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

Séptima Reunión del Grupo de Trabajo en Delito Cibernético

OEA/Ser.K/XXXIV
CIBER-VII/doc.2/11
14 noviembre 2011
Original: inglés

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

INTRODUCCIÓN

El presente cuestionario busca recolectar información útil para los propósitos de la Séptima Reunión del Grupo de Trabajo en Delito Cibernético, la cual se celebrará el 6 y 7 de febrero de 2012, en relación con las recomendaciones que han sido formuladas en las reuniones precedentes y las que han sido adoptadas en el marco del proceso de las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA), concordantes con las mismas.

Para estos efectos, el cuestionario se divide en cuatro áreas temáticas: (1) legislación; (2) unidades especializadas y esfuerzos nacionales; (3) cooperación internacional; y (4) capacitación.

Este cuestionario es sustancialmente similar al documento que se envío en noviembre de 2009, con antelación a la Sexta Reunión del Grupo de Trabajo en Delito Cibernético, y a la cual su país respondió en su momento. Para facilitar la elaboración del presente cuestionario, la respuesta de su país al cuestionario anterior se anexa a este documento.

Teniendo en cuenta lo anterior, sírvanse remitir la respuesta de su Estado al presente cuestionario, a más tardar el **viernes, 16 de diciembre de 2011**, a la Secretaría General de la OEA (Departamento de Cooperación Jurídica de la Secretaría de Asuntos Jurídicos), al correo electrónico LegalCooperation@oas.org o al número de fax: + (202) 458-3598.

Por favor adicionar el espacio que requiera en cada respuesta o anexar hojas, según lo estime necesario.

I. LEGISLACIÓN

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

a)	Acceso ilícito	Sí ( ) No (x)
b)	Interceptación ilícita	Sí (x) No ( )
c)	Ataques a la integridad de datos	Sí ( )No (x, parcialmente)*
d)	Ataques a la integridad de sistemas	Sí ( )No (x, parcialmente)*
e)	Abuso de dispositivos	Sí ( ) No (x)
f)	Falsificación informática	Sí () No (x, parcialmente)**
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:

O Brasil não possui uma legislação específica sobre crimes cibernéticos, notadamente, sobre os crimes considerados de "ALTA TECNOLOGIA" (invasão de sistemas, acesso ilícito, uso inadequado de dispositivos, etc). Entretanto, algumas condutas relacionadas ao uso de computadores para a prática de crimes já estão tipificadas em nosso Código Penal e em legislações extravagantes que podem ser consideradas, ao menos em parte, para fins de imputação penal e, em alguns casos, aumento de pena. Podemos citar alguns casos:

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

En caso afirmativo, sírvase describir esos esfuerzos:

Há varios projetos de lei em andamento no Congresso Nacional que tratam da criminalização de condutas relacionadas à segurança da informação em meio computacional, tais como, o acesso indebido a dados e sistemas, a interferencia em sistemas de informação e comunicação, o uso inadequado de dispositivos. Os dois projetos em estado mais avançado são o ***PL 84/99*** *e o* ***PL 2.793/2011****, ambos sob a análise da Câmara dos Deputados.*

Além disso, o governo brasileiro propôs ao Congresso projeto de Lei para regulamentar Direitos e deveres dos usuários e provedores de serviços na Internet, denominado "Marco Civil da Internet". O projeto recebeu o número 2126/2011 e também se encontra na Câmara dos Deputados.

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

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

Não. Nosso ordenamento jurídico ainda não prevê, expresamente, a possibilidade de requisição da Autoridade Policial (Delegado de Polícia) dirigida a qualquer provedor de serviços de Internet para que preserve dados cadastrais, dados de tráfico ou informações por estes mantidos ou armazenados. A prova da materialidade do crime é preservada com base em Termos de cooperação e Termos de Ajustamento de Conduta formulados com os provedores.

Há, entretanto, divergências em relação à questão, pois alguns juízes entendem que o acesso aos dados do IP podem ser enviados diretamente, sem necessidade de ordem judicial. Entende-se que o Código de Processo Penal, no seu artigo 6.º, prevê tal possibilidade, ainda que genericamente, dentro os chamados "poderes gerais de investigação" concedidos às Autoridades Policiais. Todavia, tal entedimento não é pacífico em nossa doutrina. No PL 2793/2011 há tal previsão, visando a pacificação do tema.

http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm

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

a) Confiscar, decomisar o secuestrar sistemas o dispositivos de almacenamiento informáticos. Sí (x) No ( )

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

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

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

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?

En caso afirmativo, sírvase describir brevemente y adjuntar copias, de preferencia electrónica, de esa legislación:

Sim. A Lei n.º 9296/1996, prevê, no parágrafo único do artigo 14.º, que a interceptação de fluxo de dados e comunicações em sistemas de informática e telemática é possível, mediante autorização da autoridade judicial, para fins de investigação e processo criminal, observados alguns requisitos de proteção dos direitos e garantias individuais, como a privacidade e intimidade.

http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm

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: Serviço de Repressão a Crimes Cibernéticos
- Institución de la que depende: Polícia Federal
- Información de contacto:
  - Nombre del Titular: Carlos Eduardo Miguel Sobral
  - Domicilio: *SAS, Quadra 06, Lote 09/10 – Brasília - DF*
  - Teléfono(s): *+55.61.2024.8329 / 8136*
  - Correo electrónico: urcc.cgpfaz@dpf.gov.br / sobral.cems@dpf.gov.br

2.2. ¿Hay en su país una unidad o entidad encargada específicamente de procesar jurídicamente la comisión de delitos cibernéticos? Sí (x[1]) No ( )

En caso afirmativo, sírvase proporcionar la siguiente información:

[1] Apenas em alguns Estados da Federação, como Rio de Janeiro e São Paulo, e apenas para os crimes de pornografia infantil e racismo cometido por meio da Internet.

- Nombre de la unidad o instancia: *Grupo de Combate aos Crimes Cibernéticos nas Procuradorias da República no Rio de Janeiro e em São Paulo*
- Institución de la que depende: *Ministério Público Federal*
- Información de contacto:
  - Nombre del Titular: *Marta Pinheiro de Oliveira Sena / Priscila Costa Schreiner*
  - Domicilio: _____
  - Teléfono(s): *(11) 3269-5077 ou (11) 3269-5042* Fax: _____
  - Correo electrónico: *mpsena@prsp.mpf.gov.br / pschreiner@prsp.mpf.gov.br*

2.3. ¿Ha establecido su país páginas en Internet para facilitar que los ciudadanos cuenten con información para prevenir ser víctimas de delitos cibernéticos y para detectarlos y denunciarlos ante las autoridades competentes cuando ellos ocurran? Sí (x[2]) 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
Páginas dos princpipais provedores de Internet

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

Embora não haja uma estratégia 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 ilíticos praticados no campo cibernético).*
Entretanto, a pesar destas iniciativas, ainda não há um documento formal que preveja a Segurança Cibernética como um sistema complexo, integrado por diferentes entes (públicos e privados) de diversos níveis governamentais (Nacional, Estadual e Municipal), estabelecendo responsabilidade e definindo metas e procedimentos.

---

[2] *Apenas para crimes específicos, notadamente pornografia infantil.*

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:

O Governo brasileiro analisou, em 2009, de forma abrangente, a Convenção do Conselho da Europa sobre Crime Cibernético, com o objetivo de identificar os méritos e imperfeições do documento, à luz das eventuais necessidades de aperfeiçoamento dos dispositivos de combate ao crime cibernético existentes no ordenamento jurídico interno, na prática e interpretação jurídicas e na jurisprudência brasileira no assunto. Constatou-se, na ocasião, a incompatibilidade de dispostivos da Convenção de Budapeste ao ordenamento jurídico interno, em razão da impossibilidade de reservas ou declarações interpretativas a artigos específicos.

Em 2011, a Convenção foi novamente considerada em encontro que reuniu diversos órgãos do Governo brasileiro. Os participantes confirmaram o entendimento supracitado.

3.2. ¿Se ha vinculado su país a la Red de Emergencia de Contactos sobre Delitos de Alta Tecnología 24 horas/7 días" del G-8? Sí (x) No ( )

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

Sí ( ) No ( ) No Conozco ( )

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

_____

_____

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

Sí (x) No ( ) No Conozco ( )

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 e apresentou propostas de acordo à Bolívia e ao Paraguai. O Brasil apresentou contraproposta para a revisão do atual acordo com a Itália e segue em negociação com mais de 20 países.

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:

De 2010 a 2011, o Brasil enviou 43 pedidos de cooperação jurídica internacional, com vistas à obtenção de provas eletrônicas relacionadas a crimes cibernéticos, dentre os quais configuram 1 ao Canadá, 1 à Alemanha, 1 aos Países Baixos e 40 aos Estados Unidos da América. No mesmo período, o Brasil recebeu 5 pedidos de cooperação jurídica internacional oriundos do Reino Unido, da Suíça, do Japão, da Itália e da Argentina. Existem, atualmente, 38 pedido em andamento, 6 pedidos cumpridos totalmente e 4 pedidos não cumpridos.

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:

O Ministério Público Federal tem núcleo técnico sobre a matéria. O Departamento de Polícia Federal (DPF), por sua vez, tem diversos treinamentos, em diversos níveis. Na fase de recrutamento, os policiais recebem treinamento básico para a investigação de crimes cibernéticos na Academia Nacional de Policia. Para 2012, serão capacitados por volta de 1000 novos policiais.Este curso introdutório tem duração de 12 horas/aula.

Para os policiais que já se encontram em atuação, desenvolvemos um curso internediário à distancia, com duração de 06 meses, o qual já capacitou mais de 750 policiais, sendo 500 em 2010 e 250 em 2011. Para 2012 serão treinados outros 250 policiais.

O DPF está desenvolvendo uma capacitação em nível avançado para os policiais que integrarão os Grupos de Repressão a Crimes Cibernéticos, criados para aperfeiçoar a atuação operacional da Polícia Federal nos Estados de nossa Federação. Este curso terá duração de 12 meses, sendo 6 semanas presencial e 4 meses à distancia, para 120 policiais. O curso terá início em Julho de 2012 e faz parte da prepação do Brasil para os Grandes Eventos – Copa do Mundo de Futebol 2014 e Jogos Olímpicos 2016.

O DPF está planejando, ainda, a realização de um curso intermediário à distancia para capacitação das polícias civis estaduais, o qual deverá ser oferecido através de parceria com a Secretaria Nacional de Segurança Pública.

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:

Em 2010 e 2011, o Departamento de Polícia Federal realizou diversos eventos, tais como, conferências, seminários, grupos de trabalho que abordaram o enfrentamento ao crimes cibernéticos, para juízes, delegados e procuradores.

Para 2012, o DPF está planejando a realização de um curso à distancia para juízes e procurados, organizado pela Polícia Federal em parceria com as Escolas Superiores da Magistratura e do Ministério Público.

A Procudaoria-Geral da República criou grupo especializado no combate a tais delitos com o auxílio de assessores ou analistas processuais com dedicação exclusiva na área e a criação de um núcleo técnico e pericial que atua junto aos procuradores para resolução de questões técnicas mais complexas.

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:

Departamento de Polícia Federal

Meta 01*: Todo policial federal deve possuir conhecimentos básicos para a investigação de crimes praticados através de computadores e possuir o conhecimento necessário para localizar informações úteis e disponíveis na Internet. Para tanto, já no seu ingresso na carreira policial, o novo servidor recebe tais conhecimentos. Para os policiais da ativa, cursos básicos à distância são oferecidos constantemente, bem como, possuímos uma comunidade temática na nossa Universidade Virtual que permite a qualquer policial interesado obter este conhecimento diretamente (https://ead.dpf.gov.br/)*

Meta 02. *Os integrantes das equipes policiais especializadas na investigação dos crimes cibernéticos devem possuir conhecimentos avançados em computação e técnicas investigativas que permitam pronta-resposta a ataques cibernéticos, busca, coleta e análise de grande volumen de dados obtidos através de fontes variadas, monitamento de canais abertos da INTERNET, como IRC, Facebook, Google, entre outras técnicas. Serão capacitados 120 policiais até o final de 2013.*

Ministério Público

Ênfase na atuação conjunta entre Polícia Federal e Ministério Público; canal único de denúncias para evitar duplicidade de investigações; capacitação cada vez maior dos operadores do direito e dos técnicos e peritos com atuação nesta área; troca de experiências e informações com os outros países, realização de acordos entre países para facilitação na obtenção rápida e eficaz das provas; realização de eventos e palestras internacionais para compartilhamento de técnicas de investigação; aumentar a produção de manuais de técnicas de investigação a ser distribuído aos fiscais e autoridades que atuam na área.

4.4. ¿Ha participado su país en los talleres de capacitación celebrados en el marco del Grupo de Trabajo en Delito Cibernético? Sí ( ) No (X) No Conozco ( )

En caso afirmativo, sírvase describir brevemente las personas que han participado; si estos talleres han ofrecido capacitación útil, y cómo los participantes han aplicado esta capacitación en el ejercicio de sus funciones:

Observação: Há Grupo de Trabalho específico no Ministério Público Federal intitulado Grupo de Trabalho na área cibernética.

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:

Iintensificar a cooperação e integração entre os países na investigação dos crimes cibernéticos, aprimorando o que já vem sendo realizado no Brasil (vide item 4.3) e

compartilhar técnicas de investigação que estejam obtendo bons resultados em outros países.

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:

Para o DPF, é importante o desenvolvimento de treinamento em nível intermediário, notadamente através de Ensino à Distância, para policiais que atuam na investigação de crimes de alta tecnologia, como acesso indevido a dados e sistemas e interferencia em sistemas informatizados.

Seria igualmente importante o desevolvimento de cursos ou especializações, em nível avançado e presencial, para dotar policiais de técnicas que permitam a busca e apreensão virtual diretamente do policial no computador do alvo, através da rede, mediante autorização judicial, bem como a interrupção de um ataque DDoS através da invasão dos computadores utilizados como "zumbi" e do Comando e Controle (C&C), quando estes estiverem no território do próprio país.

Sugere-se, ainda, o desenvolvimento de ferramentas (programas de computador) especializadas em busca, coleta e tratamento de informações disponíveis na INTERNET, permitindo aos policais trabalhar com grande volume de dados através de programas específicos e customizados para tanto.

INFORMACIÓN SOBRE LA AUTORIDAD RESPONSABLE DEL DILIGENCIAMIENTO DEL PRESENTE CUESTIONARIO

Por favor, complete la siguiente información:

(a) Estado: Brasil
(b) El funcionario a quién puede consultarse sobre las respuestas dadas a este cuestionario es:
( ) Sr.: *Leonardo Wester dos Santos Ribeiro*
( ) Sra.:_____
Título/cargo: *Terceiro Secretário*
Organismo/oficina: *Coordenação-Geral de Combate aos Ilícitos Transnacionais, Ministério das Relações Exteriores*
Domicilio: Brasíla, Setor de Autarquia Sul, Quadra 06, Lote 09-10
Número de teléfono: + 55.61.3411-8292
Número de fax:
Correo electrónico: leonardo.wester@itamaraty.gov.br