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

OEA/Ser. K/XXXIV
CIBER – VII/doc.2/11
14 de noviembre de 2011
Original: Inglés

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 lar Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las América (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; 7 (4) capacitación.

Este cuestionario es sustancialmente similar al documento que se envío en noviembre 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 ( ) No (X)
d) Ataques a la integridad de sistemas Sí (X) No ( )
e) Abuso de dispositivos Sí ( ) No (X)
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 (X) No ( )
Hurto, Daños, Terrorismo, Contra el Honor Delitos Financieros, Contra la Intimidad e Inviolabilidad de la Correspondencia, Revelación de los Secretos Empresariales y Contra la Personalidad Interna del Estado

En caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica, de la legislación: El Código Penal Panameño vigente. (Ver cuadro de anexo).

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 (X) No ( )

En caso afirmativo, sírvase describir esfuerzos: En la actualidad el Ministerio Público a través de la Fiscalía Superior Especializada en delitos Contra la Propiedad Intelectual y Seguridad Informática, por designación del señor Procurador General de la Nación, elaboró un borrador de anteproyecto de ley en delitos cibernéticos y se encuentra participando en reuniones de trabajo con diversos sectores, entre los cuales se destacan la Autoridad de Innovación Gubernamental, la Policía Nacional, Instituto de Medicina Legal, Sector Privado, además de otras organizaciones internacionales como la Organización de los Estados Americanos y Las Naciones Unidas; con el propósito de revisar el borrador de Anteproyecto de Ley relacionado a delitos *cibernéticos, el cual* fue presentado en la Asamblea Legislativa en adición a un Anteproyecto que reposaba en la Comisión de Gobierno y será discutido en enero del año 2012.

1.3. ¿Permite la legislación de emergencia de su país, por parte los investigadores criminales, requerir a los Proveedores de Servicios de Internet a preservar pruebas electrónicas sin la necesidad de una orden judicial?: En nuestro país, la preservación de las pruebas electrónicas a través de los Proveedores de servicios de Internet, requieren de la orden del Fiscal, en la Ciudad capital y en las Provincias de Chiriquí, Colón, Herrera, Los Santos y Bocas del Toro. No obstante, en las Provincias de Coclé y Veraguas se realiza a través del Sistema Penal Acusatorio.

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: Nuestra Legislación regula tanto en el Código Procesal; así como leyes especiales todo lo referente a datos informáticos y almacenamiento.

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

En caso afirmativo, sírvase describir brevemente y adjuntar copias, de preferencia electrónica, de legislación: En nuestra legislación toda incautación o aprehensión de comunicaciones de sistema de comunicación debe solicitarse ante el Tribunal.

II. UNIDADES ESPECIALIZADAS Y ESFUERZOS NACIONALES

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

Esta en proceso de creación de una unidad en la policía para investigar los delitos cibernéticos. Solo existe la Sección de delitos Informáticos del Instituto de Medicina Legal y Ciencias Forense, encargada de efectuar los peritajes.

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: _____
- Institución de la que depende: _____
- Información de contacto: _____
  - Nombre del Titula: _____
  - Domicilio: _____
  - Teléfono: _____
  - Correo Electrónico: _____

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la unidad o instancia: _Fiscalía Superior Especializada en Delitos contra la propiedad Intelectual y Seguridad Informática
- Institución de la que depende: __Ministerio Público
- Información de contacto: _____
  - Nombre del Titula: __Nayra Gisela Fernández Ruíz_____
  - Domicilio: _Vía España, Edificio Avesa, Tercer Piso.
  - Teléfono: __(507)_505-32-73_/_Fax: (507)505-32-98
  - Correo Electrónico: _nayra.fernandez@procuraduria.gob.pa; _nfernandez_ruiz@hotmail.com

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

No existe una página específica de la república de Panamá. No obstante, se creó el Centro de Incidentes a Respuesta (CERT PANAMÁ) el cual está en su periodo de adecuación.

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

_____
_____

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

En caso afirmativo, sírvase describir brevemente en qué consiste esa estrategia En estos momentos a través de un Decreto Ejecutivo se creó el CERT PANAMÁ el cual está laborando su estrategia de implementación con el apoyo y coordinación del Ministerio Público, el cual mantiene una Fiscalía Especializada en el tema informático.

III. **COOPERACIÓN INTERNACIONAL**

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

En caso negativo ¿Ha considerado su país la aplicación de los principios contenidos en dicha Convención? SI (X) NO ( ) No Conozco ( )

Actualmente el Ministerio Público, está realizando las gestiones con el Ministerio de Relaciones Exteriores, para que Panamá pueda suscribirse al Convenio de Budapest.

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? SI ( ) NO (X)

En caso negativo, ¿Ha tomado su país alguna(s) medida(s) para vincularse? SI (X) NO ( ) No Conozco ( )

El Ministerio Público está evaluando la posibilidad vincularse a la Red de Emergencia de Contactos sobre Delitos de Alta Tecnología 24 horas /7 días del G-8, dentro de las estrategia integrales sobre materia de Cibercrimen.

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

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

SI ( ) NO (X) No Conozco ( )

Hasta el momento no se ha ratificado ningún convenio de forma específica, sin embargo, se aplica el principio de reciprocidad entre los Estados.

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

3.4. ¿Ha formulado o recibido su país solicitudes de asistencia mutua para la investigación o juzgamiento de delitos cibernéticos o bien para la obtención de pruebas electrónicas y la realización de otros actos necesarios para facilitar la investigación o juzgamiento de estos delitos? SI (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. Una solicitud de la Fiscalía de Delincuencia Organizada por delito cibernético.

IV. <u>CAPACITACIÓN</u>

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

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

<u>El Ministerio Público, a través de la Fiscalía Superior Especializada en Delitos Contra la Propiedad Intelectual y Seguridad Informática, ha organizado capacitaciones en torno al tema de Seguridad Informática; además ha sido invitado por otras instituciones para participar en capacitaciones referente al tema de Seguridad Informática.</u>

<u>El cuadro anexo detalla las diferentes capacitaciones de Seguridad Informática a los Funcionarios</u>

TÍTULO	NOMBRE DEL SEMINARIO	FECHA	DURACIÓN	LUGAR	AUSPICIADO POR	Funcionarios Participantes
	Seminario Taller de Seguridad	Febrero 2011	5 días	México, D.F.	O.E.A.	1
Seguridad Informática	Seminario Taller de Seguridad	Marzo 2011	5 días	México, D.F.	O.E.A.	1
	Internet como Medio para cometer Delitos	7 de julio de 2011	1 día	Escuela Judicial - Órgano Judicial	Escuela Judicial	2
	Crimen Cibernético	15 al 19 de agosto de 2011	5 días	El Salvador	Sección de Asuntos de Narcóticos de la Embajada Americana en Panamá	1
	Criminalidad Cibernética	18 al 19 de agosto de 2011	2 días	Salón de Capacitación de Llanos de Curundú	Ministerio Público (FEPISI)	3
	Cybercriminalidad y Delitos Ciberneticos	20 al22 de septiembre de 2011	2 dias y medio	Escuela Judicial	Escuela Judicial y la Embajada Francia	5
	Taller Nacional sobre la Prevención e Investigación ante Incidentes de Seguridad Cibernética	24 y 25 de nov. 2011	2 dias	Hotel Marriot	OEA, CICTE, AIG, PGN	6
	Seminario Taller Seguridad Cibernética	Noviembre 2011	4 días	Bogotá, Colombia	O.E.A.	1
					TOTAL DE FUNCIONARIOS PARTICIPANTES	**20**

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

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

La Fiscal Superior Especializada en delitos Contra la Propiedad Intelectual y Seguridad Informática ha participado en las siguientes capacitaciones:

TÍTULO	NOMBRE DEL SEMINARIO	FECHA	DURACIÓN	LUGAR	AUSPICIADO POR
Seguridad Informática	Seminario Taller sobre Seguridad Cibernética	Mayo 2011	5 días	Miami	OEA (CICTE)
	Criminalidad Cibernética	18 al 19 de agosto de 2011	2 días	Salón de Capacitación de Llanos de Curundú	Ministerio Público (FEPISI)
	Taller Nacional sobre la Prevención e Investigación ante Incidentes de Seguridad Cibernética	24 y 25 de nov. 2011	2 dias	Hotel Marriot	OEA, CICTE, AIG, PGN

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:

	Objetivos	Condiciones para Lograrlo
1	Contar con una división de Delitos Cibernéticos en la Dirección de Investigación Judicial de la Policía Nacional	Lograr la obtención de los recursos por parte de la Dirección de Investigación Judicial (DIJ), para dar paso a la propuesta de la Procuraduría General de la Nación
2	Ejecutar el Centro de Respuesta a Incidente (CERT PANAMA)	El CERT PANAMÁ está recién creado se está realizando las gestiones para su divulgación, además se está analizando las capacitaciones en torno a delitos informáticos, además de organizar el segundo taller sobre seguridad cibernética funciones con el éxito que se espera.
3	Referencias Penales y Procesales	En enero de 2012 se reinicia las sesiones en la Asamblea Legislativa, por lo que estamos en espera que se discuta en primer debate el borrador del Anteproyecto de Ley que redacto el Ministerio Público, y que entregó a la Asamblea para que se adicionara al anteproyecto de Ley que propuso un diputado de la Asamblea.
4	Capacitación de la Policía, Peritos y Fiscalía (En noviembre de 2011 se realizó un seminario taller organizado por la OEA y CICTE) también nos apoyo REMJA	Contar con apoyo técnico de profesionales, propuesta por organizaciones internacionales para lograr la capacitación.

4.4. ¿Ha participado su país en los talleres de capacitación celebrados en el marco del Grupo de Trabajo en Delitos Cibernéticos? SI (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 estas capacitaciones en el ejercicio de sus funciones.

Los funcionarios que han recibido capacitación útil han sido el licenciado Giann Carlo Mascarin, licenciada Vanessa Barrías, licenciada Malesky Halphen, licenciada Nayra Fernández Ruiz y, la ingeniera Aixa Ruiz López. Todos han aplicado los conocimientos adquiridos.

4.5. Sírvase 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:

Los temas que debieran incorporarse son talleres prácticos que incluyan el manejos y recolección de evidencia digital de alta tecnología, manejo de evidencia en la escena del delito, actualización de los programas, equipos y herramientas informáticas que han salidos nuevos y que son utilizado para cometer delitos y finalmente una asesoría que incluyan las políticas y estándares para la construcción de laboratorio forense digital para Panamá.

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:

El REMJA debiera recomendar que la OEA prohíje la Convención sobre Delincuencia Cibernética, lo que facilitaría que los Estados miembros ratifiquen. Un mayor adiestramiento, asesoría a las personas que manejan el tema de delitos cibernético.

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: Panamá
(b) El funcionario a quién puede consultarse sobre las respuesta dada a este cuestionario es:
(c) Sr.:
(d) Sra. : Licda. Nayra Fernández Ruiz

Título / Cargo: _Fiscal Superior Especializada en Delitos contra la Propiedad Intelectual y Seguridad Informática

Organismo / Oficina: _Ministerio Público de Panamá_____

Domicilio: Vía España, Edificio Avesa; Piso 3_____

Número de teléfono: (507) 505-3278 32-55_____

Número de Fax: ____(507) 505-3256_____

Correo Electrónico: nayra.fernandez@procuraduria.gob.pa__

REPÚBLICA DE PANAMÁ CÓDIGO PENAL **Título VIII** Delitos contra la Seguridad Jurídica de los Medios Electrónicos **Capítulo I** Delitos contra la Seguridad Informática	
Acceso ilícito	**Artículo 289 - Código Penal.** Quien indebidamente ingrese o utilice una base de datos, red o sistema informático será sancionado con dos a cuatro años de prisión.
Intercepción ilícita	**Artículo 290- Código Penal**. Quien indebidamente se apodere, copie, utilice o modifique los datos en tránsito o contenidos en una **base de datos** o sistema informático, o interfiera, **intercepte**, obstaculice o impida su transmisión será sancionado con dos a cuatro años de prisión.
Atentados contra la integridad de datos	El artículo 290, antes citado, solamente contempla la modificación (alteración) de base de datos o sistema informático, por lo que no se sanciona su supresión, deterioro o daño, total o parcial.
Atentados contra la integridad del sistema	**Artículo 290- Código Penal**. Quien indebidamente se apodere, copie, utilice o modifique los datos en tránsito o contenidos en una base de datos o **sistema informático**, o interfiera, intercepte, **obstaculice** o impida su **transmisión** será sancionado con dos a cuatro años de prisión.
Abuso de equipos	Carecemos de una norma penal que sancione esta actividad.
DELITOS INFORMATIZADOS	
Falsedad informática	**Artículo 366- Código Penal.** Quien falsifique o altere, total o parcialmente, una escritura pública, un documento público o auténtico o la **firma digital** informática de otro, de modo que pueda resultar perjuicio, será sancionado con prisión de cuatro a ocho años. Igual sanción se impondrá a quien inserte o haga insertar en un documento público o auténtico declaraciones falsas concernientes a un hecho que el documento deba probar, siempre que pueda ocasionar un perjuicio a otro.
	Artículo 368- Código Penal. Quien falsifique, en todo o en parte, un documento privado, siempre que ocasione un perjuicio a otro, será sancionado con prisión de uno a dos años o su equivalente en días-multa o arresto de fines de semana. **Artículo 61- Ley 51 de 2008 [Documentos y Firmas Electrónica].** Responsabilidad penal por alteración o adulteración de documentos almacenados tecnológicamente. Las personas que incurran en cualquier alteración o adulteración de las películas, microfichas, discos o certificaciones, antes, durante o después de la fecha de reproducción del documento respectivo, responderán penalmente por su actuación y quedarán sujetas a las sanciones tipificadas en el Código Penal, relativas a los delitos contra la fe pública, sin perjuicio de la responsabilidad civil o administrativa que pudiera corresponderles.
Estafa informática	**Artículo 220- Código Penal.** Quien mediante engaño se procure o procure a un tercero un provecho ilícito en perjuicio de otro será sancionado con prisión de uno a cuatro años. La sanción se aumentará hasta un tercio cuando se cometa abusando de las relaciones personales o profesionales, o cuando se realice a través de un medio cibernético o informático.

	Artículo 226- Código Penal. Quien, para procurarse para sí o para un tercero un provecho ilícito, altere, modifique o manipule programas, bases de datos, redes o sistemas informáticos, en perjuicio de un tercero, será sancionado con cuatro a seis años de prisión. La sanción será de cinco a ocho años de prisión cuando el hecho sea cometido por la persona encargada o responsable de la base de datos, redes o sistema informático o por la persona autorizada para acceder a estos, o cuando el hecho lo cometió la persona valiéndose de información privilegiada.
Infracciones relativas a la pornografía infantil	**Artículo 184 Código Penal.** Quien fabrique, elabore por cualquier medio o produzca material pornográfico o lo ofrezca, comercie, exhiba, publique, publicite, difunda o **distribuya a través de Internet** o de cualquier medio masivo de comunicación o información nacional o internacional, presentando o **representando virtualmente** a una o varias personas menores de edad en actividades de carácter sexual, sean **reales o simuladas**, será sancionado con prisión de cinco a diez años. La pena será de diez a quince años de prisión si la víctima es una persona menor de catorce años, si el autor pertenece a una organización criminal nacional o internacional o si el acto se realiza con ánimo de lucro. **Artículo 185 Código Penal.** Quien **posea** para su propio uso material pornográfico que contenga la imagen, real o simulada, de personas menores de edad, voluntariamente adquirido, será sancionado con pena de prisión de tres a cinco años.
Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines	**Artículo 263 Código Penal.** Se impondrá pena de dos a cuatro años de prisión a quien, sin la correspondiente autorización del titular o fuera de los límites permitidos por las normas sobre los Derechos de Autor y Derechos Conexos, realice cualesquiera de las siguientes conductas: 1. Inscriba en el Registro de Derecho de Autor y Derechos Conexos una obra, interpretación o producción ajena, como si fuera propia o de persona distinta del verdadero autor, artista o productor. 2. Utilice ejemplares de la obra, sin autorización y los ponga a disposición del público, inclusive la distribución de fonogramas. 3. Presente declaraciones falsas de certificaciones de ingresos, repertorio utilizando identificación de los autores; autorización obtenida, número de ejemplares o cualquier otra adulteración de datos susceptibles de causar perjuicio a cualquiera de los titulares de derechos protegidos. 4. Realice actividades propias de una entidad de gestión colectiva, sin contar con la resolución emitida al efecto por la autoridad competente. 5. Usurpe la paternidad de una obra protegida por el Derecho de Autor y Derechos Conexos. 6. Reproduzca, copie o modifique íntegra o parcialmente una obra protegida por el Derecho de Autor y Derechos Conexos. **Artículo 264.** Se impondrá la pena de cuatro a seis años de prisión a quien, sin la correspondiente autorización del titular o fuera de los límites permitidos por las normas sobre los Derechos de Autor y Derechos Conexos, ejecute alguna de las siguientes conductas: 1. Almacene, distribuya, exporte, ensamble, fabrique, venda, alquile o ponga en circulación de cualquier otra manera reproducción ilícita de una obra protegida por el Derecho de Autor y Derechos Conexos. 2. Introduzca en el país cantidades significativas, con fines comerciales, reproducciones ilícitas de obras protegidas por el

	Derecho de Autor y Derechos Conexos. 3. Reproduzca, copie o modifique, con carácter industrial o mediante laboratorios o mediante procesos automatizados, obras protegidas por el Derecho de Autor y Derechos Conexos. **Artículo 265.** La misma pena prevista en el artículo anterior se le aplicará a quien sin autorización reproduzca o copie, por cualquier medio, la actuación de un intérprete o ejecutante, un fonograma, videograma, programas de ordenador o una emisión de radiodifusión en todo o en parte, o introduzca en el país, almacene, distribuya, exporte, venda, alquile o ponga en circulación, de cualquier otra manera, dichas reproducciones o copias.
OTRAS NORMAS PENALES	
Inviolabilidad del secreto y derecho a la intimidad	**Artículo 164.** Quien se apodere o informe indebidamente del contenido de una carta, mensaje de correo electrónico, pliego, despacho cablegráfico o de otra naturaleza, que no le haya sido dirigido, será sancionado con prisión de uno a tres años o su equivalente en días- multa o arresto de fines de semana. Cuando la persona que ha cometido el delito obtiene algún beneficio o divulgue la información obtenida y de ello resultara perjuicio, será sancionada con dos a cuatro años de prisión o su equivalente en días-multa, prisión domiciliaria o trabajo comunitario. Si la persona ha obtenido la información a que se refiere el párrafo anterior como servidor público o trabajador de alguna empresa de telecomunicación y la divulga, la sanción se aumentará de una sexta parte a la mitad. **Artículo 165.** Quien sustraiga, destruya, sustituya, oculte, extravíe, intercepte o bloquee una carta, pliego, correo electrónico, despacho cablegráfico o de otra naturaleza, dirigidos a otras personas, será sancionado con pena de prisión de dos a cuatro años o su equivalente en días-multa o arresto de fines de semana, la cual se aumentará en una sexta parte si lo divulgara o revelara. Si la persona que ha cometido la acción es servidor público o empleado de alguna empresa de telecomunicación, la sanción será de tres a cinco años de prisión, la cual se aumentará en una sexta parte si lo revelara o divulgara.
Contra el honor de la persona natural	**Artículo 195.** Cuando alguno de los delitos anteriores se cometa a través de un medio de comunicación social oral o escrito o utilizando un sistema informático, será sancionado en caso de injuria con prisión de seis a doce meses o su equivalente en días multa, y tratándose de calumnia, con prisión de doce a dieciocho meses o su equivalente en días-multa.
Delitos financieros	**Artículo 243.** Quien, en beneficio propio o de un tercero, se apodere, ocasione la transferencia ilícita o haga uso indebido de dinero, valores u otros recursos financieros de una entidad bancaria, empresa financiera u otra que capte o intermedie con recursos financieros del público o que se le hayan confiado, o realice esas conductas a través de manipulación informática, fraudulenta o de medios tecnológicos, será sancionado con prisión de cuatro a seis años. La sanción será de seis a ocho años de prisión, cuando el hecho punible es cometido por un empleado, trabajador, directivo, dignatario, administrador o representante legal de la entidad o empresa, aprovechándose de su posición o del error ajeno.

Revelación de secretos empresariales	**Artículo 288.** Quien, para descubrir innovaciones o secretos de un agente económico, se apodere de datos, información, soporte informático, procedimiento, fórmula o informe, siempre que cause perjuicio a este, será sancionado con prisión de dos a cuatro años. La prisión será de tres a seis años, si el autor se apodera de los secretos de la empresa como servidor público, trabajador de la empresa o en virtud de la prestación de servicios profesionales.
Hurto	**Artículo 213.** Quien se apodere de una cosa mueble ajena será sancionado con prisión de uno a tres años o su equivalente en días multa o arresto de fines de semana o trabajo comunitario. Igual sanción se le aplicará al copropietario, heredero o coheredero que se apodere de la cuota parte que no le corresponde, o a quien se apodere de los bienes de una herencia no aceptada. **Artículo 214.** La sanción será de cuatro a seis años de prisión, en los siguientes casos: … 13. Cuando se cometa por medios tecnológicos o maniobras fraudulentas de carácter informático.
Daños	**Artículo 230.** Quien destruya, inutilice, rompa o dañe cosa mueble o inmueble que pertenezca a otro será sancionado con pena de uno a dos años de prisión o su equivalente en días-multa o arresto de fines de semana. La sanción se aumentará de una cuarta parte a la mitad de la pena si el delito se comete: 1. En perjuicio de un servidor público, a causa del ejercicio de sus funciones. 2. Mediante intimidación o violencia contra tercero. 3. Con destrucción o grave daño en residencia, oficina particular, edificio o bien público, bien destinado al servicio público, edificio privado o destinado al ejercicio de algún culto, vehículo oficial, monumento público, cementerio o cosa de valor científico, cultural, histórico o artístico. 4. En una plantación, sementera o en las cercas protectoras de fundos agrícolas o pecuarios. 5. Mediante la utilización de sustancia venenosa o corrosiva. 6. Si el daño total ocasionado supera la suma de dos mil balboas (B/.2,000.00), independientemente del valor del bien que se haya afectado directamente con la acción. Cuando el daño se ocasione utilizando instrumentos o medios informáticos, computadora, dato, red o programa de esa naturaleza, la pena será de dos a cuatro años de prisión.
Terrorismo	**Artículo 295.** Quien utilice la Internet para enseñar a construir bombas o reclutar personas para realizar actos con fines terroristas será sancionado con prisión de cinco a diez años.
Contra la personalidad interna del Estado	**Artículo 429.** Quien, sin facultad legal para ello, acceda a la seguridad informática del Estado, levante plano o reproduzca imagen, por cualquier medio, de buque, aeronave, establecimiento, vía u obra destinado a la seguridad del Estado será sancionado con prisión de dos a cuatro años.