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 noviembre 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 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: (I) 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 mas tardar el viérnes 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	SI (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 ( )	NO (X)
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 (X)

En caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica de la legislación: **(ANEXO 1)**

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

SÍ (X) NO ( )

En caso afirmativo, sírvase describir esos esfuerzos:

1. En el marco del Grupo Técnico Intersecretarial Especializado en Seguridad de la Información (GTECSI) se creó una Comisión Redactora encargada de proponer las iniciativas de reforma a la legislación mexicana vigente para tipificar los delitos cibernéticos, o bien, elaborar el anteproyecto de ley sobre delitos cibernéticos.

2. Para efectos de la correcta investigación de un delito relacionado con dispositivos electrónicos:

   a) El 18 de mayo de 2010 se creó la Coordinación para la Prevención de Delitos Electrónicos, adscrita a la División Científica de la Policía Federal, ello con la finalidad de atender los requerimientos sociales de prevención e investigación de delitos en los que se relacionan los dispositivos electrónicos, ya sea como medio para la comisión de un hecho ilícito o que el delito tenga como resultado material y formal la directa afectación a dicho sistema o dispositivo.

   b) La Coordinación para la Prevención de Delitos Electrónicos cuenta con diversas atribuciones para el desarrollo de sus funciones, las cuales se encuentran contenidas en el artículo 27 del Reglamento de la Ley de la Policía Federal, publicado en el Diario Oficial de la Federación del 17 de mayo de 2010 y que entró en vigor el día 18 de ese mismo mes y año, destacándose las siguientes:

      - Seleccionar y actualizar permanentemente los conocimientos electrónicos para apoyar la investigación y prevención de delitos.
      - Observar los procedimientos de Cadena de Custodia para preservar la integridad y confidencialidad de las evidencias, indicios y pruebas contenidas en medios electrónicos.
      - Establecer alianzas de cooperación con organismos y autoridades nacionales e internacionales relacionados con la prevención de delitos electrónicos.
      - Vigilar, identificar, monitorear y rastrear la red pública de Internet con el fin de prevenir conductas delictivas.
      - Operar laboratorios de innovaciones tecnológicas, electrónica, informática, telecomunicaciones y demás que resulten necesarias para prevenir la comisión de delitos electrónicos.
      - Recibir y verificar la información sobre hechos que puedan ser constitutivos de delito o infracciones administrativas, materia de su competencia, conforme a la normatividad aplicable.
      - Supervisar las acciones necesarias para la investigación de los delitos electrónicos cometidos, requeridos por la autoridad competente.
      - Gestionar conforme a las disposiciones aplicables la cooperación con empresas proveedoras de servicios de Internet, para neutralizar sitios y páginas electrónicas que atentan contra la seguridad pública, así como para prevenir y combatir los delitos en los que se utilizan medios electrónicos para su comisión.
      - Promover la cultura de la prevención de los delitos en los que se utilizan medios electrónicos para su comisión, así como la difusión del marco legal que sanciona los mismos.
      - Capacitar y profesionalizar al personal bajo su mando en el uso de las nuevas tecnologías para identificación, rastreo, custodia y protección de indicios e información de las investigaciones.

1.3. ¿Permite la legislación de emergencia de su país, por parte de 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:

El artículo 44 de la Ley Federal de telecomunicaciones en su fracción XII inciso f, obliga a los concesionarios de redes públicas de telecomunicaciones a llevar la guarda de información por doce meses:

Artículo 44. Los concesionarios de redes públicas de telecomunicaciones deberán:

XII.- Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:

f) La obligación de conservación de datos a que se refiere la presente fracción cesa a los doce meses, contados a partir de la fecha en que se haya producido la comunicación.

1.4 ¿Ha adoptado su país 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 a enumerar y adjuntar copias, de preferencia electrónica de la legislación:

Se aplican los lineamientos generales para el aseguramiento y decomiso de bienes, en virtud de que no se cuenta con una legislación especial **(ANEXO 2).**

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:

La Constitución Política (art. 13, párr. 13) prescribe que "Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada". Adicionalmente, el Ministerio Público Federal y la Secretaría de Seguridad Pública Federal cuentan con facultades para solicitar dichas intervenciones.

Actualmente no se cuenta con una legislación especial relativa a la interceptación legal de comunicaciones electrónicas transmitidas en su territorios a través de sistemas de computación; sin embargo, se aplican las reglas generales de la intervención de comunicaciones señaladas en el artículo 278 ter del Código Federal de Procedimientos Penales, referente a la Solicitud de Comunicaciones Privadas, realizada por el Procurador General de la República, o bien en quien delegue esa facultad **(ANEXO 3).**

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: Coordinación para la Prevención de Delitos Electrónicos
- Institución de la que depende: POLICÍA FEDERAL
- Información del contacto:
- Nombre del Titular: Licenciado Juan Carlos Guel López
  - Domicilio: Av. Constituyentes 947 Edificio de la Policía Científica, colonia Belén de las de la Flores, México D.F.
  - Teléfono (s): 11036000 ext. 29103
  - Correo electrónico: delitocibernetico pf@ssp.gob.mx

2.2 ¿Hay en su país una unidad o entidad encargada específicamente de procesar jurídicamente la comisión de delitos cibernéticos?

Sí ( ) No (X)

En caso afirmativo, sírvase proporcionar la siguiente información:

Nombre de la unidad o instancia:_____
-Institución de la que depende: _____
-Información de contacto:
o Nombre del Titular: _____
o Domicilio: _____
o Teléfono(s): _____ Fax: _____
o Correo electrónico: _____

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:

Cabe señalar que, la Secretaría de Seguridad Pública se encuentra realizando los esfuerzos necesarios, a través de su Órgano Desconcentrado Policía Federal, a efecto de desarrollar sitios web que permitan la atención integral de los delitos electrónicos.

2.4 ¿Ha desarrollado y/o implementado su país una estrategia nacional de seguridad cibernética?

Sí (X) No ( )

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

En el seno del GTECSI se ha adoptado una Estrategia de Seguridad de la Información que incluye un apartado sobre cuestiones de seguridad cibernética.

El Gobierno mexicano se encuentra trabajando en el desarrollo de una estrategia nacional en materia de seguridad cibernética.

Como parte de ese esfuerzo, la Policía Federal cuenta con un Equipo de Atención a Incidentes, denominado Centro Especializado en Respuesta Tecnológica de México (CERT Mx), perteneciente a un órgano gubernamental y acreditado ante el Forum for Incidents Response and Security Teams (FIRTS), el cual constituye un grupo de equipos de respuesa a incidentes de seguridad cibernética y que congrega a más de 200 equipos en por lo menos 52 países.

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 ( )

En caso afirmativo, sírvase expresar en qué ha consistido dicha consideración:

Se han implementado reformas a diversas leyes mexicanas vigentes con el propósito de prevenir, perseguir y sancionar los delitos cibernéticos. Sin embargo, aún falta implementar reformas adicionales para cubrir a cabalidad las disposiciones del Convenio, así como crear los mecanismos idóneos para la investigación y persecución de tales delitos.

Se ha participado en talleres de legislación en delitos cibernéticos en los que ha participado el Consejo de Europa, el Departamento de Justicia de los Estados Unidos y la OEA, para compartir y exponer la problemática en materia de delitos cibernéticos y proponer soluciones, con base en sus experiencias, conocimientos, con el fin de unificar criterios en la descripción y clasificación de los delitos cibernéticos a efecto de que se encuentre acorde al orden internacional y se cumplan los requisitos para formar parte del convenio de delincuencia cibernética.

Asimismo, se han realizado diversas acciones para promover la inclusión de tipos penales relativos a los delitos electrónicos, brindando asesoría a grupos parlamentarios respecto de la realización de un paquete de reformas, en los que no sólo se prevén tipos penales sino legislación procesal que permita tomar en cuenta la evidencia digital.

De igual forma, con la creación de la Coordinación para la Prevención de Delitos Electrónicos se ha logrado apreciar la comisión de conductas dañosas, que atentan contra el patrimonio o bien contra la seguridad cibernética, por lo que no sólo se han establecido medidas de prevención, sino que se han tomado acciones para coadyuvar con diferentes autoridades a la generación de reformas a la legislación existente para tomar en cuenta esa clase de conductas.

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 ( )

3.3. ¿Cuenta su país con legislación que permitan 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 breve mente las normas y/u otras medidas existentes al respecto y adjunte copia, de preferencia electrónica, de las mismas:

México puede dar trámite a las solicitudes de asistencia mutua en materia penal, con base en la legislación mexicana y los convenios internacionales en la materia celebrados por el Gobierno mexicano.

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:

En julio de 2011, la Coordinación para la Prevención de Delitos Electrónicos recibió un requerimiento para cooperar con la Procuraduría General de la República, proveniente de los Estados Unidos de América, a efecto de llevar a cabo la detención de una persona, con fines de extradición por los delitos de transporte y recepción 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?

Sí (X) No ( )

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

La Coordinación para la Prevención de Delitos Electrónicos ha desarrollado diversos talleres y conferencias de capacitación a autoridades de los tres órdenes de gobierno, enfatizando el tratamiento adecuado para la investigación de esta clase de delitos.

4.2. ¿Ofrece su país capacitación a los fiscales en delito cibernético y para la obtención de pruebas electrónicas?

Sí (X) No ( )

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

La Coordinación para la Prevención de Delitos Electrónicos cuenta con un área especializada que ofrece capacitación en delitos electrónicos a las autoridades que así lo requieran, difunde medidas de prevención y lleva a acabo talleres en los que se brinda a servidores públicos, ministerios públicos y jueces, asesoría para la atención a delitos electrónicos.

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:

La Policía Federal, como área especializada en capacitación y medidas de prevención, tiene como meta generar diversos acuerdos con autoridades competentes a fin de que se proporcione la debida capacitación en delitos electrónicos a las autoridades investigadoras, persecutoras del delito, así como a los jueces.

La Coordinación para la Prevención de Delitos Electrónicos se encuentra impulsando la creación de una Fiscalía Especializada en la Investigación de Delitos Electrónicos, tomando en consideración las necesidades que se han visto en la investigación para la prevención y combate de delitos electrónicos, en función de las actividades que desempeña.

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 como los participantes han aplicado esta capacitación en el ejercicio de sus funciones:

Diversos funcionarios del gobierno mexicano han participado en talleres sobre delitos cibernéticos en el marco de OEA y de la Convención de Budapest. Adicionalmente, tres personas de la Policía Federal han participado en cursos de actualización en delitos cibernéticos, con lo cual se aportan nuevas ideas para dar respuesta a los incidentes en esta materia, se crean programas y se desarrollan estrategias para combatir este tipo de delitos.

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:

Sería importante y oportuno tratar los temas de evidencia digital, cómputo forense y sus alcances, delitos en el ciberespacio, ventajas y desventajas de Internet. El papel que juegan los proveedores de Internet y conservación de datos de identificación. Igualmente sobre el papel de los mismos como "guardianes del portal" y mecanismos para métodos forenses uniformes en el mundo.

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:

Generar un banco de datos de los delitos cibernéticos.
Brindar cursos de capacitación a profesionales de la impartición de justicia y procuradores de la misma, ya que el tema les es poco comprensible y genera dudas y errores al momento de enfrentar este tipo de delitos.
Realizar foros de discusión sobre casos específicos que generen nuevas perspectivas y conocimiento, tanto en la forma en que se desarrollaron, como en la forma en que se resolvieron.
Considerar el rol que tienen las empresas prestadoras de servicios en Internet y servicios de Internet, respecto a la aportación de datos relevantes en la investigación.

INFORMACION SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

1. (a) Estado: México
(b) El funcionario a quien puede consultarse sobre las respuestas dadas a este cuestionario:
(X) Sr.: Arturo Espiridión Ramírez Ramírez
( ) sra.:
Titulo/cargo: Comisario / Director General
Organismo y Oficina: Policía Federal / Coordinación para la Prevención de Delitos Electrónicos
Domicilio: Av. Constituyentes # 947 Edificio de la División Científica, Colonia Belén de las Flores, México D.F.
Teléfono (s): 52-55 11036000 ext. 29107 y 29115
Correo electrónico: arturo.ramirez@ssp.gob.mx

2. (a) Estado: México
(b) El funcionario a quien puede consultarse sobre las respuestas dadas a este cuestionario:
(X) Sr.: Rodrigo Labardini
( ) sra.:
Titulo/cargo: Ministro, Consultor Jurídico Adjunto,
Organismo y Oficina: Consultoría Jurídica, Secretaría de Relaciones Exteriores
Domicilio: Plaza Juárez 20, Piso 6, México, D.F. 06015
Teléfono (s): 52-55 3686-5363
Correo electrónico: rlabardini@sre.gob.mx

ANEXO 1 (En relación con la pregunta 1.1)

Delito	Legislación
Acceso Ilícito	**CÓDIGO PENAL FEDERAL** **Artículo 211 bis 1.-** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. **Artículo 211 bis 2.-** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. **Artículo 211 bis 3**.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida

	de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta. **Artículo 211 bis 5**.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero. **LEY DE INSTITUCIONES DE CRÉDITO** **Artículo 112 Quáter.-** Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de

	quien esté facultado para ello: **I.** Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.
Interceptación Ilícita	**CÓDIGO PENAL FEDERAL** **Artículo 173**.- Se aplicarán de tres a ciento ochenta jornadas de trabajo en favor de la comunidad: **I.-** Al que abra indebidamente una comunicación escrita que no esté dirigida a él, y **II.-** Al que indebidamente intercepte una comunicación escrita que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido. Los delitos previstos en este artículo se perseguirán por querella **Artículo 177**.- A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa. **LEY FEDERAL DE TELECOMUNICACIONES** **Artículo 71.** Las infracciones a lo dispuesto en esta Ley, se sancionarán por la Secretaría de conformidad con lo siguiente: **A.** Con multa de 10,000 a 100,000 salarios mínimos por: **V.** Interceptar información que se transmita por las redes públicas de telecomunicaciones, y

Ataques a la Integridad de los Datos	**CÓDIGO PENAL FEDERAL** **Artículo 211 bis 1**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. **Artículo 211 bis 2**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. **Artículo 211 bis 3**.- Al que estando autorizado para acceder a sistemas y equipos

	de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública. **Artículo 211 bis 4**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. **Artículo 211 bis 5**.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien

	a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero. **Artículo 211 bis 6**.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código. **Artículo 211 bis 7**.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno. **LEY DE INSTITUCIONES DE CRÉDITO** En materia bancaria se prevé en el numeral 113 fracción VII de la Ley de Instituciones de Crédito. **Artículo 113.-** Serán sancionados con prisión de dos a diez años y multa de quinientos a cincuenta mil días de salario, los consejeros, funcionarios o empleados de las instituciones de crédito o quienes intervengan directamente en el otorgamiento del crédito: **VII.** Que destruyan u ordenen que se destruyan total o parcialmente, información, documentos o archivos, incluso electrónicos, con el propósito de impedir u obstruir los actos de supervisión y vigilancia de la Comisión Nacional Bancaria y de Valores.

Ataques a la Integridad de los Sistemas	**CÓDIGO PENAL FEDERAL** **Artículo 62**.- Cuando por culpa se ocasione un daño en propiedad ajena que no sea mayor del equivalente a cien veces el salario mínimo se sancionará con multa hasta por el valor del daño causado, más la reparación de ésta. La misma sanción se aplicará cuando el delito culposo se ocasione con motivo del tránsito de vehículos cualquiera que sea el valor del daño. Cuando por culpa y por motivo del tránsito de vehículos se causen lesiones, cualquiera que sea su naturaleza, sólo se procederá a petición del ofendido o de su legítimo representante, siempre que el conductor no se hubiese encontrado en estado de ebriedad o bajo el influjo de estupefacientes, psicotrópicos o de cualquiera otra sustancia que produzca efectos similares y no se haya dejado abandonada a la víctima **Artículo 167**.- Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa: **VI.-** Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbrica, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos; **Artículo 399**.- Cuando por cualquier medio se causen daño, destrucción o deterioro de cosa ajena, o de cosa propia en perjuicio de tercero, se aplicarán las sanciones del robo simple. **Artículo 424 bis.-** Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa: **II.** A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Abuso de dispositivos	**LEY DE INSTITUCIONES DE CRÉDITO** **Artículo 112 Bis.-** Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier otro instrumento de pago, de los utilizados o emitidos por instituciones de crédito del país o del extranjero **VI.** Posea, adquiera, utilice o comercialice equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o reproducir información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, con el propósito de obtener recursos económicos, información confidencial o reservada. **CÓDIGO PENAL FEDERAL** **Artículo 424**.- Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa: **II.** Al editor, productor o grabador que a sabiendas produzca más números de ejemplares de una obra protegida por la Ley Federal del Derecho de Autor, que los autorizados por el titular de los derechos; **Artículo 424 bis.-** Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa: **II.** A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación

	LEY DE DERECHOS DE AUTOR **Artículo 112.-** Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior. **CÓDIGO DE COMERCIO** **Artículo 231.-** Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto: **V.** Importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación; **VII.** Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular;
Fraude Informático	**CÓDIGO PENAL FEDERAL** **Artículo 386.-** Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido. El delito de fraude se castigará con las penas siguientes: I.- Con prisión de 3 días a 6 meses o de 30 a 180 días multa, cuando el valor de lo defraudado no exceda de diez veces el salario; II.- Con prisión de 6 meses a 3 años y multa de 10 a 100 veces el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario; III.- Con prisión de tres a doce años y multa hasta de ciento veinte veces el salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario.

Pornografía Infantil	**CÓDIGO PENAL FEDERAL** **Artículo 202.-** Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa. A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito. La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores. **Artículo 202 BIS.-** Quien almacene, compre, arriende, el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa. Asimismo, estará sujeto a tratamiento psiquiátrico especializado.

Delitos contra la Propiedad Intelectual y Derechos Afines	**CÓDIGO PENAL FEDERAL** **Artículo 424.-** Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa: **I.** Al que especule en cualquier forma con los libros de texto gratuitos que distribuye la Secretaría de Educación Pública. **II.** Al editor, productor o grabador que a sabiendas produzca más números de ejemplares de una obra protegida por la Ley Federal del Derecho de Autor, que los autorizados por el titular de los derechos. **III.** A quien use en forma dolosa, con fin de lucro y sin la autorización correspondiente obras protegidas por la Ley Federal del Derecho de Autor. **Artículo 424 bis.-** Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa: I.- A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos. Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior.

	II.- A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación. **Artículo 424 ter.-** Se impondrá prisión de seis meses a seis años y de cinco mil a treinta mil días multa, a quien venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa, con fines de especulación comercial, copias de obras, fonogramas, videogramas o libros, a que se refiere la fracción I del artículo anterior. Si la venta se realiza en establecimientos comerciales, o de manera organizada o permanente, se estará a lo dispuesto en el artículo 424 Bis de este Código. **Artículo 425.-** Se impondrá prisión de seis meses a dos años o de trescientos a tres mil días multa, al que a sabiendas y sin derecho explote con fines de lucro una interpretación o una ejecución. **Artículo 426.-** Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes: I.- A quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal. II.- A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal. **Artículo 427.-** Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa, a quien publique a sabiendas una obra substituyendo el nombre del autor por otro nombre.

	Artículo 428.- Las sanciones pecuniarias previstas en el presente título se aplicarán sin perjuicio de la reparación del daño, cuyo monto no podrá ser menor al cuarenta por ciento del precio de venta al público de cada producto o de la prestación de servicios que impliquen violación a alguno o algunos de los derechos tutelados por la Ley Federal del Derecho de Autor. **Artículo 429.-** Los delitos previstos en este título se perseguirán por querella de parte ofendida, salvo el caso previsto en el artículo 424, fracción I, que será perseguido de oficio. En el caso de que los derechos de autor hayan entrado al dominio público, la querella la formulará la Secretaría de Educación Pública, considerándose como parte ofendida.

ANEXO 2 (En relación con la pregunta 1.4)

CÓDIGO FEDERAL DE PROCEDIMIENTOS PENALES

CAPITULO VII
Cateos

Artículo 61.- Cuando en la averiguación previa el Ministerio Público estime necesaria la práctica de un cateo, acudirá a la autoridad judicial competente, o si no la hubiere a la del orden común, a solicitar por cualquier medio la diligencia, dejando constancia de dicha solicitud, expresando su objeto y necesidad, así como la ubicación del lugar a inspeccionar y persona o personas que han de localizarse o de aprehenderse, y los objetos que se buscan o han de asegurarse a lo que únicamente debe limitarse la diligencia.

Al inicio de la diligencia el Ministerio Público designará a los servidores públicos que le auxiliarán en la práctica de la misma.

Al concluir el cateo se levantará acta circunstanciada, en presencia de dos testigos propuestos por el ocupante del lugar cateado o en su ausencia o negativa, por la autoridad que practique la diligencia; los servidores públicos designados por el Ministerio Público para auxiliarle en la práctica de la diligencia no podrán fungir como testigos de la misma. Cuando no se cumplan estos requisitos, la diligencia carecerá de todo valor probatorio, sin que sirva de excusa el consentimiento de los ocupantes del lugar.

La petición de orden de cateo deberá ser resuelta por la autoridad judicial de manera inmediata, en un plazo que no exceda de las veinticuatro horas siguientes a que la haya recibido. Si dentro del plazo señalado el juez no resuelve sobre el pedimento de cateo, el Ministerio Público podrá recurrir al superior jerárquico para que éste resuelva en un plazo igual.

Artículo 123 Bis.- La preservación de los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito es responsabilidad directa de los servidores públicos que entren en contacto con ellos.

En la averiguación previa deberá constar un registro que contenga la identificación de las personas que intervengan en la cadena de custodia y de quienes estén autorizadas para reconocer y manejar los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito.

Los lineamientos para la preservación de indicios, huellas o vestigios del hecho delictuoso, así como de los instrumentos, objetos o productos del delito, que

por acuerdo general emita la Procuraduría General de la República, detallarán los datos e información necesaria para asegurar la integridad de los mismos.

La cadena de custodia iniciará donde se descubra, encuentre o levante la evidencia física y finalizará por orden de autoridad competente.

Artículo 181.- Se equiparará a la resistencia y se sancionará con la misma pena que ésta, la coacción hecha a la autoridad pública por medio de la violencia física o de la moral, para obligarla a que ejecute un acto oficial, sin los requisitos legales u otro que no esté en sus atribuciones.

ACUERDO número A/002/10 Mediante el cual Se Establecen los Lineamientos que Deberán Observar Todos los Servidores Públicos para la Debida Preservación y Procesamiento del Lugar de los Hechos o del Hallazgo y de los Indicios, Huellas o Vestigios del Hecho Delictuoso, así como de los Instrumentos, Objetos o Productos del Delito.

PRIMERO. El presente Acuerdo tiene por objeto establecer los lineamientos que:

1.- Deberán seguir la policía y otros servidores públicos en ejercicio de sus atribuciones para la preservación del lugar de los hechos y/o del hallazgo.

2.- Deberán observar los agentes del Ministerio Publico de la Federación, Oficiales Ministeriales, Unidades de Policía Facultadas, Peritos y demás servidores públicos que entren en contacto con ellos para el debido procesamiento de los indicios, huellas o vestigios del hecho delictuoso, así como de los instrumentos, objetos o productos del delito.

TERCERO. Las actuaciones que se realicen para la PRESERVACION DEL LUGAR DE LOS HECHOS Y/O DEL HALLAZGO y EL PROCESAMIENTO DE LOS INDICIOS O EVIDENCIAS, hasta que finalice la CADENA DE CUSTODIA por orden del AMPF o del Juez, según el caso, se asentarán en el RCC.

CUARTO. A fin de evitar el rompimiento de la CADENA DE CUSTODIA, los servidores públicos que intervengan en las distintas fases del procesamiento de los INDICIOS O EVIDENCIAS desde su búsqueda, traslado a los servicios periciales para la realización de las pruebas correspondientes, así como para su almacenamiento, o transferencia al SAE, según el caso, o que por cualquier circunstancia entren en contacto con los INDICIOS O EVIDENCIAS, deberán asentar en el RCC la información correspondiente a su intervención, así como su nombre completo y otros datos que se requieran, su firma autógrafa, así como la razón de la entrega de unos a otros. Lo anterior, en términos de la fracción IV del artículo 123 Ter, del CFPP y en la forma y términos señalados en la GUIA anexa para el registro de la CADENA DE CUSTODIA.

Asimismo, en la forma y términos indicados en la GUIA deberán adherir al embalaje de los INDICIOS O EVIDENCIAS las señalizaciones o rótulos correspondientes con los datos que en ella se indican.

En el RCC se hará constar quién se encarga del transporte y las condiciones materiales y ambientales en que se dé el traslado de los INDICIOS O EVIDENCIAS.

Todas las diligencias que se realicen respecto de los cadáveres en las que intervengan distintos servidores públicos o cualquier persona, incluidos los familiares del fallecido, también se harán constar en el RCC.

ANEXO 3 (En relación con la pregunta 1.5)

CÓDIGO FEDERAL DE PROCEDIMIENTOS PENALES

Artículo 278 Ter.- Cuando la solicitud de intervención de comunicaciones privadas sea formulada por el Procurador General de la República o los servidores públicos en quienes delegue la facultad, la autoridad judicial otorgará la autorización cuando se constate la existencia de indicios suficientes que acrediten la probable responsabilidad en la comisión de delitos graves.

El Ministerio Público será responsable de que la intervención se realice en los términos de la autorización judicial. La solicitud de autorización deberá contener los preceptos legales que la funda, el razonamiento por el que se considera procedente, el tipo de comunicaciones, los sujetos y los lugares que serán intervenidos, así como el periodo durante el cual se llevarán a cabo las intervenciones, el cual podrá ser prorrogado, sin que el periodo de intervención, incluyendo sus prórrogas, pueda exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.

En la autorización, el juez determinará las características de la intervención, sus modalidades, límites y, en su caso, ordenará a instituciones públicas o privadas, modos específicos de colaboración.

En la autorización que otorgue el juez deberá ordenar que, cuando en la misma práctica sea necesario ampliar a otros sujetos o lugares la intervención, se deberá presentar ante el propio juez, una nueva solicitud; también ordenará que al concluir cada intervención se levante un acta que contendrá un inventario pormenorizado de las cintas de audio y video que contengan los sonidos o imágenes captadas durante la intervención, así como que se le entregue un informe sobre sus resultados, a efecto de constatar el debido cumplimiento de la autorización otorgada.

El juez podrá, en cualquier momento, verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total.

En caso de no ejercicio de la acción penal y una vez transcurrido el plazo legal para impugnarlo, sin que ello suceda, el juez que autorizó la intervención, ordenará que se pongan a su disposición las cintas resultado de las investigaciones, los originales y sus copias, y ordenará su destrucción en presencia del Ministerio Público.

APARTADO I
LEGISLACIÓN

PREGUNTA 1.1. ¿HA TIPIFICADO SU PAÍS LAS SIGUIENTES MODALIDADES DE DELITO CIBERNÉTICO?

A continuación se cita cada una de las modalidades procurando relacionarlas con el Código Penal Federal (en lo sucesivo CPF).

No se omite destacar que, con la comprensible utilización de otros "términos", es dable afirmar que diversas modalidades están previstas en la norma federal de nuestro país.

a) ACCESO ILÍCITO.

Es dable considerar que el CPF prevé el acceso con diversa hipótesis, considerando que para modificar, destruir o provocar pérdida de información, incluso revelarla, divulgarla o utilizarla, antes, seguramente existió un acceso. Al respecto se invoca la norma:

"TÍTULO NOVENO
Revelación de secretos y acceso ilícito a sistemas y equipos de informática

CAPÍTULO I
Revelación de secretos

***Artículo 210**.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.*

***Artículo 211**.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.*

***Artículo 211 Bis**.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.*

CAPÍTULO II
Acceso ilícito a sistemas y equipos de informática

***Artículo 211 bis 1**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

***Artículo 211 bis 2**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general

vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

***Artículo 211 bis 3**.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.*

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

***Artículo 211 bis 4**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.*

***Artículo 211 bis 5**.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.*

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

***Artículo 211 bis 6**.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código."*

b) <u>INTERCEPTACIÓN ILÍCITA.</u>

Nuestra legislación prevé el término interceptar, expresamente para la comunicación escrita (artículo 173 y 174 del CPF), sin embargo de acuerdo al Diccionario de la Real Academia Española (en lo sucesivo RAE), interceptar es "Interrumpir, obstruir una vía de comunicación", por lo que para el tema que nos ocupa es dable considerar la existencia del art. 167 fracción VI del CPF:

***"Artículo 167**.- Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa:*
…

***VI.-** Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos;…"*
…

Por ello sería posible considerar la interrupción de cualquier tipo de comunicación, como en el caso podría ser electrónica, con o a través de internet.

c) **ATAQUES A LA INTEGRIDAD DE DATOS, Y**
d) **ATAQUES A LA INTEGRIDAD DE SISTEMAS.**

En relación a ello, se debe considerar, que se ataca (Según RAE ataque es "Acción de atacar, perjudicar o destruir") cuando se modifique, destruya o provoque pérdida de información (datos), en cuyo sentido el CPF prevé:

"CAPÍTULO II
Acceso ilícito a sistemas y equipos de informática

***Artículo 211 bis 1**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

***Artículo 211 bis 2**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*
…

***Artículo 211 bis 4**.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.*

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa."

e) **ABUSO DE DISPOSITIVOS**

Al respecto debe resaltarse lo previsto en CPF, a tenor:

***"Artículo 424 bis.-** Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:*
…

***II.** A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación".*

f) **FALSIFICACIÓN INFORMÁTICA**

Falsificar de conformidad con el RAE, significa "falsear o adulterar algo". Por ello debe considerarse que está prevista en la norma ya invocada.

g) **FRAUDE INFORMÁTICO**

Al respecto, en el CPF no se distingue una tipificación exacta, sin embargo, puede considerarse que el utilizar medios informáticos y/o electrónicos, podría ser un medio para cometer el fraude previsto por el artículo 386, a tenor:

***"Artículo 386.-** Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido".*

h) PORNOGRAFÍA INFANTIL

Está previsto en el CPF, a tenor:

"CAPÍTULO II
Pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo.

Artículo 202.- *Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa".*

i) Delitos contra la propiedad intelectual y derechos afines

Al respecto debe considerarse lo previsto en la Ley de la Propiedad Industrial, así como en el CPF, a tenor:

"***Capítulo III***
De los Delitos

Artículo 223.- *Son delitos:*

…

II. *Falsificar, en forma dolosa y con fin de especulación comercial, marcas protegidas por esta Ley;*

III. *Producir, almacenar, transportar, introducir al país, distribuir o vender, en forma dolosa y con fin de especulación comercial, objetos que ostenten falsificaciones de marcas protegidas por esta Ley, así como aportar o proveer de cualquier forma, a sabiendas, materias primas o insumos destinados a la producción de objetos que ostenten falsificaciones de marcas protegidas por esta Ley;*

IV. *Revelar a un tercero un secreto industrial, que se conozca con motivo de su trabajo, puesto, cargo, desempeño de su profesión, relación de negocios o en virtud del otorgamiento de una licencia para su uso, sin consentimiento de la persona que guarde el secreto industrial, habiendo sido prevenido de su confidencialidad, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto;*

V. *Apoderarse de un secreto industrial sin derecho y sin consentimiento de la persona que lo guarde o de su usuario autorizado, para usarlo o revelarlo a un tercero, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto industrial o a su usuario autorizado, y*

VI. *Usar la información contenida en un secreto industrial, que conozca por virtud de su trabajo, cargo o puesto, ejercicio de su profesión o relación de negocios, sin consentimiento de quien lo guarde o de su usuario autorizado, o que le haya sido revelado por un tercero, a sabiendas que éste no contaba para ello con el consentimiento de la persona que guarde el secreto industrial o su usuario autorizado, con el propósito de obtener un beneficio económico o con el fin de causar un perjuicio a la persona que guarde el secreto industrial o su usuario autorizado.*

Los delitos previstos en este artículo se perseguirán por querella de parte ofendida."

Respecto a derechos afines, es de señalar que el derecho de autor está previsto en el CPF, a tenor:

"Artículo 424 bis.- *Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:*

I. *A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma*

dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos. Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o

II. *A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación".*

Por lo anterior es posible considerar que sí están previstas diversas modalidades de delito Cibernético.

PREGUNTA 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? SI
b) COPIAR Y CONSERVAR LOS DATOS INFORMÁTICOS CONSULTADOS? Si

Debe considerarse legalmente procedente el decomisar, asegurar, preservar los instrumentos, objetos o productos del delito, toda vez que los art. 123, 123 Bis, 123 Ter, 123 Quater y 123 Quintus del Código Federal de Procedimientos Penales (en lo sucesivo CFPP), hace referencia a todo tipo de huellas o vestigios del delito. Aún más, el art. 181 refiere expresamente al aseguramiento de los instrumentos, objeto o productos del delito.

"CAPÍTULO II
Huellas del delito.- Aseguramiento de los Instrumentos y objetos del mismo

Artículo 181.*- Los instrumentos, objetos o productos del delito, así como los bienes en que existan huellas o pudieran tener relación con éste, serán asegurados a fin de que no se alteren, destruyan o desaparezcan. El Ministerio Público, las policías y los peritos, durante la investigación y en cualquier etapa del proceso penal, deberán seguir las reglas referidas en los artículos 123 Bis a 123 Quintus. La administración de los bienes asegurados se realizará de conformidad con la ley de la materia.*

Las autoridades que actúen en auxilio del Ministerio Público pondrán inmediatamente a disposición de éste los bienes a que se refiere el párrafo anterior. El Ministerio Público, al momento de recibir los bienes, resolverá sobre su aseguramiento y sobre la continuidad o no del procedimiento al que se refieren los artículos 123 Bis a 123 Quintus de este Código, bajo su más estricta responsabilidad y conforme a las disposiciones aplicables".

"CAPÍTULO II
Reglas especiales para la práctica de diligencias y levantamiento de actas de averiguación previa

Artículo 123.- *Inmediatamente que el Ministerio Público, las policías o los funcionarios encargados de practicar en su auxilio diligencias de averiguación previa tengan conocimiento de la probable existencia de un delito que deba perseguirse de oficio, dictarán todas las medidas y providencias necesarias para: proporcionar seguridad y auxilio a las víctimas y testigos; impedir que se pierdan, destruyan o alteren los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito; saber qué personas fueron testigos; evitar que el delito se siga cometiendo y, en general, impedir que se dificulte la averiguación, procediendo a la detención de los que intervinieron en su comisión en los casos de delito flagrante y su registro inmediato.*

Lo mismo se hará tratándose de delitos que solamente puedan perseguirse por querella, si ésta ha sido formulada.

El Ministerio Público sólo podrá ordenar la detención de una persona, cuando se trate de delito flagrante o de caso urgente, conforme a lo dispuesto por el artículo 16 de la Constitución y en los términos de los artículos 193 y 194 respectivamente.

Artículo 123 Bis.- *La preservación de los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito es responsabilidad directa de los servidores públicos que entren en contacto con ellos.*

En la averiguación previa deberá constar un registro que contenga la identificación de las personas que intervengan en la cadena de custodia y de quienes estén autorizadas para reconocer y manejar los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito.

Los lineamientos para la preservación de indicios, huellas o vestigios del hecho delictuoso, así como de los instrumentos, objetos o productos del delito, que por acuerdo general emita la Procuraduría General de la República, detallarán los datos e información necesaria para asegurar la integridad de los mismos.

La cadena de custodia iniciará donde se descubra, encuentre o levante la evidencia física y finalizará por orden de autoridad competente.

Artículo 123 Ter.- *Cuando las unidades de la policía facultadas para la preservación del lugar de los hechos descubran indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito, en el lugar de los hechos, deberán:*

I. *Informar de inmediato por cualquier medio eficaz y sin demora alguna al Ministerio Público e indicarle que se han iniciado las diligencias correspondientes para el esclarecimiento de los hechos, para efectos de la conducción y mando de éste respecto de la investigación;*

II. *Identificar los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito. En todo caso, los describirán y fijarán minuciosamente;*

III. *Recolectar, levantar, embalar técnicamente y etiquetar los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito. Deberán describir la forma en que se haya realizado la recolección y levantamiento respectivos, así como las medidas tomadas para asegurar la integridad de los mismos, y*

IV. *Entregar al Ministerio Público todos los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito, sus respectivos contenedores y las actas, partes policiales o documentos donde se haya hecho constancia de su estado original y de lo dispuesto en las fracciones anteriores para efectos de la averiguación y la práctica de las diligencias periciales que éste ordene. En dichos documentos deberá constar la firma autógrafa de los servidores públicos que intervinieron en el procedimiento.*

Artículo 123 Quater.- *El Ministerio Público se cerciorará de que se han seguido los procedimientos para preservar los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito.*

Tratándose de los indicios, huellas o vestigios del hecho delictuoso, el Ministerio Público ordenará la práctica de las pruebas periciales que resulten procedentes. Respecto de los instrumentos, objetos o productos del delito ordenará su aseguramiento de conformidad con lo dispuesto en el artículo 181 de este Código, previos los dictámenes periciales a los que hubiere lugar.

En caso de que la recolección levantamiento y traslado de los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito no se haya hecho como lo señala el artículo anterior, el Ministerio Público lo asentará en la averiguación previa y, en su caso, dará vista a las autoridades que resulten competentes para efectos de las responsabilidades a las que haya lugar.

Artículo 123 Quintus.- *Los peritos se cerciorarán del correcto manejo de los indicios, huellas o vestigios del hecho delictuoso, así como de los instrumentos, objetos o productos del delito y realizarán los peritajes que se le instruyan. Los dictámenes respectivos serán enviados al Ministerio Público para efectos de la averiguación. La evidencia restante será devuelta al Ministerio Público, quien ordenará su resguardo para posteriores diligencias o su destrucción, si resulta procedente.*

Los peritos darán cuenta por escrito al Ministerio Público cuando los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito no hayan sido debidamente resguardados, de conformidad con lo dispuesto en los artículos anteriores y demás aplicables, sin perjuicio de la práctica de los peritajes que se les hubiere instruido".

Cabe también señalar que la indicada legislación prevé el **decomiso**, a tenor:

"Artículo 182-Q.- *La autoridad judicial, mediante sentencia en el proceso penal correspondiente, podrá decretar el decomiso de bienes, con excepción de los que hayan causado abandono en los términos de este Código".*

"Artículo 535*.- Cuando se decrete el decomiso, se estará a lo previsto en el Código Penal para los fines de conservación, destrucción, venta y aplicación de instrumentos, objetos y productos de los delitos".*

En este mismo aspecto del Decomiso, el Código Penal Federal lo prevé, a tenor:

"TÍTULO SEGUNDO
CAPÍTULO I
Penas y medidas de seguridad

Artículo 24*.- Las penas y medidas de seguridad son:*
1.-…
8.- *Decomiso de instrumentos, objetos y productos del delito*
…

CAPÍTULO VI
Decomiso de Instrumentos, objetos y productos del delito

Artículo 40*.- Los instrumentos del delito, así como las cosas que sean objeto o producto de él, se decomisarán si son de uso prohibido. Si son de uso lícito, se decomisarán cuando el delito sea intencional. Si pertenecen a un tercero, sólo se decomisarán cuando el tercero que los tenga en su poder o los haya adquirido bajo cualquier título, esté en alguno de los supuestos a los que se refiere el artículo 400 de este Código, independientemente de la naturaleza jurídica de dicho tercero propietario o poseedor y de la relación que aquel tenga con el delincuente, en su caso. Las autoridades competentes procederán al inmediato aseguramiento de los bienes que podrían ser materia del decomiso, durante la averiguación o en el proceso. Se actuará en los términos previstos por este párrafo cualquiera que sea la naturaleza de los instrumentos, objetos o productos del delito.*

Si los instrumentos o cosas decomisados son sustancias nocivas o peligrosas, se destruirán a juicio de la autoridad que esté conociendo, en los términos previstos por el Código de Procedimientos Penales, pero aquélla, cuando lo estime conveniente, podrá determinar su conservación para fines de docencia o investigación. Respecto de los instrumentos del delito, o cosas que sean objeto o producto de él, la autoridad competente determinará su destino, según su utilidad, para beneficio de la procuración e impartición de Justicia, o su inutilización si fuere el caso, de conformidad con las disposiciones aplicables".

Respecto a la **confiscación**, esta se encuentra prohibida por la Constitución Política de los Estados Unidos Mexicanos (en lo sucesivo CPEUM), a tenor:

"Artículo 22. *Quedan prohibidas las penas de muerte, de mutilación, de infamia, la marca, los azotes, los palos, el tormento de cualquier especie, la multa excesiva, la confiscación de bienes y cualesquiera otras penas inusitadas y trascendentales. Toda pena deberá ser proporcional al delito que sancione y al bien jurídico afectado".*

PREGUNTA 1.5. ¿PERMITE LA LEGISLACIÓN PROCESAL DE SU PAÍS LA INTERCEPTACIÓN LEGAL DE COMUNICACIONES ELECTRÓNICAS TRASMITIDAS EN SU TERRITORIO A TRAVÉS DE SISTEMAS DE COMPUTACIÓN?

Si.

Cabe señalar que si bien la norma no especifica expresamente las comunicaciones electrónicas, se debe considerar como un medio o tipo de comunicación, y toda vez que la propia norma no la excluye; resulta procedente su intervención.

CFPP

"Artículo 278 Ter.- *Cuando la solicitud de intervención de comunicaciones privadas sea formulada por el Procurador General de la República o los servidores públicos en quienes delegue la facultad, la autoridad*

judicial otorgará la autorización cuando se constate la existencia de indicios suficientes que acrediten la probable responsabilidad en la comisión de delitos graves.

El Ministerio Público será responsable de que la intervención se realice en los términos de la autorización judicial. La solicitud de autorización deberá contener los preceptos legales que la funda, el razonamiento por el que se considera procedente, el tipo de comunicaciones, los sujetos y los lugares que serán intervenidos, así como el periodo durante el cual se llevarán a cabo las intervenciones, el cual podrá ser prorrogado, sin que el periodo de intervención, incluyendo sus prórrogas, pueda exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.

En la autorización, el juez determinará las características de la intervención, sus modalidades, límites y, en su caso, ordenará a instituciones públicas o privadas, modos específicos de colaboración.

En la autorización que otorgue el juez deberá ordenar que, cuando en la misma práctica sea necesario ampliar a otros sujetos o lugares la intervención, se deberá presentar ante el propio juez, una nueva solicitud; también ordenará que al concluir cada intervención se levante un acta que contendrá un inventario pormenorizado de las cintas de audio y video que contengan los sonidos o imágenes captadas durante la intervención, así como que se le entregue un informe sobre sus resultados, a efecto de constatar el debido cumplimiento de la autorización otorgada.

El juez podrá, en cualquier momento, verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total.

En caso de no ejercicio de la acción penal y una vez transcurrido el plazo legal para impugnarlo, sin que ello suceda, el juez que autorizó la intervención, ordenará que se pongan a su disposición las cintas resultado de las investigaciones, los originales y sus copias, y ordenará su destrucción en presencia del Ministerio Público".

APARTADO II
UNIDADES ESPECIALIZADAS Y ESFUERZOS NACIONALES

PREGUNTA 2.1. ¿HAY EN SU PAÍS UNA UNIDAD O ENTIDAD ENCARGADA ESPECÍFICAMENTE DE INVESTIGAR LOS DELITOS CIBERNÉTICOS? (Autoridad de Policía)

Si.

Nombre de la unidad o instancia: **Coordinación para la Prevención de Delitos Electrónicos, dependiente de la División Científica.**
Institución de la que depende: **Policía Federal, de la Secretaría de Seguridad Pública (Federal).**
Información de contacto:

- Nombre del Titular: **Lic. Juan Carlos Guel López (Coordinador para la Prevención de Delitos Electrónicos)**
- Domicilio: **Av. Constituyentes #947, Col. Belén de las Flores, Delegación Álvaro Obregón, C.P. 01110, México D.F.**
- Teléfono(s): **11036000, extensión: 29004 o 29103.**
- Correo electrónico: **delitocibernetico_pf@ssp.gob.mx**

2.2 ¿HAY EN SU PAÍS UNA UNIDAD O ENTIDAD ENCARGADA ESPECÍFICAMENTE DE PROCESAR JURÍDICAMENTE LA COMISIÓN DE DELITOS CIBERNÉTICOS?

La investigación de delitos corresponde al Ministerio Público (Artículo 21 de la Constitución Política de los Estados Unidos Mexicanos). En el caso de la Federación (delitos federales), corresponde al Ministerio Público de la Procuraduría General de la República, y esta NO tiene una Unidad Especial o Especializada encargada para los Delitos Cibernéticos.

No obstante a ello, la Procuraduría General de la República cuenta con unidades especializadas que con relación a su objeto de investigación (secuestros, robo de vehículos, "lavado de dinero", etc); efectúan investigaciones que a su vez se vinculan con la utilización de medios electrónicos, y

también conocen de delitos como los contemplados bajo la denominación *"Revelación de secretos y acceso ilícito a sistemas y equipos de informática",* ya citados en el presente documento. Unidades como: la Especializada en Investigación de Delitos contra los Derechos de Autor y la Propiedad Industrial, la Fiscalía de Delitos Financieros, así como la Subprocuraduría de Investigación Especializada en Delincuencia Organizada (SIEDO), por citar algunas.

Institución de la que depende: **Procuraduría General de la República (investigación de delitos federales).**
Información de contacto: (Lo designaría la Procuradora)

- Nombre del Titular: **Lic. Marisela Morales Ibáñez (Procuradora General de la República)**
- Domicilio: **Av. Paseo de la Reforma #211-213, Col. Cuauhtémoc, México D.F., C.P. 06500.**
- Teléfono(s): **53460000**
- Correo electrónico: denuncia@pgr.gob.mx

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.

Para realizar denuncia respecto a delitos cibernéticos, a través de la dirección oficial:

http://www.ssp.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=false

Se advierten algunas páginas en las cuales se brinda información a la ciudadanía, algunas de Instituciones Oficiales, así como de organizaciones no gubernamentales. Como ejemplo:

www.datospersonales.sep.gob.mx, que de la Secretaría de Educación Pública: contiene consejos útiles para el uso de Internetmaterial de apoyo para el uso de internet.

http://asi-mexico.org/sitio/, de *"Alianza por la Seguridad en Internet"*, en la cual incluso se señala a quienes tiene acceso: "Línea de denuncia. A través de este portal usted puede ayudarnos a eliminar contenido ilegal, inapropiado o fraudulento que afecte a usuarios de internet en México".

2.4 HA DESARROLLADO Y/O IMPLEMENTADO SU PAÍS UNA ESTRATEGÍA NACIONAL DE SEGURIDAD CIBERNÉTICA?

Debe considerarse que está contemplada por el Plan Nacional de Desarrollo 2007-2012, Eje 1. Estado de Derecho y Seguridad, Objetivo 7, "*Estrategia 7.1 Desarrollar e implementar sistemas de información y comunicaciones de alta tecnología para el combate a la delincuencia"*.

De ahí que se continúa dotando de infraestructura a diversas áreas, entre ellas: a la Coordinación para la Prevención de Delitos Electrónicos, de la División Científica, de la Policía Federal, de la Secretaría de seguridad Pública.

El indicado Eje, puede ser consultado en la siguiente dirección:

http://pnd.calderon.presidencia.gob.mx/pdf/Eje1_Estado_de_Derecho_y_Seguridad/1_3_Informacion_e_Inteligencia.pdf

III. COOPERACIÓN INTERNACIONAL

3.1 ¿SE HA ADHERIDO SU PAÍS A LA CONVENCIÓN DEL CONSEJO DE EUROPA SOBRE DELINCUENCIA CIBERNÉTICA?

De los datos obtenidos de la página de internet oficial de "Council of Europe", se advierte que México aún no es miembro. Se advierte como Estado Observador.

http://www.coe.int/lportal/en/web/coe-portal

Específicamente respecto a *"Convention on Cybercrime"*, se advierte a México en el listado de países no miembros, pero no tiene fecha de haber realizado la firma de la Convención.

EN CASO NEGATIVO, ¿HA CONSIDERADO SU PAÍS LA APLICACIÓN DE LOS PRINCIPIOS CONTENIDOS EN DICHA CONVENCIÓN?

Es dable afirmar que sí.

Ha participado en el grupo de trabajo en delito cibernético, así como en el Grupo Plenario México-EUA, sobre procuración de justicia *donde "…se expuso la necesidad de mantener el tema de los delitos cibernéticos en la agenda…",* y se tiene previsto que en breve nuestro país se adhiera al Convenio de Cibercriminalidad de Budapest, celebrado el 23 de noviembre de 2001.

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20latam%20mex2010/2079_LA_Pres_procuraduria.pdf

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, México es miembro.

http://www.oas.org/juridico/spanish/cyb20_network_sp.pdf

http://www.oas.org/juridico/english/cyb_pan_G8_sp.pdf

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, actualmente México cuenta con Tratados de Cooperación sobre Asistencia Jurídica Mutua con diversos países, entre ellos: Argentina, Brasil, Canadá, Chile, Colombia (Acuerdo), Costa Rica, Ecuador (Convenio), El Salvador, Estados Unidos de América, Guatemala, Honduras, Nicaragua, Panamá, Paraguay, Perú (Convenio), Uruguay y Venezuela.

Cabe señalar que muchos Tratados hacen referencia a la tramitación de pruebas en general, por ende, es dable afirmar que están contempladas aquellas pruebas electrónicas.

http://www.oas.org/juridico/MLA/sp/mex/index.html

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 ESOS DELITOS?

La Coordinación Para la Prevención de Delitos Electrónicos de la División Científica de la Policía Federal, Secretaría de Seguridad Pública, de acuerdo a la normatividad, ha procurado colaborar con diversas instancias de los Estados Unidos de América.

De conformidad a lo establecido en el Quinto Informe de Gobierno del Presidente de los Estados Unidos Mexicanos: Felipe Calderón Hinojosa, acerca de las diferentes solicitudes recibidas para la investigación de diversos delitos, por parte de países como Estados Unidos y Canadá, así como de requerimientos de información por parte de países integrantes de los Centros de Información de Drogas (Centroamérica, Sudamérica, el Caribe, Europa, Asía y África). Dirección:

http://quinto.informe.gob.mx/archivos/informe_de_gobierno/pdf/1_3.pdf

En relación con lo anterior, implementación del programa "Alerta Amber" con la participación de la Policía Federal, la PGR, la SEGOB y los gobiernos estatales con el fin de fortalecer el intercambio de información con agencias policiales y de seguridad de los gobiernos de EUA y Canadá. Aunado a lo anterior, en mayo de 2011 se firmó el Protocolo en la Seguridad de la Interconexión entre la Agencia de Inmigración y Control de Aduanas (ICE) y la SSP con el objetivo de intercambiar información.

http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/952013//archivo

También de informe proporcionado por la Agencia ICE, se tuvo conocimiento de la detección de una IP en México a través de la cual se transmitió pornografía infantil. Por lo que en colaboración con elementos de la Policía Federal, se logró la detención de una persona como probable responsable del almacenamiento de imágenes de pornografía infantil.

http://www.pgr.gob.mx/temas%20relevantes/Informes%20Institucionales/Informes%20Institucionales.asp#

IV. CAPACITACIÓN

4.1 ¿OFRECE SU PAÍS CAPACITACIÓN A FUNCIONARIOS RESPONSABLES DE LA APLICACIÓN DE LA LEGISLACIÓN CONTRA EL DELITO CIBERNÉTICO Y PARA LA OBTENCIÓN DE PRUEBAS ELECTRÓNICAS?

Si.

A través de la colaboración de instituciones y organismos de seguridad internacional con reconocida experiencia en las distintas áreas de seguridad y combate a la delincuencia se logró fortalecer el esquema de formación, adiestramiento y profesionalización de los integrantes de la Secretaría y de la Policía Federal.

De septiembre de 2009 al mes de agosto de 2010 se concertó la colaboración de expertos e instructores de agencias internacionales en la impartición de 96 cursos y seminarios, en los que recibieron capacitación 2,217 funcionarios de la SSP y de la Policía Federal en temas como: *Accountability* y Modernización Policial; administración avanzada e identificación y aseguramiento de evidencia digital; delitos cibernéticos; entrevista e interrogatorio; inteligencia y análisis táctico; investigación de drogas y crimen organizado transnacional; mecanismos de control de confianza; derechos humanos, entre otros.

http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/815854//archivo

También, en el periodo de 2010-2011, la SSP se enfocó, entre otros a los temas de: cadena de custodia, lavado de dinero, trata de personas, investigación, análisis e inteligencia, seguridad cibernética. etc

http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/952013//archivo

Por su parte la Procuraduría General de la República impartió cursos de actualización dirigidos a agentes del Ministerio Público de la Federación, sobre "Delitos informáticos: cibercriminalidad", y "Extinción de dominio", "Informática aplicada a la criminalística y aplicación del G.P.S.", entre otros.

http://www.pgr.gob.mx/Temas%20Relevantes/Documentos/Informes%20Institucionales/4o%20Informe%20PGR%20completo.pdf

Asimismo fueron capacitados integrantes de las delegaciones estatales de la PGR, SIEDO y FEPADE, Mediadores del Tribunal Superior de Justicia del Distrito Federal (TSJDF), integrantes del observatorio ciudadano de la justicia, magistrados, jueces, proyectistas, secretarios de acuerdo, actuarios, conciliadores, de primera y segunda instancia, respectivamente; policías judiciales y peritos criminalistas de la SEDENA, de Justicia Militar del Ejército y Fuerza Aérea Mexicana, el tema fue, entre otros, "*Informática aplicada a la criminalística".*

http://www.pgr.gob.mx/Temas%20Relevantes/Documentos/Informes%20Institucionales/ConvFrame2.asp

4.2 ¿OFRECE SU PAÍS CAPACITACIÓN A LOS FISCALES EN DELITO CIBÉRNETICO Y PARA LA OBTENCIÓN PRUEBAS ELECTRÓNICAS?

Si se ofrecen diferentes cursos en los cuales han sido constantes los temas de cadena de custodia y preservación de indicios, dentro en los cuales se contempla el tema de objetos electrónicos.

Al igual que en la pregunta que antecede (4.1), cabe recordar que en nuestro país, la investigación de los delitos corresponde al Ministerio Público de la Federación (en materia federal), y próximamente se les denominará fiscal, como en otro países. (Al "fiscal" se le considera como equivalente a la función de "agente del Ministerio Público")

4.3 DE ACUERDO CON LOS ESFUERZOS DE SU PAÍS PARA OFRECER CAPACITACIÓN EN LA INVESTIGACIÓN Y PRESECUCIÓN 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:

El Plan Nacional de Desarrollo, en el Eje 1. Estado de Derecho y Seguridad, establece los puntos 1.3 Información e inteligencia, 1.10 Cooperación Internacional así como 1.11 Prevención del Delito.

http://pnd.calderon.presidencia.gob.mx/index.php?page=documentos-pdf

En el marco del Plan Ejecutivo Conjunto de la Asociación Estratégica México-UE se tiene como uno de los objetivos el de *"Fortalecer la cooperación bilateral en materia de lucha contra los delitos cibernéticos".*

http://www.europarl.europa.eu/intcoop/eurolat/key_documents/mexico/strategic_partnership_es.pdf

4.4 ¿HA PARTICIPADO SU PÁIS EN LOS TALLERES DE CAPACITACIÓN CELEBRADOS EN EL MARCO DEL GRUPO DE TRABAJO EN DELITO CIBERNÉTICO?

Si.

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20LATAM%20Mex2010/2079_LA_Pres_aseger_legis.pdf

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20LATAM%20Mex2010/default_en.asp

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:

La necesidad de contar con estrategia nacional de seguridad cibernética.
Derecho comparado en materia de Delitos Cibernéticos y/o electrónicos.
Formación sobre 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 SUS CAPACIDAD PARA ENFRENTAR LOS DELITOS RELACIONADOS CON LAS COMPUTADORAS Y EL INTERNET:

- Proporcionando capacitación en todos los ámbitos de los Delitos Cibernéticos.
- Intercambio de experiencias sobre el tratamiento que se ha dado a los diferentes casos.

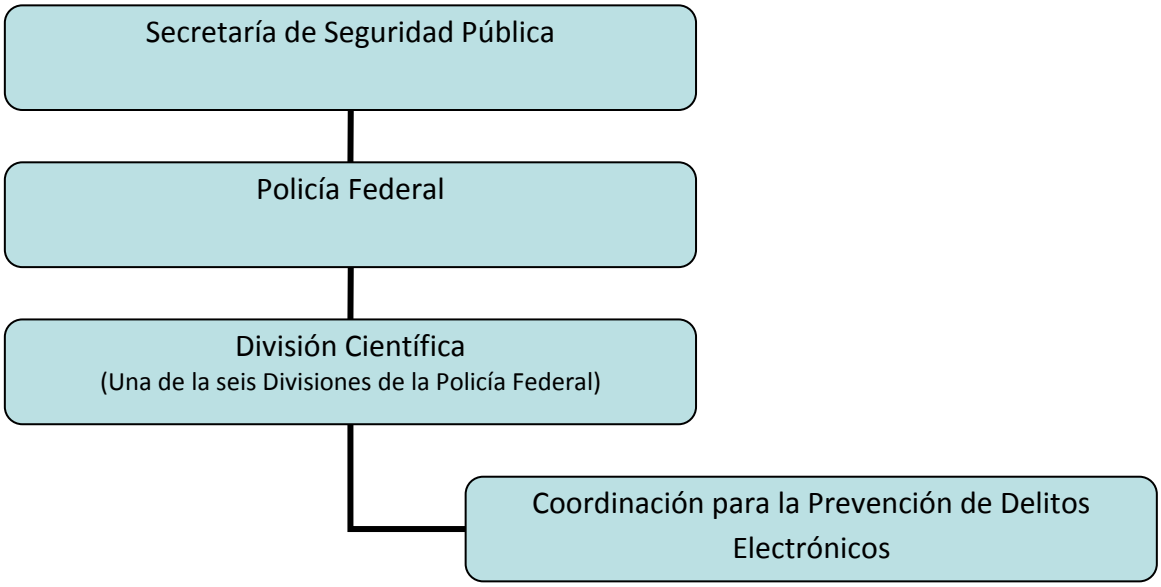
INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO.

El cuestionario que se hizo llegar a la División Científica de la Policía Federal de la Secretaría de Seguridad Pública.

Dr. Ciro Humberto Ortiz Estrada.
Titular de la División Científica. En donde está la Coordinación para la Prevención de Delitos Electrónicos.
Titular que encomendó la elaboración al área a cargo del lic. Rubén Hernández Hernández, Inspector General en la División.

Ing. Facundo Rosas Rosas.
Comisionado de la Policía Federal. Alto Mando de la Policía.

Ing. Genaro García Luna.
Secretario de Seguridad Pública Federal.


Secretaría de Seguridad Pública
Policía Federal
División Científica
(Una de la seis Divisiones de la Policía Federal)
Coordinación para la Prevención de Delitos Electrónicos