

Séptima Reunión del Grupo de Trabajo en Delito Cibernético

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

INTRODUCCIÓN

El presente cuestionario busca recolectar información útil para los propósitos de la Séptima Reunión del Grupo de Trabajo en Delito Cibernético, la cual se celebrará el 6 y 7 de febrero de 2012, 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) unidades especializadas y esfuerzos nacionales; (3) cooperación internacional; y (4) capacitación.

Este cuestionario es sustancialmente similar al documento que se envió en noviembre de 2009, con antelación a la Sexta Reunión del Grupo de Trabajo en Delito Cibernético, y a la cual su país respondió en su momento. Para facilitar la elaboración del presente cuestionario, la respuesta de su país al cuestionario anterior se anexa a este documento.

Teniendo en cuenta lo anterior, sírvanse remitir la respuesta de su Estado al presente cuestionario, a más tardar el **viernes, 16 de diciembre de 2011**, 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 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 (X) No () |
| e) Abuso de dispositivos | Sí (X) No () |
| f) Falsificación informática | Sí (X) No () |
| g) Fraude informático | Sí (X) No () |
| h) Pornografía infantil | Sí (X) No () |
| i) Delitos contra la propiedad intelectual y derechos afines | Sí (X) No () |
| j) Otras (sírvase enumerarlas): _____ | Sí () No () |

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

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

En caso afirmativo, sírvase describir esos esfuerzos:

- 1.3. ¿Permite le legislación de emergencia de su país, por parte los investigadores criminales, requerir a los Proveedores de Servicios de Internet a preservar pruebas electrónicas sin la necesidad de una orden judicial? Sí (X) No ()

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

- 1.4. ¿Ha adoptado su país la legislación sustantiva y procesal 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 ()

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

- 1.5. ¿Permite la legislación procesal de su país la interceptación legal de comunicaciones electrónicas transmitidas en su territorio a través de sistemas de computación? Sí (X) No ()

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

Efectivamente se puede intervenir las comunicaciones, sin embargo como lo que se transgrede es una derecho de rango constitucional (Artículos: 24 Constitución Política) se determinar la necesidad de que para imponerse del contenido privado de comunicaciones sea previamente autorizado por un juez de la República, y para ellos existe legislación especial, la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones.

II. UNIDADES ESPECIALIZADAS Y ESFUERZOS NACIONALES

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: Sección de Delitos Informáticos del Organismo de Investigación Judicial.
- Institución de la que depende: Organismo de Investigación Judicial, es la dependencia policial que en el caso de Costa Rica, como policía represiva pertenece al Poder Judicial.
- Información de contacto:
 - o Nombre del Titular: Erick Lewis Hernández.
 - o Domicilio: XX XX.
 - o Teléfono(s): 22953068.
 - o Correo electrónico: elewis(arroba)poder-judicial.go.cr

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: Fiscalía Adjunta en Fraudes, I Circuito Judicial de San José.
- Institución de la que depende: Ministerio Público, Poder Judicial.
- Información de contacto:
 - o Nombre del Titular: Melissa Cristina Román Quesada.
 - o Domicilio: XX XX.
 - o Teléfono(s): 506-2295-3000 Ext. 3450 Fax: 2295-3858
 - o Correo electrónico: mroman@poder-judicial.go.cr

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

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

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

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

III. COOPERACIÓN INTERNACIONAL

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

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

En caso afirmativo, sírvase expresar 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 () No Conozco (X)

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

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

Sí (X) No () No Conozco ()

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

En realidad existen varios instrumentos internacionales sobre cooperación en materia penal que son aplicables a este tipo de delitos, desde instrumentos tan viejos como el Código de Bustamante, sine embargo no hay ningún tratado internacional específico para la materia, lo cuál podría provocar que a la hora de implementar en el caso concreto se pueda entorpecer el asunto. Asimismo el Código Procesal Penal autoriza las investigaciones conjuntas.

- 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 (X) No () No Conozco ()

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

No se lleva un registro específico de este tipo de asistencias, sin embargo de la entrevista a los fiscales de más años en la fiscalía especializada, refieren de al menos dos casos, con Estados Unidos de América y con Panamá. _____

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 () 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 () No (X)

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

- 4.3. De acuerdo con los esfuerzos de su país para ofrecer capacitación en la investigación y persecución de los delitos que 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:

Consultada la Unidad de Capacitación del Ministerio Público, no se establece necesariamente planes de capacitación en este tema en específico, lo que ha provocado que quienes tramitamos o conocemos de este tipo de delito, debamos acudir a la autocapacitación o investigación personal.

- 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 () No Conozco ()

En caso afirmativo, sírvase describir brevemente las personas que han participado; si estos talleres han ofrecido capacitación útil, y cómo los participantes han aplicado esta capacitación en el ejercicio de sus funciones: En realidad no es posible detallar esos alcances, dado a que uno de los funcionarios capacitados ya no labora en la Fiscalía encargada de estas investigaciones y el otro funcionario ha sido ascendido y atiende otro tipo de delincuencias.

- 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:

a- formación básica para los profesionales en derecho que se dedican al ejercicio de la acción penal en estos delitos sobre sistemas informáticos.

b- Tipologías y modus operandi en la región sobre delincuencia cibernética

c- Investigación y coordinación internacional en los delitos cibernéticos.

d- Manejo y cadena de custodia en la prueba del 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: _____

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: Costa Rica

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

() Sr.: Osvaldo Henderson García

() Sra.: _____

Título/cargo: Fiscal Adjunto (jefe)

Organismo/oficina: Fiscalía Adjunta de Fraudes, Ministerio Público.

Domicilio: San José, Costa Rica

Número de teléfono: (506) 2295-4430 y (506) 8730-0438

Número de fax:

Correo electrónico: ohenderson@poder-judicial.go.cr ohenderson@necdata.net

ANEXOS

Respuesta 1.1

Artículo 196 bis.-

Violación de comunicaciones electrónicas

Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.

(Así adicionado por Ley N° 8148 de 24 de octubre del 2001)

"Artículo 217 bis.-

Fraude informático

Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."

(Así adicionado por el artículo 1° de la Ley N° 8148 de 24 de octubre del 2001)

Artículo 229 bis.-

Alteración de datos y sabotaje informático

Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, *borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión.* Si el *programa de cómputo, la base de datos o el*

sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años.

(Así adicionado por Ley N° 8148 de 24 de octubre del 2001)

Fabricación, producción o reproducción de pornografía

Artículo 173.-

Será sancionado con pena de prisión de tres a ocho años, quien fabrique, produzca o reproduzca material pornográfico, utilizando a personas menores de edad, su imagen y/o su voz.

Será sancionado con pena de prisión de uno a cuatro años, quien transporte o ingrese en el país este tipo de material con fines comerciales.

(Así reformado mediante el artículo 1° de la ley N° 8590 del 18 de julio del 2007).

Tenencia de material pornográfico

Artículo 173 bis.-

Será sancionado con pena de prisión de seis meses a dos años, quien posea material pornográfico en el que aparezcan personas menores de edad, ya sea utilizando su imagen y/o su voz.”

(Así adicionado mediante el artículo 1° de la ley N° 8590 del 18 de julio del 2007).

Difusión de pornografía

ARTÍCULO 174.-

Quien comercie, difunda o exhiba material pornográfico a personas menores de edad o incapaces, será sancionado con pena de prisión de uno a cuatro años. La misma pena se impondrá a quien exhiba, difunda, distribuya o comercie, por cualquier medio y cualquier título, material pornográfico en el que aparezcan personas menores de edad o donde se utilice su imagen, o lo posea para estos fines". (Así reformado por el artículo 1° de la ley No.7899 de 3 de agosto de 1999, y posteriormente adicionado el párrafo segundo por Ley N° 8143 de 5 de noviembre del 2001)

Participación de terceros relacionados con la víctima por parentesco o que abusen de su autoridad o cargo.

ARTÍCULO 175.-

Los ascendientes o descendientes por consanguinidad o afinidad, el cónyuge, los hermanos y cualesquiera personas que abusando de su autoridad o de su cargo, cooperaren por cualquier acto directo a la perpetración de los delitos correspondientes a esta Sección y cuya participación no haya sido tipificada expresamente, serán reprimidos con la pena de los autores.

CODIGO DE NORMAS Y PROCEDIMIENTOS TRIBUTARIOS N° 4755

ARTÍCULO 94.- Acceso desautorizado a la información

Será sancionado con prisión de uno a tres años quien, por cualquier medio tecnológico, acceda a los sistemas de información o bases de datos de la Administración Tributaria, sin la autorización correspondiente.

(Así reformado por el artículo 2º de la ley No.7900 de 3 de agosto de 1999)

ARTÍCULO 95.- Manejo indebido de programas de cómputo

Será sancionado con pena de tres a diez años de prisión, quien sin autorización de la Administración Tributaria, se apodere de cualquier programa de cómputo, utilizado por ella para administrar la información tributaria y sus bases de datos, lo copie, destruya, inutilice, altere, transfiera, o lo conserve en su poder, siempre que la Administración Tributaria los haya declarado de uso restringido, mediante resolución.

(Así reformado por el artículo 2º de la ley No.7900 de 3 de agosto de 1999)

ARTÍCULO 96.- Facilitación del código y la clave de acceso

Será sancionado con prisión de tres a cinco años, quien facilite su código y clave de acceso, asignados para ingresar a los sistemas de información tributarios, para que otra persona los use.

(Así reformado por el artículo 2º de la ley No.7900 de 3 de agosto de 1999)

ARTÍCULO 97.- Préstamo de código y clave de acceso

Será sancionado con prisión de seis meses a un año quien, culposamente, permita que su código o clave de acceso, asignados para ingresar a los sistemas de información tributarios, sean utilizados por otra persona.

(Así reformado por el artículo 2º de la ley No.7900 de 3 de agosto de 1999)

Ley General de Aduanas 7557

ARTÍCULO 221.- Delitos informáticos

Será reprimido con prisión de uno a tres años quien:

a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por el Servicio Nacional de Aduanas.

b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el Servicio Nacional de Aduanas, siempre que hayan sido declarados de uso restringido por esta autoridad.

c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos diseñados para las operaciones del Servicio Nacional de Aduanas, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona.

d) Facilite el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos. La pena será de seis meses a un año si el empleo se facilita culposamente.

ARTÍCULO 222.- Agravante

La pena será de tres a cinco años cuando, en alguna de las causales del artículo anterior, concurra una de las siguientes circunstancias:

- a) Intervengan en el hecho tres o más personas, en calidad de autoras.
- b) Intervenga, en calidad de autor, instigador o cómplice, un funcionario público en ejercicio de sus funciones, con ocasión de ellas o con abuso de su cargo.

Ley de la Administración Financiera de la República y Presupuestos Públicos Ley N° 8131

ARTÍCULO 111.- Delito informático

Cometerán delito informático, sancionado con prisión de uno a tres años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la Administración Financiera y de Proveeduría, alguna de las siguientes acciones:

- a) Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido.
- b) Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.
- c) Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas.
- d) Utilizar las facilidades del Sistema para beneficio propio o de terceros.

Respuesta 1.3

Faculta el ordenamiento procesal penal a actuar para asegurar las evidencias o rastros de un delito. Es importante aclarar que además con la inclusión de una Ley Especial sobre la Delincuencia Organizada, determina sanciones hasta la revocatoria de la concesión a las operadoras privadas.

ARTICULO 198.-

Orden de secuestro

El juez, el Ministerio Público y la policía podrán disponer que sean recogidos y conservados los objetos relacionados con el delito, los sujetos a confiscación y aquellos que puedan servir como medios de prueba; para ello, cuando sea necesario, ordenarán su secuestro. En los casos urgentes, esta medida podrá delegarse en un funcionario de la policía judicial.

Ley Contra la Delincuencia Organizada 8754

ARTÍCULO 17.- Obligaciones de los responsables de las empresas de Comunicación

Cualquier empresa, pública o privada, que provea servicios de comunicaciones en el país, estará obligada a realizar lo necesario para la oportuna y eficaz operación del Centro Judicial de Intervención de las Comunicaciones (CJIC), según los requerimientos de este Centro.

Serán obligaciones de las empresas y de los funcionarios responsables de las empresas o las instituciones públicas y privadas a cargo de las comunicaciones, las siguientes:

- 1) Dar todas las facilidades para que las medidas ordenadas por el juez competente se hagan efectivas.
- 2) Acatar la orden judicial, de manera tal que no se retarde, obstaculice ni se impida la ejecución de la medida ordenada.

El incumplimiento de esta norma traerá como consecuencia la sanción de cancelación de la concesión o el permiso de operación de la empresa, para la actividad de comunicaciones.

Los órganos encargados de aplicar la sanción anteriormente indicada, a las empresas, serán los establecidos en la Ley general de telecomunicaciones, N.º 8642, de 4 de junio de 2008, y en las demás leyes, los reglamentos y las que regulen las condiciones de la concesión

1.4 Sobre posibilidad de confiscar, decomisar o secuestrar sistemas o dispositivos de almacenamiento informáticos; así como copiar y conservar los datos informáticos consultados, se regulan no solo en las potestades de investigación que refieren normativas generales como el Código Procesal Penal en sus artículos 185, 189, 190, 193, 194 y 198, sino que además la Ley Orgánica del Organismo de Investigación Judicial en sus numerales 5 y siguientes establecen las atribuciones de la policía judicial ante la comisión de un delito.

ARTICULO 185.-

Inspección y registro del lugar del hecho

Cuando sea necesario inspeccionar lugares o cosas por existir motivos suficientes para sospechar que se encontrarán rastros del delito o por presumirse que, en determinado lugar, se oculta el imputado o alguna persona evadida, se procederá a su registro.

Mediante la inspección se comprobará el estado de las personas, los lugares, las cosas, los rastros y otros efectos materiales existentes, que resulten de utilidad para averiguar el hecho o individualizar a sus autores o partícipes.

El representante del Ministerio Público será el encargado de realizar la diligencia, salvo que se disponga lo contrario. Se invitará a presenciar la inspección a quien habite el lugar o esté en él cuando se efectúa o, en su ausencia, a su encargado o a cualquier persona mayor de edad. Se preferirá a familiares del primero.

ARTICULO 186.-

Acta

De la diligencia de inspección y registro, se levantará un acta que describirá, detalladamente, el estado de las cosas y las personas y, cuando sea posible, se recogerán o se conservarán los elementos probatorios útiles. Si el hecho no dejó rastros, ni produjo efectos materiales o si estos desaparecieron o fueron alterados, el encargado de la diligencia describirá el estado existente y, en lo posible, verificará el anterior. En caso de desaparición o alteración, averiguará y hará constar el modo, el tiempo y la causa que la provocó.

ARTICULO 187.-

Facultades coercitivas

Para realizar la inspección y el registro, podrá ordenarse que, durante la diligencia, no se ausenten quienes se encuentran en el lugar o que cualquier otra persona comparezca inmediatamente.

ARTICULO 188.-

Inspección corporal

Cuando sea necesario, el juez o el fiscal encargado de la investigación podrá ordenar la inspección corporal del imputado y, en tal caso cuidará que se respete su pudor. Con la misma limitación, podrá disponer igual medida respecto de otra persona, en los casos de sospecha grave y fundada o de absoluta necesidad.

Si es preciso, la inspección podrá practicarse con el auxilio de peritos.

Al acto sólo podrá asistir una persona de confianza del examinado, quien será advertido previamente de tal derecho.

ARTICULO 189.-

Requisa

El juez, el fiscal o la policía podrán realizar la requisa personal, siempre que haya motivos suficientes para presumir que alguien oculta pertenencias entre sus ropas o que lleva adheridos a su cuerpo objetos relacionados con el delito. Antes de proceder a la requisa, deberá advertir a la persona acerca de la sospecha y del objeto buscado, invitándola a exhibirlo. La advertencia e inspección se realizará en presencia de un testigo, que no deberá tener vinculación con la policía. Las requisas se practicarán separadamente, respetando el pudor de las personas. Las requisas de mujeres las harán otras mujeres. Se elaborará un acta, que podrá ser incorporada al juicio por lectura.

ARTICULO 190.-

Registro de vehículos

El juez, el fiscal o la policía podrán registrar un vehículo, siempre que haya motivos suficientes para presumir que una persona oculta en él objetos relacionados con el delito. En lo que sea aplicable, se realizará el mismo procedimiento y se cumplirá con las mismas formalidades previstas para la requisa de personas.

ARTICULO 193.-

Allanamiento y registro de morada

Cuando el registro deba efectuarse en un lugar habitado, en sus dependencias, casa de negocio u oficina, el allanamiento y registro será realizado personalmente por el juez y deberá iniciarlo entre las seis y las dieciocho horas. Podrá procederse a cualquier hora cuando el morador o su representante consienta o en los casos sumamente graves y urgentes. Deberá dejarse constancia de la situación de urgencia en la resolución que acuerda el allanamiento.

ARTICULO 194.-

Allanamiento de otros locales

El allanamiento de locales públicos, establecimientos de reunión o recreo mientras estén abiertos al público y no estén destinados a habitación, será acordado por el juez, quien podrá delegar la realización de la diligencia en funcionarios del Ministerio Público o de la policía judicial. No regirán las limitaciones horarias establecidas en el artículo anterior. En estos casos, deberá avisarse a las personas encargadas de los locales, salvo que sea perjudicial para la investigación.

Respuesta 1.5

Efectivamente se puede intervenir las comunicaciones, sin embargo como lo que se transgrede es un derecho de rango constitucional (Artículos: 24 Constitución Política) se determinar la necesidad de que para imponerse del contenido privado de comunicaciones sea previamente autorizado por un juez de la República, y para ellos existe legislación especial, la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones.

Respuesta 3.5

ARTICULO 65.-

Cooperación internacional

Cuando las actividades delictivas se realicen, en todo o en parte, fuera del territorio nacional, o se les atribuyan a personas ligadas a una organización de carácter regional o internacional, en los casos en que deba aplicarse la legislación penal costarricense, el Ministerio Público podrá formar equipos conjuntos de investigación con instituciones extranjeras o internacionales.

Los acuerdos de investigación conjunta deberán ser aprobados y supervisados por el Fiscal General.