intercambio electrónico de datos, internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen; (...)

II. COOPERACIÓN INTERNACIONAL

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

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

Sí () No (**X**) No lo sé ()

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

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

Sí () No (**X**) No lo sé ()

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

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

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

III. UNIDADES ESPECIALIZADAS Y ESFUERZOS NACIONALES

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: Dirección de Investigación Criminal e INTERPOL
- Institución de la que depende: Policía Nacional de Colombia
- Dirección en internet de la unidad o instancia: www.ccp.gov.co
- Información de contacto: CAI Virtual
 - o Nombre del titular: Fredy Bautista García
 - o Domicilio: Avenida el Dorado Nro. 75 – 25 Barrio Modelia
 - o Teléfono(s): (+57) (1) 4266241 - 4266302 Fax: (+57) (1) 4266241
 - o Correo electrónico: caivirtual@correo.policia.gov.co

- Nombre de la unidad o instancia: Policía Judicial
- Institución de la que depende: Dirección Nacional del Cuerpo Técnico de Investigaciones - CTI
- Dirección en internet de la unidad o instancia: _____
- Información de contacto: Grupo de Delitos Informáticos
 - o Nombre del titular: Ramiro Augusto Alvarado Figueroa
 - o Domicilio: Carrera 28 No. 17 A – 00 Piso 1 Oficina 125
 - o Teléfono(s): (571) 408 8000 Ext. 3110 Fax: _____
 - o Correo electrónico: oficina.informatica@fiscalia.gov.co

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: Unidad Nacional de Fiscalías Especializadas en delitos contra la propiedad intelectual y comunicaciones.
- Institución de la que depende: Dirección Nacional de Fiscalías
- Dirección en internet de la unidad o instancia: _____
- Información de contacto: Jefe de Unidad
 - o Nombre del titular: Carlos Ricardo Gaitán Bazurto
 - o Domicilio: Carrera 28 No. 18 - 64
 - o Teléfono(s): (571) 408 8000 Ext. 3588 Fax: _____
 - o Correo electrónico: carlos.gaitan@fiscalia.gov.co

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

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

CAI Virtual - Primer servicio de Policía de respuesta a incidentes informáticos en Latinoamérica (www.ccp.gov.co)

Servicio interactivo online dedicado a la ciudadanía con el fin de dar respuesta a cualquier inquietud o atención a los incidentes informáticos en Colombia.

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

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

CAI Virtual - Primer servicio de Policía de respuesta a incidentes informáticos en Latinoamérica. A través del portal web www.ccp.gov.co se envía constantemente recomendaciones de ciberseguridad.

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

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

a) Acceso ilícito	Número de investigaciones: 826
b) Interceptación ilícita	Número de investigaciones: 15
c) Ataques a la integridad de datos	Número de investigaciones: 15
d) Ataques a la integridad de sistemas	Número de investigaciones: 15
e) Abuso de dispositivos	Número de investigaciones: 830
f) Falsificación informática	Número de investigaciones: 102
g) Fraude informático	Número de investigaciones: 5710
h) Pornografía infantil	Número de investigaciones: 117
i) Delitos contra la propiedad intelectual y derechos afines	Número de investigaciones: 61

Fuente: Policía Nacional de Colombia, Dirección de Investigación Criminal e INTERPOL, Área Información y Análisis Criminal; datos extraídos el día 03 de diciembre 2013 a las 14:00 horas, sujeto a variación.

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

a) Acceso ilícito	Casos enjuiciados: <u> -- </u> Condenas <u> -- </u>
b) Interceptación ilícita	Casos enjuiciados: <u> -- </u> Condenas <u> -- </u>

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

Los tipos penales tienen una denominación distinta, razón por la cual se envía anexo a este cuestionario una relación de las condenas que se encuentran registradas en los sistemas de información de la Fiscalía General de la Nación sobre las conductas mencionadas con la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos, pornografía infantil e interceptaciones ilícitas de comunicaciones.

Se adjunta información estadística correspondiente a registros de condenas proferidas por los delitos señalados, durante el periodo comprendido entre el 1 de enero de 2012 al 4 de diciembre de 2013.

Fuente: Fiscalía General de la Nación.

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

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

Se ha encontrado dificultades debido a que la Fiscalía General de la Nación no cuenta con una unidad especializada en la materia que permita una mayor efectividad en la investigación y el enjuiciamiento de estos delitos.

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

Sí () No ()

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

Toda aquella cooperación dirigida al fortalecimiento de las capacidades técnicas y operativas de:

- El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT)
- El Comando Conjunto Cibernético de las Fuerzas Militares (Ccoc)
- El Centro Cibernético Policial (CCP)
- La Fiscalía General de la Nación (Especialmente aquella que permita establecer con mayor agilidad la identificación y ubicación de las direcciones IP desde donde se hayan podido cometer estos delitos)

V. CAPACITACIÓN

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

Sí (**X**) No ()

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

- Seminario de Delitos Informáticos, 50 funcionarios capacitados de las Seccionales de Investigación Criminal SIJIN.
- Diplomado en Informática Forense, 30 funcionarios capacitados de las Seccionales de Investigación Criminal SIJIN.
- Seminario de actualización frente a la estrategia de los delitos informáticos, 18 funcionarios capacitados de las Seccionales de Investigación Criminal SIJIN.

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

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

- Marco penal y procedimental frente a la evidencia digital, 7 funcionarios capacitados de la Unidad de Trata de Personas de la Fiscalía General de la Nación.

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

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

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

- (a) Estado: República de Colombia
(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:
(c) Sr.: Juan Miguel Gómez Valencia
Título/cargo: Coordinador de Prevención del Delito
Organismo/oficina: Ministerio de Relaciones Exteriores
Domicilio: Calle 10 No. 5 - 51
Número de teléfono: (+57) (1) 381400 Ext. 1301 / 3814285
Número de fax: (+57) (1)
Correo electrónico: juanmiguel.gomez@cancilleria.gov.co
MJ00585E01