Cuestionario Preparatorio de la Sexta Reunión del
Grupo de Trabajo en Delito Cibernético

I. INTRODUCCIÓN

1.1 . ¿ha adoptado su país legislación para prevenir, investigar y sancionar el delito cibernético?
Si (√) No ( )
En caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica de la legislación: Adjunto lo Indicado .

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

a)	Accedo Ilícito	Si (√) No ( )
b)	Interceptación Ilícita	Si (√) No ( )
c)	Ataques a la integridad de datos	Si ( ) No (√)
d)	Ataques a la integridad de sistemas	Si (√) No ( )
e)	Abuso de dispositivos	Si ( ) No (√)
f)	Falsificación Informática	Si (√) No ( )
g)	Fraude Informático	Si (√) No ( )
h)	Pornografía Infantil	Si (√) No ( )
i)	Delitos contra la Propiedad Intelectual y derechos afines	Si (√) No ( )
j)	Otros (sírvase enunciar)	Si (√) No ( )

El Código Penal también contempla otros delitos informatizados: hurto, daños, terrorismo, contra el honor, contra la intimidad e inviolabilidad de la correspondencia, delitos financieros, revelación de secretos empresariales, contra la personalidad interna del estado

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

Si su país ha tipificado alguna de las anteriores conductas, mencione brevemente los resultados que se han obtenido al respecto, tales como procesos judiciales en curso y sus resultados: La legislación es reciente, (entró a regir el 23 de mayo de 2008), por lo que las experiencias son escasas. La Fiscalía Superior Especializada en Delitos Contra la Propiedad Intelectual y Seguridad Informática, desde entonces, a la fecha ha investigado 12 causas por actos que atentan contra la Seguridad Informática. De estos, 3 culminaron con sobreseimiento, 1 con solicitud de llamamiento a juicio y los otros están bajo investigación.

En caso de que su país no haya tipificado alguna de las anteriores conductas, indique si está desarrollando algunas acciones para hacerlo: Se han adelantado

conversaciones con algunos sectores, pero no se ha presentado propuesta de reforma al Código Penal.

1.3. ¿Ha adoptado su país la legislación sustantiva y procesal u otras medidas necesarias para asegurar la obtención y conservación electrónicas de cualquier delito?
Si (√) No ( )

En caso afirmativo, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjunte copia, de preferencia electrónica de las mismas: Es aplicable la normativa "tradicional", por lo que la obtención de las evidencias electrónicas se hará a través de diligencias de interceptación de comunicaciones, allanamientos, registros e inspecciones, pudiendo participar en esta última peritos. (Ver cuadro adjunto).

1.4. ¿Ha adoptado su país la legislación sustantiva y procesal u otras medidas necesarias para permitir la admisibilidad en los procesos y juicios penales de pruebas electrónicas?
Si (√) No ( )

En caso afirmativo, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjunte copia, de preferencia electrónica de las mismas: En materia documental en lo que respecta a documentación privada, el artículo 873, del Código Judicial señala no obstante falta actualizar el resto de la normativa para incluir otros supuestos en referencia al valor de la prueba electrónica.

> **Artículo 873**. Los documentos que se acompañen a los escritos o aquéllos cuya incorporación se solicite a título de prueba, podrán presentarse en su original, en copia en los casos del artículo 857, en copia fotostática, fotográfica o fotocopia o mediante cualquier otro procedimiento similar. Las copias fotográficas y similares que reproduzcan el documento y sean claramente legibles, se tendrán por fidedignas, salvo prueba en contrario.
> Si el juez o la parte contraria lo solicitare, deberá ser exhibido el documento original, o su equivalente electrónico, siempre y cuando se haya almacenado tecnológicamente conforme a la ley.
> Se exceptúan los documentos negociables y cualquier otro que contenga crédito cedible o endosable.

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

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

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

En caso afirmativo, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjunte copia, de preferencia electrónica, de las mismas: Ley 51 de 2009;

a) El requerimiento de información a particulares se hace a través de diligencias de allanamiento y con posterioridad una inspección con la participación de las partes

> **Artículo 2178.** El funcionario de instrucción puede allanar un edificio de cualquier clase, establecimiento o finca cuando haya indicio grave de que allí se encuentra el presunto imputado, efectos o instrumentos empleados para la infracción, libros, papeles, documentos o cualesquiera otros objetos que puedan servir para comprobar el hecho punible o para descubrir a sus autores y partícipes.
> Tales allanamientos se practicarán entre las seis de la mañana y las diez de la noche; pero podrán verificarse a cualquier hora, en lugares en que el público tiene libre acceso en los casos de flagrante delito o cuando sea urgente practicar la diligencia. En todo caso, el allanamiento deberá ser decretado por el funcionario de instrucción.
>
> **Artículo 2077.** Cuando fuere conveniente para esclarecer y comprobar el hecho, se ordenará la práctica de una inspección ocular que se comunicará a los interesados con la anticipación debida y no se suspenderá por la no comparencia de éstos.

b) El requerimiento a un proveedor se regula por lo dispuesto en la Ley 51 de 2009.

> **Artículo 1.** Las empresas concesionarias, los distribuidores, los agentes autorizados y los revendedores de telefonía móvil, fija y troncal, los Internet cafés, las infoplazas y las redes de comunicación que presten el servicio y/o lo comercialicen, en o desde la República de Panamá, deberán establecer y conservar un registro de datos que proporcione la identificación y dirección suministradas por los usuarios que contraten sus servicios, en cualquiera de sus modalidades, en todo el territorio nacional.

Artículo 3. Las empresas concesionarias, los distribuidores, los agentes autorizados y los revendedores de telefonía móvil, fija y troncal, los Internet cafés, las infoplazas y las redes de comunicación establecidos en el territorio nacional están obligados a adoptar las medidas necesarias para garantizar que los datos señalados en el artículo anterior se conserven debidamente en tales empresas, en la medida en que sean generados por estas en el marco de la prestación de los servicios de comunicación y comercialización de que se traten, y por el término que se establece en el artículo 6 de la presente Ley.

Artículo 6. La obligación de conservar los datos señalados en esta Ley por parte de las empresas prestadoras de los servicios cesa a los seis meses, contados desde la fecha en que se haya generado la información. No obstante, a solicitud de autoridad judicial de información específica, se podrá ampliar el plazo de conservación para determinados datos, hasta un máximo de seis meses adicionales al periodo anterior, tomando en consideración el costo del almacenamiento y la conservación de los datos, así como el interés de estos para los fines de detención, investigación y enjuiciamiento de los delitos.

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

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

En aquellos casos afirmativos, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adicione copia, de preferencia electrónica, de las mismas: Como se mencionara en respuesta anterior son aplicables para la confiscación y aseguramiento de sistemas informáticos la normativa tradicional (allanamiento, registro e inspección). Por su parte lo referente a la preservación de la integridad de los datos informáticos se rigen por lo dispuesto en la ley 51 del 2009 (ver artículos transcritos en respuesta 1.5).

1.7. ¿Ha adoptado su país la legislación sustantiva y procesal u otras medidas necesarias que permitan a sus autoridades competentes, obtener e intercambiar

información relativa al tráfico y contenido de comunicaciones especificas transmitidas en su territorio a través de sistemas informáticos?
Si (√) No ( )

En caso afirmativo, sírvase describir brevemente las normas u otras medidas existentes al respecto y adjunte copia, de preferencia electrónica, de las mismas: Nuestra Constitución Nacional en si Articulo 29 contempla la posibilidad de interceptar cualquier tipo de información correspondiente a las autoridades judiciales y autorizar dichas diligencias.

II. UNIDADES ESPECIALIZADAS

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la Unidad o Instancia:
- Institución de la que depende:
- Información de Contacto:
    - Nombre del Titular: _____
    - Domicilio: _____
    - Teléfonos: _____ Fax: _____
    - Correo Electrónico: _____

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

En caso afirmativo, sírvase proporcionar la siguiente información:

- Nombre de la Unidad o instancia: FEPISI
- Institución de la que depende: Ministerio Público
- Información de contacto:
    - Nombre del Titular: Ramiro Esquivel Morales
    - Domicilio: Vía España, Edificio Avesa
    - Teléfonos: +507-505-3298 Fax: +507-505-3255
    - Correo electrónico:

2.3. Qué medidas ha adoptado su país para fomentar las relaciones entre autoridades responsables de la investigación y persecución de delitos cibernéticos y el sector privado, especialmente con aquellas empresas proveedoras de servicios de tecnología de la información y las comunicaciones, en particular de servicios de internet? __Ninguna Conocida____

III. COOPERACIÓN INTERNACIONAL

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

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

En caso afirmativo, sírvase desarrollar en que ha consistido dicha consideración: Se tomaron en cuenta al momento de redactar la norma penal; no obstante está pendiente lo referente al aspecto procesal y de cooperación Internacional.

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 (√)

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

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

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

En caso afirmativo sírvase describir brevemente las normas y/u otras medias existentes al respecto y adjunte copia, de preferencia electrónica, de las mismas: Se aplica en esta materia el procedimiento común que rige para la cooperación Internacional que se sustenta en el principio de reciprocidad, debiendo mencionarse que Panamá es suscriptor del Código de Bustamante.

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

En caso afirmativo, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjunte copia, de preferencia electrónica, de las mismas: Si bien no existe una legislación especial en materia de pruebas electrónicas, la normativa "tradicional" es aplicable por lo que las pruebas requeridas se obtienen y aseguran través de allanamientos, registros e inspecciones.

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 (√) No ( )

a) En caso afirmativo, sírvase indicar el número de solicitudes que ha formulado y/o recibido y el estado en que se encuentran dichas solicitudes: En el caso de la Fiscalía Superior Especializada en Delitos Contra la Propiedad Intelectual y Seguridad Informática, se recibió una solicitud la cual en estos momentos está en trámite. En cuanto a delitos informatizados, estas solicitudes son atendidas según se trate por las fiscalías especializadas en delitos financieros o en delitos de contra la integridad y libertad sexual, registrándose experiencias positivas de cooperación Internacional respecto a investigaciones de pornografía infantil.

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?
Si ( ) No (√)

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?
Si ( ) No (√)

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

4.3. De acuerdo con los esfuerzos de su país para ofrecer capacitación en la investigación y persecución de los delitos que involucren el uso de computadoras e internet, sírvase describir las metas de su país para los próximos dos años y las condiciones necesarias para alcanzar esas metas:

	OBJETIVOS	**CONDICIONES PARA LOGRARLO**
1.	Contar con una división de Delitos Cibernéticos en la DIJ.	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.	Contar con un centro de respuesta inmediata.	Se están realizando aproximaciones con el Órgano Ejecutivo destinadas a lograr la creación del centro.
3.	Referencias Penales y Procesales.	Esperar el momento oportuno para presentar proyectos y discusiones por parte de la Asamblea.
4.	Capacitación de la policía, peritos y la fiscalía. (*en agosto 2009, se celebró en Panamá un taller organizado por la OEA-REMJA; igualmente en septiembre 2009 con el apoyo de la embajada de los EE.UU. se dicto un seminario de Propiedad Intelectual que incluyo temas de Seguridad Informática).*	Contar con apoyo técnico de Profesionales, propuestos 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 Delito Cibernético?
Si (√) No ( )

En caso afirmativo, sírvase describir brevemente las personas que han participado; si estos talleres han ofrecido capacitación útil, y como los participantes han aplicado esta capacitación en el ejercicio de sus funciones: En el caso de La Fiscalía Superior Especializada en Delitos Contra la Propiedad Intelectual y Seguridad Informática, la Licenciada Doris Guerra, quien ocupó el cargo de Secretaria Judicial de la Fiscalía, asistió a la V Reunión del Grupo de Trabajo en Delitos Cibernéticos en el 2007.
Los insumos proporcionados por la Licda. Guerra, sirvieron como base para la elaboración de la propuesta de creación de la división de delitos cibernéticos y el Centro de Respuesta Inmediata CSIRT, de la Dirección de Investigación Judicial

(DIJ), aun pendiente de la implementación, igualmente, los conocimientos adquiridos fueron multiplicados a través de seminarios internos.

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:
- Talleres prácticos (que incluyan recolección y análisis de evidencias y adecuación normativa).
- Actualización en programas y herramientas informáticas utilizando por cometer delitos.
- Manejo de las pruebas electrónicas y su protección.

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 lo ratifiquen
- Asesoría para la creación e implementación de un CSIRT.
- Capacitación a peritos, policías y funcionarios de las fiscalías.

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por Favor, complete la siguiente Información:

b) Estado: Panamá
c) El funcionario a quien puede consultarse sobre las respuestas dadas en este cuestionario es el Señor: RAMIRO A. ESQUIVEL M.
d) Titulo /cargo: Fiscal Superior
e) Organismo/Oficina: Fiscalía Especializada en Delitos Contra la Propiedad Intelectual y Seguridad Informática.
f) Domicilio: Vía España, Edificio AVESA, tercer piso, Panamá, República de Panamá.
g) Número Telefónico: (507)-505-3298
h) Número de Fax: (507-505-3255)
i) Correo Electrónico: fepi@procuraduria.gob.pa, resquivel@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 285 - 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 286- 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 286, 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 286- 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 362- 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 364- 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 216- 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 222- 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 181 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 182 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 259 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 260.** 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 261.** 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 162.** 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 163.** 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 192.** 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 239.** 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 284.** 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 210.** 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 211.** 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 (art. 226)	**Artículo 226.** 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 291.** 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 425.** 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.