

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](mailto: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 ( )  
Nuestra legislación contempla la figura de acceso ilícito señalada en el formulario en la reciente ley sancionada 4439/2011 que modifica y amplía varios artículos del Código Penal. De esta forma el Art. 146 b (**Acceso indebido a datos**) sanciona hasta con tres años de pena privativa de libertad o multa a: al que sin autorización y violando sistemas de seguridad obtuviera para sí o para un tercero, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado.
- b) Interceptación ilícita Sí ( X ) No ( )  
Esta misma ley 4439/2011, modificatoria del Código Penal contempla en el artículo 146 c la figura denominada como **Interceptación de datos**, sancionando con una pena

privativa de libertad de hasta dos años o con multa al que: sin autorización y utilizando medios técnicos, obtuviera para sí o para un tercero datos. En el inciso 2° se castiga al que diera a otro una transferencia no publica de datos, sin autorización y el inciso 3° castiga también al que sin autorización transferencia de la radiación electromagnética de un equipo de procesamiento de datos.

Por otro lado, el artículo 146 b de la misma ley que modifica el Código Penal castiga los **actos preparatorios de los dos hechos punibles anteriores.**

- c) Ataques a la integridad de datos Sí ( X ) No ( )  
Nuestra legislación contempla la figura denominada como **Alteración de Datos** señalada en el Artículo 174 del Código Penal, estableciendo que será castigado con una pena privativa de libertad de hasta tres años o con multa el que: lesionando el derecho de disposición de otro sobre datos, los suprimiera, inutilizara o cambiara.
- d) Ataques a la integridad de sistemas Sí ( X ) No ( )  
La ley 4439/2011 que modifica el Art. 175 del Código Penal, tipifica la conducta denominada como **Sabotaje de sistemas informáticos**, describiendo la conducta como: el que obstaculizando un procesamiento de datos de un particular, de una empresa, asociación o de una entidad de la administración pública, mediante: 1) la alteración de datos (Art. 174 inc. 1° Código Penal); 2) mediante la destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otras de sus partes componentes indispensables. La pena prevista en estos casos es de hasta cinco años de pena privativa de libertad o de multa, castigándose también la tentativa.
- e) Abuso de dispositivos Sí ( X ) No ( )  
Esta figura esta prevista en el Artículo 146 d de la Ley 4439/2011 que prevé el castigo a la preparación de los hechos punibles descritos en el artículo 146 b y 146 c de la misma Ley.
- f) Falsificación informática Sí ( X ) No ( )  
Hace en relación a la falsificación de Software y Hardware u otro conjunto de componentes lógicos de un sistema informático y estos estarían dentro del tipo penal de Hechos Punibles contra la propiedad intelectual señalados en el punto i.
- g) Fraude informático Sí ( X ) No ( )  
Nuestra legislación penal contempla esta figura requerida en el formulario. La misma la encontramos en el artículo **188 del Código Penal - Operaciones Fraudulentas por Computadora**, que fue modificado por el Art. 188 de la Ley 4439/2011 el cual queda redactado de la siguiente manera: **Estafa mediante sistemas informáticos** – 1° El que, con la intención de obtener para sí o para un tercero un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante: 1) una programación incorrecta; 2) el uso de datos falsos o incorrectos; 3) el uso indebido de datos; u 4) la utilización de otra maniobra no autorizada; y con ello causara un perjuicio al patrimonio de otro, será castigado con pena privativa de libertad de hasta cinco años o con multa.  
Esta figura es similar a la figura de estafa contemplada en el artículo 187 del CP con la diferencia de que en este caso no existe un sujeto engañado sino que la conducta que

perjudica el patrimonio ajeno se realiza, no con una declaración falsa (mentira), sino que mediante cualquiera de las conductas descritas en los numerales 1, 2, 3 o 4.

También es posible adecuar esta figura requerida en el cuestionario (fraude informático), a lo descrito en el artículo 248 b del CP sobre **Falsificación de tarjetas de debito o crédito y otros medios electrónicos de pago**.

- h) Pornografía infantil Sí ( X ) No ( )  
La ley 4439/2011 ha modificado nuevamente el artículo 140 del Código Penal tipificando la denominada conducta prohibida **Pornografía relativa a niños y adolescentes**, castigando varias acciones, entre la que se mencionan: producir publicaciones que representen actos sexuales con participación de personas menores de 18 años, o exhibiere sus partes genitales. Por otro lado tipifica y castiga al que organice, financie, promueva espectáculos públicos o privados en los que participen personas menores de 18 años en la realización de actos sexuales. También se castiga la distribución, importación, exportación de material pornográfico con menores de 18 años, entre otras. La pena prevista para estos tipos penales es de cinco años o con multa, pudiendo ser aumentada hasta diez años en casos especiales también descritos en el mismo artículo.
- i) Delitos contra la propiedad intelectual y derechos afines Sí ( X ) No ( )  
El Código Penal en su artículo 184 – **Violación del derecho de autor o inventor**, modificado por ley 3440/2008, contempla el tipo penal de Violación del derecho de autor y derechos conexos, castigando hasta con cinco años de pena privativa de libertad o con multa. El artículo 184 b describe el tipo penal de Violación de los derechos de marca, prescribiendo una pena privativa de libertad de hasta cinco años o con multa. Por otro lado el artículo 184 c describe y castiga el tipo penal de Violación de los derechos sobre dibujo y modelos industriales, prescribiendo una pena privativa de libertad también de hasta cinco años.
- j) Otras (sírvase enumerarlas): Sí ( X ) No ( )  
Nuestro Código Penal, desde su promulgación en 1997, contempla en su artículo **175 el tipo penal denominado “Sabotaje de Computadoras”**, describiendo en su inciso 1º la obstaculización de un procesamiento de datos de importancia vital para una empresa o establecimiento ajeno o de una administración del Estado, mediante la destrucción, inutilización, sustracción o alteración de procesamiento de datos, de una unidad de almacenamiento o de otras partes accesorias, previendo una castigo de hasta cinco años o con multa, castigando también la tentativa.

- 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 ( )

Las conductas descriptas están tipificadas en la legislación paraguaya (Código Penal y sus modificaciones y ampliaciones).

- 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? Sí ( X ) No ( )  
La legislación nacional permite requerir a las empresas prestadoras de servicio, sin orden judicial, datos de tráfico no así de contenido que necesita orden judicial.

De esta forma el Art. 228 del Código Procesal Penal establece: “El juez y el Ministerio Público podrán requerir informes a cualquier persona o entidad pública o privada. Los informes se solicitarán verbalmente o por escrito, indicando el procedimiento en el cual se requieren, el nombre del imputado, el lugar donde debe ser entregado el informe, el plazo para su presentación y las consecuencias previstas para el incumplimiento del deber de informar”

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 ( )  
Nuestra legislación permite, según el Código Procesal Penal, confiscar, decomisar y secuestrar sistemas o dispositivos informáticos. Así tenemos los siguientes artículos del Código Procesal Penal sobre este punto: **Art. 176 (Inspección del lugar del hecho), Art. 183 (Registro), Art. 192 (Operaciones Técnicas), Art. 195 (Orden de Secuestro), Art. 198 (Intercepción y Secuestro de Correspondencia), Art. 199 (Apertura y examen de correspondencia), Art. 200 (Intervención de comunicaciones).**

b) Copiar y conservar los datos informáticos consultados. Sí ( X ) No ( )

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?  
Nuestra legislación contempla la posibilidad de la intercepción de comunicación electrónica. Así tenemos lo dispuesto en **Arts. 198 (Intercepción y secuestro de correspondencia), art. 199 (Apertura y examen de correspondencia), y art. 200 (Intervención de comunicaciones), todos estos artículos corresponden al Código Procesal Penal.**

## 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: División Especializada contra Delitos Informáticos
- Institución de la que depende: **Policía Nacional**
- Información de contacto:
  - o Nombre del Titular: Oficial Inspector **Diosnel Alarcón González**
  - o Domicilio: Haedo 725 e/ Oleari y Ayolas. Asunción, Paraguay
  - o Teléfono(s): +595 21 443 159; Móvil: +595 981 797 734
  - o Correo electrónico: diosnel-alarcon@hotmail.com

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: Unidad Especializada en Delitos Informáticos
- Institución de la que depende: Ministerio Público
- Información de contacto:
  - o Nombre del Titular: **María Teresa Aguirre Allou. Fiscal Adjunta de Delitos Informáticos**
  - o Domicilio: Nuestra Señora de la Asunción c/ Haedo. 6to Piso. Sede II del Ministerio Público. Asunción, Paraguay
  - o Teléfono (s): +595 21 415-5000 int.183./ Móvil: +595 981111 841
  - o Correo electrónico: [taguirreallou@gmail.com](mailto:taguirreallou@gmail.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?      Sí ( X ) No ( )
- En caso afirmativo, sírvase proveer las direcciones en Internet respectivas, y una descripción breve de las mismas:

Paraguay cuenta con lo siguiente:

Página electrónica: [www.csirt.gov.py](http://www.csirt.gov.py);

Correo electrónico: [abuse@csirt.gov.py](mailto:abuse@csirt.gov.py)

- 2.4. ¿Ha desarrollado y/o implementado su país una estrategia nacional de seguridad cibernética?      Sí ( ) No ( )
- En caso afirmativo, sírvase describir brevemente en qué consiste esa estrategia:

En el marco de esta estrategia se ha creado y conformado el CSIRT-Py e, igualmente, la Unidad Especializada de Delitos Informáticos del Ministerio Público y División Especializada contra Delitos Informáticos de la Policía Nacional, así como las adecuaciones legislativas en materia de Delitos Informáticos. Se han efectuado desde el CSIRT PY capacitaciones, socializaciones y se tiene previsto realizar importantes refuerzos respecto a la estructura interna.

### 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 ( X ) No ( ) No Conozco ( )

El país está considerando la adhesión al citado Instrumento. Técnicos del Ministerio Público han participado recientemente de la VIII Conferencia *OCTOPUS*.

- 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 ( X ) No ( )

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

Sí ( ) No ( ) No Conozco ( )

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 ( )

La Constitución Nacional de la República del Paraguay en su artículo 143, de las Relaciones Internacionales, establece que: *“La República del Paraguay, en sus relaciones internacionales, acepta el derecho internacional y se ajusta a los siguientes principios: ... 4) la solidaridad y la cooperación internacional...”*. Al respecto, el artículo 137 dispone que: *“La ley suprema de la República es la Constitución. Esta, los tratados, Convenios y acuerdos internacionales aprobados y ratificados, las leyes dictadas por el Congreso y otras disposiciones jurídicas de inferior jerarquía, sancionadas en consecuencia, integran el derecho positivo nacional en el orden de prelación enunciado”* Asimismo, el Código Procesal Penal, en su artículo 146 enuncia que: *“Los requerimientos dirigidos a Jueces o autoridades extranjeras se efectuarán por exhortos y se tramitarán en la forma establecida por el derecho internacional vigente, por las leyes y las costumbres internacionales...”*.

En tal sentido, la República del Paraguay firmó varios acuerdos bilaterales y multilaterales en materia de cooperación jurídica internacional, los cuales pueden ser utilizados para la obtención de elementos probatorios. En los casos de ausencia de tratados o acuerdos, también es posible otorgar asistencia jurídica bajo los términos del principio de la reciprocidad. En este caso, la solicitud debe ser tramitada por la vía diplomática.

- 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:

Se han formulado 2 (dos) solicitudes de asistencia que a la fecha han sido diligenciadas por las autoridades requirentes. Asimismo, se ha recibido una información espontánea sobre la comisión de un delito cibernético que actualmente se encuentra en etapa de investigación.

#### 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 ( )

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 ( )

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: \_\_\_\_\_

\_\_\_\_\_

- 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:

Miembros del CSIRT PY

- Ing. Gustavo Ibarra: Uruguay;
- Federico Ribeiro: Uruguay;
- Ing. Santiago Vázquez: Colombia/EE.UU. Universidad Carnegie Melon,
- María Inés Lippmann: EE.UU.;
- Herman Mereles: EE.UU. Universidad Carnegie Melon;
- Lic. Marcelo Maltese: Colombia;
- Lic. Ernaldo Vera: Colombia.

- 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: \_\_\_\_\_

\_\_\_\_\_

- 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:

Una de las prioridades del Equipo CSIRT-Py es establecer a mediano plazo un Centro Nacional de Capacitación sobre seguridad cibernética y lucha contra este flagelo. La cooperación técnica para este fin es identificada como una herramienta fundamental.

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: PARAGUAY

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

( ) Sr.: Julio Duarte Van Humbeck

( ) Sra.: \_\_\_\_\_

Título/cargo: Ministro – Director General de Asuntos Especiales

Organismo/oficina: Ministerio de Relaciones Exteriores

Domicilio: Palma esq. 14 de Mayo

Número de teléfono: +595 21 450 520; +595 21 498 561

Número de fax: +595 21 450 520

Correo electrónico: [jduarte@mre.gov.py](mailto:jduarte@mre.gov.py)



**“Bicentenario de la Independencia Nacional: 1811 - 2011”****PODER LEGISLATIVO****LEY N° 4439****QUE MODIFICA Y AMPLIA VARIOS ARTICULOS DE LA LEY N° 1160/97  
“CODIGO PENAL”****EL CONGRESO DE LA NACION PARAGUAYA SANCIONA CON FUERZA DE****LEY**

**Artículo 1°.-** Modifícanse los Artículos 140, 175, y 188 de la Ley N° 1160 “CODIGO PENAL”, de fecha 26 de noviembre de 1997, modificado parcialmente por la Ley N° 3440 del 16 de julio de 2008 y ampliase el Código Penal, introduciendo en la misma los Artículos 146 b, 146 c, 146 d, 174 b, 175 b, y 248 b, los cuales quedan redactados de la siguiente manera:

**“Art. 140.-** Pornografía relativa a niños y adolescentes.

1° El que:

1. produjere publicaciones, en el sentido del Artículo 14, inciso 3°, que representen actos sexuales con participación de personas menores de dieciocho años de edad o la exhibición de sus partes genitales;
2. organizara, financiara o promocionara espectáculos, públicos o privados, en los que participe una persona menor de dieciocho años en la realización de actos sexuales, o;
3. distribuyera, importara, exportara, ofertara, canjeara, exhibiera, difundiera, promocionara o financiara la producción o reproducción de publicaciones en sentido del numeral 1,

será castigado con pena privativa de libertad de hasta cinco años o multa.

2° El que reprodujera publicaciones según el numeral 1 del inciso 1°, será castigado con pena privativa de libertad de hasta tres años o multa.

3° La pena de los incisos anteriores podrá ser aumentada hasta diez años cuando:

1. las publicaciones y espectáculos en el sentido de los incisos 1° y 2° se refieran a menores de catorce años o se dé acceso a los menores de dicha edad a publicaciones y espectáculos, en sentido de los incisos citados;
2. el autor tuviera la patria potestad, deber de guarda o tutela del niño o adolescente, o se le hubiere confiado la educación o cuidado del mismo;
3. el autor operara en connivencia con personas a quienes competa un deber de educación, guarda o tutela respecto del niño o adolescente;
4. el autor hubiere procedido, respecto del niño o adolescente, con violencia, fuerza, amenaza, coacción, engaño, recompensa o promesa remuneratoria de cualquier especie; o

NCR

*“Bicentenario de la Independencia Nacional: 1811 – 2011”*

PODER LEGISLATIVO

Pág. N° 2/4

LEY N° 4439

5. el autor actuara comercialmente o como miembro de una banda dedicada a la realización reiterada de los hechos punibles señalados.

4° El que obtuviera la posesión de publicaciones en el sentido de los incisos 1° y 3°, será castigado con pena privativa de libertad de hasta tres años o con multa.

5° Se aplicará, en lo pertinente, también lo dispuesto en los Artículos 57 y 94.”

“Artículo 146 b.- Acceso indebido a datos.

1° El que sin autorización y violando sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será castigado con pena privativa de libertad de hasta tres años o multa.

2° Como datos en sentido del inciso 1°, se entenderán solo aquellos, que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible.”

“Artículo 146 c.- Interceptación de datos.

El que, sin autorización y utilizando medios técnicos:

1° obtuviere para sí o para un tercero, datos en sentido del Artículo 146 b, inciso 2°, no destinados para él;

2° diera a otro una transferencia no pública de datos; o

3° transfiriera la radiación electromagnética de un equipo de procesamiento de datos,

será castigado con pena privativa de libertad de hasta dos años o multa, salvo que el hecho sea sancionado por otra disposición con una pena mayor.”

“Artículo 146 d.- Preparación de acceso indebido e interceptación de datos.

1° El que prepare un hecho punible según el Artículo 146 b o el Artículo 146 c produciendo, difundiendo o haciendo accesible de otra manera a terceros:

1. las claves de acceso u otros códigos de seguridad, que permitan el acceso a datos en sentido del Artículo 146 b, inciso 2°; o

2. los programas de computación destinados a la realización de tal hecho,

será castigado con pena privativa de libertad de hasta un año o multa.

2° Se aplicará, en lo pertinente, lo previsto en el Artículo 266, incisos 2° y 3°.”

“Artículo 174 b.- Acceso indebido a sistemas informáticos.

1° El que accediere a un sistema informático o a sus componentes, utilizando su identidad o una ajena; o excediendo una autorización, será castigado con pena privativa de libertad de hasta tres años o multa.

*“Bicentenario de la Independencia Nacional: 1811 – 2011”*

## PODER LEGISLATIVO

Pág. N° 3/4

## LEY N° 4439

2° Se entenderá como sistema informático a todo dispositivo aislado o al conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus componentes, sea el tratamiento de datos por medio de un programa informático.”

“**Art. 175.-** Sabotaje de sistemas informáticos.

1° El que obstaculizara un procesamiento de datos de un particular, de una empresa, asociación o de una entidad de la administración pública, mediante:

1. un hecho punible según el Artículo 174, inciso 1°; o
2. la destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra de sus partes componentes indispensable.

será castigado con pena privativa de libertad de hasta cinco años o con multa.

2° En estos casos será castigada también la tentativa.”

“**Artículo 175 b.-** Instancia.

En los casos de los Artículos 174 y 175, la persecución penal dependerá de la instancia de la víctima; salvo que la protección del interés público requiera la persecución de oficio.”

“**Artículo 188.-** Estafa mediante sistemas informáticos.

1° El que, con la intención de obtener para sí o para un tercero un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante:

1. una programación incorrecta;
2. el uso de datos falsos o incompletos;
3. el uso indebido de datos; u
4. la utilización de otra maniobra no autorizada;

y con ello causara un perjuicio al patrimonio de otro,

será castigado con pena privativa de libertad de hasta cinco años o con multa.

2° En estos casos, se aplicará también lo dispuesto en el Artículo 187, incisos 2° al 4°.

3° El que preparare un hecho punible señalado en el inciso 1°, mediante la producción, obtención, venta, almacenamiento u otorgamiento a terceros de programas de computación destinados a la realización de tales hechos, será castigado con pena privativa de libertad de hasta tres años o con multa.

4° En los casos señalados en el inciso 3°, se aplicará lo dispuesto en el Artículo 266, incisos 2° y 3°.”

“**Artículo 248 b.-** Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago.

*“Bicentenario de la Independencia Nacional: 1811 – 2011”*

PODER LEGISLATIVO

Pág. N° 4/4

LEY N° 4439

1° El que, con la intención de inducir en las relaciones jurídicas al error o de facilitar la inducción a tal error:

1. falsificare o alterar una tarjeta de crédito o débito u otro medio electrónico de pago; o
2. adquiera para sí o para un tercero, ofreciere, entregare a otro o utilizare tales tarjetas o medios electrónicos,

será castigado con pena privativa de libertad de hasta cinco años o con multa.

2° Se castigará también la tentativa.

3° Cuando el autor actuara comercialmente o como miembro de una organización criminal dedicada a la realización de los hechos punibles señalados, la pena privativa de libertad podrá ser aumentada hasta diez años.

4° Tarjetas de crédito, en sentido del inciso 1°, son aquellas que han sido emitidas por una entidad de crédito o de servicios financieros para su uso en dicho tipo de transacciones y que, por su configuración o codificación, son especialmente protegidas contra su falsificación.

5° Medios electrónicos de pago en el sentido del inciso 1°, son aquellos instrumentos o dispositivos que actúan como dinero electrónico, permitiendo al titular efectuar transferencias de fondos, retirar dinero en efectivo, pagar en entidades comerciales y acceder a los fondos de una cuenta.”

**Artículo 2°.-** Comuníquese al Poder Ejecutivo.

Aprobada el Proyecto de Ley por la Honorable Cámara de Senadores, a **treinta días del mes de mayo del año dos mil once**, quedando sancionado el mismo, por la Honorable Cámara de Diputados, a **ocho días del mes de setiembre del año dos mil once**, de conformidad a lo dispuesto en el Artículo 207, numeral 1) de la Constitución Nacional.

**Víctor Alcides Bogado González**  
Presidente  
H. Cámara de Diputados

**Jorge Oyiedo Matto**  
Presidente  
H. Cámara de Senadores

**Mario Soto Estigarribia**  
Secretario Parlamentario

**Mario Cano Yegros**  
Secretario Parlamentario

Asunción, 3 de octubre de 2011

**Téngase por Ley de la República, publíquese e insértese en el Registro Oficial.**

**El Presidente de la República**



**Fernando Armindo Lugo Méndez**

**Humberto Blasco**  
Ministro de Justicia y Trabajo