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

OEA/Ser.K/XXXIV
CIBER-VIII/doc.1/11
6 Noviembre 2013
Original: inglés

Octava Reunión del Grupo de Trabajo en Delito Cibernético

CUESTIONARIO PREPARATORIO DE LA OCTAVA REUNIÓN DEL GRUPO DE TRABAJO EN DELITO CIBERNÉTICO

INTRODUCCIÓN

El presente cuestionario busca recolectar información útil para los propósitos de la Octava Reunión del Grupo de Trabajo en Delito Cibernético, la cual se celebrará a principios de 2014, en relación con las recomendaciones que han sido formuladas en las reuniones anteriores 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 cinco áreas temáticas: (I) Legislación; (II) Cooperación internacional; (III) Unidades especializadas y esfuerzos nacionales; (IV) Resultados de investigaciones y enjuiciamientos en materia de delito cibernético; y (V) Capacitación.

Teniendo en cuenta lo anterior, sírvase remitir la respuesta de su Estado al presente cuestionario, a más tardar el **martes 10 de diciembre de 2013,** 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

A. LEGISLACIÓN SUSTANTIVA:

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

a)	Acceso ilícito	Sí (X) No ( )
b)	Interceptación ilícita	Sí (X) No ( )
c)	Ataques a la integridad de datos	Sí (X) No ( )
d)	Ataques a la integridad de sistemas	Sí (X) No ( )
e)	Abuso de dispositivos	Sí (X) No ( )
f)	Falsificación informática	Sí ( ) No (X, parcial)
g)	Fraude informático	Sí (X) No ( )
h)	Pornografía infantil	Sí (X) No ( )
i)	Delitos contra la propiedad intelectual y derechos afines	Sí (X) No ( )
j)	Otras (sírvase enumerarlas): _____	Sí ( ) No ( )

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

Segue abaixo a primeira lei brasileira específica para a tipificação criminal de delitos informáticos, que modificou o Código Penal Brasileiro:

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

"Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

"Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266. .....

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR)

"Falsificação de documento particular

Art. 298. .....

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito." (NR)

Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.

Em adição a essa lei, existem outras leis e artigos de lei brasileiros que são usados de forma análoga para a punição de crimes cibernéticos:

Interceptação Ilícita *– Crime previsto na Lei n.º 9.296/96. Artigo 10*
**** Ataque a integridade de Sistema*** *– Crime previsto, em parte, no Código Penal, artigo 313-A e 313-B. Nestes artigos há proteção, tão somente, a sistemas informatizados e banco de dados da Administração Pública, não disciplinando ataques a sistemas de pessoas físicasou entidades privadas.*

***Falsidade Informática** - Crime previsto, em parte, no Código Penal, artigo 313-A Neste artigo há proteção, tão somente, a sistemas informatizados e banco de dados da Administração Pública, não disciplinando falsidade de dados de pessoas físicas ou entidades privadas.*
***Ataque de Negação de Serviço (DDoS) –** Crime previsto no artigo 265 do Código Penal quando o ataque atentar contra o funcionamento de um serviço de utilidade pública.*
***Fraude Informática** – Crime previsto no artigo 163 do Código Penal (dano).*
***Pornografia Infantil** – Crime previsto no artigo 241 e seguintes do Estatuto da Criança e do Adolescente. Tipifica-se a produção, a venda, distribuição, a aquisição e a posse. Além do mais, os responsáveis pelo acesso ao material pornográfico também são puníveis, após oficialmente notificados.*
***Violação de Direito Autoral** – Crime previsto no Artigo 184 do Código Penal,interpretado com as disposições da Lei n.º 9.609/98 e Lei n.º 9.610/98.*
***Racismo** – Crime previsto no art. 20, inciso 2 da Lei 7716/89.*
***Crimes contra a honra cometidos através de meios que facilitem a divulgação –** previsto no art. 141, III, do Código Penal..*

1.2. ¿Ha promulgado su país legislación que:

a) Tipifique la tentativa de comisión de cualquiera de las modalidades de delito cibernético enumeradas arriba? Sí (X) No ( )

En caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica, de la legislación: A tentativa de cometimento de crimes relacionados à pornografia infantil é punida no Estatuto da Criança e Adolescente no Brasil, como pode ser vistos pelos artigos que colaciono abaixo:
"Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
§ 1° Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
§ 2° Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
I – no exercício de cargo ou função pública ou a pretexto de exercê-la;
II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou
III – prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento."
Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:
Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
Parágrafo único. Nas mesmas penas incorre quem:
I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;
II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.

b) Tipifique la complicidad y la instigación en la comisión de cualquiera de las modalidades de delito cibernético enumeradas arriba? Sí (X) No ( )

En caso afirmativo, sírvase enumerar y adjuntar copia, de preferencia electrónica, de la legislación: *vide os exemplos anexados à resposta da letra a.*

c) Contemple posibilidad de responsabilidad institucional por delitos cibernéticos, es decir, legislación según la cual puede hacerse responsables a personas morales por delitos penales de tipo cibernético? Sí ( ) No (X)

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

B. LEGISLACIÓN PROCESAL:

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

O Congresso Nacional brasileiro aprovou no ano 2012 as Leis 12.735 e 12.737. A Lei 12.737 foi reproduzida acima. Existem outros projetos que visam a criminalização de condutas relacionadas à segurança da informação em meio computacional, mas o projeto atualmente mais desenvolvido é o denominado "Marco Civil da Internet", o Projeto de Lei 2126/2011, que além da regulamentação de direitos e deveres dos usuários e provedores de serviços na Internet, conterá determinações sobre a retenção e a obtenção de informações sobre provedores de acesso e de serviço na internet.
.

1.4. ¿Permite la legislación de su país, por parte los investigadores criminales, requerir a los Proveedores de Servicios de Internet a preservar pruebas electrónicas sin la necesidad de una orden judicial?

Sí (x) No ( )

En caso afirmativo, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjuntar copia, de preferencia electrónica, de las mismas:
Neste ano foi promulgada a Lei 12.830/2013, que contém a previsão de que o Delegado de Polícia pode requisitar informações que interessem a uma investigação. Segue abaixo o texto da Lei:
LEI Nº 12.830, DE 20 DE JUNHO DE 2013.
http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12830.htm
Dispõe sobre a investigação criminal conduzida pelo delegado de polícia.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei dispõe sobre a investigação criminal conduzida pelo delegado de polícia.
Art. 2º As funções de polícia judiciária e a apuração de infrações penais exercidas pelo delegado de polícia são de natureza jurídica, essenciais e exclusivas de Estado.
§ 1º Ao delegado de polícia, na qualidade de autoridade policial, cabe a condução da investigação criminal por meio de inquérito policial ou outro procedimento previsto em

lei, que tem como objetivo a apuração das circunstâncias, da materialidade e da autoria das infrações penais.
§ 2º Durante a investigação criminal, cabe ao delegado de polícia a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos.
§ 3º (VETADO).
§ 4º O inquérito policial ou outro procedimento previsto em lei em curso somente poderá ser avocado ou redistribuído por superior hierárquico, mediante despacho fundamentado, por motivo de interesse público ou nas hipóteses de inobservância dos procedimentos previstos em regulamento da corporação que prejudique a eficácia da investigação.
§ 5º A remoção do delegado de polícia dar-se-á somente por ato fundamentado.
§ 6º O indiciamento, privativo do delegado de polícia, dar-se-á por ato fundamentado, mediante análise técnico-jurídica do fato, que deverá indicar a autoria, materialidade e suas circunstâncias.
Art. 3º O cargo de delegado de polícia é privativo de bacharel em Direito, devendo-lhe ser dispensado o mesmo tratamento protocolar que recebem os magistrados, os membros da Defensoria Pública e do Ministério Público e os advogados.
Art. 4º Esta Lei entra em vigor na data de sua publicação.
Brasília, 20 de junho de 2013; 192º da Independência e 125º da República.

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

a) Confiscar, decomisar o secuestrar sistemas o dispositivos de almacenamiento informático? Sí (X) No ( )

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

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

O Código de Processo Penal, no seu artigo 240, permite a busca e apreensão de qualquer objeto necessário à prova da infração, dentre eles, mídias, computadores, sistemas ou qualquer elemento útil à investigação e processo penal.
Lei 9296/96, sobre interceptação para prova em investigação criminal e em instrução processual penal.
http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm
http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm

II. COOPERACIÓN INTERNACIONAL

2.1. ¿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 lo sé ( )

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

2.2. ¿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 lo sé ( )

En caso afirmativo, sírvase describir brevemente las normas y/u otras medidas existentes al respecto y adjuntar copia, de preferencia electrónica, de las mismas:
O Brasil pode atender aos pedidos de cooperação jurídica internacional com base no princípio da reciprocidade, mesmo na ausência de tratado com o país que faz o pedido.
Ademais, a fim de proporcionar o mais amplo auxílio nas investigações e procedimentos de natureza criminal, o Brasil conta com um conjunto de disposições nesta matéria, dentre as quais cumpre destacar os tratados bilaterais em vigor e os intrumentos multilaterais ratificados, tais como a Convenção das Nações Unidas contra a Corrupção; a Convenção das Nações Unidas contra o Crime Organizado Transnacional; a Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais da Organização para a Cooperação e Desenvolvimento Econômico (OCDE); e o Protocolo de Assistência Jurídica Mútua em Asssuntos Penais do Mercosul (Argentina, Paraguai e Uruguai). Aguarda a promulgação do Protocolo de Assistência Jurídica Mútua em Assuntos Penais do Mercosul (Bolívia e Chile). Encontra-se no Congresso Nacional a Convenção de Auxílio Judiciário em Matéria Penal entre os Estados Membros da Comunidade dos Países de Língua Portuguesa – CPLP.
Atualmente, encontram-se em vigor os seguintes acordos bilaterais de cooperação jurídica internacional em matéria penal: Canadá, China, Colômbia, Coreia do Sul, Cuba, Espanha, Estados Unidos da América, França, Itália, México, Nigéria, Panamá, Peru, Portugal, Suíça, Suriname e Ucrânia. Os acordos com Alemanha, Bélgica, El Salvador e Jordânia encontram-se em tramitação no Congresso Nacional e aqueles com Angola, Hondura, Líbano e Reino Unido estão pendentes de ratificação.
Além disso, o Brasil firmou acordos bilaterais de cooperação jurídica internacional em matéria penal com Israel, Hong Kong e Turquia. Seguem em negociação propostas de acordos com mais de 20 países.

2.3. ¿Ha formulado o recibido su país solicitudes de asistencia mutua para la investigación o enjuiciamiento de delitos cibernéticos o bien para la obtención de pruebas electrónicas y la realización de otros actos necesarios para facilitar la investigación o enjuiciamiento de estos delitos? Sí (X) No ( ) No lo sé ( )

En caso afirmativo, sírvase indicar el número de solicitudes que ha formulado y/o recibido y el estado en que se encuentran dichas solicitudes:
Considerando uma amostragem desde 2011, diligenciamos um total de 63 pedidos nessa temática, sendo 05 casos relacionados à investigação de crimes cibernéticos e 58 para obtenção de provas telemáticas para elucidação de outros crimes.
Dos passivos, 02 ainda estão em andamento, 02 foram integralmente cumpridos e 01 parcialmente cumprido.
Em relação aos ativos, o total é bem maior: 58. Desses, 24 foram restituídos, sendo 18 deles não cumpridos, 05 cumpridos e 01 restituído independente do cumprimento; 22 ainda se encontram em andamento.

III. UNIDADES ESPECIALIZADAS Y ESFUERZOS NACIONALES

3.1. ¿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: Serviço de Repressão a Crimes Cibernéticos

- Institución de la que depende: Polícia Federal

- Información de contacto:

o Nombre del Titular: João Vianey Xavier Filho

o Domicilio: SAS, Quadra 06, Lote 09/10 – Brasília - DF

o Teléfono(s): +55.61.2024.8329

o Correo electrónico: urcc.cgpfaz@dpf.gov.br

3.2. ¿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: *Ministerio Público Federal*
- Institución de la que depende: _____
- Dirección en internet de la unidad o instancia: http://www.mpf.mp.br/
- Información de contacto:_____
    - Nombre del titular: _____
    - Domicilio:_____
    - Teléfono(s): _____ Fax: _____
    - Correo electrónico:_____

3.3. ¿Ha establecido su país páginas en internet para facilitar que los ciudadanos cuenten con información para evitar 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:
www.prsp.mpf.gov.br
www.safernet.org.br
www.prgr.mpf.gov.br
www.dpf.gov.br

3.4. ¿Ha implementado su país algún programa de probidad o creación de conciencia sobre los riesgos del delito cibernético, o ha producido manuales o guías para orientar y alertar a la

ciudadanía sobre los riesgos del delito cibernético y formas para evitar convertirse en víctima del mismo? Sí (X) No ( )

En caso afirmativo, sírvase proveer una descripción breve de dichos programas, manuales o guías:
Embora não haja um programa nacional, há iniciativas isoladas, como unidade de esforços e trabalho conjunto entre os órgãos de persecução penal no combate aos crimes cibernéticos; campanhas de prevenção junto a escolas e à mídia; distribuição de cartilhas entre estudantes e professores para o uso consciente da internet; e realização de parcerias e acordos com ONG´s, autoridades, empresas que atuam no setor para promover o bom uso da internet com o objetivo de diminuir a prática dos crimes cibernéticos Há, igualmente, iniciativas de diversos órgãos governamentais sobre o tema, notadamente, do Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República, (foco na proteção da informação e infraestruturas críticas da Nação) do Ministério da Defesa, através do Exército Brasileiro (foco na Defesa Cibernética do país) e da própria Polícia Federal (prevenção e repressão a ilícitos praticados no campo cibernético).

IV. RESULTADOS DE INVESTIGACIONES Y ENJUICIAMIENTOS EN MATERIA DE DELITO CIBERNÉTICO

4.1. Sírvase indicar el número de **investigaciones** que ha realizado su país con respecto a cada uno de los siguientes delitos cibernéticos o conductas desde enero de 2012 hasta la fecha:

a) Acceso ilícito — Número de investigaciones: ____
b) Interceptación ilícita — Número de investigaciones: ____
c) Ataques a la integridad de datos — Número de investigaciones: ____
d) Ataques a la integridad de sistemas — Número de investigaciones: ____
e) Abuso de dispositivos — Número de investigaciones: ____
f) Falsificación informática — Número de investigaciones: ____
g) Fraude informático — Número de investigaciones: ____
h) Pornografía infantil — Número de investigaciones: ____
i) Delitos contra la propiedad intelectual y derechos afines — Número de investigaciones: ____

4.2. Si su país ha tipificado cualquiera de los delitos cibernéticos a que se refiere la pregunta 1.1 anterior, sírvase indicar el número de **enjuiciamientos** que ha realizado su país con respecto a cada uno de los delitos cibernéticos correspondientes, desde enero de 2012 hasta la fecha, así como el número de casos que dieron lugar a una **condena**:

a) Acceso ilícito — Casos enjuiciados: ____Condenas ____
b) Interceptación ilícita — Casos enjuiciados: ____Condenas ____
c) Ataques a la integridad de datos — Casos enjuiciados: ____Condenas ____
d) Ataques a la integridad de sistemas — Casos enjuiciados: ____Condenas ____
e) Abuso de dispositivos — Casos enjuiciados: ____Condenas ____
f) Falsificación informática — Casos enjuiciados: ____Condenas ____
g) Fraude informático — Casos enjuiciados: ____Condenas ____
h) Pornografía infantil — Casos enjuiciados: ____Condenas ____

i) Delitos contra la propiedad intelectual y derechos afines Casos enjuiciados: ____Condenas ____

4.3. ¿Han enfrentado alguna dificultad con respecto a la investigación o el enjuiciamiento de estos delitos? Sí ( ) No ( )

En caso afirmativo, sírvase proveer una descripción detallada y específica del tipo de dificultades que se han enfrentado: _____
_____
_____
_____

4.4. ¿Existen ámbitos relativos al combate del delito cibernético en que su país podría beneficiarse de cooperación técnica suministrada por otros Estados miembros?

Sí ( ) No ( )

En caso afirmativo, sírvase proveer una descripción detallada y específica del tipo de cooperación técnica que podría ser benéfica para su país:_____
_____
_____
_____

V. CAPACITACIÓN

5.1. ¿Ofrece su país capacitación sobre delito cibernético y sobre la obtención de pruebas electrónicas a los funcionarios responsables de la aplicación de la legislación?

Sí (X) No ( )

En caso afirmativo, sírvase describir brevemente el tipo de capacitación y el número de funcionarios capacitados:
O Departamento de Polícia Federal (DPF), treina os seus servidores de diversas formas e em diversos níveis. Na fase de recrutamento, os policiais recebem treinamento básico para a investigação de crimes cibernéticos na Academia Nacional de Policia. Para 2014, serão capacitados mais de 200 novos policiais. O curso introdutório tem duração de 20 horas/aula.
Para os policiais que já se encontram em atuação, desenvolvemos um curso internediário à distancia, com duração de 06 meses, que já capacitou mais de 750 policiais.
O DPF provê treinamento contínuo para os policiais que integram os Grupos de Repressão a Crimes Cibernéticos, criados para aperfeiçoar a atuação operacional da Polícia Federal nos Estados de nossa Federação. O DPF participa, ainda, da capacitação das polícias civis estaduais, por meio de parceria com a a Secretaria Nacional de Segurança Pública.
Dentro do Programa Nacional de Capacitação e Treinamento de Combate à Corrupção e à Lavagem de Dinheiro (PNLD), 05 módulos, ocorridos em 05 diferentes Estados da Federação, capacitaram cerca de 810 agentes públicos no que tange a Delitos Cibernéticos durante o ano de 2013.

Vale destacar que, devido a questões logísticas e de demanda, esses treinamentos tiveram destinação a juízes, policiais, membros do Ministério Público e outros servidores públicos, de níveis federal, estadual e municipal, simultaneamente.

5.2. ¿Ofrece su país capacitación a los fiscales sobre delito cibernético y obtención de pruebas electrónicas? Sí (X) No ( )

En caso afirmativo, sírvase describir brevemente el tipo de capacitación y el número de funcionarios capacitados:
O Departamento de Polícia Federal realiza periodicamente conferências, seminários, grupos de trabalho que abordaram o enfrentamento ao crimes cibernéticos, para juízes, delegados e procuradores. O DPF planeja a realização de um curso à distância para juízes e procuradores, organizado pela Polícia Federal em parceria com as Escolas Superiores da Magistratura e do Ministério Público.

5.3. ¿Ofrece su país capacitación a los jueces sobre delito cibernético y obtención de pruebas electrónicas? Sí (X) No ( )

En caso afirmativo, sírvase describir brevemente el tipo de capacitación y el número de funcionarios capacitados: *Vide resposta 5.1*

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: _____
(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:
( ) Sr.: _____
( ) Sra.: _____
Título/cargo:_____
Organismo/oficina:_____
Domicilio: _____
_____
Número de teléfono:_____
Número de fax:_____
Correo electrónico:_____