

MEMORIA DEL “TALLER SOBRE LEGISLACIÓN EN MATERIA DE CIBERDELINCUENCIA EN AMÉRICA LATINA”, CO-AUSPICIADO POR EL GOBIERNO DE MÉXICO Y EL CONSEJO DE EUROPA

México, D.F., 31 de marzo al 2 de abril de 2014

Sinópsis

Bajo el auspicio del Gobierno de México y del Consejo de Europa, del 31 de marzo al 2 de abril de 2014 tuvo lugar en la Ciudad de México el “Taller sobre legislación en materia de ciberdelincuencia en América Latina”. El propósito del taller consistió en apoyar los procesos de armonización de la legislación y de adhesión al Convenio del Consejo de Europa sobre la Ciberdelincuencia (Budapest, 2001; Serie de Tratados Europeos no. 185), por los países de América Latina que han sido invitados a adherirse, que han manifestado su interés en este sentido, o que ya son Parte.

Todos los países invitados al evento -Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú y República Dominicana- respondieron positivamente, con el envío de representantes primordialmente de los ministerios de relaciones exteriores, justicia, y/o ciencia y tecnología, así como de las fiscalías especializadas en la materia. Se sumaron asimismo altas autoridades de la Secretaría de Seguridad Multidimensional de la Organización de los Estados Americanos (OEA) y expertos tanto del Departamento de Justicia de los Estados Unidos como del Consejo de Europa.

Por parte de México –invitado a adherirse al Convenio de Budapest desde el 31 de enero del 2007–, participaron altas autoridades de la Oficina de la Presidencia de la República, de la Cancillería y de la Procuraduría General de la República (PGR); del Poder Judicial de la Federación y del propio Poder del Distrito Federal; de ambas Cámaras del Congreso de la Unión; y de los Institutos Federales de Telecomunicaciones y de Acceso a la Información y Protección de Datos, entre otras instancias, además de asociaciones de la industria digital, especialistas y académicos de diversas instituciones de educación superior.

Se concordó en que:

- La adhesión del Estado Mexicano al Convenio de Budapest, aunado a la aprobación de las reformas necesarias para actualizar el marco jurídico nacional, permitirán a México colocarse a la vanguardia, a fin de responder a las necesidades de la sociedad y convertirse en un líder en la zona en el combate a la ciberdelincuencia.
- Están dadas las condiciones políticas y jurídicas para que a más tardar el próximo periodo legislativo se aprueben las medidas antes señaladas.
- La adhesión al Convenio de Budapest debe ser complementada por los Estados con el Convenio 108 del Consejo de Europa, del 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos

de Carácter Personal, abierto igualmente a todos los países interesados y cuyo proceso de adhesión por parte de México está también en curso.

- Para México y los países hermanos representados en el Taller, el Convenio de Budapest representa un referente obligado en los esfuerzos de la comunidad internacional en pro del fortalecimiento del Estado de derecho en el ciberespacio.
- Sobre la base de iniciativas tales como la reforma constitucional en materia de telecomunicaciones y del lanzamiento presidencial de la Estrategia Digital Nacional, por parte de México, los procesos de adhesión al Convenio de Budapest representan además una oportunidad de compartir las mejores prácticas de los países de la región en este ámbito.
- La concurrencia de los tres Poderes del Estado Mexicano, sector privado, sociedad civil y academia en el Taller, es inédita, y refleja el compromiso de cada uno de ellos en su ámbito, por lo que será un referente para la celebración de otros eventos análogos a nivel internacional.

Anexos:

- I. Programa del Taller (español e inglés).
- II. Lista de participantes.
- III. Memoria cronológica del “Taller sobre legislación en materia de ciberdelincuencia en América Latina”.
- IV. Comunicado inicial del Gobierno de México.
- V. Palabras de la Mtra. Mariana Benítez Tiburcio, Subprocuradora Jurídica y de Asuntos Internacionales (PGR, México), en ocasión de la inauguración del segmento nacional del Taller.
- VI. Presentación del Dr. Ciro Humberto Ortiz Estrada, Comisario General Titular de la División Científica, Policía Federal (Comisión Nacional de Seguridad – SEGOB, México) “Impacto y gravedad de los ciberdelitos”.
- VII. Intervención del Lic. Ulises Gómez Nolasco, Coordinador General de Agregadurías y Asuntos Internacionales (PGR, México) “Posicionamiento del Poder Ejecutivo frente al fenómeno de la ciberdelincuencia”.
- VIII. Presentación del Secretario Ejecutivo del Comité del Convenio sobre la Ciberdelincuencia, Sr. Alexander Seger, “Introducción al Convenio de Budapest sobre la Ciberdelincuencia”.
- IX. Presentación del Lic. Gerardo Guerrero Gómez, Consultor Jurídico Adjunto B (S.R.E., México) “Adhesión al Convenio de Budapest: Opciones y reservas permitidas”.
- X. Palabras del Emb. Juan Manuel Gómez – Robledo Verduzco, en ocasión de la inauguración del segmento internacional del Taller.
- XI. Presentación del Ing. Óscar Manuel Lira Arteaga, Director de Ingeniería y Comunicaciones, Coordinación General de Servicios Periciales (PGR, México), “La amenaza del cibercrimen y el desafío de las evidencias electrónicas”.
- XII. Presentación del Sr. William Hall (Departamento de Justicia, EUA) “La ciberdelincuencia y pruebas electrónicas en el Continente Americano: la perspectiva de Estados Unidos”.

- XIII. Presentación del Secretario Ejecutivo del Comité del Convenio sobre la Ciberdelincuencia, Sr. Alexander Seger, “El Convenio de Budapest sobre la Ciberdelincuencia”.
- XIV. Presentación del Sr. Pedro Verdelho (experto portugués, Consejo de Europa) “Substantive provisions” (i.e., Estado actual de la legislación sobre ciberdelincuencia en América Latina: derecho penal sustantivo).
- XV. Presentación del Sr. Jimmy Cruz (Ministerio de Ciencia, Tecnología y Telecomunicaciones, Costa Rica) “Estado actual de la política pública y legislación sobre ciberdelito en Costa Rica. Política, armonización y avances en Costa Rica”.
- XVI. Presentación del Dr. Cristos Velasco (experto mexicano, Consejo de Europa) “Medidas sobre derecho procesal – Convenio de Budapest”.
- XVII. Presentación del Sr. William Hall (Departamento de Justicia, EUA) “Trabajo con Estados Unidos y sus proveedores”.
- XVIII. Presentación del Dr. Erick Iriarte (experto peruano, Consejo de Europa) “Protección de datos personales, *habeas data* y privacidad en América Latina”.
- XIX. Presentación del Secretario Ejecutivo del Comité del Convenio sobre la Ciberdelincuencia, Sr. Alexander Seger, “Convenio sobre la Ciberdelincuencia: Condiciones y salvaguardias”.
- XX. Palabras de la Lic. Alejandra Lagunes Soto Ruíz, Coordinadora de la Estrategia Digital Nacional (Presidencia de la República, México), en ocasión de la clausura del Taller.
- XXI. Comunicado final del Gobierno de México.
- XXII. Nota relacionada del diario *Excélsior*, “Promueven en México Convenio europeo sobre cibercrimen” (31/03/2014).
- XXIII. Nota relacionada de *Yahoo noticias*, “Gastélum pide suscribir Convenio de Budapest contra ciberdelincuencia” (01/04/2014; fuente: Notimex).
- XXIV. Nota relacionada del diario *Milenio*, “México se adhiere al Convenio de Budapest” (03/04/2014).



Version Mar 28

Taller sobre Legislación en materia de Ciberdelincuencia en América Latina

Secretaría de Relaciones Exteriores, Salón José María Morelos y Pavón
Plaza Juárez #20, piso 1, Col. Centro, Del. Cuauhtémoc.
México, D. F. 06010

31 de marzo 2014 (taller nacional)

1 - 2 de abril (taller internacional)

Organizado por el Gobierno de México y el Consejo de Europa

Ideas generales

Antecedentes

Varios eventos han sido organizados en los últimos años para apoyar a los países de Latinoamérica en el desarrollo de su legislación en materia de ciberdelincuencia, de conformidad con los estándares internacionales, es decir, el Convenio de Budapest sobre la Ciberdelincuencia. Dichos eventos han incluido talleres y asesoría de la Organización de Estados Americanos, del Consejo de Europa y otros.

Mientras tanto, muchos Estados de la región han realizado reformas de su legislación penal y algunos de ellos completaron el proceso para incorporarse a la Convención de Budapest. Argentina, Chile, Colombia, Costa Rica y México han sido invitados para adherirse a este tratado. Asimismo, Paraguay y Perú han manifestado su interés en incorporarse al mismo. Sin embargo, por ahora, solamente República Dominicana y Panamá completaron este proceso pasando a ser Parte.

Objetivos y participantes

El propósito del taller es apoyar los procesos de armonización de la legislación y de adhesión al Convenio sobre la Ciberdelincuencia por los países mencionados anteriormente.

Debido a que los Parlamentos ejercen el papel más crucial reformando la legislación, este taller está destinado principalmente a los miembros de Parlamentos dispuestos a culminar estos procesos, así como a los representantes de los Ministerios de Justicia responsables de proponer las iniciativas legislativas y de los Ministros de Relaciones Exteriores a cargo de los tratados internacionales.

Se espera que al final de este taller los participantes profundicen su conocimiento de las cuestiones a tomar en cuenta al momento de adecuar la legislación sobre ciberdelincuencia y de los beneficios de la cooperación internacional en el marco de tratados tales como la Convención sobre Ciberdelincuencia. El taller se ofrecerá en español y en inglés.

Programa

Lunes, 31 de marzo de 2014 – Taller nacional para los participantes mexicanos

Legislación sobre ciberdelincuencia en México y adhesión al Convenio sobre Ciberdelincuencia

Moderador: PGR

Registro de participantes (entrega de gafetes): 9h00 – 9h25

9h30	Inauguración del taller nacional - Mtra. Mariana Benítez Tiburcio, Subprocuradora Jurídica y de Asuntos Internacionales, Procuraduría General de la República - Sr. Alexander Seger, Secretario del Comité del Convenio sobre la Ciberdelincuencia, Consejo de Europa - Senador Omar Fayad Meneses, Presidente de la Comisión de Seguridad Pública, Senado de la República (por confirmar) - Diputado Ricardo Fidel Pacheco Rodríguez, Presidente de la Comisión de Justicia, Cámara de Diputados (por confirmar) - Magistrado Luis Fernando Angulo Jacobo, Secretario Ejecutivo, Secretaría General de la Presidencia del Consejo de la Judicatura Federal - Declaratoria de inauguración por la Suprocuradora Benítez
10h00	Impacto y gravedad de los ciberdelitos - Panorama general (Dr. Ciro Humberto Ortíz Estrada, Comisario General Titular de la División Científica, Policía Federal) - Comentarios (Lic. Carlos Ponce, Asociación Mexicana de Internet - AMIPCI)
11h00	Posicionamiento del Poder Judicial frente al fenómeno de la ciberdelincuencia - Juez de Distrito Fernando Córdova del Valle, Juzgado Décimo Segundo de Distrito de Amparo en Materia Penal en el Distrito Federal - Magistrada Elsa del Carmen Arzola Muñoz, 3a Sala Penal del Tribunal Superior de Justicia del DF
11h45	<i>Pausa café</i>
12h00	Perspectiva desde el Poder Legislativo frente al fenómeno de la ciberdelincuencia - Senador Omar Fayad Meneses, Presidente de la Comisión de Seguridad Pública, Senado de la República (por confirmar) - Diputado Ricardo Fidel Pacheco Rodríguez, Presidente de la Comisión de Justicia, Cámara de Diputados (por confirmar)
12h45	Posicionamiento del Poder Ejecutivo frente al fenómeno de la ciberdelincuencia - Lic. Ulises Gómez Nolasco, Coordinador de Asuntos Internacionales y Agregadurías, PGR
13h30	<i>Almuerzo</i>

15h00	Introducción al Convenio de Budapest Beneficios y retos para México - catálogo de delitos, persecución de delitos informáticos, evidencia digital y cadena de custodia, justiciabilidad, protección de niños y niñas, cooperación internacional - Panorama general del Convenio de Budapest (Alexander Seger) - Aspectos procesales y evidencias electrónicas (Cristos Velasco, México) - Salvaguardias del Estado de derecho y protección de datos (Erick Iriarte, Perú) - Comentarios de los participantes
16h30	<i>Pausa café</i>
16h45	Adhesión al Convenio de Budapest: opciones y reservas permitidas - Presentación de opciones: Lic. Gerardo Guerrero Gómez, Consultor Jurídico Adjunto B, Consultoría Jurídica, Secretaría de Relaciones Exteriores - Comentarios del Consejo de Europa (Alexander Seger)
17h30	Conclusiones: pasos para completar el proceso de adhesión - Consejo de Europa (Alexander Seger) - Dr. Roberto Dondisch Glowinski, Director General para Temas Globales, S.R.E. - Mtro. Ulises Gómez Nolasco, Coordinador de Asuntos Internacionales y Agregadurías, PGR - Ing. Víctor Lagunes Soto, Director General de Tecnologías de la Información, Coordinación de Estrategia Digital Nacional, Oficina de la Presidencia de la República -
18h30	Fin del taller nacional

Martes, 1o de abril de 2014

Legislación sobre ciberdelincuencia en América Latina – Día 1

Moderador: S.R.E.

Registro de participantes (entrega de gafetes): 9h00 – 9h25

9h30	Inauguración del taller internacional - Emb. Juan Manuel Gómez – Robledo Verduzco, Subsecretario para Asuntos Multilaterales y Derechos Humanos, Secretaría de Relaciones Exteriores - Senadora Diva Hadamira Gastélum Bajo, Integrante de la delegación mexicana ante la Asamblea Parlamentaria del Consejo de Europa, promovente de punto de acuerdo para la adhesión de México al Convenio de Budapest sobre la Ciberdelincuencia - Senadora Laura Angélica Rojas Hernández, Presidenta de la Comisión de Relaciones Exteriores. Organismos Internacionales - Alexander Seger, Secretario Ejecutivo del Comité del Convenio sobre la Ciberdelincuencia, Consejo de Europa - Declaratoria de inauguración por el Subsecretario Gómez - Robledo
------	--

10h00	Ciberdelincuencia y evidencias electrónicas en las Américas - La amenaza del cibercrimen y el desafío de las evidencias electrónicas: Descripción general (Ing. Óscar Manuel Lira Arteaga, Director de Ingeniería y Telecomunicaciones adscrito a la Coordinación General de Servicios Periciales, Procuraduría General de la República) - La perspectiva del Departamento de Justicia de los Estados Unidos (William Hall, Departamento de Justicia de los Estados Unidos) - Retos, respuestas y reformas legislativas en curso en América Latina. Mesa redonda con intervenciones de los representantes de: - Argentina - Chile - Colombia - Costa Rica - México (Lic. Horacio Benjamín Pérez ortega, Director General de Análisis Legislativo y Normatividad, PGR) - Panamá - Paraguay - Perú - República Dominicana
11h45	<i>Pausa café</i>
12h00	El Convenio de Budapest sobre la Ciberdelincuencia - Presentaciones (Alexander Seger, Cristos Velasco, Erick Iriarte) seguidas de preguntas y respuestas sobre: - Contenido y alcance - Delitos (derecho penal sustantivo) - Poderes y procedimientos (derecho procesal) - Salvaguardias del Estado de derecho - Cooperación internacional - Procedimiento de adhesión - Mecanismo de seguimiento: el papel del Comité del Convenio sobre la Ciberdelincuencia (T-CY) - Fortalecimiento de capacidades
13h30	<i>Almuerzo</i>
15h00	Estado actual de la legislación sobre ciberdelincuencia en América Latina: derecho penal sustantivo - Panorama general (Pedro Verdelho, miembro del Comité del Convenio sobre la Ciberdelincuencia, Portugal) - Análisis y propuestas país por país, incluyendo experiencias prácticas en torno de la legislación en vigor: - Argentina - Chile - Colombia - Costa Rica - México (Lic. Azucena Mayela Sahagún Segoviano, Directora de

	Negociación de Instrumentos Jurídicos Internacionales, PGR)
16h30	<i>Pausa café</i>
16h45	- Panamá - Paraguay - Perú - República Dominicana
17h30	Comentarios generales sobre el estado actual de la legislación sobre ciberdelincuencia en América Latina: derecho penal sustantivo - Comentarios de Alexander Seger (Consejo de Europa) - Preguntas de los asistentes
18h30	Fin de la sesión
19h00	Traslado a coctel
19h30 – 22h00	Coctel en honor de participantes. Museo de Arte de la Secretaría de Hacienda y Crédito Público (antiguo Palacio del Arzobispado). Moneda 4, Centro Histórico (a un costado de Palacio Nacional)

Miércoles, 2 de abril de 2014 (nivel técnico)

Legislación sobre ciberdelincuencia en América Latina – Día 2

Moderador: Secretario Técnico del Comité Especializado en Seguridad de la Información

9h30	Estado actual de la legislación sobre ciberdelincuencia en América Latina: derecho penal procesal - Panorama general (Cristos Velasco/Erick Iriarte/Pedro Verdelho) - Análisis y propuestas país por país
11h00	Acceso a datos por agencias de aplicación de la ley – Cooperación con el sector privado - Cuestiones y ejemplos a destacar (Pedro Verdelho, Portugal) - Cooperación con proveedores de servicios con sede en los Estados Unidos (William Hall, Departamento de Justicia de los Estados Unidos) - Experiencias en América Latina (abierto a intervenciones de los participantes)
11h45	<i>Pausa café</i>
12h00	Salvaguardias del Estado de derecho y protección de datos - Panorama general (Erick Iriarte/Alexander Seger) - Protección de datos en México (Lic. Adriana Báez, Directora de Autorregulación, Secretaría de Protección de Datos, Instituto Federal de Acceso a la Información y Protección de Datos - IFAI)
13h30	<i>Almuerzo</i>
15h00	Adhesión al Convenio de Budapest sobre la Ciberdelincuencia

	- Panorama general (Alexander Seger, Consejo de Europa) - La experiencia de República Dominicana y Panamá (representantes de República Dominicana y Panamá) - Análisis país por país: pasos a seguir
17h00	Conclusiones / Clausura - Sr. Alexander Seger, Secretario del Comité de la Convención sobre Ciberdelitos, Consejo de Europa - Diputado Héctor Humberto Gutiérrez de la Garza, Presidente, Comisión de Comunicaciones - Lic. Ulises Gómez Nolasco, Coordinador de Asuntos Internacionales y Agregadurías, PGR - Lic. Alejandra Lagunes Soto Ruíz, Coordinadora de Estrategia Digital Nacional, Oficina de la Presidencia de la República mexicana

Contacto

Consejo de Europa	Gobierno de México
Alexander Seger Secretario del Comité de la Convención sobre Ciberdelitos Consejo de Europa Estrasburgo, Francia Tel: +33-3-9021-4506 Correo electrónico: alexander.seger@coe.int	Jorge Cicero Fernández Director General Adjunto para Temas Globales Dirección General para Temas Globales Secretaría de Relaciones Exteriores México, D.F. Tel. +52 (55) 3686-5100, ext. 5699 Correo electrónico: tallerciberdelito@sre.gob.mx

www.coe.int/cybercrime



Project Cybercrime@Octopus



Version Mar 28

Workshop on cybercrime legislation in Latin America

Mexico City

-Secretaría de Relaciones Exteriores, Salón José María Morelos y Pavón,
Plaza Juárez # 20, piso 1, Col. Centro, Del. Cuauhtémoc, México D.F. 06010-

31 March 2014 (national workshop)

1 - 2 April (international workshop)

Organised by the Government of Mexico and the Council of Europe

Programme

Background

Several events have been organised in recent years to support countries of Latin America in the drafting of legislation on cybercrime in line with international standards, that is, the Budapest Convention on Cybercrime. These include workshops and advice by the Organization of American States, the Council of Europe and others.

In the meantime, many States have thus undertaken reforms of their criminal legislation and a number of them have taken steps to join the Budapest Convention. Argentina, Chile, Colombia, Costa Rica, Mexico and Panama have been invited to accede to this treaty. Others are interested in joining this treaty, including Paraguay and Peru. However, so far, only the Dominican Republic and Panama have completed this process and become Parties.

Objective and participants

The aim of the workshop is to support the process of reform of legislation and of accession to the Convention on Cybercrime in the above countries.

As Parliaments exercise the most crucial role in reforming legislation, this workshop is primarily aimed at members of Parliaments prepared to take this process forward as well as at representatives of Ministries of Justice responsible for drafting legislation and of Ministries of Foreign Affairs responsible for international treaties.

It is expected that by the end of the workshop participants will have a better understanding of the issues to be taken into account when preparing legislation on cybercrime and of the benefits of an efficient international cooperation on the basis of treaties such as the Convention on Cybercrime.

The workshop will be held in Spanish and English.

Programme (draft)

Monday, 31 March 2014 National workshop for Mexican participants

Cybercrime legislation in Mexico and accession to the Convention on Cybercrime

Moderator: Office of the Republic's Attorney General of Mexico

Registration (distribution of badges): 9h00 – 9h25

9h30	Opening session - Mariana Benítez, Deputy Attorney General for Legal and International Affairs, Office of the Republic's Attorney General of Mexico - Senator Omar Fayad, Chairperson, Public Security Committee, Senate of the Republic (to be confirmed) - Representative Ricardo Pacheco, Chairperson, Justice Committee, Federal Chamber of Representatives (to be confirmed) - Magistrate Fernando Angulo, Representative of the Federal Judiciary Council of Mexico - Alexander Seger, Executive Secretary, Cybercrime Convention Committee, Council of Europe - Official inauguration by Deputy Attorney General Benítez
10h00	Cybercrime: magnitude and damages - Overview: Ciro Humberto Ortiz, Commissioner General, Federal Police of Mexico, Scientific Division - Comments by Carlos Ponce, Mexican Internet Association
11h00	Stance of the Judiciary vis-à-vis the cybercrime phenomenon - Federal Judiciary Council of Mexico (Federal Judge Fernando Córdova, 12th Criminal Habeas Corpus Court Federal District), - Federal District Supreme Tribunal of Justice (Magistrate Elsa del Carmen Arzola, 3rd Criminal Matters Chamber)
11h45	<i>Coffee break</i>
12h00	Stance from the Legislative Branch vis-à-vis the cybercrime phenomenon - Senator Omar Fayad, Chairperson, Public Security Committee, Senate of the Republic - Representative Ricardo Pacheco, Chairperson, Justice Committee, Federal Chamber of Representatives
12h45	Stance of the Executive Branch vis-à-vis the cybercrime phenomenon - Ulises Gómez, International Affairs Coordinator, Office of the Republic's Attorney General of Mexico
13h30	<i>Lunch break</i>

15h00	Introduction to the Budapest Convention Benefits and challenges for Mexico – catalogue of cybercrimes – the prosecution thereof- digital evidence – chain of custody – justiciability – child protection – international cooperation – Overview of the Budapest Convention on Cybercrime (Alexander Seger) – Procedural issues and electronic evidence (Cristos Velasco, Mexico) – Rule of law safeguards and data protection (Erick Iriarte, Peru) – Comments by participants
16h30	<i>Coffee break</i>
16h45	Acceding to the Convention: options and admissible reservations – Presentation of options: Gerardo Guerrero, Deputy Legal Advisor, Foreign Affairs Ministry – Comments by Council of Europe (Alexander Seger)
17h30	Conclusion: steps to complete the accession process – Alexander Seger, Council of Europe – Roberto Dondisch, Global Affairs Director General, Foreign Affairs Ministry – Ulises Gómez, International Affairs Coordinator, Office of the Republic's Attorney General of Mexico – Víctor Lagunes, Information Technologies Director General, Digital Strategy Coordination, Presidency of Mexico
18h30	End of national workshop

Tuesday, 1 April 2014

Cybercrime legislation in Latin America – Day 1

Moderator: Foreign Affairs Ministry

Registration (distribution of badges): 9h00 – 9h25

9h30	Opening session – Juan Manuel Gómez – Robledo, Deputy Secretary for Human Rights and Multilateral Affairs, Foreign Affairs Ministry of Mexico – Senator Diva Gastelum, member, Mexican delegation to the Parliamentary Assembly of the Council of Europe, author of legislative initiative to promote the accession of Mexico to the Budapest Convention – Senator Laura Rojas, Chairperson, Foreign Affairs Committee – Alexander Seger, Executive Secretary, Cybercrime Convention Committee, Council of Europe – Official inauguration by Deputy Secretary Gómez - Robledo
10h00	Cybercrime and electronic evidence in the Americas – The threat of cybercrime and the challenge of electronic evidence: overview: Oscar Lira, Engineering and Telecommunications Director,

	General Coordination of Forensic Services, Office of the Republic's Attorney General of Mexico - The perspective of the US Department of Justice (William Hall, US Department of Justice) - Challenges, responses and legislative reforms underway in Latin America. Round table with interventions by representatives of*: - Argentina - Chile - Colombia - Costa Rica - Mexico (Horacio Pérez, Legislative Analysis General Director, Office of the Republic's Attorney General of Mexico) - Panama - Paraguay - Peru - Dominican Republic
11h45	<i>Coffee break</i>
	The Budapest Convention on Cybercrime - Presentations (Alexander Seger, Erick Iriarte) followed by questions and answers on: - Contents and scope - Offences (substantive criminal law) - Enforcement powers (procedural law) - Rule of law safeguards - International cooperation - The accession procedure - Follow up mechanism: the role of the Cybercrime Convention Committee (T-CY) - Capacity building
13h30	<i>Lunch break</i>
15h00	The current state of cybercrime legislation in Latin America: substantive criminal law - Overview (Pedro Verdelho, Member of the Cybercrime Convention Committee, Portugal) - Country-by-country review and proposals, including practical experience of of legislation in place*: - Argentina - Chile - Colombia - Costa Rica - Mexico (Azucena Sahagún, International Legal Negotiations Director, Office of the Republic's Attorney General) - Panama
16h30	<i>Coffee break</i>

16h45	- Paraguay - Peru - Dominican Republic
17h30	General comments on the current state of cybercrime legislation in Latin America: substantive criminal law - Comments of the Council of Europe (Alexander Seger) - Questions of participants
18h30	End of session
19h00	Transportation to cocktail
19h30	Cocktail in honour of participants. Venue: Museo de Arte de la Secretaría de Hacienda y Crédito Público (antiguo Palacio del Arzobispado). Moneda 4, Centro Histórico (a un costado de Palacio Nacional)
Wednesday, 2 April 2014 (Technical level)	
Cybercrime legislation in Latin America – Day 2	
Moderator: Special Committee on Information Security Secretariat	
9h30	The current state of cybercrime legislation in Latin America: Criminal procedural law - Overview (Cristos Velasco/Pedro Verdelho/Erick Iriarte) - Country-by-country review and proposals
11h00	Law enforcement access to data – Cooperation with the private sector - Issues and examples (Pedro Verdelho, Portugal) - Cooperation with US-based service providers (William Hall, US Department of Justice) - Experience of countries in Latin America (interventions by participants)
11h45	<i>Coffee break</i>
12h00	Rule of law safeguards and data protection - Overview (Erick Iriarte/Alexander Seger) - Data protection in Mexico (Adriana Baez, Self-Regulation Director, Data Protection Secretariat, Federal Institute on Access to Public Information and Data Protection)
13h30	<i>Lunch break</i>
15h00	Acceding to the Budapest Convention on Cybercrime - Overview (Alexander Seger, Council of Europe) - The example of the Dominican Republic and Panama (speakers from DomRep and Panama) - Country-by-country review: Steps to be taken
17h00	Conclusions / Closing session - Alexander Seger, Council of Europe - Héctor Gutiérrez, Chairperson, Communications Committee, Federal Chamber of Representatives

	- Ulises Gómez, International Affairs Coordinator, Office of the Republic's Attorney General of Mexico - Alejandra Lagunes, National Digital Strategy Coordinator, Presidency of Mexico
--	--

*Spanish alphabetical order

Contact

Council of Europe	Government of Mexico
Alexander Seger Executive Secretary Cybercrime Convention Committee Head of Data Protection and Cybercrime Division Council of Europe Strasbourg, France Tel: +33-3-9021-4506 Email: alexander.seger@coe.int	Jorge Cicero-Fernández Deputy Director General for Global Affairs Directorate – General for Global Affairs Ministry of Foreign Affairs Mexico City, Mexico Tel. +52 (55) 3686-5100, ext. 5699 Email: tallerciberdelito@sre.gob.mx

www.coe.int/cybercrime



Project Cybercrime@Octopus

Lista preliminar de participantes (28/03/2014 rev)

Taller sobre legislación en materia de ciberdelincuencia en América Latina (México, D.F., 31 de marzo al 2 de abril)

Coordinación de Estrategia Digital Nacional (CEDN), Oficina de la Presidencia de la República

1. Lic. Alejandra Lagunes, Coordinadora de Estrategia Digital Nacional
2. Ing. Víctor Lagunes, Director General de Tecnologías de la Información
3. Lic. Silvia Alanís, Directora General Adjunta de Asuntos Jurídicos
4. Lic. Ernesto Ibarra, Subdirector de Asuntos Jurídicos
5. Carlos Ayala
6. Ricardo Fernández
7. Arcadio Sánchez G.

Secretaría de Relaciones Exteriores (S.R.E.)

8. Emb. Juan Manuel Gómez – Robledo, Subsecretario para Asuntos Multilaterales y Derechos Humanos
9. Lic. Ignacio Ernesto Vásquez, Oficial Mayor
10. Lic. Max Alberto Diener, Consultor Jurídico
11. Dr. Roberto Dondisch, Director General para Temas Globales
12. Lic. Salvador Alonso y Caloca, Director General de Tecnologías de la Información e Innovación
13. Dr. Jorge Cicero, Director General Adjunto para Temas Globales
14. Lic. Gerardo Guerrero, Consultor Jurídico Adjunto B
15. Lic. Xavier Ocampo, Director de Seguridad Tecnológica (DGTII)
16. Lic. Graciela Galvany, Directora General Adjunta de Enlace con el Senado de la República
17. Lic. Alejandro Martínez Peralta, Jefe Adjunto de la Oficina de México en Estrasburgo
18. Lic. Verónica Juárez Casimiro, Directora de Tratados II (Consultoría Jurídica)
19. Lic. Jorge Niño de Rivera Matus, Encargado del Área de Organismos Internacionales (Consultoría Jurídica)
20. Lic. Sergio Valdivia, Subdirector de Enlace con la Cámara de Diputados (DGCP)
21. Lic. Diego Sandoval Pimentel, en traslado a la Oficina de México en Estrasburgo
22. Consejero Gustavo Martínez, Dirección General para América Latina y el Caribe (observador)
23. Omar Jesús Camacho Orihuela, Dirección General para Europa (observador)
24. Lic. Helden De Paz, Jefa de Departamento de Asuntos Especiales, Subsecretaría para América del Norte (observadora)
25. Lic. Jorge Paolo Rosano Fernández, Dirección General para América del Norte

Procuraduría General de la República (PGR)

26. Mtra. Mariana Benítez, Subprocuradora Jurídica y de Asuntos Internacionales
27. Mtro. Rodrigo Archundia Barrientos, Subprocurador Especializado en Investigación de Delincuencia Organizada.
28. Lic. Ulises Gómez, Coordinador de Asuntos Internacionales y Agregadurías
29. Lic. Tomás Zerón de Lucio, Director en Jefe de la Agencia de Investigación Criminal.
30. Mtra. Nelly Montealegre Díaz, Fiscal Especial para los Delitos de Violencia contra las Mujeres y Trata de Personas.
31. Lic. Ricardo Cacho, Coordinador General de Asesores, Coordinación de Asuntos Internacionales y Agregadurías
32. Lic. Diana Corona, Directora General de Cooperación Internacional
33. Lic. José Galileo de López Juárez, Director General Adjunto de Coordinación Ejecutiva
34. Lic. Ricardo Guzmán Cruz, Director General Adjunto y Encargado del Despacho de la Coordinación General Técnica
35. Lic. Azucena Sahagún, Directora de Negociación de Instrumentos Jurídicos Internacionales
36. Ing. Oscar Manuel Lira Arteaga, Director de Ingeniería y Telecomunicaciones en Materia Forense
37. Lic. Cristina Patricia Rivera Acosta, Directora de Área
38. Mtra. Cynthia I. Reyes Alvarez, Subdirectora de Seguimiento de Instrumentos Jurídicos Internacionales
39. Lic. Javier Guerrero Bugarini, Jefe de Departamento de Seguimiento de Instrumentos Jurídicos Internacionales
40. Lic. Miguel Ángel Uribe Hernández, Subdirector de Negociación de Instrumentos Jurídicos Internacionales

Consejería Jurídica del Ejecutivo Federal

41. Lic. Friné Arredondo Gutiérrez

Comisión Nacional de Seguridad (CNS) – Secretaría de Gobernación

42. Dr. Ciro Humberto Ortiz Estrada, Comisario General Titular de la División Científica, Policía Federal
43. Mtro. Jacobo Bello, Coordinador para la Prevención de Delitos Electrónicos
44. Ing. Oliver González, Coordinación para la Prevención de Delitos Electrónicos
45. Mtro. Marcos Arturo Rosales
46. Mtra. Valeria Ivonne Muñoz
47. Lic. Juan Carlos López

Comité Especializado en Seguridad de la Información (plenario y grupos)

Oficina de la Presidencia de la República: Ver numerales 1 al 7.

- 48. Lic. Marlene Gómez Villaseñor, Secretariado Consejo de Seguridad Nacional
- 49. Lic. Carlos Castañeda
- 50. Lic. Herve Hernández

Secretariado del Comité – Secretaría de Gobernación (SEGOB)

- 51. Lic. Jorge Colín, Secretario Técnico del CESI
- 52. Lic. Guillermo Cuevas
- 53. Lic. Ulises Castro
- 54. Lic. Leticia Ortiz
- 55. Lic. Mario Montes
- 56. Lic. Adelaida Hernández

S.R.E.: Ver numerales 20 y siguientes.

Secretaría de Gobernación

- 57. Lic. Bertha Cecilia Villafaña Arellano, Directora de Área de Estudios Legislativos, de la Subsecretaría de Enlace Legislativo y Acuerdos Políticos

Secretaría de la Defensa Nacional (SEDENA)

- 58. Mayor Efrén Gámez
- 59. Capitán Onésimo Ramírez
- 60. Alejandro Quezada
- 61. Mirna López Rosiles

Secretaría de Marina (SEMAR)

- 62. Capitán Francisco Eduardo Díaz
- 63. Teniente Iván Pérez
- 64. Teniente Marisol Azpeitia

Secretaría de Hacienda y Crédito Público (SHCP)

- 65. Mtra. Cecilia Calderón
- 66. Ing. Julio César Juárez

Secretaría de Energía (SENER)

- 67. Lic. José Isaac Nequiz

Secretaría de Comunicaciones y Transportes (SCT)

- 68. Ing. Daniel Alejandro Méndez

Secretaría de la Función Pública (SFP)

- 69. Lic. Tonatiuh Alejandro Ríos
- 70. Lic. Rafaela Rangel

PGR: Ver numerales 8 y siguientes

Servicio de Administración Tributaria (SAT)

- 71. C.P. Jorge Said González
- 72. Ing. Emanuel Rodríguez

Comisión Federal de Electricidad (CFE)

- 73. Ing. Américo Castillo
- 74. Lic. Jonathan Valdez

Banco de México

- 75. Dr. José de Jesús Vázquez
- 76. Lic. Octavio Francisco Espinosa

Instituto Federal de Telecomunicaciones:

- 77. Dr. Ante Salcedo
- 78. Lic. Juan Pablo González

Cámara de Senadores

- 79. Sen. Laura Rojas (PAN), Presidenta de la Comisión de Relaciones Exteriores. Organismos Internacionales
- 80. Sen. Diva Gastélum (PRI), integrante de la delegación mexicana ante la Asamblea Parlamentaria del Consejo de Europa
- 81. Sen. Marcela Guerra (PRI), Presidenta de la Comisión de Relaciones Exteriores. América del Norte
- 82. Lic. Jesús Ramírez Díaz, Secretario Técnico de la Comisión de Ciencia y Tecnología, en representación del Sen. Alejandro Tello (PRI)
- 83. Lic. Guadalupe Antonio Miguel, en representación de la Senadora María Verónica Martínez Espinoza, Secretaria de Asuntos Legislativos

Cámara de Diputados

- 84. Dip. Aleida Alaves (PRD), integrante de la delegación mexicana ante la Asamblea Parlamentaria del Consejo de Europa, Vicepresidenta de la Mesa Directiva de la Cámara
- 85. Dip. Héctor Gutiérrez (PRI), Presidente, Comisión de Comunicaciones
- 86. Dip. Adriana González (PAN), Secretaría de la Comisión de Relaciones Exteriores

87. Lic. Vanessa Roberta Pastor Alvarado, asesora jurídica de la Comisión de Ciencia y Tecnología del Partido Nueva Alianza

Poder Judicial, Consejo de la Judicatura Federal

88. Mgdo. Luis Fernando Angulo, Secretario Ejecutivo, Secretaría General del Consejo de la Judicatura Federal
89. Dr. Fernando Córdova, Juez Décimo Segundo de Distrito de Amparo en Materia Penal en el Distrito Federal
90. Mtra. Daniela Bautista, Secretaria Técnica del Pleno y de la Presidencia del Consejo de la Judicatura Federal

Poder Judicial de DF, Consejo de la Judicatura DF

91. Mgda. Elsa del Carmen Arzola Muñoz (Integrante de la 3era Sala Penal del Tribunal de Justicia del DF)

Asamblea Legislativa del Distrito Federal

92. Ing. José Ramón Serrano Valdés, Director de TI

Consejo de Europa (Secretariado y ponentes)

93. Alexander Seger, Secretario Ejecutivo, Comité del Convenio sobre la Ciberdelincuencia
94. Pedro Verdelho, experto - Portugal
95. Erik Iriarte, experto - Perú
96. Cristos Velasco, experto - México

Argentina

97. Raúl Palenque, Consultor, Ministerio de Relaciones Exteriores
98. Gabriel Casal, Ministerio de Justicia y Derechos Humanos

Chile

99. Iván Couso, Jefe de Unidad de Cooperación Internacional, Ministerio de Justicia
100. Diego Moreno Torres, abogado del Departamento de Asesoría y Estudios de la División Jurídica del Ministerio de Justicia
101. Andrés Salazar Cádiz, abogado de la Unidad especializada de lavado de dinero, delitos económicos, medioambientales y crimen organizado (ULDDECO) del Ministerio Público de Chile

Colombia

102. Sandra Tafur, Coordinación de Prevención del Crimen, Dirección de Asuntos Políticos Multilaterales, Ministerio de Relaciones Exteriores
103. Gloria Edith Martínez, asesora del Viceministro, Ministerio Telecomunicaciones

- 104. Senador Jesús Ignacio García Valencia
- 105. Senador Edgar Alfonso Gómez Román

Costa Rica

- 106. Emilia Navas, Fiscalía General
- 107. Rolando Madrigal, Comisionado Presidencial Adjunto, Proyecto Mesoamérica, Ministerio de Relaciones Exteriores y Culto
- 108. Jimmy Cruz, Departamento de Sociedad de la Información, Ministerio de Ciencia, Tecnología y Telecomunicaciones
- 109. Consejero Andrés Vargas Ramírez, Embajada de Costa Rica
- 110. Mrs. Andrea Vargas Chen-Apuy, Ministerio de Justicia

República Dominicana

- 111. John Henry Reynoso, Fiscal Especial contra Delitos Informáticos, Procuraduría General
- 112. Jayro Cuevas, Analista forense - Policía Nacional
- 113. Valerio Ezer Vidal Rodríguez, Dirección de Asuntos Jurídicos, Ministerio de Asuntos Exteriores

Organización de Estados Americanos

- 114. Neil Klopfenstein, Secretario Ejecutivo, Comité Interamericano contra el Terrorismo

Panamá

- 115. Darya Botello, Ministerio Público
- 116. Alfredo Callejas Concepción, Agregado de Seguridad, Embajada de Panamá en México
- 117. Rodney González Gaitán, Fiscal Adjunto de Propiedad Intelectual y Seguridad de la Información

Paraguay

- 118. María Teresa Aguirre, Fiscal Adjunta de Delitos Cibernéticos. Ministerio Público
- 119. Ariel Martínez Fernández, Fiscal, Ministerio de Justicia
- 120. Weldon Black, Director General de Justicia del Ministerio de Justicia

Perú

- 121. Desirée Alayza, Dirección de Ciencia y Tecnología, Ministerio de Relaciones Exteriores
- 122. Dr. José Luis Medina, Ministerio de Justicia y Derechos Humanos

EUA

123. William Hall, Departamento de Justicia

Academia

Instituto Politécnico Nacional (IPN)

124. Dr. Antonio Castañeda Solís, Profesor e investigador
125. Dr. Luis Alfonso Villa Vargas, Director dl Centro de Investigación en Computación
CIC-IPN
126. Dra. Gabriela Sánchez Pérez, Coordinadora Académica de la MISTI
127. Dr. Moisés Salinas Rosales, Jefe del Departamento de Desarrollo de Aplicaciones
del Centro de Investigación en Computación

Universidad Nacional Autónoma de México (UNAM)

128. Dra. Leoba Castañeda, Directora, Facultad de Derecho UNAM
129. Mtra. Marcela Peñaloza (DGTIC UNAM)
130. Ing. Rubén Aquino Luna (UNAM Cert)
131. Dr. Julio Téllez (Investigador Jurídicas UNAM)
132. Mtro. Rodolfo Romero Flores (Fac. Derecho - UNAM)
133. Mtra. Lorena Pichardo F. (Fac. Derecho UNAM)
134. Lic. Alejandra Morán Espinosa, Laboratorio de Derecho Informático Centro de
Desarrollo Tecnológico, FES Acatlán
135. Eleazar Aguirre Anaya, Profesor-Investigador del Centro de Investigación en
Computación

Industria

Fondo de Información y Documentación para la Industria

136. Dr. Alberto Enrique Nava Garcés
137. Dr. Federico Lefranc
138. Mtra. Andréa Olivia Mendoza

Asociación Mexicana de Internet (AMIPCI)

139. Carlos Ponce BELTRAN, CGMPS Consultores Especializados
140. Julio César Vega, Director General de la AMIPCI
141. Alfredo Reyes Krafft, BBVA Bancomer
142. Verónica Vizzuet, Secretaria General de HP
143. Lina Ornelas, Google
144. María Cristina Capelo, Google
145. Andrés Rengifo, Microsoft

- 146. Alejandro Marin, PWC
- 147. David Fernández, Symantec
- 148. Agustín Ríos, R1OS Abogados
- 149. Manuel Aces, Nic México

Instituto Federal de Telecomunicaciones (IFT)

- 150. Ing. Mario Germán Fromow Rangel (Comisionado)
- 151. Lic. Vladimir Salazar Altamirano (Asesor de Presidencia)
- 152. Ing. José Guadalupe Rojas, Director General
- 153. Lic. Eduardo Alvarez Ponce (Director General de Vinculación Institucional)
- 154. Mtro. Roberto Martínez Illescas (Director General)
- 155. Brenda Guzmán Torres, Directora de área
- 156. Cristina Flores Sánchez, Directora de área
- 157. Ing. Alfredo E. Ulloa Rey, Director de Área, Oficina Comisionado Borjón Figueroa
- 158. Juan Pablo González Ramírez (Subdirector de Área)
- 159. Lic. Etzel Salinas Morales (Subdirector de Área)
- 160. Lic. Alma Delia Cedillo Hernández, Oficina Comisionado Borjón Figueroa
- 161. Lic. Eric Darío Arreazola Pérez (asesor del Comisionado Ernesto Estrada González)
- 162. Mtro. Luis Felipe Lucatero Govea (Jefe de la Unidad de Política Regulatoria)

Instituto Federal de Acceso a la Información (IFAI)

- 163. Mtra. Sigrid Arzt, Comisionada
- 164. Lic. María Fernanda Garcíazarco Sánchez, Oficina de la propia Comisionada
- 165. Lic. Adriana Báez Ricardez – Directora General de Autoregulación, Secretaría de Protección de Datos

Asociación Mexicana de la Industria de Tecnologías de Información (AMITI)

- 166. Juan Alberto González Esparza (Presidente)

Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI)

- 167. Víctor Gutiérrez Martínez

Otros

Instituto Mexicano de Propiedad Industrial (IMPI)

- 168. Lic. Miguel Ángel Margáin González Director General.

Instituto Nacional del Derecho de Autor (INDAUTOR)

- 169. Lic. Manuel Guerra Zamorro, Director General
- 170. Jesús Chávez Martínez, Subdirector de Asuntos Contenciosos

Expertos Soc-Civil

- 171. Ing. Andrés Velásquez, Director de Investigaciones Digitales Mattica (Análisis forense)
- 172. Ricardo Quijada
- 173. Lic. Mariela Benitez Barrera (hace practicas profesionales en CEDN Presidencia)

Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios

- 174. Lic. Luis Ricardo Sánchez Hernández Encargado del Área de Protección de Datos Personales

MEMORIA CRONOLÓGICA DEL “TALLER SOBRE LEGISLACIÓN EN MATERIA DE CIBERDELINCUENCIA EN AMÉRICA LATINA”, CO-AUSPICIADO POR EL GOBIERNO DE MÉXICO Y EL CONSEJO DE EUROPA (México, D.F., 31 de marzo al 2 de abril de 2014)

Lunes, 31 de marzo de 2014 – Taller nacional para los participantes mexicanos

(Moderador: Lic. Ricardo Andrés Cacho García, Coordinador General de Asesores, Coordinación de Agregadurías y Asuntos Internacionales, Procuraduría General de la República – PGR)

Inauguración del Taller nacional

PGR

La Subprocuradora Jurídica y de Asuntos Internacionales de la PGR, **Mtra. Mariana Benítez Tiburcio**, mencionó que este Taller constituye una oportunidad para dar a conocer el peligro de los delitos informáticos, en el contexto de un proceso de globalización y de avance en materia de telecomunicaciones que han transformado a la sociedad, así como a las organizaciones criminales, las cuales ejecutan actividades ilícitas en contra de millones de personas alrededor del mundo y obtienen una importante cantidad de recursos por medio del ciberdelito.

La Subprocuradora afirmó que la adhesión de México al Convenio de Budapest le permitirá posicionarse como un líder regional en el combate a la ciberdelincuencia y colocarse a la vanguardia en la procuración de justicia en dicho ámbito.

Asimismo, identificó cinco retos para nuestro país en torno a este tema:

- 1) Tipificación precisa.
- 2) Cadena de custodia adecuada.
- 3) Análisis forense de evidencia electrónica.
- 4) Desarrollo de capacidades técnicas en los funcionarios públicos.
- 5) Ejecución de mecanismos de cooperación internacional.

De igual forma, celebró la presencia de los tres Poderes de la Unión en el Taller, con base en la cual pronosticó que los resultados del evento tendrán un impacto positivo para México.

Consejo de Europa

El Secretario Ejecutivo del Comité del Convenio sobre la Ciberdelincuencia (Budapest, 23 de noviembre de 2001; Serie de Tratados Europeos no. 185), **Sr. Alexander Seger**:

- Reconoció que entre las prioridades de los gobiernos se encuentra garantizar el acceso a la información y la tecnología, lo cual se considera parte del respeto a los derechos humanos, el Estado de derecho y el desarrollo humano de la sociedad.
- Enfatizó que los Estados tienen la obligación de proteger los derechos de los individuos en Internet, lo cual implica tomar medidas que garanticen su seguridad.

- Explicó que, bajo el marco del Convenio citado, el combate a la ciberdelincuencia es una materia focalizada específicamente en investigaciones criminales, que no debe confundirse con las medidas relacionadas con la seguridad nacional.
- Mencionó que el Convenio de Budapest tiene las ventajas de establecer las reglas mínimas que permiten cubrir las necesidades de todos los países y felicitó a México por la organización del evento, y confió en que nuestro país podrá adherirse a dicho tratado internacional en un futuro cercano.

Senado de la República

La Presidenta del Comité de Garantía y Acceso y Transparencia de la Información, de la Cámara Alta, **Senadora Arely Gómez González:**

- Reflexionó sobre la importancia que tiene la tecnología en nuestra vida cotidiana, así como en la existencia de los beneficios y vulnerabilidades que ésta representa para la sociedad.
- Citó algunos ejemplos de ciberdelitos (pornografía infantil, suplantación de identidad y fraude financiero) para ilustrar el hecho de que nadie está exento de ser víctima de la ciberdelincuencia. De ahí la necesidad, observó, de las adecuaciones legislativas pertinentes, así como de capacitar al personal que atenderá este delito en las instituciones competentes del Estado Mexicano.
- Invitó a los presentes a aprovechar los resultados del Taller para alcanzar un cambio positivo en la atención y el combate de este ilícito en México.

Cámara de Diputados

El Presidente de la Comisión de Justicia de la Cámara de Diputados, **Diputado federal Ricardo Fidel Pacheco Rodríguez:**

- Manifestó que el ciberdelito es un tema de actualidad y de gran relevancia para el futuro del país, por lo que la participación de los legisladores en este Taller se centra en una mejor comprensión de este tema.
- Consideró que en el contexto de la reforma penal en curso será fundamental incluir la ciberdelincuencia, y se comprometió a trabajar en el ámbito de su competencia para facilitar un proceso ágil que permita a México contar con los elementos para enfrentar este flagelo.

Poder Judicial de la Federación (PJF)

El Secretario Ejecutivo de la Secretaría General de la Presidencia del Consejo de la Judicatura Federal, **Magistrado Luis Fernando Angulo Jacobo:**

- Informó que el Poder Judicial está comprometido en salvaguardar los derechos de la ciudadanía, así como en velar por el cumplimiento de los tratados internacionales de los que México forma parte.

- Reconoció que nuestro país padece de una tasa de ciberdelincuencia que se incrementa continuamente, ante lo que propuso actuar de manera proactiva para combatir, sancionar e inhibir tal práctica delictiva.
- Estimó que, desde la óptica del órgano supervisor del sistema de justicia, la intención de adhesión al Convenio de Budapest por parte de México tiene como sustento el combate al ciberdelito; y exhortó al involucramiento de todas las instituciones de la administración pública federal, así como de la sociedad en su conjunto, para combatir este ilícito de alcance global.

Instituto Federal de Telecomunicaciones (IFT)

El Comisionado Mario Germán Fromow Rangel:

- Se refirió a la Ley Federal de Telecomunicaciones, que menciona las obligaciones de las empresas en materia de seguridad en el ciberespacio.
- Aseguró que el uso del Internet contribuirá a la prosperidad del país en la medida en que logren redes seguras, haciéndose indispensable un enfoque técnico para enfrentar a la ciberdelincuencia, de forma que México avance con seguridad e integralmente en el uso de las telecomunicaciones.

Impacto y gravedad de los ciberdelitos

Comisión Nacional de Seguridad (CNS), Secretaría de Gobernación (SEGOB)

El Comisario General Titular de la División Científica de la Policía Federal, Dr. Ciro Humberto Ortiz Estrada:

- Mencionó que alrededor del 40% de la población en México (50.1 millones de personas) utiliza el Internet y comentó que existe una gran diversidad de delitos que se pueden cometer a través de medios electrónicos, lo cual pone en riesgo principalmente a los menores de edad, toda vez que el principal delito cometido en contra de este sector de la población es la pornografía infantil.
- Destacó que el perfil de los responsables de los ciberdelitos es muy particular: su edad oscila entre los 18 y 25 años; tienen un nivel económico medio; poseen una formación profesional. No obstante, aclaró que nuestro país no dispone de estadísticas sobre ciberdelincuencia, siendo un pendiente en la agenda del combate a este ilícito.
- Informó que la estrategia de la Policía Federal en contra de la ciberdelincuencia también es preventiva, especialmente en lo que se refiere a la protección de los niños, así como a la protección de la ciudadanía, principalmente en las actividades relacionadas con el comercio electrónico.
- Señaló que alrededor del país hay 14 policías cibernéticas, entre cuyas competencias figura la de realizar actividades de cooperación internacional con policías cibernéticas de otros países.

Consejo de Europa

El **Sr. Alexander Seger** manifestó que la generación de estadísticas en materia de ciberdelincuencia en México servirá de sustento para el otorgamiento de más recursos que permitan llevar a cabo la capacitación de la policía y los funcionarios públicos, al sustentar la relevancia y gravedad que tiene este ilícito para la sociedad.

Asociación Mexicana de Internet (AMIPCI)

El **Lic. Carlos Ponce Beltrán** (CGMPS Consultores Especializados):

- Celebró el esfuerzo que hace el Gobierno de México relativo al fortalecimiento del uso del Internet como medio de desarrollo económico, educativo y cultural del país.
- Sugirió que el campo del ciberdelito se aborde con cautela, toda vez que se requiere la participación del gobierno, la industria, la sociedad civil y la academia para combatir este flagelo.
- Comentó que las principales víctimas de la inseguridad en las redes de cómputo son usuarios con conocimientos básicos. No obstante, defendió la idea de que el beneficio que la sociedad adquiere del Internet es mayor al daño que infringe la ciberdelincuencia.
- Respaldó la intención del Gobierno de México de adherirse al Convenio de Budapest, que refrenda el compromiso del Estado de brindar seguridad para la ciudadanía.

Posicionamiento del Poder Judicial frente al fenómeno de la ciberdelincuencia

PJF

El Juez de Distrito **Fernando Córdova del Valle** (Juzgado Décimo Segundo de Distrito de Amparo en Materia Penal en el Distrito Federal):

- Puso de relieve que, llendo de la mano el avance de la tecnología con la creación de nuevos delitos, el legislador tiene ante sí la difícil labor de prever adecuadamente en las leyes los nuevos tipos de crimen.
- Resaltó que el Poder Judicial se suma a toda decisión que contribuya a la protección de los derechos humanos y afirmó que la cooperación internacional es necesaria tanto para la elaboración de una legislación clara y precisa como en el combate de los ciberdelitos, cuyo carácter es trasnacional.
- Señaló la importancia de sensibilizar al Gobierno y a la sociedad respecto a la ciberdelincuencia, a la que calificó como una amenaza a los derechos humanos, resultando imperativa la adhesión al Convenio de Budapest por parte de México.

Tribunal Superior de Justicia del Distrito Federal (TSJDF)

La **Magistrada Elsa del Carmen Arzola Muñoz**, integrante de la Tercera Sala Penal del TSJDF:

- Destacó que la Organización de las Naciones Unidas incluyó el acceso libre a Internet como parte de los derechos humanos en 2011, y concibió la ciberdelincuencia como un fenómeno de carácter técnico que ha obligado al Derecho a reposicionarse para atender este fenómeno.
- Señaló la voluntad del Tribunal Superior de Justicia del Distrito Federal de sumarse a toda acción que combata la ciberdelincuencia, ya que dicha institución mantiene su compromiso con la sociedad y el pleno respeto de sus derechos fundamentales.

Perspectiva desde el Poder Legislativo frente al fenómeno de la ciberdelincuencia

Delegación mexicana ante la Asamblea Parlamentaria del Consejo de Europa, Cámara de Diputados

La **Diputada federal Aleida Alavez Ruiz**, Vicepresidenta de la Mesa Directiva de la Cámara de Diputados e integrante de la delegación mexicana ante la Asamblea Parlamentaria del Consejo de Europa:

- Recapituló los cambios sociales que han ocurrido en la era digital, en donde el contacto entre las personas se registra cada vez menos de manera física y cada vez más de forma cibernética; en este contexto, el principio que rige la labor legislativa es garantizar la seguridad de la ciudadanía y robustecer el sistema de seguridad mexicano, estimó.
- Se enfocó en la preocupación que existe por la protección de datos e invitó a la discusión y el debate sobre los estándares que deben regir con relación al tratamiento de datos personales de parte de los sectores público y privado, así como en las autoridades locales y federales.
- Sostuvo que el Estado debe garantizar la protección de estos datos, siendo la única excepción asuntos que tengan efectos en el ámbito de la seguridad y la impartición de justicia.

Presidencia de la Comisión de Justicia, Cámara de Diputados

El Diputado Ricardo Fidel Pacheco Rodríguez:

- Consideró que la ciberdelincuencia es un reto en materia de normas, toda vez que tiene que ver con conductas y acciones realizadas a través de los equipos informáticos, ya sea como medio o fin.
- Aseveró que en la Cámara de Diputados existen grupos de legisladores que trabajan en materia de ciberdelincuencia, quienes buscan reafirmar la integralidad del tratamiento de dicho tema. Lo anterior, en el entendido de que el ciberespacio debe ser un lugar seguro y no un coto para las actividades criminales.

Posicionamiento del Poder Ejecutivo frente al fenómeno de la ciberdelincuencia

El Coordinador de Agregadurías y Asuntos Internacionales de la PGR, **Lic. Ulises Gómez Nolasco**:

- Se preguntó si las autoridades mexicanas están preparadas para combatir la ciberdelincuencia y enumeró algunas de las variables de la ciberdelincuencia: pornografía infantil, robo de identidad, estafas en línea y fraudes con tarjetas de crédito.
- Reconoció que el marco jurídico mexicano no ha avanzado a la par de las complejas conductas que utiliza la delincuencia, lo cual implica que las organizaciones criminales aprovechan el ciberespacio bajo el conocimiento de que en ese ámbito difícilmente se generan pruebas que puedan ser utilizadas por las instituciones de procuración de justicia.
- Enmarcó la adhesión de México al Convenio de Budapest con el cumplimiento de la meta “México con Responsabilidad Global”, recogida en el Plan Nacional de Desarrollo 2013-2018.

Introducción al Convenio de Budapest

El **Sr. Cristos Velasco**, experto mexicano del Consejo de Europa:

- Afirmó que México tiene que adherirse al único convenio internacional que abarca el tema del tratamiento y combate a la ciberdelincuencia.
- Precisoó que el Convenio de Budapest abarca tanto la ciberdelincuencia como las evidencias electrónicas.
- Comentó que entre los principales retos para nuestro país figuran la admisibilidad como pruebas de los elementos contenidos en dispositivos móviles, así como la capacitación de jueces y magistrados en materia de ciberdelincuencia.

El **Sr. Alexander Seger** señaló que el Convenio de Budapest es un instrumento jurídico disponible para todos los países del mundo, no un convenio circunscrito al ámbito europeo, que exige tres aspectos fundamentales a los Estados parte:

1. Tipificar los ciberdelitos en el derecho penal sustantivo.
2. Aceptar la evidencia electrónica.
3. Cooperar a nivel internacional en los aspectos relacionados con la ciberdelincuencia y la evidencia electrónica de índole transnacional.

Al explicar el contenido del Convenio de Budapest, aseveró que entre más países se adhieran la cooperación internacional será más efectiva; y que la experiencia internacional demuestra que en investigaciones criminales hay más confianza en la interacción entre el sector privado y el público, cuando el Estado concernido ya es parte de este tratado internacional especializado en la materia.

Comentó que los beneficios de ser parte del Convenio de Budapest son los siguientes:

- Cooperación confiable con otros países.
- Mayor confianza del sector privado para cooperar en investigaciones criminales.
- Asistencia técnica y creación de capacidades.

Mencionó que el único costo que debe asumir un país que se adhiera a dicho tratado internacional es el compromiso de cooperar, lo que ningún país puede considerar una desventaja.

El **Sr. Erick Iriarte Ahon**, experto peruano del Consejo de Europa:

- Explicó que el mundo digital no está separado del mundo real, sino que es complementario y reflexionó sobre el mundo virtual y los delitos que se llevan a cabo en éste: pornografía infantil, fraude, robo de identidad, trata de personas, entre otros.
- Calificó al Convenio de Budapest como un instrumento que enmarca los mínimos necesarios respecto al combate a la ciberdelincuencia.
- También comentó que las reglas de protección de los datos personales deben ser totalmente respetadas por el Estado, salvo en procedimientos de persecución jurídica; reafirmó que el desarrollo de Internet no es anárquico; y recalcó la importancia de capacitar a los encargados de aplicar la ley, así como de la necesidad de ejecutar un cambio en el aspecto normativo.

Adhesión al Convenio de Budapest

El Consultor Jurídico Adjunto B de la Cancillería, **Lic. Gerardo Guerrero Gómez**:

- Definió al Convenio de Budapest como un instrumento cuyo objetivo principal es proteger a las personas del cibercrimen y salvaguardar sus derechos en Internet.
- Confirmó que México utilizará la adhesión para formar parte del Convenio y que actualmente el proceso se encuentra en la etapa de consulta con las dependencias, de manera que el instrumento se someterá al Senado en el siguiente periodo de sesiones, a partir del próximo 1° de septiembre.
- Puntualizó que hasta el momento México no ha considerado plantear una reserva al citado tratado, y que la culminación de la adhesión de nuestro país se prevé para diciembre próximo o enero de 2015.

Conclusiones: pasos para completar el proceso de adhesión

Secretaría de Relaciones Exteriores (S.R.E.)

El Director General para Temas Globales, **Dr. Roberto Dondisch Glowinski**, reconoció que la ciberdelincuencia es un problema global que ningún país podría combatir por sí sólo, siendo la cooperación internacional la base de cualquier estrategia exitosa para luchar contra ese ilícito.

Consejo de Europa

El **Sr. Alexander Seger**:

- Se congratuló POR la presencia de los responsables de formular las políticas públicas de México en el Taller, toda vez que las instituciones representadas en el

mismo son las más importantes en torno a los trabajos de adhesión de México Al Convenio de Budapest.

- Subrayó la importancia del compromiso de fijar una fecha de adhesión (diciembre de 2014 o enero de 2015) y felicitó al Gobierno de México por haber logrado conjuntar el interés y participación de representantes de las tres funciones de Gobierno, de la industria y de la sociedad civil, al tiempo de puntualizar que este evento sienta un modelo a replicar en otros países.

Coordinación de Estrategia Digital Nacional (CEDN), Oficina de la Presidencia de la República

El Director General de Tecnologías de la Información de la CEDN, **Ing. Víctor Lagunes Soto**:

- Recordó que uno de los intereses primordiales del Presidente Enrique Peña Nieto es habilitar los servicios informáticos para la sociedad, tal y como se refleja en el lanzamiento por el Jefe del Estado Mexicano de la Estrategia Digital Nacional.
- Reconoció que falta crear el marco jurídico que garantice la preservación del interés de la ciudadanía respecto a la protección de sus datos personales y de su seguridad en el ciberespacio, por lo que se refirió a la responsabilidad social de la actual administración cuyo enfoque es fomentar el uso de las tecnologías en un ambiente seguro.

PGR

El **Lic. Ulises Gómez Nolasco** resumió el trabajo que tiene frente a sí el Gobierno de la República en dos vertientes:

1. Desarrollo institucional: capacitación de los servidores públicos y fortalecimiento del marco jurídico en torno a la ciberdelincuencia.
2. Adhesión de México al Convenio de Budapest.

Martes, 1º de abril de 2014 - Legislación sobre ciberdelincuencia en América Latina
Taller internacional (moderador: Dr. Jorge Cicero Fernández, Director General Adjunto para Temas Globales, S.R.E.)

Inauguración del Taller internacional

S.R.E.

El Subsecretario para Asuntos Multilaterales y Derechos Humanos, **Emb. Juan Manuel Gómez Robledo**, al hacer alusión a las metas del Plan Nacional de Desarrollo relacionadas con un “México en paz”, un “México incluyente”, un “México con educación de calidad” y un “México con responsabilidad global”, consideró que el fortalecimiento de la lucha contra la ciberdelincuencia mediante la adhesión al Convenio de Budapest está vinculada a la consecución de las referidas metas, como referente para el desarrollo de la

normativa nacional e internacional y herramienta para la cooperación y el intercambio de las mejores prácticas de nuestro país.

Al resaltar que el estatus de observador de México ante el Consejo de Europa ha sido un privilegio, que permite que nuestro país conozca de primera mano los convenios que se formulan en las reuniones que celebra este organismo, hizo votos para que México cumpla con los procesos de armonización legislativa a la brevedad e invitó a los participantes procedentes de América Latina y el Caribe a compartir sus experiencias y mejores prácticas en materia de ciberdelincuencia.

Delegación mexicana ante la Asamblea Parlamentaria del Consejo de Europa, Cámara de Senadores

La **Senadora Diva Hadamira Gastélum Bajo**, integrante de la delegación mexicana ante la Asamblea Parlamentaria del Consejo de Europa y promovente de un punto de acuerdo para la adhesión de México al Convenio de Budapest, se refirió a ésta como una oportunidad para combatir las acciones ilícitas de la ciberdelincuencia y para que México regule este fenómeno.

Presidencia de la Comisión de Relaciones Exteriores – Organismos Internacionales, Cámara de Senadores

La Presidenta de la Comisión de Relaciones Exteriores – Organismos Internacionales, **Senadora Laura Angélica Rojas Hernández**, puso énfasis en las dificultades que implica la ciberdelincuencia frente a la territorialidad, puesto que en muchas ocasiones el ilícito no tiene nacionalidad. Asimismo, lamentó que los Estados hayan reaccionado tarde y que, particularmente, México sea vulnerable a este ilícito. También consideró importante una política preventiva, toda vez que las empresas, las familias y la ciudadanía en general deben conocer las oportunidades y los riesgos que representa el Internet.

Consejo de Europa

El **Sr. Alexander Seger** resaltó que el propósito de este Taller es explicar y comprender el Convenio de Budapest, tratado que versa sobre justicia penal al brindar los elementos necesarios para llevar a cabo las investigaciones penales. Se congratuló de la adhesión de República Dominicana y Panamá al Convenio de Budapest y manifestó que, si bien hay Estados parte de otras regiones, consideró a América Latina esencial para el éxito de este tratado. Fue enfático en la envergadura, alcance y nivel del Taller convocado en México, sin precedente en este tipo de eventos a nivel internacional.

Ciberdelincuencia y evidencias electrónicas en las Américas

Organización de los Estados Americanos (OEA)

El Secretario Ejecutivo del Comité Interamericano contra el Terrorismo (CICTE), de la OEA, **Sr. Neil Klopfenstein**:

- Habló sobre los esfuerzos que ha llevado a cabo dicha organización en los últimos 10 años para combatir el ciberdelito y promover la ciberseguridad.
- Mencionó que el dinamismo y constante evolución del ambiente cibernético, las organizaciones internacionales involucradas deben responder con igual agilidad al problema.
- Rememoró que hace 10 años comenzaron a trabajar el tema y cómo, en ese entonces, se enfocaban únicamente en crear conciencia, pero muchos Estados no creían que el ciberdelito fuera un gran problema, a diferencia de hoy, donde todos lo reconocen como una complicación real.
- Destacó que actualmente se cuenta con estrategias y planes de ciberseguridad. Entre las lecciones que se han aprendido durante esta década de trabajo en el tema se encuentran las siguientes: importancia de crear redes de cooperación, de promover el intercambio de experiencias, y de conocer a las autoridades de otros países, ya que resulta de gran relevancia para las labores que ejecutan los Estados en el quehacer cotidiano.

PGR

El Director de Ingeniería y Telecomunicaciones adscrito a la Coordinación General de Servicios Periciales, **Ing. Óscar Manuel Lira Arteaga:**

- Se refirió al cambio de perspectiva en cuanto a los objetivos del cibercrimen precisando, en particular, que hoy en día la amenaza comienza desde casa, ya que aunque las grandes empresas siguen siendo el objetivo de este delito, en primera instancia los individuos son el objetivo primordial. La amenaza puede darse por la publicación de información personal, ya sea por parte de los menores del hogar (hijos) o por el compartir dispositivos de almacenamiento de información (USB) tanto en el hogar como en el trabajo. En las redes sociales, la infección mediante códigos maliciosos se da de manera exponencial, por el número de amigos virtuales que se van infectando.
- En cuanto a la definición de ciberdelincuencia, expresó que ésta se refiere a diversos delitos que son castigados por nuestros distintos códigos penales, pero que se realizan a través de tecnologías de la información (ya sea como medio o como fin). Dentro de los ejemplos, se refirió al *phishing*, mediante el cual se pretende la obtención de información delicada o confidencial, y al beneficio final que se deriva como falsificación de documentos y fraude financiero. No debe confundirse el medio por el que se comete el delito con el delito tal cual, que es el tipificado en los códigos penales.
- Abordó los beneficios políticos, sociales, y económicos que pueden obtenerse de estos delitos, así como los riesgos existentes teniéndose como víctimas potenciales a las escuelas, los amigos y los colegas de trabajo. Esto tiene que ver con un paradigma generacional, donde los menores de 35 años son más vulnerables y dependientes de las tecnologías, tal y como se ilustra con el uso de los celulares. La causa de muchos de estos riesgos radica en la ignorancia y la presión social (el competir por hacerse de muchos amigos en las redes sociales).

- Estimó que los ciberdelitos tuvieron un impacto de 39 mil millones de pesos durante 2013, ya sea por diversos medios como la mensajería instantánea, correos electrónicos, redes sociales y telefonía celular. Entre otro de los riesgos ubicó a los niños navegando en internet sin supervisión de los padres, en un mundo donde se estima que el 1% de la población tiene tendencias delictivas. Además, tenemos un falso sentido de seguridad al contar con antivirus, los cuales en realidad no proveen un cien por ciento de seguridad. Los niños que utilizan internet se ven expuestos a robo de información, acceso a sitios inseguros, acceso a información falsa, distribución de pornografía, depredadores sexuales, acoso, extorsión, fraude (*spam y phishing*), suplantación de personalidad, secuestro, sabotaje, venta de obras protegidas, venta de sustancias prohibidas.
- El experto recomendó que los hijos compartan con sus padres los nombres de usuarios y contraseñas de sus cuentas de redes sociales. En caso de desapariciones, esto proporcionaría las herramientas a los ministerios públicos para localizarlos en solo unas horas. En materia de cooperación internacional, recomendó la homologación de procesos y metodologías en la región.

Departamento de Justicia de los Estados Unidos de América

El **Sr. William Hall**, de la División de Justicia Penal – Delitos Informáticos y contra la Propiedad Intelectual, comenzó por plantear la pregunta de por qué es importante el Convenio de Budapest y la adhesión al mismo. A ello, respondió que se debe a la gran facilidad que tiene un criminal actualmente para conseguir una dirección IP falsa, de otro país en el que no se encuentra, es decir, se ocultan detrás de varios servidores alrededor del mundo que sirven sólo como intermediarios. El Convenio de Budapest permite el nivel de cooperación internacional necesario y adecuado para que las autoridades de los países involucrados recuperen evidencias producto de estas investigaciones. Entre los requisitos mínimos, figura que el delito perseguido sea tipificado como un delito en ambos países.

Uno de los elementos básicos del Convenio se denomina “datos de tráfico”. El Convenio permite a los países parte compartir estos datos, y así llevar a la identificación del individuo que es sujeto de la investigación. Asimismo, algunos países cuentan con requisitos para retener datos, lo que les permite preservar la evidencia en caso que se requiera para alguna investigación, y que no se eliminen inmediatamente.

Entre los avances que se han dado en los últimos años gracias al Convenio, está el enorme crecimiento en el número de solicitudes de asistencia jurídica mutua. Finalmente, se refirió a la iniciativa “24/7 Network”, la cual se enfoca en preservar evidencia, y en tener la posibilidad de compartirla y pedirla a otros miembros de la red. También permite que los países puedan realizar solicitudes de asistencia jurídica mutua, aun cuando no sean parte del Convenio.

Retos, respuestas y reformas legislativas en curso de América Latina

Argentina

El **Dr. Gabriel Casal** (Ministerio de Justicia y Derechos Humanos) se refirió a la estrategia digital de la Presidencia de su país, donde el gobierno está comprometido a garantizar la seguridad de los “ciberciudadanos”. En Argentina se ha comenzado un proceso de reformas, mediante el cual se han tipificado en el Código Penal federal algunos de los nuevos delitos, ya sea como nuevas figuras o como nuevas modalidades de comisión de los delitos. De acuerdo a Casal, en la nación austral se han alcanzado los requisitos mínimos para adherirse al Convenio de Budapest. Desde 2010, las autoridades argentinas solicitaron al Consejo de Europa ser invitadas a formar parte del Convenio de Budapest. Actualmente, el proyecto se encuentra en la Jefatura de Gabinete que lo enviará a la Presidencia de la Nación. Esta, a su vez, lo someterá al Poder Legislativo. En 2010 se creó una Comisión encargada de formular las reformas procesales y penales necesarias para la adhesión, es decir, para armonizar las políticas nacionales con las exigencias internacionales. Se ha establecido un Centro de Observación de delitos informáticos, encargado de levantar las estadísticas y análisis en la materia. La estrategia de ciberseguridad debe distinguirse de la estrategia de lucha contra el ciberdelito.

Chile

El **Dr. Diego Moreno Torres** (Departamento de Asesoría y Estudios de la División Jurídica del Ministerio de Justicia) manifestó que su país es pionero en materia de legislación de delitos informáticos, contando con una ley al respecto desde 1992, registrándose más recientemente varias modificaciones al Código Penal. En materia de cooperación internacional, Chile no ha tenido problemas para reconocer la figura y dar resolución criminal cuando se ha dado el delito de *phishing*, ya sea dentro o fuera del país.

Colombia

La **Dra. Sandra Tafur** (Coordinación de Prevención del Crimen, Dirección de Asuntos Políticos Multilaterales, Ministerio de Relaciones Exteriores) recalcó la necesidad de adoptar medidas y controles que permitan proteger al Estado, ante las nuevas amenazas presentadas por los avances tecnológicos con fines delictivos. En Colombia, es un asunto de la mayor preocupación e interés nacional. Exhortó a la comunidad internacional a enfrentar de manera conjunta este fenómeno. En Colombia, los avances en la materia se han dado en tres etapas:

- La primera, en 2005, con la creación de una norma en materia de calidad de la gestión de la información dentro de entidades nacionales.
- En 2009, se modificó el Código Penal judicial para incluir como bien jurídico la protección de información y datos.
- Finalmente, en 2011 se creó un documento de política pública en razón del Plan de Desarrollo del gobierno que crea una estrategia nacional y se da la creación de las instituciones necesarias para respaldar dicha estrategia.

Señaló que, a fin de fortalecer la cooperación internacional, se llegó a la conclusión que el Convenio de Budapest es la opción más óptima y viable para combatir los delitos

electrónicos. Derivado de ello, se crearon cuatro nuevas instancias en el país: (1) la Comisión Intersectorial encargada de fijar la visión estratégica y la gestión de la información en Colombia; (2) Grupo de respuesta a emergencias cibernéticas; (3) Comando conjunto cibernético de las fuerzas militares; (4) Centro cibernético policial. Concluyó que, a pesar de la institucionalidad desarrollada por Colombia, aún existen grandes retos como la concientización de la sociedad, políticas de prevención, el fortalecimiento de las capacidades técnicas de los funcionarios y de las Red 24/7, propuesta por el Consejo de Europa, y finalmente, la armonización de las legislaciones entre los países de la región.

Costa Rica

El **Sr. Jimmy Cruz** (Departamento de Sociedad de la Información, Ministerio de Ciencia, Tecnología y Telecomunicaciones) comentó que en febrero de 2014, se creó una división dentro del Ministerio de Telecomunicaciones, que se encargará específicamente del tema de ciberseguridad: la Dirección de Políticas Digitales. Con ello, se busca llenar un vacío existente a nivel institucional. El Plan Nacional de Desarrollo de las Telecomunicaciones contiene elementos específicos para garantizar la seguridad física a proveedores de servicios, así como continuidad de los servicios.

Informó que el citado Ministerio se ha enfocado en la creación de la legislación vigente en ciberseguridad. Un ejemplo de esta legislación es la creación en 2011 de la *Ley de protección de la niñez y adolescencia frente al contenido nocivo en Internet y otros medios electrónicos*. Respecto al Convenio de Budapest, mencionó que el mismo ya se encuentra aprobado en el primer debate, ha sido turnado a Comisiones y volvería al Plenario del Senado para la votación definitiva, esperando se apruebe antes de terminar la administración actual.

México

El **Lic. Horacio Benjamín Pérez Ortega** (Director General de Análisis Legislativo y Normatividad, PGR) se refirió al tema como un reto regional e internacional, frente al que los esfuerzos de los distintos países deberían estar coordinados. Desde 1999 se creó la primera reforma legislativa en la materia en México, la cual creaba un capítulo de delitos relacionados con el acceso a sistemas informáticos, y acceso a redes privadas y del Estado. Después de un largo receso en la legislación mexicana, se creó un Comité Especializado en Seguridad de la Información (CESI), donde se discutió un proyecto de reformas con el fin de hacer frente al fenómeno de una manera más completa. En la presente administración, el proyecto se retomó con el fin de lograr la adhesión al Convenio de Budapest.

Aclaró que actualmente el proyecto se encuentra en una etapa de análisis con el fin de presentarse ante el Congreso de la Unión de una manera exitosa, por parte de la Consejería Jurídica del Ejecutivo Federal. La iniciativa abarca los siguientes aspectos:

- Realización del terrorismo por medio de las redes.

- Creación de un nuevo tipo penal para aquellas actividades por medio de redes que transmitan información discriminatoria con el fin de incitar a la violencia, y a la agresión u odio por razones de discriminación.
- Se establece también un tipo penal para sancionar a los particulares cuando la autoridad solicite colaboración o información y no la proporcionen (concesionarios de telecomunicaciones).
- A nivel internacional, se promueve el establecimiento de una sanción específica para aquellos casos en que las redes y sistemas informáticos sean utilizados con fines de pornografía infantil (posesión, distribución, comercialización, contacto con menores).
- Se establece un agravante para instigadores de delitos cibernéticos (apología).
- Se reordenan delitos creados en 2009 (acceso a redes).
- Se incorpora un nuevo tipo penal para el acceso a los sistemas de seguridad nacional.
- Con el fin de armonizar la legislación nacional con el Convenio de Budapest, se establecen los mismos tipos penales previstos en este instrumento.

En cuanto al fraude cibernético, que va en correspondencia a la recompensa económica que se obtenga, observó que el Convenio contempla el hecho de acceder y hacerse de la información que permitirá cometer el fraude, que en México es considerado sólo como un hecho preparatorio ya que no ha obtenido un solo peso del fraude.

La iniciativa bajo estudio plantea un capítulo específico en materia de cooperación internacional, lo cual muestra la seria convicción de México de adherirse al Convenio de Budapest, a la vez que busca fortalecer nuestros lazos con la comunidad internacional.

Panamá

La **Lic. Yamileth del Carmen Rodríguez Moreno** (Departamento de Seguridad de la Información y Propiedad Intelectual, Procuraduría General de la Nación) resaltó que como Estado miembro del Convenio de Budapest desde el 2013, Panamá se ha visto en la necesidad de adoptar medidas de seguridad legislativas a fin de tipificar toda conducta que afecte los medios informáticos. Entre los retos de Panamá se refirió al tema de la existencia de dos legislaciones distintas en el país, el sistema inquisitivo que se ejerce en la Ciudad de Panamá, a diferencia del sistema acusatorio presente en las provincias.

Consideró que lo importante es implementar políticas de comunicación constante con otros países en aras de llevar a cabo investigaciones más expeditas, dada la volatilidad de la información digital, en virtud de que el tiempo transcurrido en una investigación puede ser un determinante crucial para enjuiciar al delincuente. Asimismo, se refirió a los laboratorios forenses, cuya labor consiste en levantar la evidencia digital, por lo que existe la necesidad de separar este cuerpo de investigación de acuerdo a sus funciones. Otro reto es la aplicación de un protocolo sobre el manejo de información, para evitar su fuga.

Destacó la creación de la unidad especializada en la materia para evitar ciberataques, así como la elaboración de un protocolo en el manejo de evidencia digital. En materia

legislativa, se ha presentado una propuesta de reforma para que Panamá pueda responder a los intentos de ataque que reciban tanto entidades de gobierno como las privadas. Admitió que, desde la adhesión al Convenio, se sigue trabajando en las deficiencias identificadas para su completa implementación en el país.

Paraguay

La **Dra. María Teresa Aguirre** (Fiscal Adjunta de Delitos Cibernéticos, Fiscalía General del Estado) manifestó que desde 1998 se encuentran tipificadas ciertas conductas relacionadas con ciberdelitos en su país, lo cual ha significado diversas reformas. Por ejemplo, en 2011 con la Ley contra delitos informáticos, que modifica el Código Penal vigente, adoptando nuevos delitos y fortaleciendo las sanciones para otros. Anteriormente los datos definidos como preparatorios no eran punibles, pero tras su tipificación en el Código Penal, ya son considerados hechos delictivos. El gobierno paraguayo puede solicitar a los proveedores de servicios, mediante una orden judicial, que provean evidencias digitales. Asimismo, se creó un acuerdo de colaboración con el Centro Nacional para Niños Desaparecidos y Explotados, en materia de prevención de pornografía infantil. El país cuenta también con una ley sobre firma digital y comercio electrónico y se encuentran trabajando para la adhesión al Convenio de Budapest. Recordó que en 2013 se creó como institución la Secretaría de la Tecnología de la Información, con la finalidad de realizar y promover políticas de ciberseguridad a nivel nacional. Concluyó que la globalización del fenómeno del ciberdelito ha generado la necesidad de cooperación internacional para su país y para toda la región.

Perú

El **Dr. José Luis Medina Frisancho** (Ministerio de Justicia y Derechos Humanos) indicó que en el año 2000 nace la primera legislación penal en la materia de su país, aunque de manera un poco superficial e incipiente, haciéndose menester su actualización a la luz de los estándares establecidos por el Convenio de Budapest. Es hasta 2012 que se promulga la nueva ley de delitos informáticos contando con la participación de varios sectores, como representantes del sector privado. En 2013 se generó una propuesta por parte del Ejecutivo sobre delitos informáticos, derivada de una larga serie de mesas de trabajo.

Señaló que el Estado Peruano ha expresado su interés de poner el tema en la agenda para ser discutido durante el 13° Congreso de las Naciones Unidas de Prevención del Delito y Justicia Penal que tendrá lugar en Qatar en 2015. Este mismo año 2014, se han llevado a cabo ciertas modificaciones a la Ley de delitos informáticos para ajustarla al Convenio de Budapest. Entre las incorporaciones se contemplan conductas delictivas como acceso ilícito, *hacking*, atentados o daños contra datos y sistemas informáticos, acoso, interceptación de datos informáticos, fraude informático, posesión de dispositivos y mecanismos diseñados para cometer delitos informáticos y se plantea la existencia de agentes encubiertos.

Identificó una serie de retos comunes para la región, cual son: la incorporación al Convenio de Budapest, continuar las reformas legislativas a nivel nacional, la cooperación internacional, la conservación de datos informáticos, reforzar el ámbito de la prevención, y fortalecer las unidades de investigación nacionales.

República Dominicana

El **Dr. John Henry Reynoso** (Fiscal Especial contra Delitos Informáticos, Procuraduría General de la República) destacó que desde el año 2003 y hasta 2007, las autoridades dominicanas se concentraron en los esfuerzos de creación de una nueva ley de alta tecnología, la cual actualmente abarca todas las partes del Convenio de Budapest. La ley contempla delitos como códigos de acceso, clonación, acceso ilícito, uso de datos y dispositivos fraudulentos, interceptación de telecomunicaciones, daño o alteración de datos, entre otros.

Apuntó que el Convenio de Budapest le ha dado a las autoridades dominicanas las herramientas para poder compartir información y enfrentar este tipo de delincuencia organizada, el sabotaje, atentados, robos de información y estafas informáticas, y sobre todo la pornografía infantil. Existe en el país una Comisión Intersecretarial que convoca a reuniones al menos 4 veces al año, donde se discuten estos temas. Actualmente, se han sometido a consideración una modificación a la Ley de alta tecnología, una ley de “spam comercial” y otra para regular la obtención, uso y conservación de la información.

Debido a la naturaleza transversal del fenómeno, exhortó a todos los países a adherirse al Convenio y ayudar a toda la comunidad internacional y al mismo Convenio a actualizarse, ya que cada país puede aportar su valiosa experiencia en cuanto a su implementación y cómo han enfrentado los problemas derivados de la misma.

El Convenio de Budapest sobre la Ciberdelincuencia

El **Sr. Alexander Seger** recordó que el Convenio de Budapest versa también sobre la evidencia electrónica con relación a cualquier crimen y puntualizó que la adhesión provoca automáticamente que el Estado parte sea miembro del Comité del Convenio, el cual es un mecanismo de evaluación dinámico cuyo objetivo es concretar las metas que se establecen en el tratado.

Detalló los pasos a seguir por los Estados interesados en adherirse:

1. Envío por el Canciller o Embajador de una carta oficial al Consejo de Europa en donde se mencione que el país está interesado en adherirse. El Consejo de Europa responderá a través de una invitación oficial.
2. El Estado debe realizar un proceso doméstico de armonización legislativa, toda vez que su marco jurídico debe ser acorde al del Convenio.
3. El Estado debe realizar el depósito del instrumento de adhesión.

Estado actual de la legislación sobre ciberdelincuencia en América Latina: derecho penal sustantivo

El **Sr. Pedro Verdelho**, experto portugués del Consejo de Europa, subrayó que la importancia del Convenio de Budapest radica en que provee los estándares mínimos para atacar la ciberdelincuencia y recapituló sobre el tratamiento de este ilícito en los códigos penales de Argentina, Chile, Colombia, Costa Rica, Panamá, Perú, Paraguay, República Dominicana y México, comparándolos con el contenido del Convenio.

Análisis y propuestas país por país, incluyendo experiencias prácticas en torno a la legislación en vigor

Argentina

El **Dr. Gabriel Casal** (Ministerio de Justicia y Derechos Humanos) mencionó que en su país la tenencia de pornografía infantil no está penada, sólo se penaliza cuando ésta se posee con fines de comercialización, siendo muy problemático demostrar esto último.

Destacó a la Fiscalía Especializada en Ciberdelito de Buenos Aires, la cual fue creada en noviembre de 2012. Dicha oficina sí tiene la facultad de considerar la prueba digital en los procedimientos de procuración de justicia y resaltó que la mayoría de los ciberdelitos que se cometen en la capital argentina tienen su origen en España, por lo que aseguró que la cooperación internacional es básica para combatir este ilícito.

Chile

El **Dr. Andrés Salazar Cádiz** (Unidad especializada de lavado de dinero, delitos económicos, medioambientales y crimen organizado, del Ministerio Público) estimó que los delitos relacionados con el ciberespacio (pornografía infantil, fraude, entre otros) están cubiertos por el Código Penal chileno, que acepta la evidencia electrónica en los procedimientos de procuración de justicia.

Reconoció que el déficit está en el ámbito de la cooperación internacional, ya que cuando un ciudadano chileno o un extranjero que reside en Chile es víctima de un ciberdelito, generalmente éste se comete en otro país. Por tal motivo, reconoció que la utilidad que tendría el Convenio de Budapest para esa nación sudamericana radica en los elementos que brinda a los Estados parte para facilitar la cooperación internacional.

Colombia

La **Dra. Gloria Edith Martínez** (asesora del Viceministro, Ministerio de Telecomunicaciones), externó que las autoridades colombianas se encuentran en un proceso de reformas al Código Penal en aras de hacer frente a la ciberdelincuencia, y destacó que su país ya cuenta con instituciones que se ocupan de la ciberseguridad.

No obstante, reconoció que los jueces suelen carecer del conocimiento de este tema, de ahí la necesidad de la capacitación judicial, la clasificación de los delitos y la unificación de criterios.

Costa Rica

La **Dra. Andrea Vargas Chen Apuy** (Ministerio de Justicia) refirió que la forma en la que se ha atacado la ciberdelincuencia es a través de la modificación de artículos de diversas leyes (servicios financieros, derechos de autor, aduanas, telecomunicaciones).

Destacó que su país espera la pronta adopción del Convenio de Budapest por su importancia a nivel sustantivo, procesal y de cooperación internacional.

México

La **Mtra. Azucena Mayela Sahagún Segoviano** (Directora de Negociación de Instrumentos Jurídicos Internacionales, PGR) coincidió en que para la PGR es igualmente importante la capacitación integral de todos los actores de la cadena de procuración de justicia, aludió a la función de la PGR como Autoridad Central para la asistencia jurídica mutua por parte de México, y detalló que los retos que enfrenta el país son la modificación de la legislación de acuerdo a un fenómeno en continua transformación y la armonización de del marco jurídico con las normas del Convenio de Budapest, así como la generación de estadísticas.

Panamá

El **Dr. Rodney González Gaitán** (Fiscal Adjunto de Propiedad Intelectual y Seguridad de la Información) resaltó que:

- El interés de su país se centra en una reforma a su Código Penal que asegure la protección de las “infraestructuras críticas”: Canal de Panamá, aeropuerto de la capital, sistema bancario, ministerios y policía, así como los cables ópticos submarinos.
- A raíz de la adhesión panameña al Convenio de Budapest se ha incrementado el desarrollo institucional para combatir a la ciberdelincuencia.
- Las recomendaciones recibidas del Consejo de Europa son en torno a no especificar demasiadas conductas penales, sino abordar cada caso con base en aspectos genéricos.

Paraguay

La **Dra. María Teresa Aguirre** (Fiscal Adjunta de Delitos Cibernéticos):

- Aludió a la alianza público-privada que ha tenido lugar en su país en aras de fomentar las denuncias, lo cual permitió comprobar que los casos sí existían anteriormente y refrendó la confianza de la ciudadanía en el combate a este ilícito.
- Resaltó que la Policía de Paraguay cuenta con un laboratorio forense informático que trabaja en las investigaciones y en la recaudación de pruebas.

Perú

El **Dr. José Luis Medina** (Ministerio de Justicia y Derechos Humanos) recordó que el Convenio de Budapest contiene los estándares mínimos que los Estados deben tener para combatir la ciberdelincuencia y que cada país tiene la prerrogativa de hacer las adecuaciones que estime conveniente.

En ese sentido, informó que en el marco jurídico peruano se han llevado a cabo variantes que tienen que ver con el desarrollo amplio del Convenio de Budapest y citó algunos ejemplos: suplantación de identidad, abuso de dispositivos, daños a sistemas informáticos y *grooming*.

República Dominicana

El Fiscal Especial contra Delitos Informáticos, **John Henry Reynoso**, resaltó:

- La tipificación por la legislación dominicana de todas las definiciones requeridas por el Convenio de Budapest; más algunas conductas ilícitas adicionales como *sexting*, *grooming* y *spam*.
- Las campañas de concientización que realiza la Procuraduría General de la República para advertir y sensibilizar a la ciudadanía respecto a los peligros que entraña la ciberdelincuencia.

Miércoles, 2 de abril de 2014- Continuación del Taller internacional (moderador: Lic. Jorge Alejandro Colín Elías, Secretario Técnico del Comité Especializado en Seguridad de la Información)

Comentarios generales sobre el estado actual de la legislación sobre ciberdelincuencia en América Latina: derecho penal sustantivo

Con base en las preguntas y comentarios que se le hicieron al **Sr. Alexander Seger** se destacan las siguientes respuestas:

- Negociar un tratado internacional y ratificarlo es un proceso que demora aproximadamente veinte años en comparación con un proceso de adhesión que, de acuerdo a la experiencia en el marco de la Convención de Budapest, demora una década; si se llegara a negociar un tratado sobre ciberdelincuencia a nivel regional, éste debería considerar al Convenio de Budapest como el tratado con los estándares mínimos.
- El Convenio de Budapest no abarca el terrorismo ni provee elementos sobre los diversos delitos de manera integral; el “paquete completo” que necesita un país para combatir la delincuencia organizada transnacional se adquiere al ratificar o adherirse a otros tratados, enfatizando que un solo tratado no dará los elementos para solucionar todas las amenazas de seguridad que existen en la actualidad.

Estado actual de la legislación sobre ciberdelincuencia en América Latina: derecho penal procesal

- El **Dr. Cristos Velasco** celebró que muchos de los países latinoamericanos cuenten con una legislación que ya cubre varios aspectos del Convenio de Budapest. Aclaró que en América Latina hay que hacer un “mapeo” que conlleve una numerosa cantidad de leyes (Ley sobre Delincuencia Organizada, Ley de Telecomunicaciones, Ley de Trata de Personas, entre otras) para definir si el marco jurídico de un país es compatible con el citado tratado internacional. Recomendó que cualquier medida en materia de derecho procesal debe ser ejecutada tomando en cuenta tanto la protección de los derechos fundamentales, como los tratados internacionales y las mejores prácticas de otros países.
- El **Sr. Pedro Verdelho** percibió que en América Latina hay una amplia normatividad en materias específicas (telecomunicaciones, finanzas, protección de datos) pero faltan normas generales para regular el marco digital.
- El **Dr. Erick Iriarte** sugirió la elaboración de un compendio de leyes que permita el fortalecimiento de las capacidades de los ministerios públicos, las fiscalías y los jueces, toda vez que los códigos penales de los países latinoamericanos no abarcan todo lo que tiene que ver con la ciberdelincuencia. Dicho compendio facilitaría la labor de los encargados de procurar e impartir justicia.

Acceso a datos por agencias de aplicación de la ley – Cooperación con el sector privado

Consejo de Europa

El **Sr. Pedro Verdelho** resaltó que las compañías de Internet operan a nivel global y que las más importantes se encuentran en Estados Unidos, por lo que la cooperación internacional es la solución para los países que requieran solicitar información a empresas tales como Microsoft, Google o Facebook. Se refirió a la experiencia de la Procuraduría General de la República de Portugal, la cual elaboró un formulario de pedido de tal forma que se enmarcó de manera concreta la información que se puede pedir sobre el usuario. La respuesta de las empresas fue positiva, ya que se logró reducir el tiempo de respuesta de 10 a 15 días en lugar de varios meses que se demoraba anteriormente.

EUA

El **Sr. William Hall** explicó que el gobierno estadounidense y el sector privado trabajan juntos para favorecer la cooperación internacional y manifestó que si un país requiere evidencia electrónica que se encuentre en Estados Unidos hay dos caminos: tratados de asistencia legal mutua o el Convenio de Budapest. Aclaró que el Gobierno de Estados Unidos únicamente envía la solicitud de asistencia de otro país a la empresa pero no interviene directamente en el proceso de respuesta, toda vez que sólo funge como facilitador. Al respecto, recomendó contactar a la *Computer Crime and Intellectual Property Section* (CCIPS) que forma parte del Departamento de Justicia de Estados Unidos, ya que es la oficina responsable de este tipo de cooperación internacional.

Salvaguardias del Estado de derecho y protección de datos

Consejo de Europa

El **Sr. Alexander Seger** hizo hincapié en que el Convenio de Budapest debe ser complementado por los Estados con el Convenio 108 del Consejo de Europa, del 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal. En los procesos de armonización jurídica en curso en varios países de América Latina, debe tenerse presente que el Convenio de Budapest es un tratado internacional de derecho penal, que tiene que ver con las investigaciones criminales, siendo indispensable que las leyes sean precisas, claras, accesibles y acordes con una sociedad democrática en cuanto a las salvaguardas del Estado de derecho y la protección de datos se refiere.

El **Dr. Erick Iriarte** recomendó fomentar las agencias de protección de datos en América Latina, así como la creación de Centros de Alerta Temprana (CERT) para robustecer esta labor; y reafirmó que el respeto a los derechos humanos por parte del Estado debe ser completo, de lo contrario la sociedad cuestionará las decisiones del gobierno, aunque éstas se enfoquen a atacar a la ciberdelincuencia.

Instituto Federal de Acceso a la Información y Protección de Datos (IFAI)

La **Lic. Adriana Báez** (Directora General de Autoregulación, Secretaría de Protección de Datos del IFAI) observó que el IFAI es un órgano autónomo cuya misión incluye salvaguardar los datos personales. Asimismo:

- Se refirió a la Ley Federal de Protección de Datos Personales, la cual establece las medidas administrativas y técnicas para la protección de dichos datos, así como establece mecanismos para la cooperación internacional, por lo que se mostró a favor de la adhesión de nuestro país al Convenio de Budapest, así como al Convenio 108 sobre protección de datos.
- Expresó que la adhesión a estos tratados internacionales no debe dar lugar a que el Estado cometa abusos respecto a las solicitudes que haga a las empresas, especialmente si se toma en cuenta que estos instrumentos jurídicos internacionales no consideran la opción de que los proveedores de servicios se pueden negar a brindar la información.
- Externó su preocupación respecto al envío internacional de datos personales, toda vez que la privacidad de las personas es un derecho fundamental y existen países

que no garantizan que esta clase de información estará debidamente protegida en su territorio.

Adhesión al Convenio de Budapest sobre la Ciberdelincuencia – Experiencias de República Dominicana y Panamá

- El **Sr. Alexander Seger** reiteró la apertura del Convenio de Budapest a la adhesión de los Estados interesados, tanto como la invitación del Consejo de Europa para que todos los países representados en el Taller pase a formar parte de dicho tratado.
- El **Dr. John Henry Reynoso** (República Dominicana) relató que la experiencia de su país al solicitar la cooperación del Gobierno de Estados Unidos ha tenido resultados limitados, toda vez que la respuesta más frecuente de la parte norteamericana es que la solicitud de evidencia electrónica que hacen las autoridades dominicanas para sancionar un delito tiene que ver con una acción privada, por lo que no se recibe el apoyo solicitado.
- El **Dr. Rodney González Gaitán** (Panamá) mencionó que la experiencia de Panamá en el Convenio de Budapest es prácticamente nula, ya que todavía no se ha formulado solicitud alguna de cooperación internacional por el escaso lapso como Estado parte del país istmeño. También se refirió a la elaboración de protocolos sobre evidencias digitales que hacen las autoridades de su país e informó sobre la creación de una fiscalía de asuntos internacionales a la que le corresponderá tanto solicitar como transmitir la evidencia electrónica hacia otras naciones.

Conclusiones / Clausura

CEDN

La Coordinadora de Estrategia Digital Nacional de la Presidencia de la República, **Lic. Alejandra Lagunes Soto Ruíz**, subrayó que la citada Estrategia contempla como uno de sus habilitadores el marco jurídico que permita generar un entorno de certeza para los usuarios de tecnologías de la información; que el ciberespacio debe permanecer como una herramienta que potencie el ejercicio de la libertad de expresión y no un medio para el desarrollo de actividades criminales; y que es necesario generar estadísticas sobre este fenómeno que contribuyan a establecer las políticas públicas pertinentes, así como fortalecer los esquemas de cooperación internacional.

Como conclusiones emanadas de este Taller destacó:

1. El impacto económico de la ciberdelincuencia es alto y afecta directamente a la sociedad.
2. Se requiere trabajar en la generación de estadísticas respecto a este delito, lo cual debe convertirse en una política pública.
3. Se debe fomentar la denuncia de este ilícito entre la ciudadanía.
4. La ciberdelincuencia es un crimen global y transfronterizo.

5. Es indispensable adecuar nuestra legislación al Convenio de Budapest.

Cámara de Diputados

El Presidente de la Comisión de Comunicaciones, **Diputado federal Héctor Humberto Gutiérrez de la Garza**, afirmó que falta mucho por hacer respecto a la adecuación de la legislación mexicana para brindar la protección que necesita nuestra sociedad; que, tanto la Cámara de Senadores como la de Diputados, tienen el compromiso de resolver tal rezago; y que los trabajos en el Poder Legislativo se harán bajo la lógica de proteger al usuario, lo cual incluye la revisión de la ley secundaria de la Ley Federal de Telecomunicaciones, de tal forma que se garantice la libertad de acción siempre y cuando no se atente en contra de la sociedad.

Consejo de Europa

El **Sr. Alexander Seger** agradeció a las autoridades mexicanas la hospitalidad y la organización de un evento que calificó de “histórico”, se congratuló de que representantes del sector público, privado y de la sociedad civil se hayan sumado; y aseguró que, una vez que México culmine su proceso de adhesión al Convenio de Budapest, formará parte de un proceso dinámico de cooperación internacional, actualización normativa e intercambio de experiencias y mejores prácticas en el combate a la ciberdelincuencia.

TALLER SOBRE LEGISLACIÓN EN MATERIA DE CIBERDELINCUENCIA EN AMÉRICA LATINA

Martes 01.04.14 | México, D. F. | Comunicado conjunto Presidencia - SRE - PGR

Bajo la organización de la Presidencia de la República, la Procuraduría General de la República (PGR) y la Secretaría de Relaciones Exteriores (SRE), con el apoyo de la Comisión Nacional de Seguridad de la Secretaría de Gobernación (SEGOB), y el auspicio del Consejo de Europa, se inauguró el 31 de marzo el Taller sobre Legislación en materia de Ciberdelincuencia en América Latina.

La ceremonia, realizada en la sede de la Cancillería, fue presidida por la subprocuradora Jurídica y de Asuntos Internacionales de la Procuraduría General de la República, Mariana Benítez Tiburcio, acompañada de la secretaria de la Comisión de Justicia y Presidenta del Comité de Garantía de Acceso y Transparencia de la Información del Senado de la República, senadora Arely Gómez González; el presidente de la Comisión de Justicia de la Cámara de Diputados, diputado Ricardo Fidel Pacheco; el secretario ejecutivo de la Secretaría General de la Presidencia del Consejo de la Judicatura Federal, magistrado Luis Fernando Angulo Jacobo; el comisionado del Instituto Federal de Telecomunicaciones, maestro Mario Germán Fromow Rangel, y el secretario ejecutivo del Comité del Convenio sobre la Ciberdelincuencia, del Consejo de Europa, Alexander Seger.

El taller consiste en un ejercicio de análisis y reflexión dividido en tres jornadas: la primera dedicada al ámbito nacional y las subsecuentes orientadas al ámbito internacional, con el objetivo común de sensibilizar a los participantes sobre el fenómeno creciente de la ciberdelincuencia y los graves daños que ocasiona a la sociedad, ya sean patrimoniales, físicos, morales o sobre la infraestructura institucional crítica.

Se pretende que impulse las modificaciones necesarias al marco jurídico mexicano, que permitan enfrentar, de manera más efectiva, las amenazas y retos que plantea la ciberdelincuencia así como brindar las condiciones para la adhesión del Estado mexicano al citado tratado -conocido como Convenio de Budapest.

Las intervenciones de los ponentes tuvieron como puntos coincidentes los siguientes:

México y la comunidad internacional enfrentan un reto complejo en materia de combate a la impunidad. La ciberdelincuencia aprovecha la naturaleza altamente técnica de los medios que utiliza, de la omnipresencia y de la operación transfronteriza que la tecnología posibilita.

En este sentido, se consideraron como acciones a implementar de manera compartida: la actualización del marco jurídico, la adhesión al Convenio de Budapest así como el impulso al desarrollo y especialización institucional, y el fortalecimiento de las capacidades de los servidores públicos involucrados en la persecución de tales delitos.

Los representantes de los tres poderes coincidieron en que existen las condiciones políticas y jurídicas para que a más tardar el próximo periodo legislativo se aprueben las medidas antes señaladas.

Finalmente, es importante resaltar como un hecho inédito, las respectivas participaciones de los tres Poderes de la Unión, en las que quedó plasmada la preocupación, el compromiso y la necesidad de tomar acciones inmediatas y concretas, desde sus diversos ámbitos de actuación.

Al respecto, el secretario Seger subrayó que gran parte del carácter exitoso de la jornada de hoy, derivó de haber logrado conjuntar el interés y participación de representantes de las tres funciones de gobierno, de la industria y de la sociedad civil, y puntualizó que constituye un modelo a replicar en otros países.



Palabras de la Mtra. Mariana Benítez Tiburcio,
Subprocuradora Jurídica y de Asuntos Internacionales,
en ocasión del **Taller sobre Legislación en materia de
Ciberdelincuencia en América Latina.**

Ciudad de México, lunes 31 de marzo de 2014.

Muy buenos días a todos.

Sr. Alexander Seger, Secretario del Comité del Convenio sobre la
Ciberdelincuencia del Consejo de Europa;

[Senador Omar Fayad Meneses/Diputado Ricardo Pacheco Rodríguez];

Magistrado Luis Fernando Angulo Jacobo, Secretario Ejecutivo de la
Secretaría General de la Presidencia del Consejo de la Judicatura Federal;

Saludo a los representantes e invitados de los Poderes Ejecutivo, Legislativo
y Judicial que el día de hoy nos acompañan.

Estimados todos.

Es para mí un honor participar en este Taller sobre Legislación en materia de
Ciberdelincuencia en América Latina, el cual constituye una valiosa oportunidad para
abordar una temática de gran relevancia para la región.

En primer término, agradezco mucho el apoyo del Consejo de Europa para
realizar este evento, el cual estoy convencida que permitirá analizar los retos que este
fenómeno nos presenta, así como plantear soluciones conjuntas, a través de la
coordinación de esfuerzos entre los distintos actores involucrados en la atención a los
delitos cibernéticos.

Actualmente, el fenómeno de la globalización y los avances en materia de tecnología y telecomunicaciones generan escenarios y desafíos radicalmente distintos a los observados décadas atrás. Han provocado profundas transformaciones en prácticamente todos los aspectos de la vida cotidiana. La criminalidad no ha quedado fuera de esta evolución, al valerse de estos avances para la comisión de delitos más sofisticados y la generación de estructuras criminales cada vez más complejas, que comprometen y dañan de manera más grave los bienes jurídicos tutelados por el Estado.

La ciberdelincuencia registra un incremento preocupante en los años recientes. Para dimensionar la gravedad del problema cabe destacar que durante 2013, 378 millones de personas fueron víctimas de este delito alrededor del planeta, lo que equivale a 12 víctimas por segundo.¹

Al caracterizarse por la utilización de medios electrónicos, que incluyen no sólo equipos de cómputo, sino también teléfonos inteligentes, redes de internet, cadenas de servidores y plataformas virtuales, entre otros, para la comisión de los ilícitos, el margen de actividad para los perpetradores de éstos es infinito.

En términos económicos, tan sólo en 2013 los delitos cibernéticos tuvieron un costo de 113 mil millones de dólares americanos a nivel global, cifra que rebasa los ingresos anuales generados por diversas actividades perpetradas por la delincuencia organizada. En el caso específico de nuestro país, se calcula que el costo de los delitos informáticos asciende a alrededor de 39 mil millones de pesos, encabezando la lista de países latinoamericanos en los que la población ha sido víctima de algún tipo de ciberdelito, seguido por Colombia y Brasil.²

Conscientes de los riesgos inminentes para la sociedad que representa dicho ilícito, los miembros del Consejo de Europa adoptaron en Budapest, Hungría, el 23 de noviembre de 2001, el Convenio sobre la Ciberdelincuencia, también conocido como

¹ Cifra tomada del Reporte Norton correspondiente al año 2013.

² *Ídem* nota al pie 1.

Convenio de Budapest, instrumento que actualmente cuenta con 42 Estados Parte,³ de los cuales únicamente República Dominicana y Panamá pertenecen a la región Latinoamericana y del Caribe. La adhesión de nuestro país a dicho instrumento, aunada a la aprobación de las reformas necesarias para actualizar nuestro marco jurídico, permitirán a México convertirse en un líder en la zona y colocarse a la vanguardia en este rubro.

El Convenio de Budapest es hasta la fecha el instrumento internacional más avanzado en materia de combate a la ciberdelincuencia, por lo que resulta imperativo concretar la vinculación al mismo a la brevedad posible. Dicho instrumento nos permitirá establecer mecanismos de cooperación más eficientes y expeditos para investigar y sancionar esta clase de conductas, cuya mayor fortaleza radica en que trascienden las fronteras geográficas y jurisdiccionales de nuestros países.

Desde la Procuraduría General de la República, consideramos que la adhesión de México a dicho Convenio constituirá un cimiento importante para la actualización de la legislación en materia de ciberdelito. Aunado a ello, y en respuesta a este fenómeno delictivo que avanza ante nuestros ojos, deben fortalecerse las instituciones a través de la transformación y modernización de nuestras estructuras, así como de las técnicas de investigación que se utilizan.

En materia de ciberdelincuencia tenemos diversos retos por delante. El primero de ellos es la tipificación precisa de las conductas delictivas. El segundo, la conservación y resguardo de la evidencia mediante la implementación de cadenas de custodia adecuadas. En tercer lugar, la ejecución adecuada del análisis forense sobre dicha evidencia, debido a su alta complejidad técnica. En cuarto lugar, tenemos el reto de desarrollar las capacidades institucionales mediante la capacitación y especialización de los servidores públicos involucrados en la persecución de este tipo de delitos. Quinto. La eliminación de barreras entre países mediante el fortalecimiento de la cooperación internacional. Sin evidencia jurídicamente válida que permita

³ Albania, Alemania, Armenia, Australia, Austria, Azerbaiyán, Bélgica, Bosnia y Herzegovina, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estados Unidos de América, Estonia, Finlandia, Francia, Georgia, Hungría, Islandia, Italia, Japón, Letonia, Lituania, Macedonia, Malta, Mauricio, Moldavia, Montenegro, Noruega, Países Bajos, Panamá, Portugal, Reino Unido, República Checa, República Dominicana, Rumania, Serbia, Suiza y Ucrania.

sostener nuestras investigaciones ante el órgano jurisdiccional, seguirá existiendo impunidad.

Este taller será el foro idóneo para intercambiar experiencias y conocimientos entre expertos, provenientes del ámbito nacional e internacional. Estoy segura que nos proporcionará las herramientas necesarias para plantear soluciones a los retos mencionados, asumir nuevos compromisos internacionales y generar la legislación de vanguardia que México necesita, no sólo para resolver las carencias actuales, sino para ocupar una posición de liderazgo regional en la materia.

De manera muy particular celebro que las conclusiones y resultados que se obtengan, sin lugar a duda tendrán eco en el ejercicio de las funciones de los miembros de los tres poderes de la Unión. Esta labor de reflexión y análisis sobre un tema tan lacerante para nuestra sociedad sin duda unificará nuestra perspectiva sobre la materia y nos proporcionará una idea más precisa de la magnitud de los esfuerzos que se requieren para evitar que la realidad nos rebase como autoridades.

Gracias.



DIVISIÓN CIENTÍFICA

Impacto y gravedad de los ciberdelitos

Taller: Legislación en materia de Ciberdelincuencia en América Latina

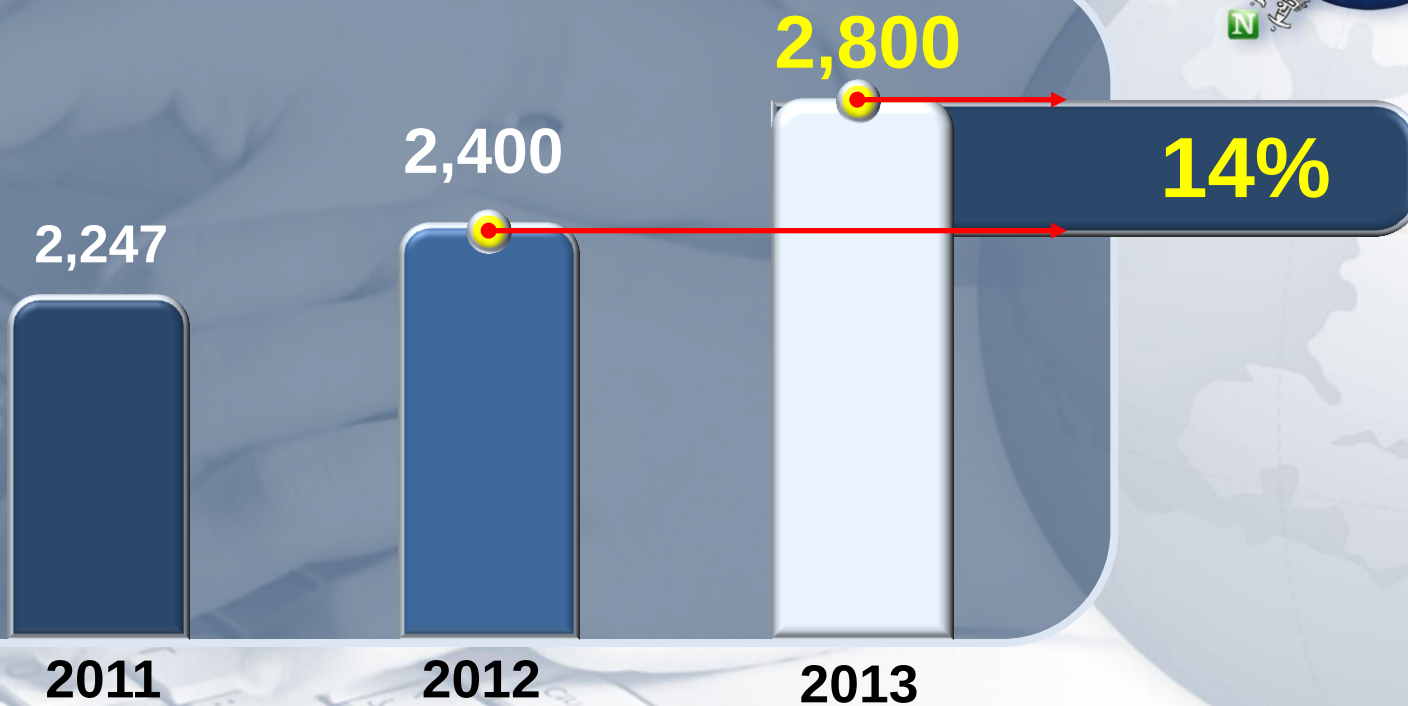
31 de marzo 2014

ÍNDICE

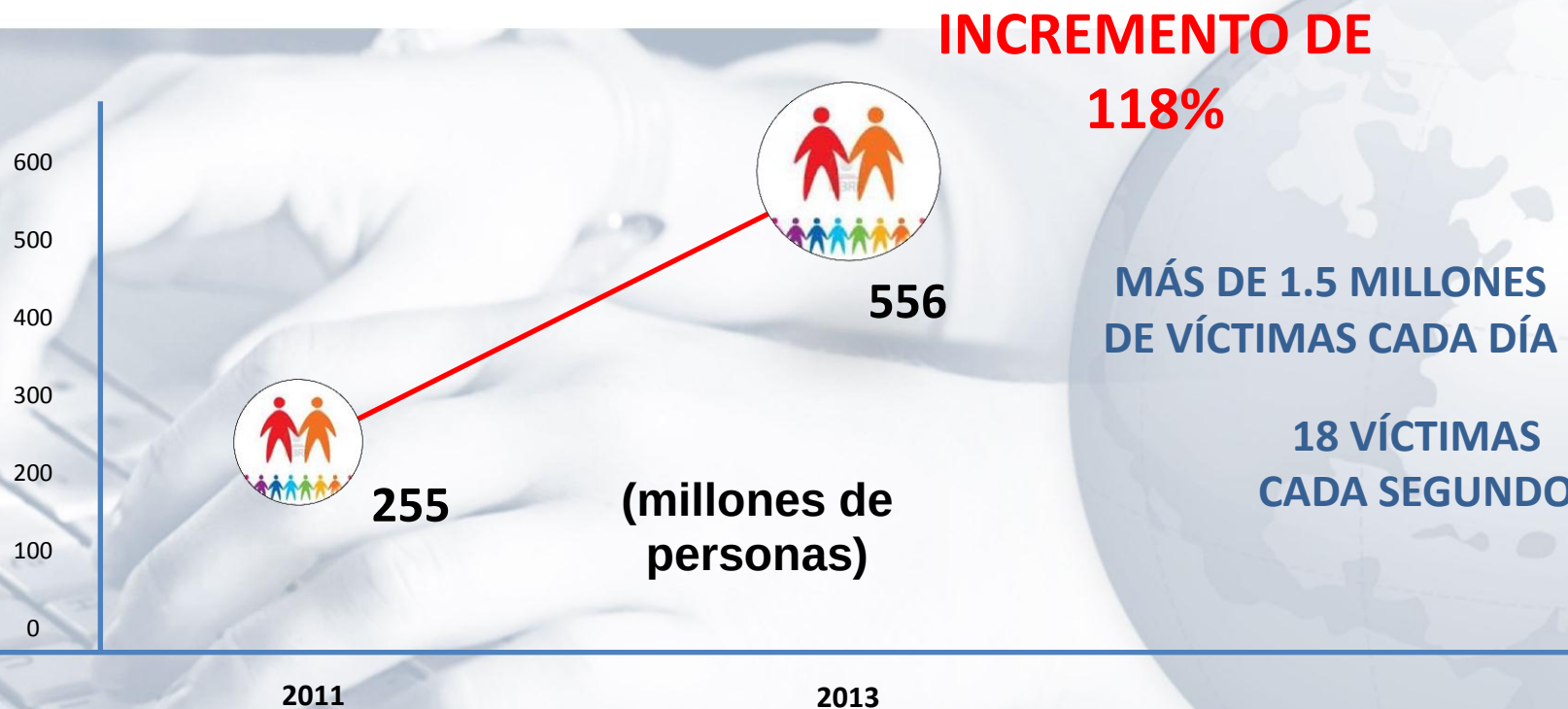
- I. Cibercrimen a nivel mundial**
- II. Cibercrimen en América Latina**
- III. Cibercrimen en México**
- IV. Impacto y gravedad de los delitos cibernéticos**
- V. Estrategia de Ciberseguridad de la Policía Federal**

I. Panorama del Cibercrimen a Nivel Mundial

Cibernautas a nivel Mundial (millones)



Víctimas del Cibercrimen a nivel mundial 2011-2013



Impacto económico del Cibercrimen a nivel mundial (2011-2012)

martes 06, agosto 2013

b:Secure

INICIO INTERNET OPINIÓN REPORTES SEGURIDAD

8 May, 2012

El cibercrimen cuesta a 1 millones de dólares al año

Por Netmedia

Email | ¿Desea imprimir? Regístrese ahora

Follow @bssecuremagazine 5,863 followers

I
u
f
a
I

K
P
C

está haciendo cada vez más transnacional. la Universidad Metropolitana de Londres se están vinculados con bandas internacionales.

"El hampa ahora puede reclutar miembros cometer delitos en el exterior, operando de países equipados con la tecnología más avanzada."

Huí agregó que la policía malaya arrestó el de China y Taiwán que hacían fraude en línea instrucciones de un jefe taiwanés común.

Al usar bases temporales seguras en el Lej miles de millones de dólares por medio de i

Putting Malicious Cyber Activity in Context			
CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	\$1 billion to \$16 billion	0.008% to 0.02%	IMB
Drug Trafficking	\$600 billion	5%	UNODC
Global cyber activity	300 a 500 MMD		Various
US ONLY			
Car Crashes	\$99 billion to \$168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	\$70 billion to \$280 billion	0.5% to 2%	NRF
US- cyber activity	\$24 billion to \$120 billion	0.2% to 0.8%	Various

Quiénes utilizan su teléfono móvil para acceder a Internet son los más vulnerables (Reuters)

Por Mundo Contact | 12 febrero 2013 | Actualidad, Tecnología

Actualmente, las empresas gastan sumas considerables de dinero para limpiar los daños causados por el malware. Los ciberataques han costado a las empresas millones de pesos al año, y algunas compañías llegan a gastar miles más al mes. Las empresas más pequeñas también son blanco cada vez más seguido de estos ataques, ya que se encuentran más propensas por no estar protegidas de forma adecuada.

"Las empresas no sólo gastan para eliminar el malware, sino que también tienen costos de productividad, pérdida de datos, investigación y gestión post-incidentes", señaló Pekka Usva, Vicepresidente de Seguridad Corporativa en F-Secure. "Además de todo esto, el malware que ha pasado desapercibido puede tener graves consecuencias para un negocio. Una tasa de detección más alta puede ahorrar millones de pesos."

Los ataques pueden incluir el robo de la propiedad intelectual de una organización, la apropiación de cuentas bancarias en línea, propagación de virus, la publicación de información confidencial de la compañía en Internet y la interrupción de la red de una empresa, con suspensión del servicio.

Según F-Secure, una mejora en la detección de amenazas del ciberespacio de hasta un 1% permitiría a las compañías ahorrar dinero y evitar altos costos en la limpieza de malware.

martes 06, agosto 2013

b:Secure

INICIO INTERNET OPINIÓN REPORTES SEGURIDAD

McAfee An Intel Company

500,000

encia tiene un :onomía global) y \$500,000 ares al año, de e reporte con el que pacto económico i y el en el mundo.

r realizada por la jurisdicción McAfee y tudios Estratégicos es (CSIS, por sus), asegura que tan es de dólares, elinuencia

osa con la pérdida Políticas Públicas

Lo más importante

- El número de quienes afirman ser víctimas de delitos en internet creció tres veces más

(Reuters) — El costo mundial de los delitos cometidos por internet es de 114,000 millones de dólares anuales, según un estudio de Symantec, el fabricante de las aplicaciones de seguridad informática Norton.

El informe 2011 de la firma indica que 431 millones de adultos fueron

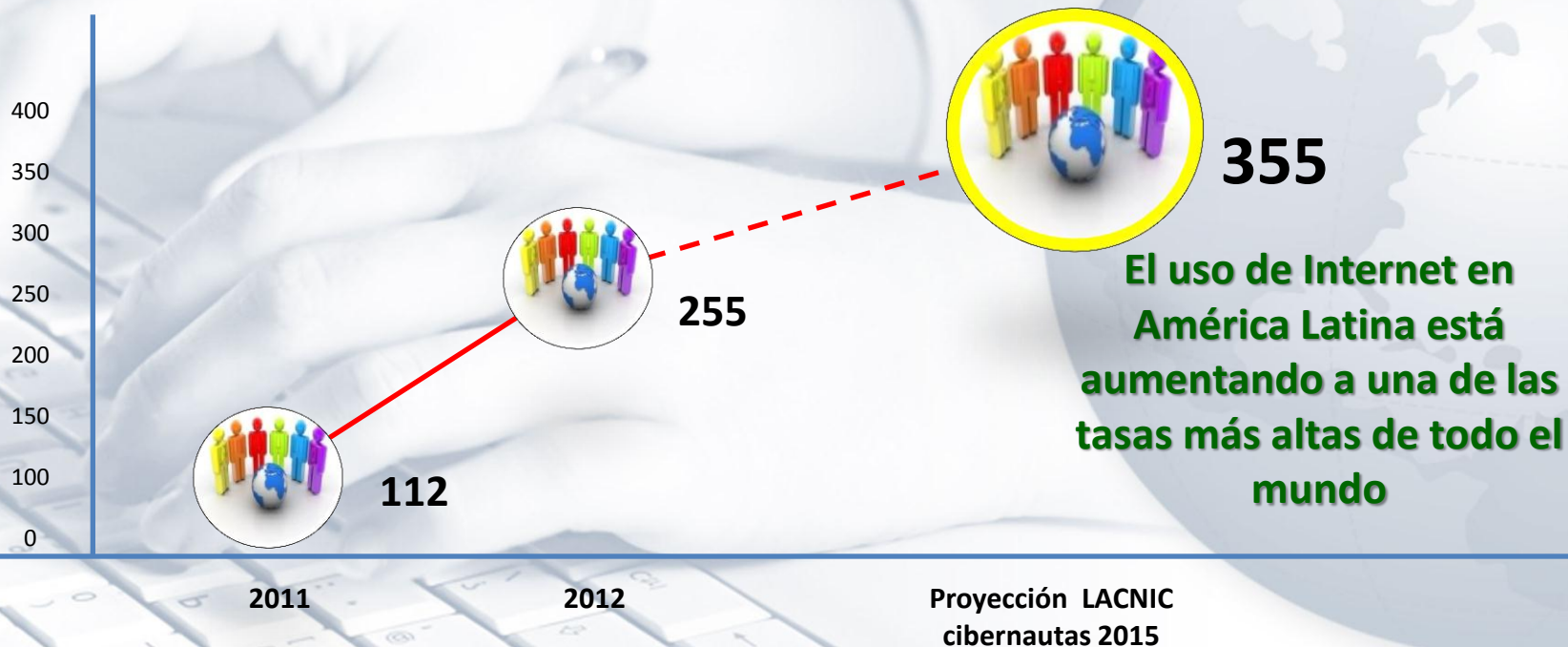
114.000 millones de dólares

274.000 millones de dólares

LOS COSTOS DIRECTOS EN EFECTIVO DEL CIBERCRIPTO (DINERO ROBAO POR LOS MALINTANTES CIBERNÉTICOS O GASTADO EN RESOLVER LOS ATAQUES CIBERNÉTICOS) SUMARON 114.000 MILLONES DE DÓLARES EN TOTAL

II. Panorama Cibercrimen Latino América

Millones de Cibernautas en América Latina 2011-2015



Fuente: ONU, Estudios AMIPCI (2005-2012), COFETEL, ITU
LACNIC: Registro de Direcciones de Internet Para América Latina y Caribe

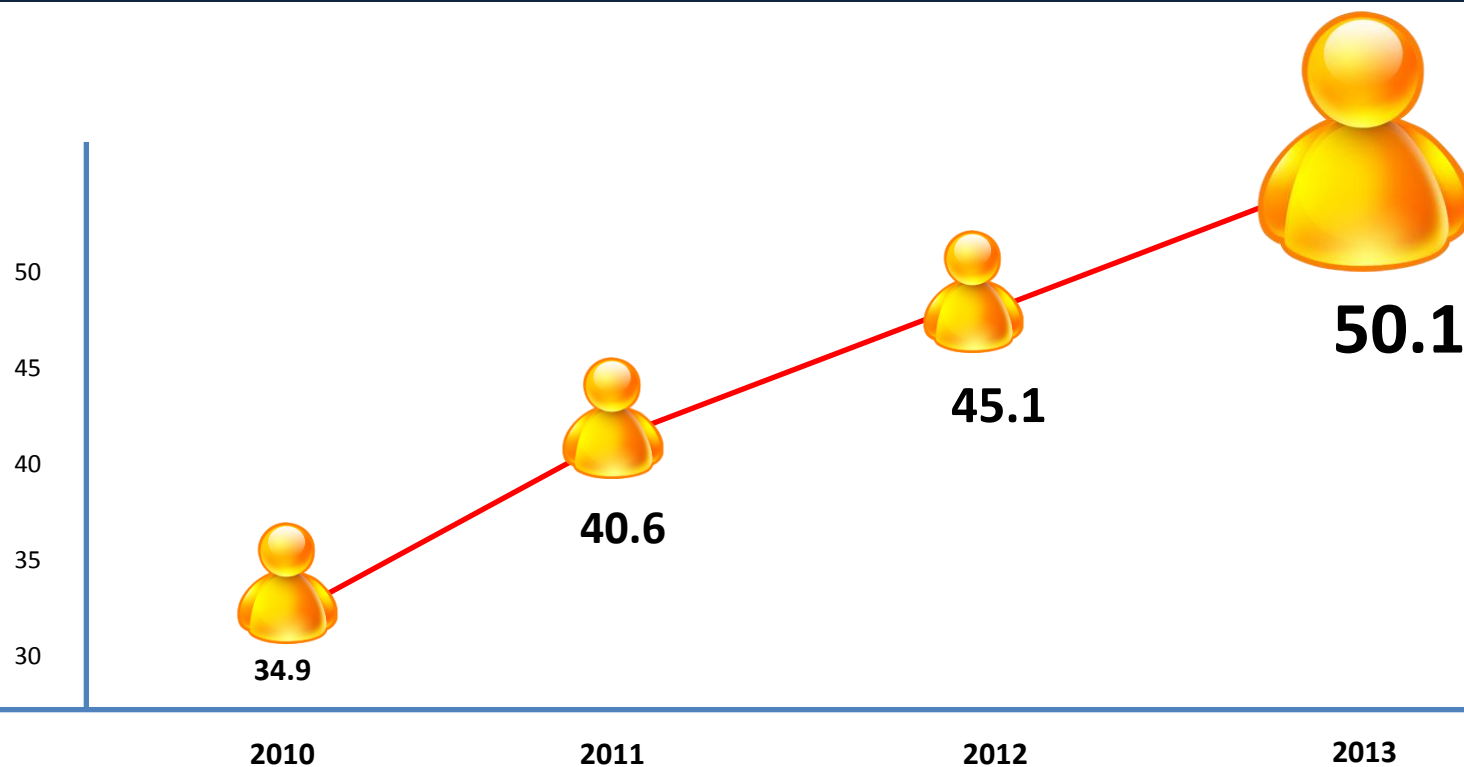
Ranking de fraudes Cibernéticos en América Latina



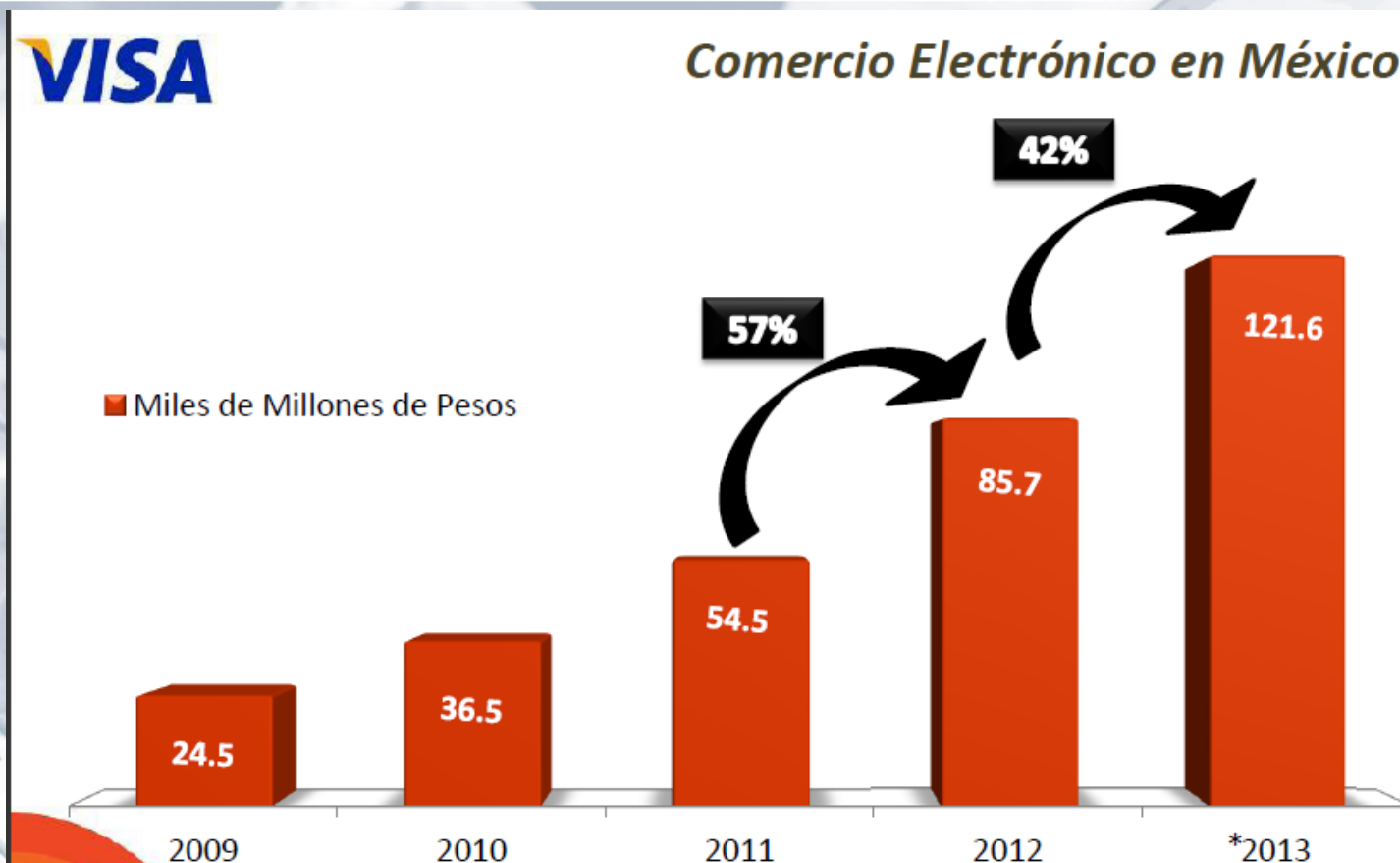
III. Panorama Cibercrimen México

Cibernautas en México

2010-2013 (cifras en millones)



Comercio Electrónico en México



Datos del Cibercrimen en México

El malware es una de las principales afecciones en México

México es uno de los países que más se conecta a la red a nivel mundial

En 2012, se **incrementó en un 40%** el número de incidentes cibernéticos en México.

Fuente: [*“Latin American and Caribbean Cybersecurity Trends and Government Responses”*](#) 2012 pág. 8

Fuente: Estudios AMIPCI (2005-2012)

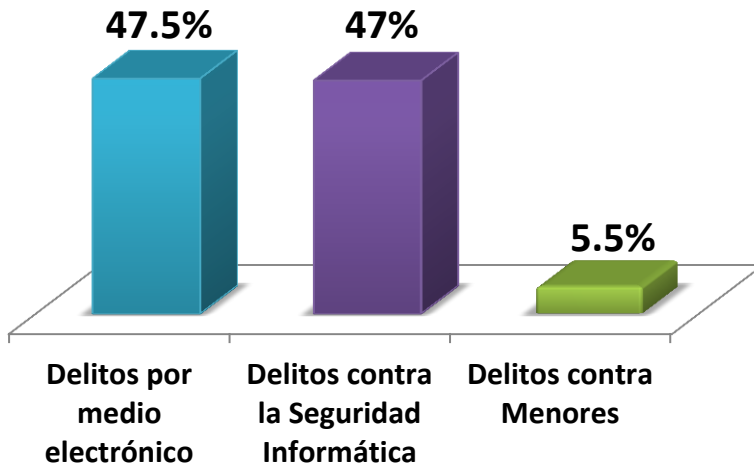
IV. Impacto y gravedad de los Ciberdelitos (tendencias registradas por la Policía Federal)

Fuentes de Información Diciembre 2012 – Febrero 2014



Denuncia ciudadana. Centro de Atención del Comisionado 088

20,996 Denuncias Ciudadanas



Delitos por medio electrónico con mayor incidencia

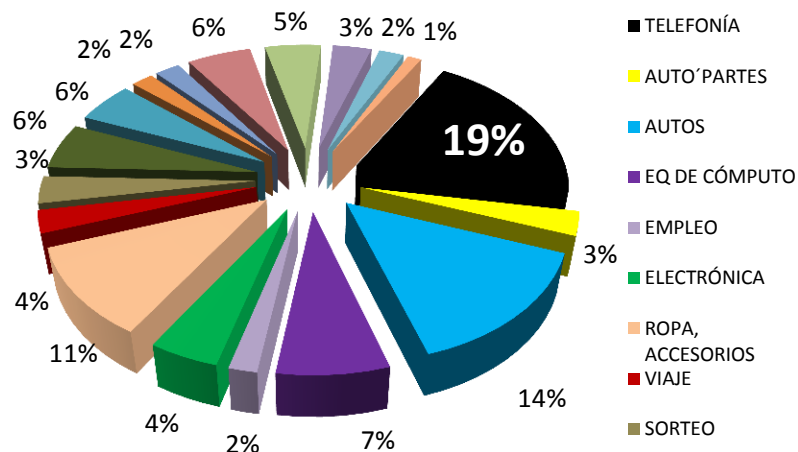
47.5% delitos por medio electrónico

28.5% FRAUDE Y EXTORSIÓN		Total
	FRAUDE AL COMERCIO ELECTRÓNICO	59%
	FRAUDES DIVERSOS	24%
	FRAUDE NIGERIANO	13%

17% AGRAVIO CONTRA PERSONAS		Total
	DIFAMACIÓN	31%
	AMENAZAS	24%
	ROBO DE CONTRASEÑAS	20%
	SUPLANTACIÓN DE IDENTIDAD	15%

Fraudes al comercio electrónico

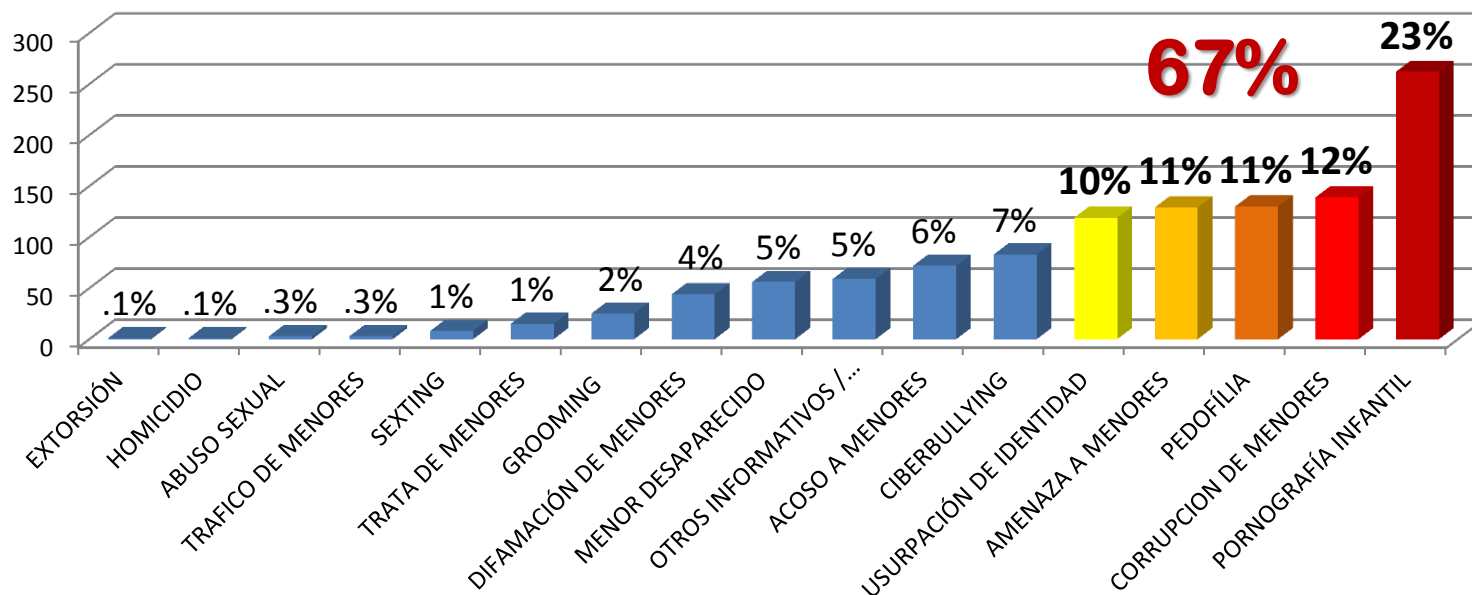
ARTICULO POR CATEGORÍA	TELEFONÍA	19%
	AUTOS	14%
	ROPA, ACCESORIOS	11%
	EQ DE CÓMPUTO	7%



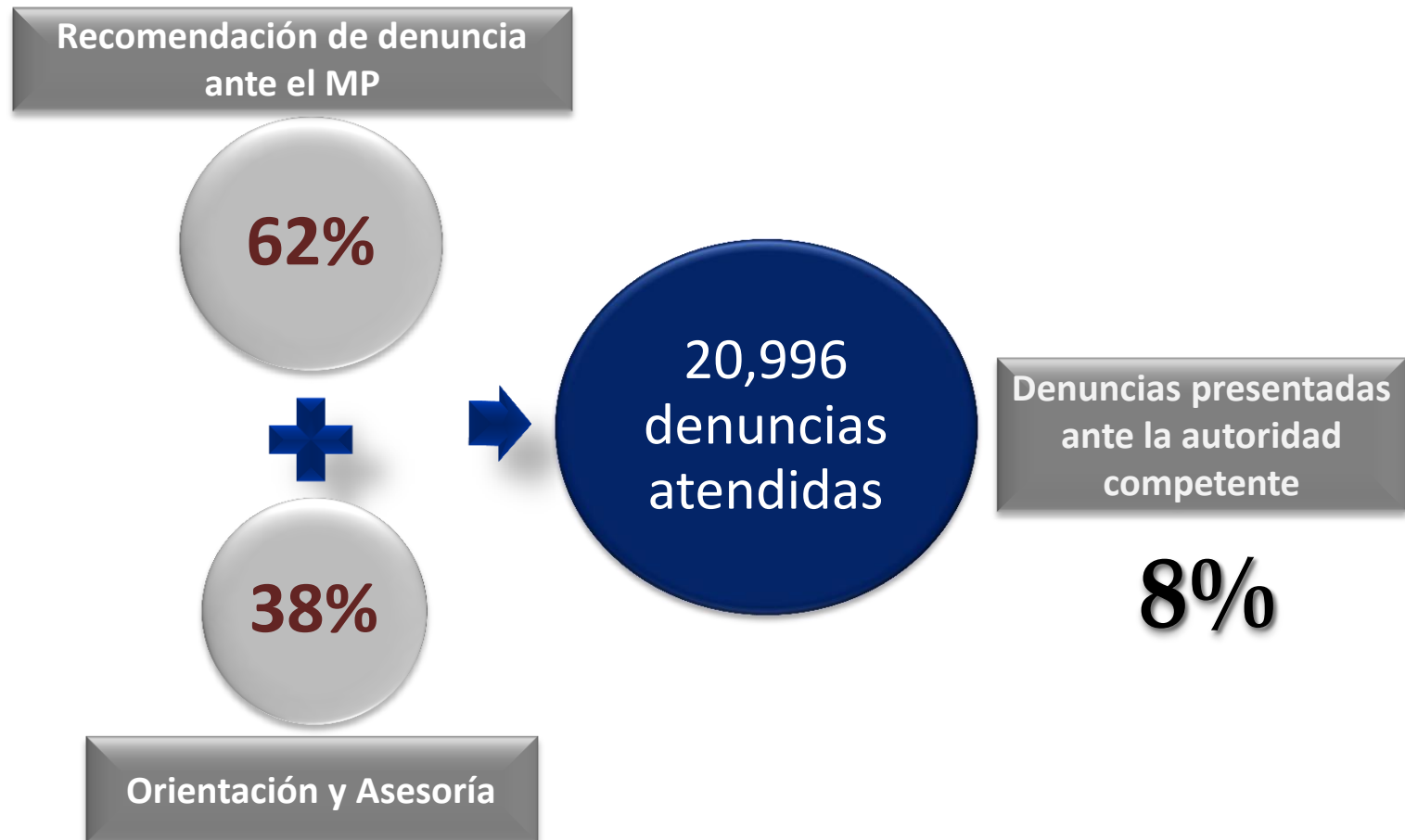
Delitos contra la Seguridad Informática (47%)

AFECCIÓN	TOTAL
MALWARE	98%
PHISHING	2%

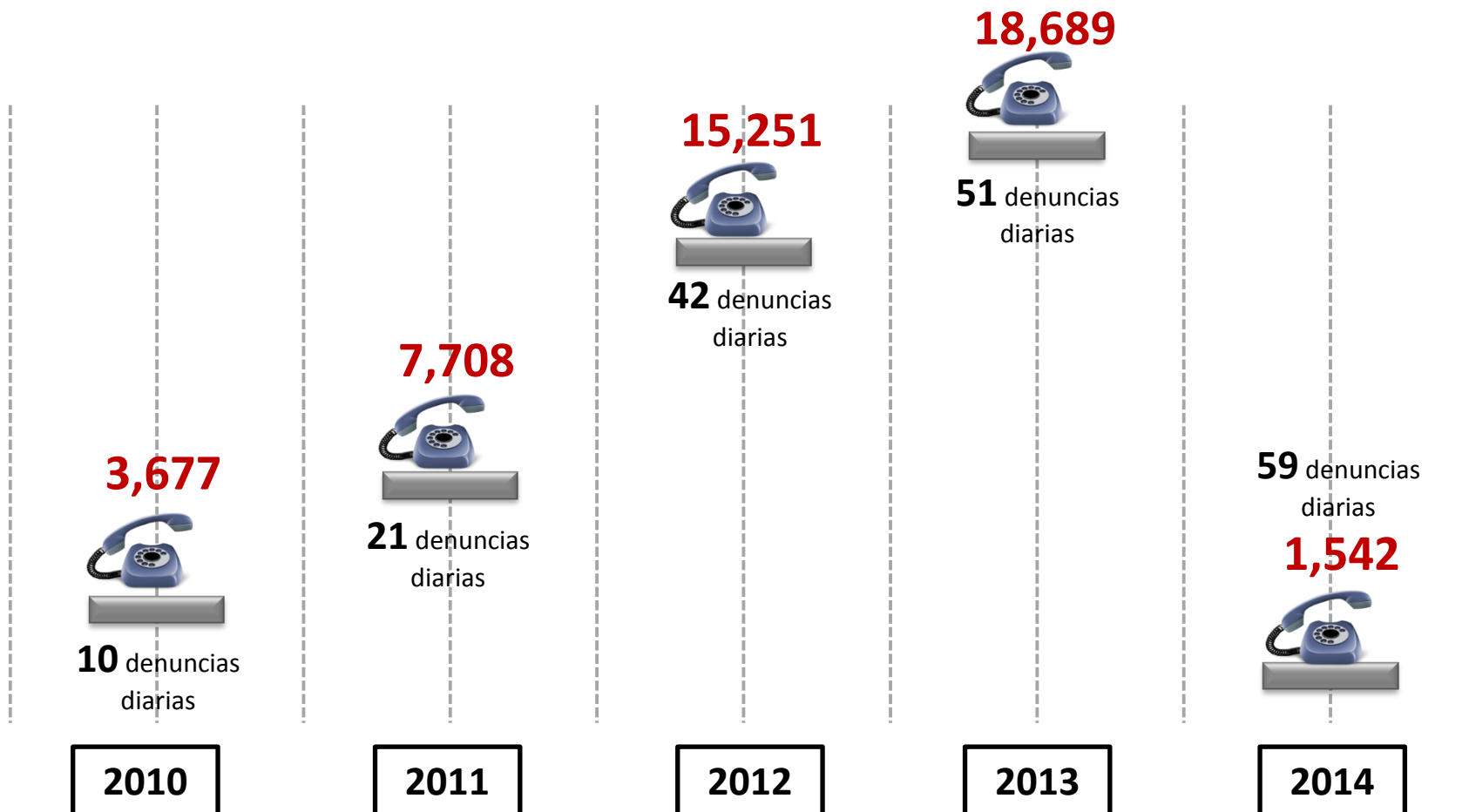
Delitos contra menores a nivel nacional (5.5%)



Atención proporcionada al ciudadano



Comparativo de actividad

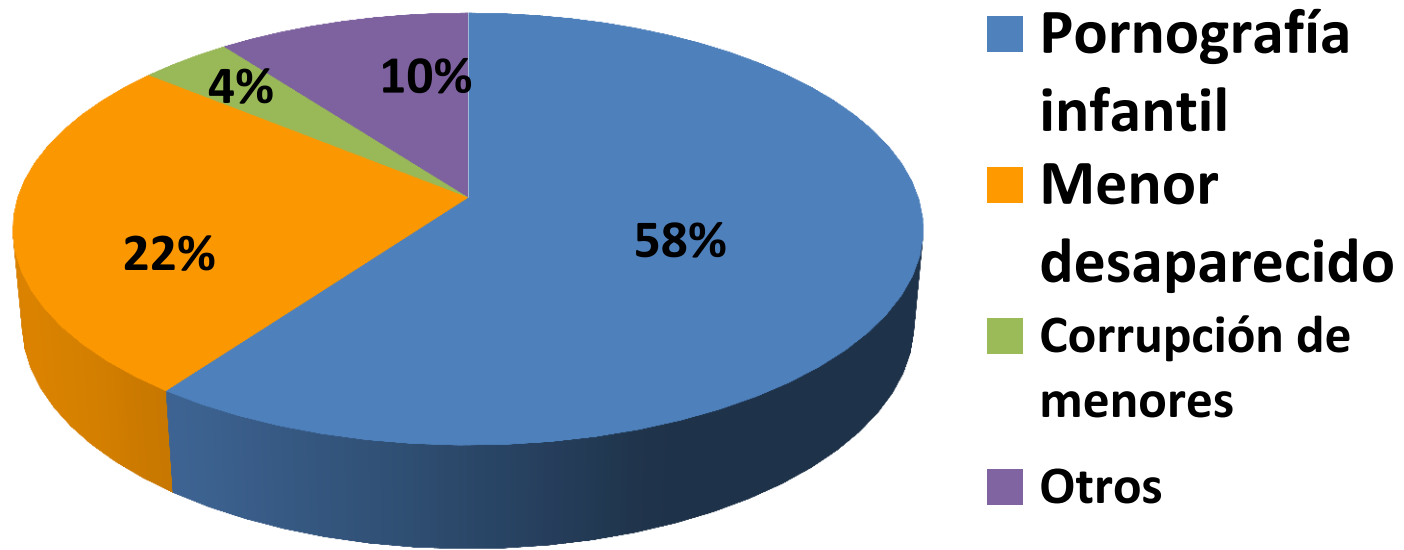


DELITOS CONTRA MENORES

MANDAMIENTOS MINISTERIALES

Delitos contra menores Centro de Delitos Contra Menores (CENADEM)

Atención a Mandamientos Ministeriales



CENADEM. Delitos contra menores a nivel nacional

Año	Cateos	Detenidos
2009	1	1
2010	2	2
2011	7	5
2012	27	16
2013	35	20
2014	8	10

Del total de probables responsables:

- 18-25 años de edad.
- Estrato social medio.
- Nivel Superior.

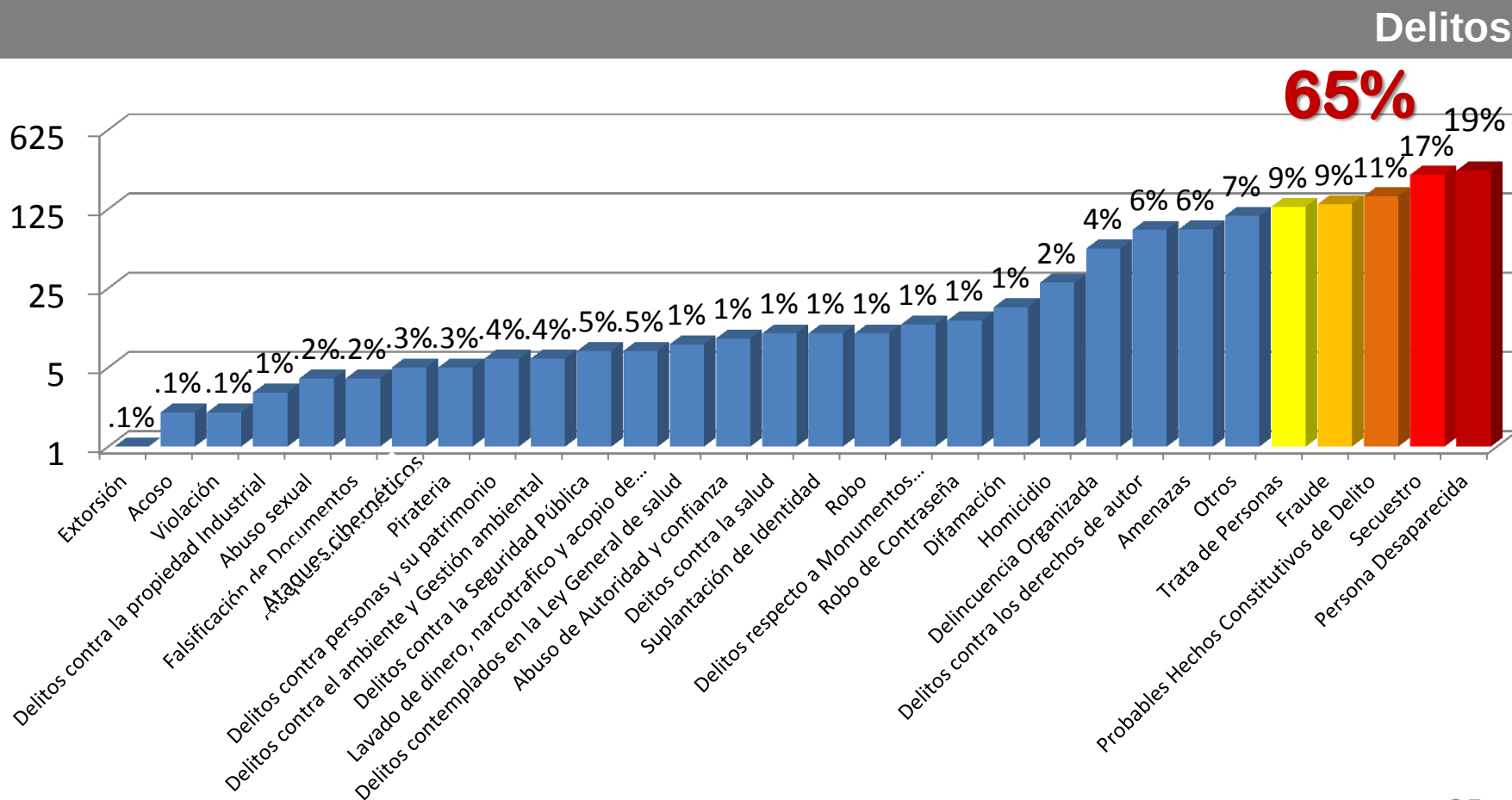
Alerta Amber:

- 13-17 años de edad.
- Sexo femenino.

DELITOS ALTO IMPACTO

MANDAMIENTOS MINISTERIALES

Tendencia nacional de delitos de alto impacto Mandamientos ministeriales



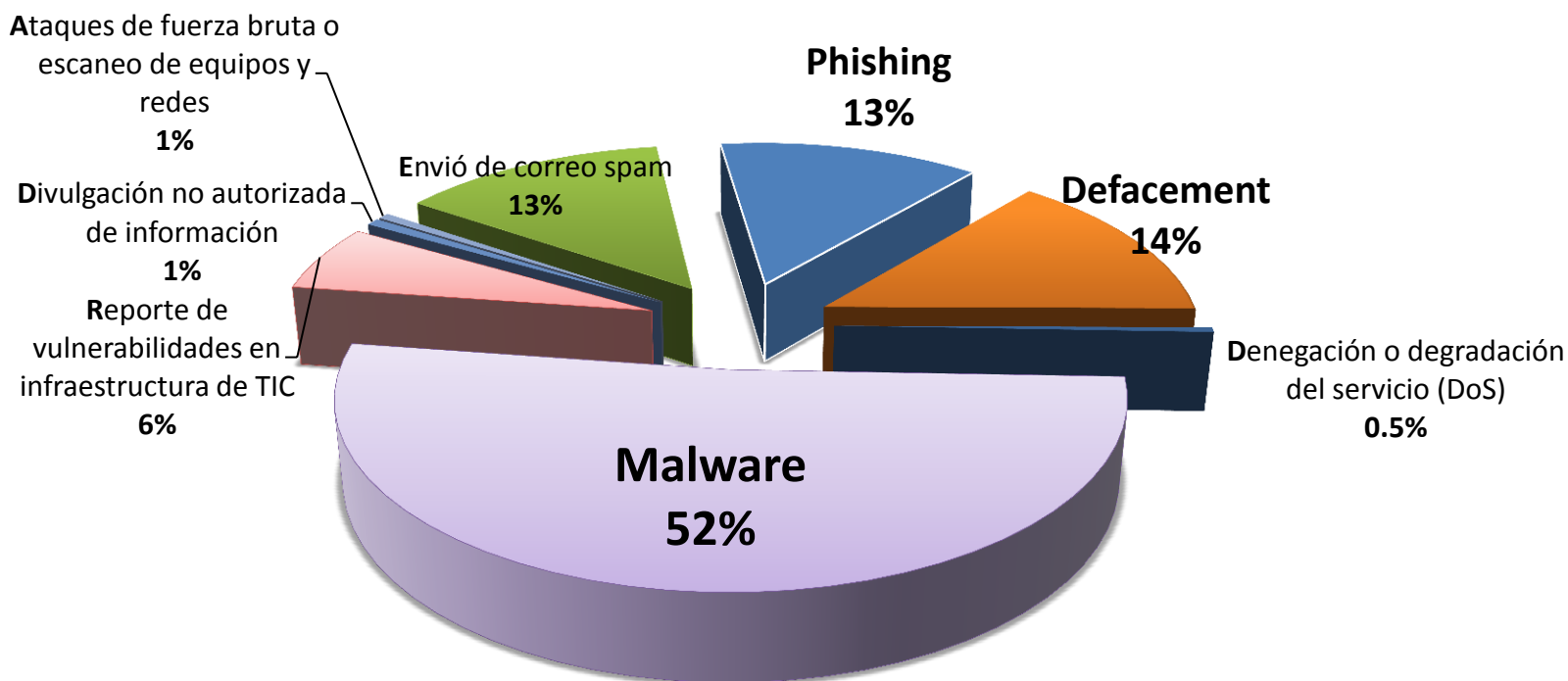
CERT-MX

ATENCIÓN DE INCIDENTES

AMENAZAS Y ATAQUES

Tendencia nacional de delitos contra la seguridad informática

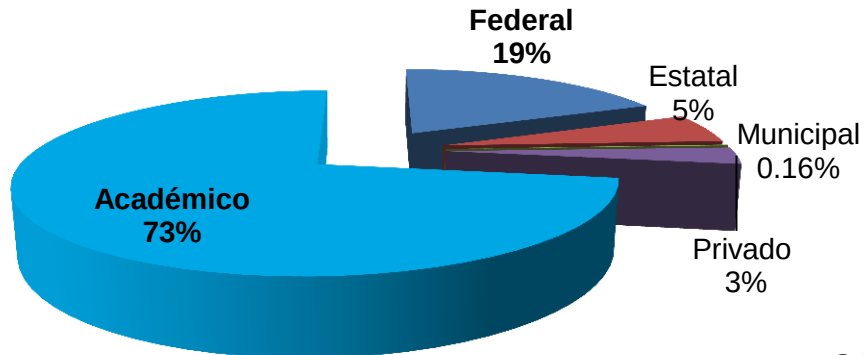
23,549 Incidentes de Seguridad



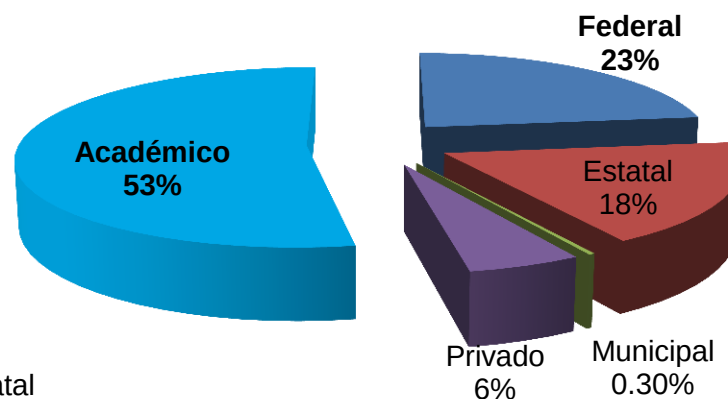
Tendencia nacional de delitos contra la seguridad informática

Malware

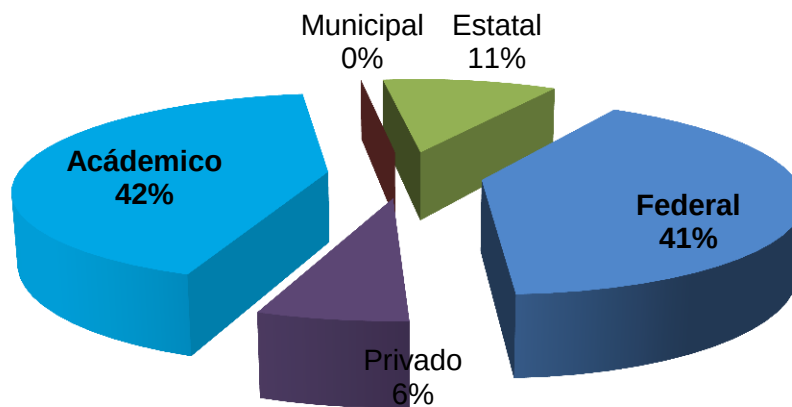
2012



2013

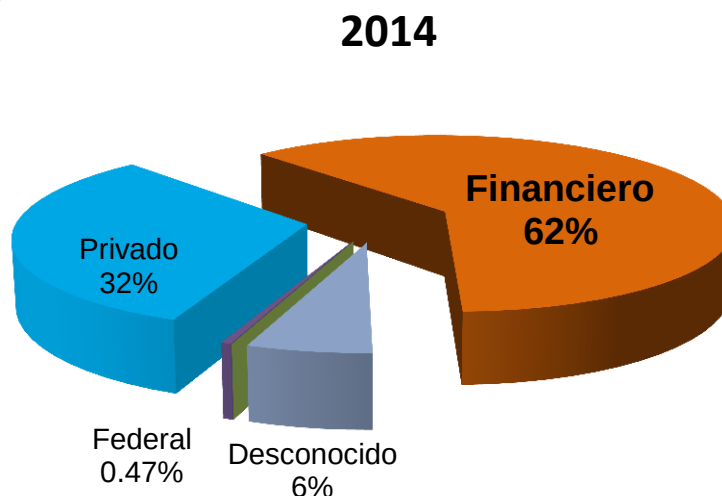
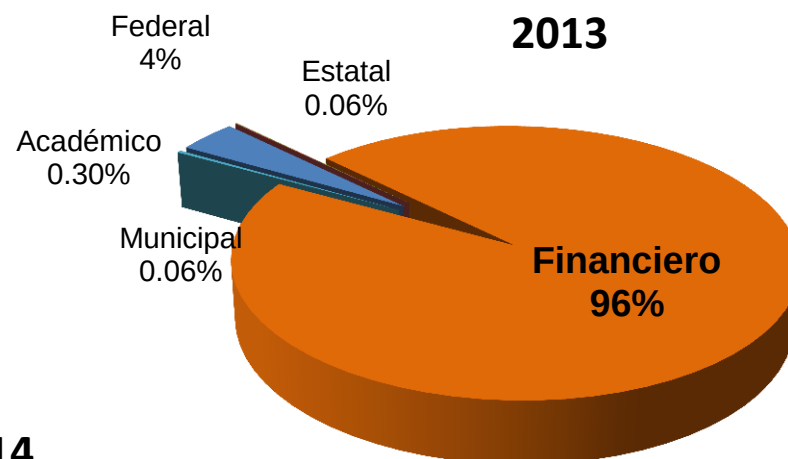
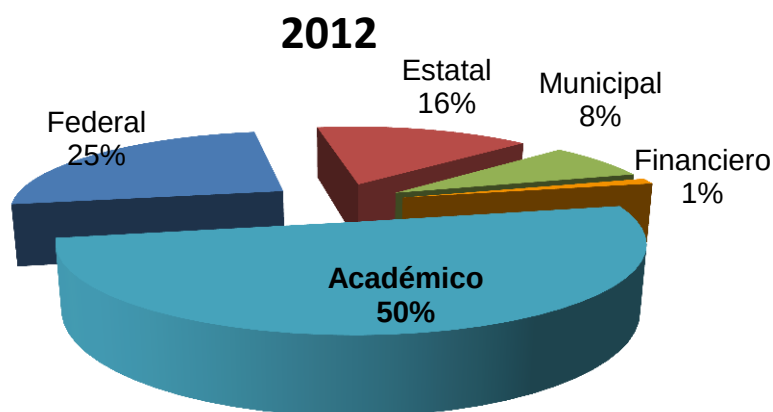


2014



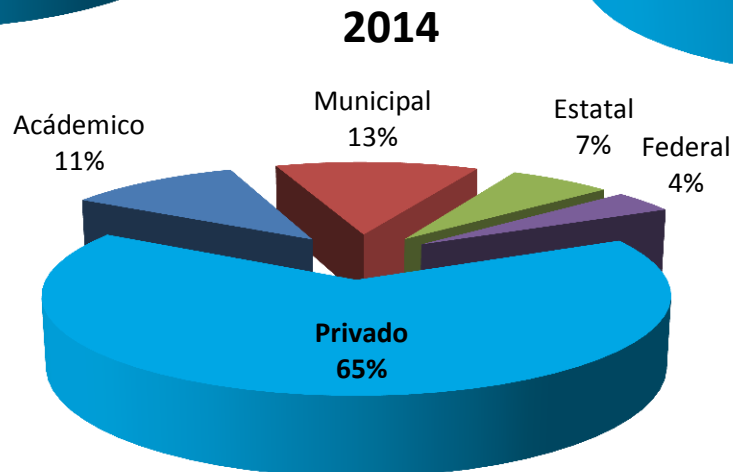
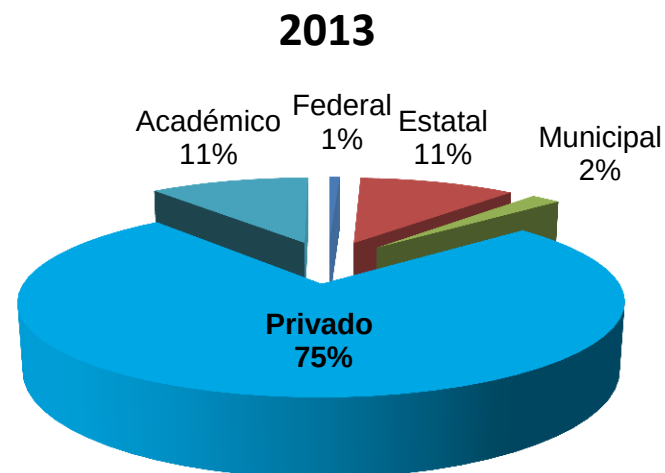
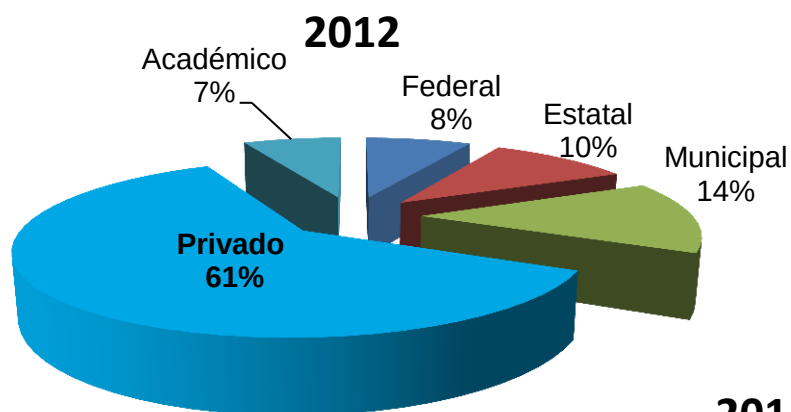
Tendencia nacional de delitos contra la seguridad informática

Phishing



Tendencia nacional de delitos contra la seguridad informática

Acceso no autorizado a sistemas de información (Defacement)



Implicaciones y acciones

- **Cultura de la prevención** (sociedad, empresas y sector público).
- Cultura de la **denuncia ciudadana**.
- **Indicadores y estadísticas sobre ciberdelincuencia**. Política Pública.
- **Mayor colaboración y coordinación institucional**: empresas-gobierno.
- **Fortalecer el sistema de justicia** para la tipificación de los delitos cibernéticos.
- **Incremento en las capacidades técnicas** en este tipo de delitos (policías cibernéticas, ministerios públicos y jueces).
- Inversión en **sistemas de seguridad y monitoreo**.
- La Policía Federal dispone de un **Programa de Ciberseguridad**.

Principales Acciones del Programa de Ciberseguridad de la Policía Federal

Promover la Cultura de
Prevención de Delitos
Cibernéticos

Fortalecer la Atención
Ciudadana

Indicadores y Estadísticas
de Delitos Cibernéticos



Principales Acciones del Programa de Ciberseguridad de la Policía Federal



Modelo de Policía
Cibernética Nacional

Convenios de
colaboración e impulso al
sistema penal de justicia

Colaboración con Policías
Cibernéticas Extranjeras



Principales Acciones del Programa de Ciberseguridad de la Policía Federal

Detección y atención de incidentes cibernéticos

CERT-MX



Protección de Infraestructuras Críticas Informáticas e Industriales

CERT-MX

Investigación Científica en Materia Cibernética



Medios de contacto y atención

Para denunciar cualquier delito cibernético puede hacerlo a los siguientes números y medios de contacto.

Centro de Atención del Comisionado

088

www.facebook.com/ceac.cns

ceac@cns.gob.mx

[@ceac_cns](#)

Atención Ciudadana en Delitos Electrónicos

(01) 55-11-03-6000 Ext. 29218 o 29123

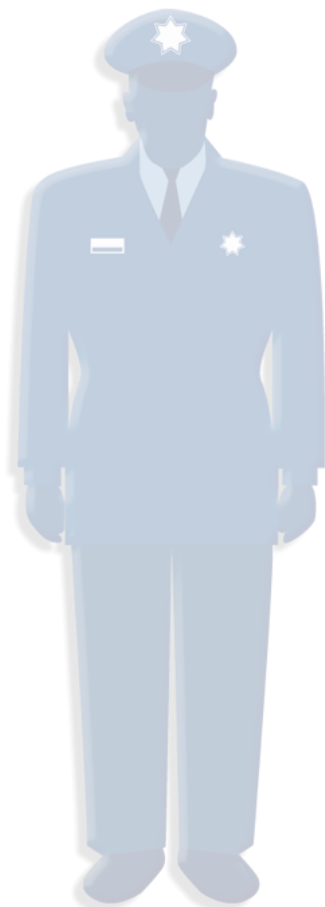
delitocibernetico_pf@cns.gob.mx

Centro Especializado en Respuestas Tecnológicas

phishing@cns.gob.mx

malware@cns.gob.mx

cert-mx@cns.gob.mx





**“PROTEGER Y SERVIR A LA
COMUNIDAD”**

31 DE MARZO DE 2014

POSICIONAMIENTO DEL PODER EJECUTIVO FRENTE AL FENOMENO DE LA CIBERDELINCUENCIA – Ulises Gómez Nolasco

Saludo a los representantes de los poderes legislativo y judicial, y les externo nuestro gran aprecio por su presencia en este foro.

Agradezco al Secretario Seger por su apoyo para la realización de este taller.

Parece claro que enfrentamos un problema. Debemos preguntarnos como autoridades si estamos preparados. ¿Estamos preparados para dar respuestas a nuestra sociedad?

Un día recibes un mail del SAT. El mail dice que hay un problema con tu devolución de impuestos. Contiene un link donde tienes que dirigirte para resolver el problema. Sin saberlo, el click de un botón te lleva a un sitio falso donde tu computadora es infectada de ‘malware’, (sí de ‘malware’, -malicious software-, un tipo de programa que puede incluir virus, gusanos, trojanos y spyware)... estamos empezando a hablar en otro idioma, pasando a otra dimensión, la dimensión del ciberespacio y del cibercrimen... ¿estamos preparados?

Una vez infectada de malware, los hackers -esta mezcla de piratas, asaltantes y ladrones...- se hacen de toda tu información bancaria que hay almacenada en tu computadora -derivado de su uso cotidiano- y esa información la usan para acceder a tu cuenta y robar tu dinero.

Desde luego que ahí no termina. Tu dinero, junto con el de otras personas, es transmitido a la cuenta de una joyería de alto nivel en Europa donde se utiliza para comprar piedras preciosas, joyas o relojes. La joyería no lo sabe porque acuerda la transacción mediante una llamada de teléfono celular. Al día siguiente una persona acude a recoger la mercancía. Una vez que se verifica la transferencia, la mercancía es entregada.

Una vez que la mercancía es vendida, el dinero en efectivo sirve para financiar nuevas actividades criminales como puede ser terrorismo, corrupción, tráfico de armas, de drogas, secuestro y nuevos ataques cibernéticos.

Cabe señalar que la persona que recoge la mercancía fue contratada vía Internet y le fue exigida una cuenta para depositar su pago por su breve y simple servicio. En muchos casos estas cuentas son utilizadas como puente de las transacciones, sin que las personas se den cuenta de que colaboraron en la comisión de un delito de diversas formas.

En este punto, el rastreo del dinero y de las personas que intervinieron en la comisión del delito, imponen retos jurídicos e investigativos monumentales.

Después de esa experiencia, para evitar ser víctima de ‘phishing’ nuevamente, la próxima vez que usaste tu computadora verificaste que todos los correos a los que contestas sean originales, sin embargo estás por ser nuevamente víctima de la ciberdelincuencia... Tratas de ingresar directamente al sitio web de tu banco. Escribes la dirección en tu computadora sin saber que el servidor DNS, el que se encarga de dirigirte a la dirección IP de tu banco, ha sido hackeado y te redirecciona a una página falsa donde al ingresar tus códigos, tu información vuelve a ser susceptible de ser robada...

El ciberdelito desde luego no se agota con estos ejemplos, los nuevos términos, posibilidades y vertientes son casi infinitas:

- robo de propiedad intelectual;
- fraude y delitos financieros por disposiciones en tarjetas de crédito y cuentas bancarias;
- robo de identidad;
- secuestro de información de computadoras personales o de empresas;
- pornografía infantil y propuestas de contenido sexual a menores;
- espionaje y ataques a la infraestructura informática de servicios críticos para la estabilidad del país, como los financieros y de áreas estratégicas

Esta lista solo enuncia una muestra de posibilidades, donde como puede advertirse, cada una, en lo individual, es suficientemente grave por los daños que ocasiona a la sociedad.

En el Informe de delitos cibernéticos de Norton 2011 se advierten los alcances de los ciberdelitos, los costos que representan, así como la falta de justicia que manifiestan las víctimas.

El informe señala que cerca del 65% de adultos en el mundo han sido víctimas de algún tipo de ciberdelito, tales como estafas online, ataques de phishing, actividades de piratas informáticos en perfiles de redes sociales y fraudes con tarjetas de crédito. En cuanto a los responsables de estas conductas ilícitas, un 56% son delincuentes anónimos y un 21% grupos organizados.

En cuanto al daño económico que representa la comisión de un ciberdelito, la encuesta señala que el monto por las actividades de la ciberdelincuencia que han erogado las víctimas supera los 388 mil millones de dólares. Asimismo, destaca que se gastaron directamente 114 mil millones de dólares debido al dinero robado por los delincuentes, o bien, al monto gastado en resolver los ataques cibernéticos. Igualmente, se determina que el gasto equivalente al tiempo perdido valuado por las víctimas, se estima en 274 mil millones de dólares.

Por lo que respecta al Reporte efectuado en 2012 por Norton, las ganancias anuales a nivel mundial de la ciberdelincuencia ascienden a cien mil millones de dólares y específicamente en el caso de México se elevan a dos mil millones de dólares, mientras que cada año 556 millones de personas son víctimas de estos delitos, lo que equivale a más de 1.5 millones diariamente, es decir 18 víctimas por segundo.

México y la comunidad internacional enfrentamos una amenaza que no es de ninguna manera futura, es presente y es creciente.

Reitero la pregunta ¿estamos preparados?

Es momento de reconocer que vamos tarde. Es momento de reconocer que no estamos preparados. Nuestro orden jurídico ha quedado rebasado en la tipificación de las nuevas, diversas y complejas conductas y tramas de operación de la delincuencia. Nuestras capacidades institucionales no se han desarrollado en la medida en que las circunstancias lo exigen, los procesos de investigación, custodia y obtención de pruebas, así como su judicialización para la obtención de sentencias que permitan castigar y disuadir este tipo de conductas, representan grandes áreas de oportunidad que la delincuencia aprovecha día a día.

El Plan Nacional de Desarrollo 2013-2018 establece 5 Metas Nacionales que rigen las funciones de la Administración Pública Federal, siendo la primera de ellas lograr “Un México en Paz”. La estrategia nacional en la materia está enfocada a reducir la impunidad y la violencia, a través de una real y eficaz coordinación entre los tres órdenes de Gobierno, con el fin de conseguir que las generaciones presentes y futuras puedan vivir en una sociedad segura y en armonía.

En ese sentido, el combate a la cibercriminalidad es una meta indispensable para poder reducir los espacios de impunidad en nuestro país.

Consciente de lo anterior, el Gobierno Federal ha realizado un extraordinario trabajo de coordinación para consolidar los esfuerzos y perspectivas de más de quince dependencias e instituciones federales con el firme objetivo de que México esté en posibilidad de cumplir con los estándares internacionales en la materia y se establezcan las bases para un combate real y efectivo de esta amenaza.

El Convenio sobre la Ciberdelincuencia adoptado en Budapest el 23 de noviembre de 2001 en el seno del Consejo de Europa constituye el avance más notable en el ámbito internacional.

En este sentido resulta pertinente la adhesión de México a este instrumento para que constituya un catalizador de la actualización legislativa que necesitamos implementar como una de las muchas acciones de respuesta a la amenaza de la ciberdelincuencia.

Nuestra adhesión a este convenio igualmente constituye una acción obligada para el cumplimiento de otras metas contenidas en el Plan Nacional de Desarrollo, como lograr un “México con Responsabilidad Global” y constituye una piedra fundamental para complementar programas de gobierno ambiciosos y clave para el avance del país, como la Estrategia Digital Nacional encabezada desde la propia Presidencia de la Republica.

La ciberdelincuencia, como una variante de la delincuencia organizada, no solo no reconoce fronteras, sino que, como parte de la esencia de su *modus operandi*, se vale de la omnipresencia que la tecnología permite, para tratar de ponerse fuera del alcance de las autoridades.

Los delincuentes no tienen fronteras, la cooperación internacional tampoco debe tenerlas. Las autoridades involucradas tenemos el reto y la obligación de desarrollar los esquemas institucionales necesarios para actuar en colaboración entre nuestros gobiernos con oportunidad, con eficacia, con efectividad, pero también, con pleno respeto a la soberanía de nuestros países y a los principios de nuestras legislaciones.

La decisión de México de adherirse a la Convención de Budapest impactará en la generación de un nuevo liderazgo regional en la materia al ser el tercer país latinoamericano que asume el compromiso de dar cumplimiento a sus disposiciones mediante las actualizaciones legislativas necesarias.

Esta conciencia de la problemática no se ha resumido solo en buenas intenciones. En el Gobierno Federal hemos emprendido un dedicado y profundo trabajo de estudio para llevar a cabo la actualización del ordenamiento jurídico mexicano en materia de ciberdelito.

El Gobierno Federal a través de las dependencias y entidades miembros del Comité Especializado en Seguridad en la Información ha formulado un proyecto de iniciativa que introduce no solo modificaciones para cumplir con las disposiciones del Convenio de Budapest sino que va aún más allá del estándar que establece, al incorporar disposiciones sobre proposiciones a menores con fines sexuales mediante sistemas informáticos y robo de identidad.

El proyecto formulado propone la reforma y/o adición de disposiciones relativas a:

- Daños o atentados contra la integridad o disponibilidad de los sistemas informáticos
- Difusión de mensajes con contenidos discriminatorios
- Localización geográfica en tiempo real
- Conservación de datos de tráfico o de contenido
- Conductas vinculadas a la pornografía infantil
- Apología de los delitos contra la humanidad
- Propositiones a menores con fines sexuales
- Acceso no autorizado a sistemas
- Falsificación informática
- Interceptación de información
- Acceso no autorizado a sistemas
- Abuso de dispositivos
- Falsificación informática
- Suplantación de sistemas informáticos
- Suplantación de identidad
- Fraude informático
- Responsabilidad de las personas jurídicas

Este proyecto se encuentra en análisis en la Consejería Jurídica del Ejecutivo Federal para su presentación ante el Poder Legislativo, lo que dará contenido y congruencia clara y oportuna a la adhesión de México al Convenio de Budapest.

Reconocer lo que falta por hacer, lejos de ser una debilidad, debe percibirse como una clara señal de voluntad y compromiso para llevar a cabo lo que sea necesario desde nuestras posiciones y finalmente llevar a nuestro país a resolver de manera definitiva y constante la diversidad de retos que los tiempos nos imponen y nos seguirán imponiendo.

Quienes tenemos el honor de servir a México estamos avanzando y no vamos a detenernos.

Gracias.



Workshop on cybercrime legislation in Latin America

Mexico City

31 March (national workshop)

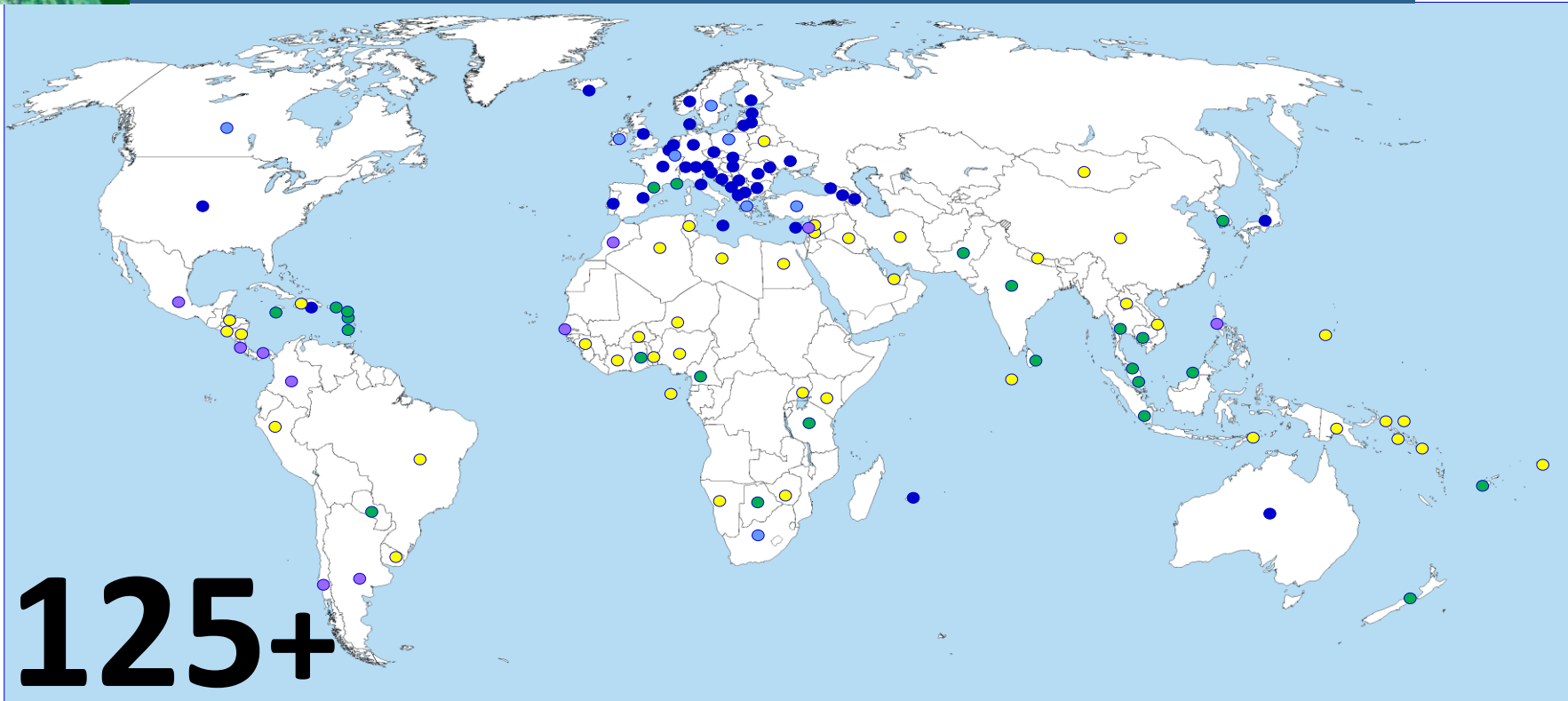
Overview of Budapest Convention on Cybercrime

Convención de Budapest sobre la Ciberdelincuencia

Alexander.seger@coe.int

www.coe.int/cybercrime

Reach of Budapest Convention



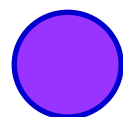
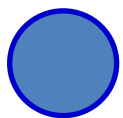
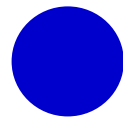
125+

Indicative map only

Ratified/acceded: 42

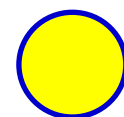
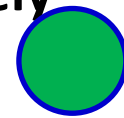
Signed: 11

Invited to accede: 9
= 62



Other States with laws/draft laws largely
in line with Budapest Convention = 20

Further States drawing on Budapest
Convention for legislation = 43+



La Convención de Budapest

- 1. Derecho penal sustantivo**
- 2. Derecho procesal**
- 3. Cooperación internacional**

Convención de Budapest: Derecho penal sustantivo



Article	Budapest Convention	
Art. 1	Definitions	Definiciones
Art. 2	Illegal access	Acceso ilícito
Art. 3	Illegal interception	Interceptación ilícita
Art. 4	Data interference	Ataques a la integridad de los datos
Art. 5	System interference	Ataques a la integridad del sistema
Art. 6	Misuse of devices	Abuso de los dispositivos

Convención de Budapest: Derecho penal sustantivo

Article	Budapest Convention	
Art. 7	Computer-related forgery	Falsificación informática
Art. 8	Computer-related fraud	Fraude informático
Art. 9	Child pornography	Delitos relacionados con la pornografía infantil
Art. 10	IPR offences	Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
Art. 11	Attempt, aiding, abetting	Tentativa y complicidad
Art. 12	Corporate liability	Responsabilidad de las personas jurídicas
Art. 13	Sanctions and measures	Sanciones y medidas

Convención de Budapest: Derecho procesal

Article	Budapest Convention	
Art. 14	Scope	Ámbito de aplicación de las disposiciones de procedimiento
Art. 15	Conditions and safeguards	Condiciones y salvaguardias
Art. 16	Expedited preservation	Conservación rápida de datos informáticos almacenados
Art. 17	Expedited preservation and partial disclosure of traffic data	Conservación y revelación parcial rápidas de los datos relativos al tráfico
Art. 18	Production order	Orden de presentación
Art. 19	Search and seizure	Registro y confiscación de datos informáticos almacenados
Art. 20	Real-time collection traffic data	Obtención en tiempo real de datos relativos al tráfico
Art. 21	Interception of content data	Interceptación de datos relativos al contenido
Art. 22	Jurisdiction	Jurisdicción

Artículo 15 – Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

Convención de Budapest: Cooperación internacional



Article	Budapest Convention	Principios generales
Art. 23	General princip. (subsidiarity)	Principios generales relativos a la cooperación internacional
Art. 24	Extradition	Extradición
Art. 25	General rules	Principios generales relativos a la cooperación
Art. 26	Spontaneous information	Información espontánea
Art. 27	MLA in absence of treaty	Procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable
Art. 28	Confidentiality	Confidencialidad y restricciones de uso

Convención de Budapest: Cooperación internacional



Article	Budapest Convention	Disposiciones específicas
Art. 29	Expedited preservation	Conservación inmediata de datos informáticos almacenados
Art. 30	Partial disclosure traffic data	Comunicación inmediata de los datos informáticos conservados
Art. 31	MLA accessing data	Asistencia concerniente al acceso a datos informáticos almacenados
Art. 32	Transborder access	Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso
Art. 33	MLA collection traffic data	Asistencia para la recogida en tiempo real de datos de tráfico
Art. 34	MLA interception content	Asistencia en materia de interceptación de datos relativos al contenido
Art. 35	24/7 point of contact	Red 24/7

Artículo 37 – Adhesión a la Convención

[el] Consejo de Europa podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo de Europa y que no haya participado en su elaboración

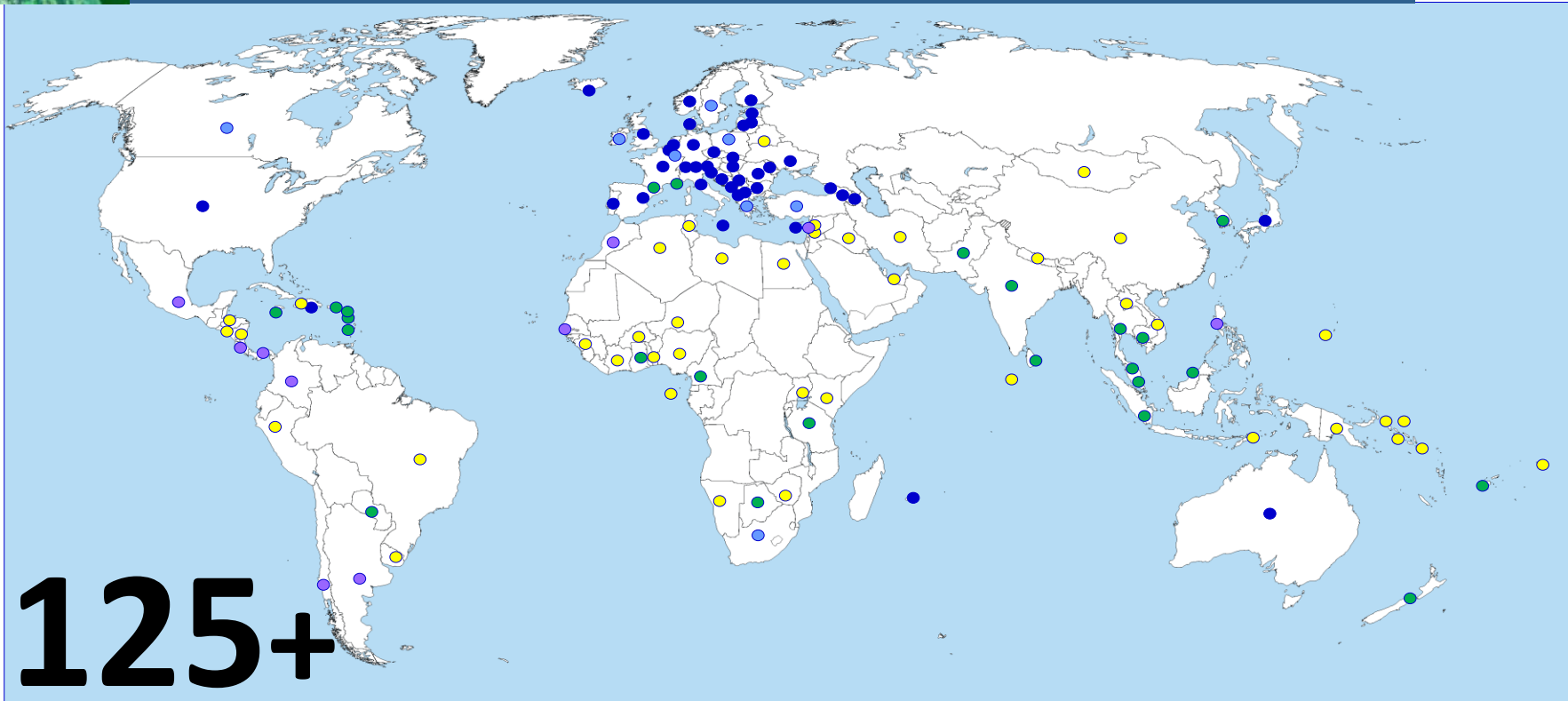
Fase 1:

- Un país con legislación vigente o en etapa avanzada
- Carta del Gobierno al Consejo de Europa expresando su interés de adhesión
- Consultas (CoE/Partes) sobre la decisión de invitar
- Invitación a acceder

Fase 2:

- Procedimiento nacional (e.g. decisión del Parlamento nacional)
- Depósito del instrumento de adhesión

Reach of Budapest Convention



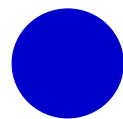
Indicative map only

Ratified/acceded: 42

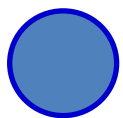
Signed: 11

(incl. 5 EU m/s)

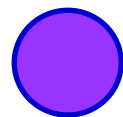
**Invited to accede: 9
= 62**



**Other States with laws/draft laws largely
in line with Budapest Convention = 20**



**Further States drawing on Budapest
Convention for legislation = 43+**



Partes:

- Estados europeos
- Australia
- República Dominicana
- Japón
- Mauricio
- Panamá
- EUA

Firmada:

- Canadá
- Sudáfrica
- Países europeos

Invitados a acceder:

- Argentina
- Chile
- Colombia
- Costa Rica
- Israel
- México
- Marruecos
- Filipinas
- Senegal

COE approach on cybercrime

1 Elaborar normas : Convenio de Budapest

2 Supervisar el cumplimiento:
Cybercrime
Convention
Committee (T-CY)

“Protecting you
and your rights
in cyberspace”

3 Capacity building:
C-PROC ►
Cooperación técnica



Convención de Budapest: impacto

- **Proceso de reformas legislativas en todo el mundo**
- **Más medidas en justicia penal**
- **Mas confianza y cooperación entre las partes**
- **Alcance global, impacto global: 56 países ratificados, firmados, invitados a acceder. Cooperación con 50 países más por lo menos**
- **Catalizador para creación de capacidad**
- **Mayor certeza legal y confianza del sector privado**
- **Un elemento esencial de normas de conducta para el ciberespacio**
- **Contribución a los derechos humanos y el estado de derecho en el ciberespacio**
- **Protección personal y de sus derechos**

Beneficios

- ✓ Cooperación confiable y eficiente con otras Partes
- ✓ Participación en el Comité de la Convención para la Ciberdelincuencia (T-CY)
- ✓ Participación en establecimientos futuros de normas (Notas de Guía, Protocolos y otras adiciones a la Convención de Budapest)
- ✓ Mayor confianza del sector privada
- ✓ Asistencia técnica y creación de capacidad

“Costo”: Compromiso de cooperar

¿Desventajas?

Taller sobre la Legislación en Materia de Ciberdelincuencia

Adhesión al Convenio de Budapest: opciones y reservas permitidas

Mecanismos de Vinculación

Capítulo IV

- Firma sujeta a Ratificación
- Adhesión

FIRMA - RATIFICACIÓN (Artículo 36)

El Convenio está abierto a la firma de los Estados miembros del COE y de los Estados no miembros del COE, que hayan participado en su elaboración:

- ☐ Canadá
- ☐ Japón
- ☐ Sudáfrica
- ☐ Estados Unidos de América

FIRMA - RATIFICACIÓN (Artículo 36)

- Estados miembros:

45 firmas / 36 ratificaciones

- Estados no miembros:

4 firmas / ratificación de Japón y EUA

ADHESIÓN (Artículo 37)

Los Estados no miembros del COE y que no hayan participado en su elaboración, pueden adherirse al Convenio, por invitación del Comité de Ministros del COE, una vez que el Convenio haya entrado en vigor.

- 4 adhesiones: Australia, Mauricio, Panamá y República Dominicana

Definición de Adhesión:

Convención de Viena sobre el Derecho de los Tratados:

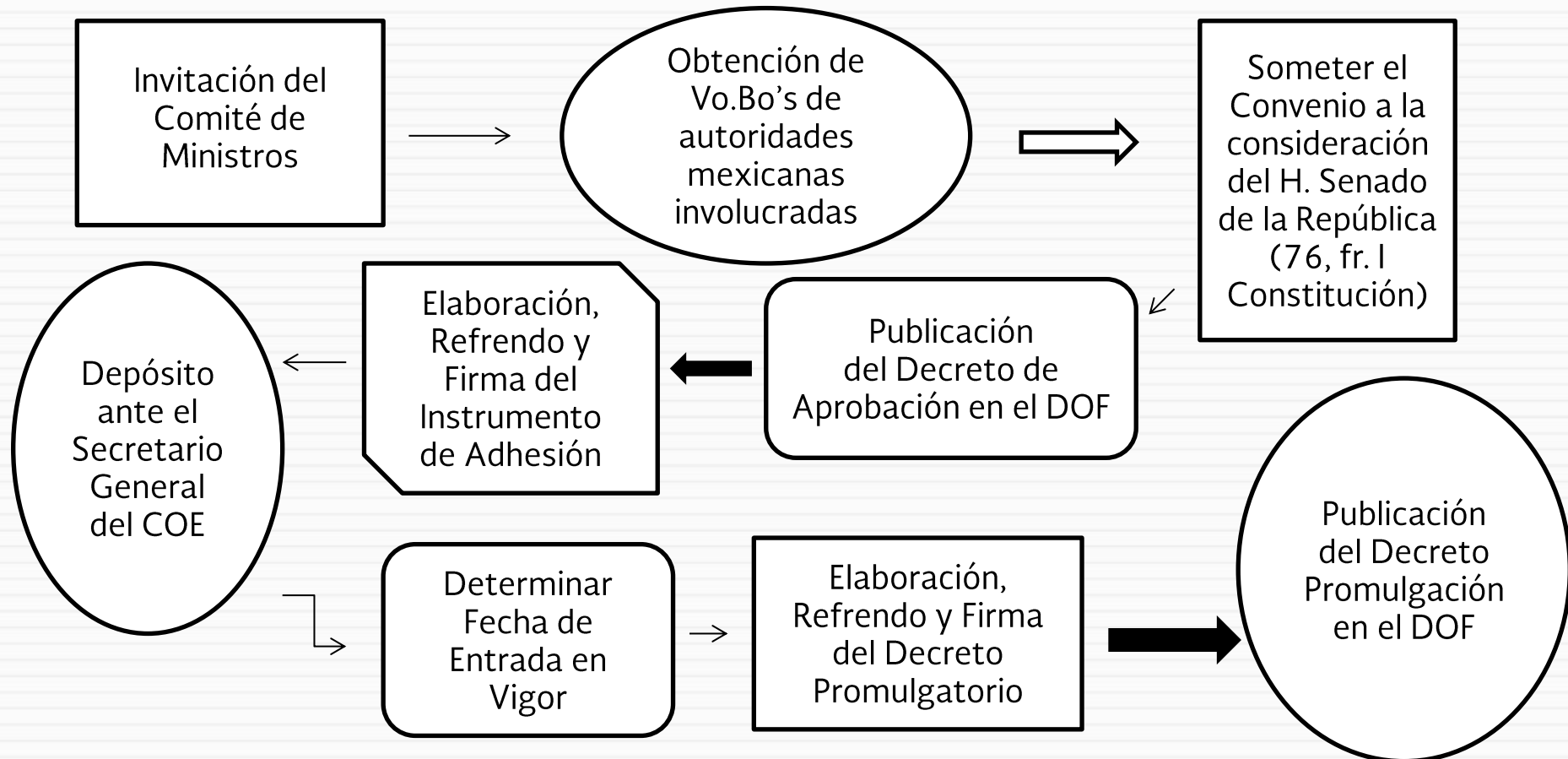
“el acto internacional así denominado por el cual un Estado hace constar en el ámbito internacional su consentimiento en obligarse por un tratado”

Opción de Vinculación para México

Adhesión

- No es Estado miembro del COE
- No participó en la negociación del Convenio

Proceso de Vinculación de México



RESERVAS

Definición

“declaración unilateral, cualquiera que sea su enunciado o denominación, hecha por un Estado o por una organización internacional al firmar, ratificar, aceptar o aprobar un tratado o al adherirse a él, con objeto de excluir o modificar los efectos jurídicos de ciertas disposiciones del tratado en su aplicación a ese Estado o a esa organización”

Convenio de Budapest

Artículo 42, admite reservas sobre los Artículos:

- Artículo 4, párrafo 2
- Artículo 6, párrafo 3
- Artículo 9, párrafo 4
- Artículo 10, párrafo 3
- Artículo 11, párrafo 3
- Artículo 14, párrafo 3
- Artículo 22, párrafo 2
- Artículo 29, párrafo 4
- Artículo 41, párrafo 1

Artículo 4 – Ataques a la Integridad de Datos

Obligación de tipificar como delito los actos deliberados e ilegítimos que dañen, borren, deterioren, alteren o supriman datos informáticos.

RESERVA: Posibilidad de exigir que tales actos causen daños graves

Artículo 6 – Abuso de los Dispositivos

Obligación de tipificar como delito la producción, venta, obtención para uso, importación o difusión de dispositivos o contraseñas para acceder a sistemas informáticos con el propósito de cometer un ilícito.

RESERVA: Posibilidad de no aplicar esta disposición, en la medida que no afecte a la venta, distribución o disposición de tales dispositivos o contraseñas.

Artículo 9 – Pornografía Infantil

RESERVA:

No tipificar como delito las siguientes conductas:

- Hacerse de pornografía infantil para si mismo o para otros a través de un sistema informático
- Poseer pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos

No incluir en la definición de “pornografía infantil”, el material que contenga la representación visual de:

- una persona que parezca ser un menor comprometida en una conducta sexualmente explícita
- imágenes realistas que representen a un menor comprometido en una conducta sexualmente explícita.

Solicitar un límite de edad inferior de 18 años, que no sea menor a 16 años

Artículo 10 – Derechos de Propiedad Intelectual

RESERVA: Posibilidad de no tipificar como delito las infracciones de la propiedad intelectual y derechos conexos, siempre que existan otros recursos efectivos para proteger tales derechos y no se vulneren las obligaciones internacionales de las Partes conforme a los tratados que le sean vinculantes en la materia.

Artículo 11 – Tentativa y Complicidad

RESERVA: Posibilidad de no establecer como delito, la tentativa deliberada de cometer los delitos de interceptación ilícita de datos, interferencia de datos, interferencia de sistema, delitos relacionados con los dispositivos y delitos relacionados con la pornografía infantil.

Artículo 14 –Disposiciones de Procedimiento

RESERVA: Posibilidad de aplicar las medidas mencionadas en el Artículo 20 (obtención de datos informáticos en tiempo real), únicamente en el caso de los delitos o categoría de delitos que se especifiquen en la reserva, y en la medida que el rango de esos delitos no sea más restringido que el de los delitos a los que se aplique las medidas del Artículo 21 (interceptación de datos relativos al contenido).

Artículo 22 – Jurisdicción

RESERVA: Posibilidad de no aplicar o aplicar, en casos o circunstancias específicas, su jurisdicción sobre los delitos cometidos a bordo de un buque de su bandera o aeronave registrada bajo sus leyes, en caso de ser cometido por uno de sus nacionales, siempre que el delito sea punible penalmente en el lugar en el que se cometió o si el delito fue cometido fuera de la jurisdicción territorial de algún Estado.

Artículo 29 – Conservación de Datos Informáticos

RESERVA: Posibilidad de solicitar una doble tipificación penal, como condición para responder a una solicitud de asistencia para la búsqueda o acceso similar, embargo o aseguramiento similar, o revelar los datos almacenados, en relación con delitos distintos de los previstos en los Artículos 2 a 11 del Convenio, en los casos en que existan razones para creer que la condición de la doble tipificación penal no se cumplirá al momento de revelar los datos.

Artículo 41 – Cláusula federal

RESERVA: Posibilidad para un Estado federal de reservarse el derecho de contraer obligaciones por virtud de las medidas a ser adoptadas a nivel nacional, siempre que éstas sean consistentes con los principios fundamentales que rigen la relación entre el gobierno central y los estados que lo constituyen u otras entidades territoriales similares, y con la condición de que pueda seguir cooperando internacionalmente.

Registro de Reservas

Diversos países han formulado RESERVAS al Convenio. Sin embargo, el Secretario General del COE realiza consultas periódicas a los Estados Contratantes que las formularon, exhortándolos a retirar las mismas y lograr, con ello, un cumplimiento más eficaz del Convenio.

Posición de México

De conformidad con el proceso de consultas sostenido, hasta el momento, a nivel interno, México no tiene contemplado formular reservas al Convenio de Budapest, al momento de formalizar su adhesión al mismo.

El Gobierno de México realiza -en paralelo- la armonización legislativa necesaria, para dar cabal cumplimiento a sus disposiciones.

Taller sobre legislación en materia de ciberdelincuencia en América Latina

Palabras de bienvenida a cargo del Subsecretario para Asuntos
Multilaterales y Derechos Humanos, Emb. Juan Manuel Gómez –
Robledo Verduzco

-1º de abril de 2014-

Señoras y señores legisladores, comisionados de órganos autónomos, fiscales, policías y funcionarios participantes en este Taller sobre legislación en materia de ciberdelincuencia en América Latina;

Señor Secretario Ejecutivo del Comité del Convenio sobre la Ciberdelincuencia, señores expertos del Consejo de Europa que le acompañan;

Señoras y señores miembros de las asociaciones de internet y tecnologías de la información, y de instituciones de educación superior e investigación;

Señoras y señores miembros del Cuerpo Diplomático;

Colegas y amigos:

Es un honor para la Secretaría de Relaciones Exteriores ser sede de este importante evento, como co-organizadora del mismo junto con la Coordinación de Estrategia Digital Nacional, la Procuraduría General de la República, y el Consejo de Europa. Y es, desde luego, un gusto dar a ustedes la bienvenida, a nombre del Gobierno de México y del

Canciller José Antonio Meade Kuribreña en particular, a este segmento regional del Taller sobre legislación en materia de ciberdelincuencia en América Latina.

El proceso de adhesión de México al Convenio sobre la Ciberdelincuencia, del Consejo de Europa -si bien pasa por las competencias sustantivas, tecnológicas y procesales de diversas instancias mexicanas de procuración de justicia, seguridad de la información y telecomunicaciones, así como del Congreso de la República, de todas las cuales esta Cancillería es respetuosa- tiene una innegable dimensión de política exterior.

Como es del dominio público, como uno de sus ejes esenciales de política el Gobierno del Presidente Enrique Peña Nieto pugna por un México globalmente responsable. Un México que, a la par de contribuir activamente a la construcción de la arquitectura mundial del Siglo XXI y a las mejores causas de la humanidad, fomente la cooperación internacional para un México en paz, incluyente y con educación de calidad. Un México que, a la vez, reciba y comparta las mejores prácticas en beneficio del desarrollo en plano de igualdad soberana.

El proceso de adhesión al Convenio sobre la Ciberdelincuencia, adoptado en Budapest en el 2001, se encuadra, naturalmente, en cada uno de estos parámetros. Con 42 Estados Parte y 11 signatarios pendientes de ratificación se trata, al momento, del único acuerdo internacional jurídicamente vinculante en materia de combate a la ciberdelincuencia, abierto a la adhesión de todos los países interesados previa invitación del Comité de Ministros del Consejo de Europa.

En virtud del equilibrio que guardan sus disposiciones entre las legítimas actividades de aplicación de la ley, por una parte, y las justas salvaguardias de los derechos humanos y la protección de datos en una sociedad democrática, por otra parte, para México el Convenio de Budapest representa un referente obligado en los esfuerzos de la comunidad internacional en pro del fortalecimiento del Estado de derecho en el ciberespacio. Esfuerzos que, en el sentir de México, pueden y deben desarrollar y fortalecer progresivamente, pero bajo ningún pretexto menoscabar los referidos estándares consagrados en el propio convenio.

Este proceso de adhesión significa una asignatura pendiente del Estado Mexicano, en su carácter de país con estatuto de Observador ante el Consejo de Europa desde 1999, y de invitado a adherirse al Convenio de Budapest desde el 2007. Sobre la base de la reforma constitucional en materia de telecomunicaciones, del lanzamiento presidencial de la Estrategia Digital Nacional, y de la experiencia adquirida por México en el seno del Comité Especializado en Seguridad de la Información del Consejo de Seguridad Nacional, este ejercicio representa, además, una oportunidad de evaluar y sintonizar la normatividad interna con las tendencias internacionales, tanto como de compartir nuestras mejores prácticas en este ámbito.

La cooperación internacional contra la ciberdelincuencia, al amparo del Convenio de Budapest, ciertamente fortalecerá la protección de la niñez y la juventud contra deleznable ataques a su integridad en el internet; pero también, la certidumbre jurídica esencial para fomentar

las transacciones financieras y comerciales, la prestación de servicios y las oportunidades educativas en línea.

La adhesión permitirá a México, adicionalmente, sumarse de pleno derecho a las deliberaciones sobre la pertinencia de un protocolo adicional en materia de acceso a datos transfronterizos; deliberaciones que son, en sí, ilustrativas de la problemática más amplia del ejercicio de jurisdicción en el ciberespacio bajo las normas del derecho internacional.

El hecho de que República Dominicana y Panamá sean ya parte en el Convenio de Budapest; que Argentina, Chile, Colombia y Costa Rica asimismo hayan sido invitados a adherirse; que Paraguay y Perú hayan manifestado su interés en incorporarse; y que la Organización de Estados Americanos favorezca la armonización de las leyes de sus miembros en concordancia con el acuerdo europeo, no hacen sino subrayar los beneficios de este Convenio para la región latinoamericana.

Al inaugurar el presente taller no me resta sino hacer votos por que cumpla su propósito de apoyar los procesos de armonización de la legislación y de adhesión al Convenio sobre la Ciberdelincuencia por México y los países hermanos mencionados anteriormente.

Quisiera, también, dejar constancia del reconocimiento de la Subsecretaría para Asuntos Multilaterales y Derechos Humanos:

- Al Secretariado del Comité del Convenio de Budapest;
- A la Coordinación de Estrategia Digital Nacional;
- A la Procuraduría General de la República;

- A la Comisión Nacional de Seguridad – División Científica de la Policía Federal de la Secretaría de Gobernación;
- A toda la membresía y al Secretario Técnico del Comité Especializado en Seguridad de la Información, del Consejo de Seguridad Nacional;
- A la Oficina de México ante el Consejo de Europa;
- A la Oficialía Mayor y las Direcciones Generales de Tecnologías de la Información e Innovación, y de Coordinación Política de esta Cancillería.

Todas ellas contribuyeron en sus respectivos ámbitos a hacer posible este encuentro.

Agradezco igualmente a todos ustedes por su respuesta y participación, que sin duda enriquecerá las deliberaciones en torno de esta rama emergente del derecho nacional e internacional.

La amenaza del cibercrimen y el desafío de las evidencias electrónicas



Taller sobre Legislación en materia de Ciberdelincuencia en América Latina

Ciberdelincuencia

Conducta delictiva sancionada por los distintos códigos penales de nuestro país, que utiliza como fin o medio sistemas de comunicación, procesamiento y almacenamiento de datos.

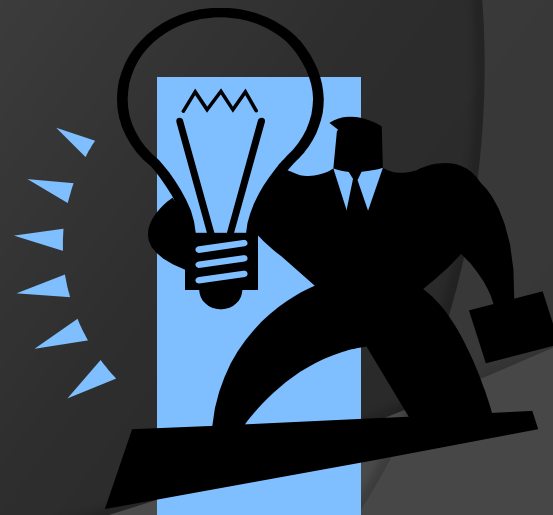


Taller sobre Legislación en materia de Ciberdelincuencia en América Latina

OBJETIVO DE LOS CIBERDELINCUINTES



**Obtención de beneficios
políticos, económicos y
sociales.**



Taller sobre Legislación en materia de Ciberdelincuencia en América Latina

Víctima potencial

Origen: Escuela, Amigos
Trabajo.

Causa: Ignorancia
Negligencia
Moda



Impacto: > 45 millones de usuarios de Internet.
> 20 millones de usuarios bancarizados.
\$39 000 millones en el 2013.
\$4 381.00 pesos por víctima.

Medio de acceso

www

Mensajería instantánea

Correo electrónico

Redes sociales

Telefonía Celular

Riesgos y amenazas

- Distribución de códigos maliciosos.
- Robo de información.
- Acceso a sitios inseguros.
- Acceso a información falsa.
- Distribución de pornografía.
- Depredadores sexuales
- Acoso.
- Extorción.
- Fraude. (spam, phishing)
- Suplantación de personalidad.
- Secuestro.
- Sabotaje (negación de servicios)
- Venta de obras protegidas.
- Venta de sustancias prohibidas

Taller sobre Legislación en materia de Ciberdelincuencia en América Latina

Desafío de las evidencias electrónicas



Fraudes Financieros



Redes sociales
como medio



Trata de personas

Bulling o acoso



Investigación
Eficaz



Leyes

Sabotaje y espionaje



Procesos en la Investigación

Solicitud
de Intervención

➤ Procesamiento del lugar de los hechos

Identificación

Fijación y
Aseguramiento

Embalaje y
Preservación

➤ Procesamiento de la
posible evidencia

Preservación

Procesamiento

➤ Emisión de
resultados

Análisis

Conclusiones

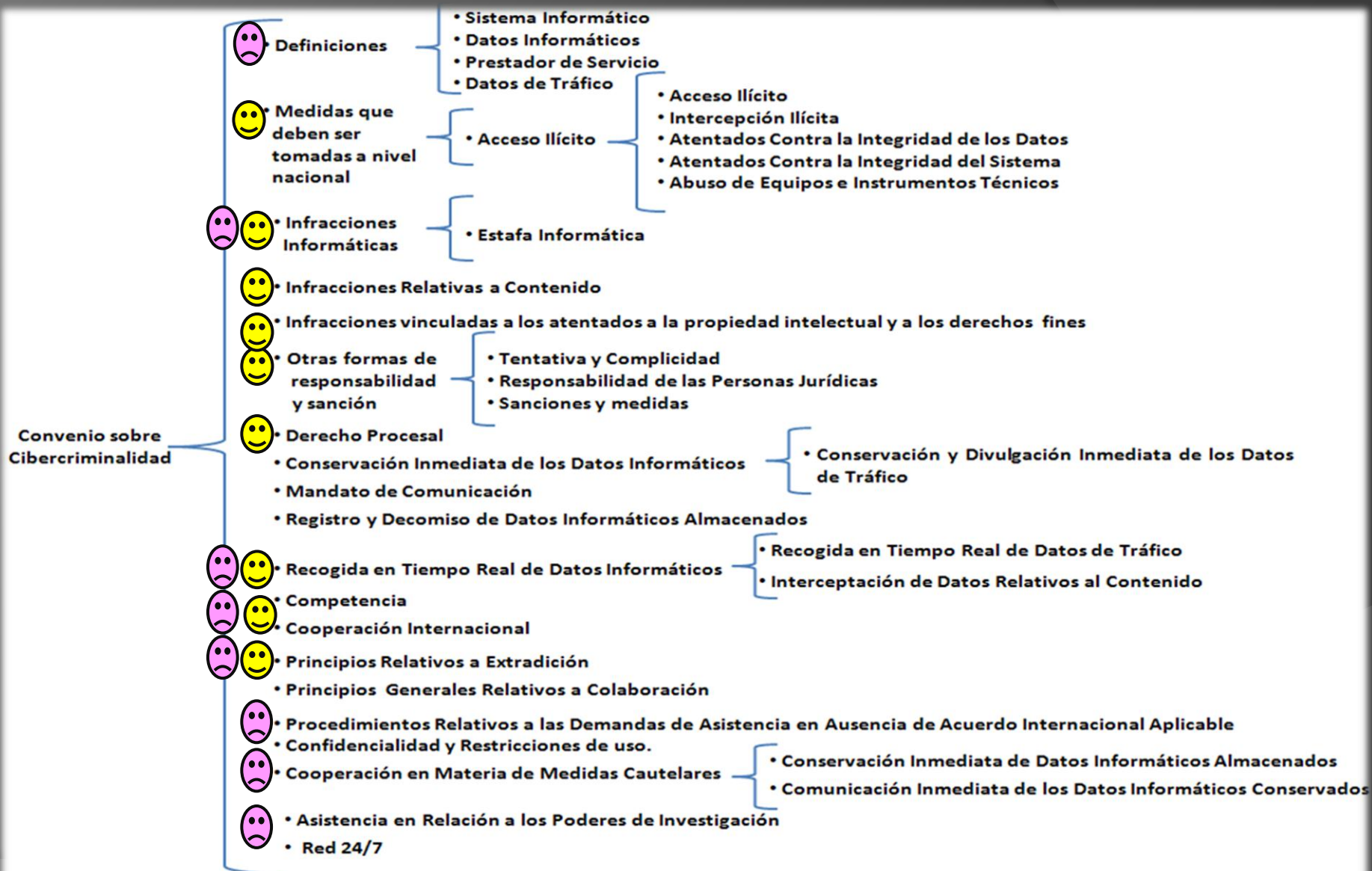
Integración
de la Investigación

Cadena de Custodia

Código Penal Federal

- **Espionaje Art 127 al 129**
(Códigos maliciosos, ingeniería social, intervención de comunicaciones)
- **Rebelión Art 133 al 135** (Páginas WEB, Comunicaciones Móviles)
- **Terrorismo Art 133 a 135** (Códigos maliciosos, páginas WEB, Comunicaciones móviles)
- **Sabotaje Art 140**
(Códigos maliciosos, ingeniería social, Accesos no autorizados)
- **Conspiración Art 141**
(Difusión a través de Internet y dispositivos móviles)
- **Delitos en materia de vías de comunicación Art 167 a 168**
(Códigos maliciosos, intervención de comunicaciones, decodificación de comunicaciones)
- **Violación de correspondencia Art 173, 176, 177**
(Códigos maliciosos, intervención de comunicaciones, decodificación de comunicaciones)
- **Delitos contra la salud Art 193 y 194** (Difusión a través de Internet y dispositivos móviles)
- **Corrupción de personas Art 200, 202, 202 bis** (Difusión a través de Internet y dispositivos móviles)
- **Trata de personas Art 205, 206 bis**
(Difusión a través de Internet y dispositivos móviles)
- **Revelación de secretos Art 210, 211, 211 bis** (códigos maliciosos, ingeniería social, redes bot)
- **Accesos no autorizados a sistemas de cómputo Art 211 bis 1 al 211 bis 7**
(Códigos maliciosos, ingeniería social, redes bot)
- **Falsedad Art 234 al 246**
(Falsificación de documentos a través de software y hardware, Phishing, distribución a través de Internet y dispositivos móviles)
- **Delitos contra la paz y seguridad de las personas (amenazas) Art 282 y 283**
(Correo electrónico, mensajería instantánea, mensajes escritos, telefonía móvil)
- **Homicidio Art 302** (Códigos maliciosos, , redes informáticas , sistemas informáticas)
- **Robo Art 367, 368** (Códigos maliciosos, ingeniería social, redes informáticas, sistemas informáticos)
- **Fraude Art 286** (Phishing, pharming, ingeniería social, códigos maliciosos, redes bot)
- **Extorción Art 390** (Correos electrónicos, mensajería instantánea, mensajes de texto)
- **Operaciones con recursos de procedencia ilícita Art 400** (Fraudes financieros, páginas WEB, dispositivos móviles)
- **Delitos electorales Art 403, 405** (correos electrónicos, redes sociales, mensajería instantánea)
- **Delitos en materia de derechos de autor Art 424** (Códigos maliciosos, ingeniería social, redes bot)

Taller sobre Legislación en materia de Ciberdelincuencia en América Latina



Taller sobre Legislación en materia de Ciberdelincuencia en América Latina

PLANTEAMIENTO

- Metodología de Investigación
- Equipo Forense
- Capacitación constante
- Investigación alineada a la legislación

DICTAMEN

Muchas Gracias

M.T.I. Oscar Manuel Lira Arteaga
Director de Ingenierías y Telecomunicaciones
en Materia Forense
Coordinación General de Servicios Periciales

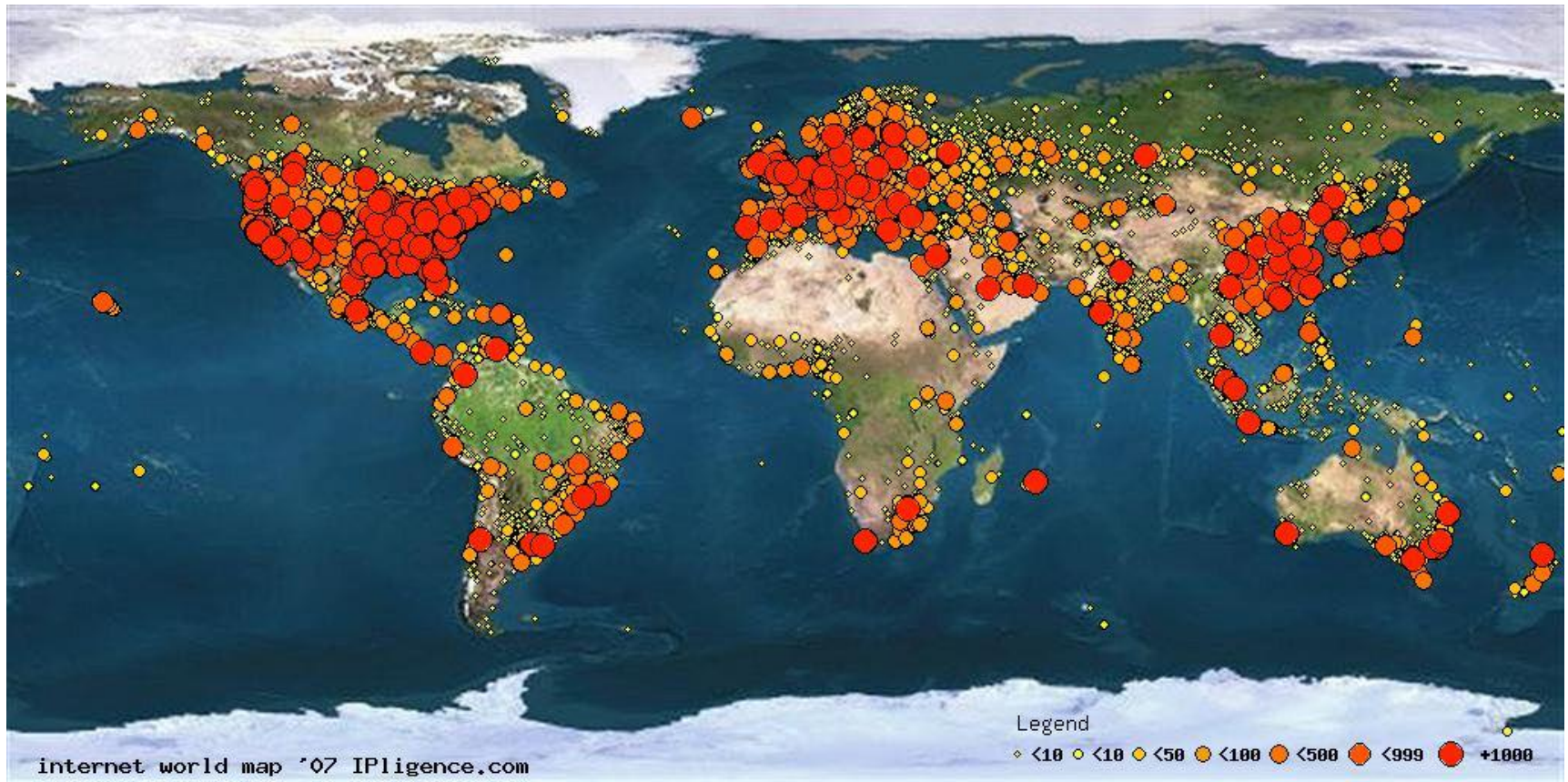


La ciberdelincuencia y pruebas electrónicas en el
Continente Americano :
la perspectiva de Estados Unidos



William Hall
Departamento de Justicia de Estados Unidos

¿Por qué tienen importancia los asuntos internacionales?



Número de direcciones IP en el lugar



Convertir los ataques a redes de cómputo en un delito

- ▶ Por lo general, “la criminalidad doble” es necesaria para que dos países cooperen en un asunto criminal en particular
- ▶ La criminalidad doble representa la base para:
 - ▶ Los tratados de extradición
 - ▶ Los Tratados de Asistencia Legal Mutua

Cómo superar la división de la criminalidad doble

- ▶ Un esfuerzo importante para lograrlo: Convención de Budapest sobre la Ciberdelincuencia
- ▶ Tres funciones principales:
 - ▶ Crea una base sustancial para criminalizar la ciberdelincuencia
 - ▶ Crea una base sustancial para recolectar y usar pruebas electrónicas
 - ▶ Sirve como la base para la asistencia legal mutua formal y requiere que los miembros proporcionen un punto de contacto 24/7 para comunicación internacional rápida e informal
- ▶ Los puntos en azul necesitan implementarse a través de sus leyes nacionales

La Convención de Budapest

- ▶ Es el único tratado internacional en vigencia diseñado para permitir que los países compartan pruebas y trabajen juntos en la investigación y procesamiento de la ciberdelincuencia
- ▶ Las leyes nacionales deben estar alineadas con las bases de la Convención de Budapest
- ▶ ¡CCIPS puede ayudar!

El problema de localizar e identificar a los delincuentes

- ▶ El paso primordial de la investigación es localizar la fuente del ataque o de la comunicación
 - ▶ Lo que ocurrió podría ser relativamente fácil de descubrir
 - ▶ Identificar a la persona responsable es muy difícil
- ▶ Se aplica a los delitos de piratería informática (hacking) y a otros facilitados por las redes de cómputo

Rastreo de una comunicación

- ▶ La infraestructura debe generar datos de tráfico
- ▶ Las compañías de comunicaciones / otros deben conservar datos suficientes para que el rastreo sea posible
- ▶ Las leyes y procedimientos deben permitir un acceso oportuno por las autoridades competentes que no envíe alertas al cliente
- ▶ La información debe compartirse con rapidez

Compartir las pruebas

- ▶ Los países deben mejorar su capacidad de compartir los datos *con rapidez*
- ▶ Si no se hace rápidamente, el “rastreo” electrónico desaparecerá
- ▶ Cuando las autoridades competentes reciben una solicitud, deben ser capaces de :
 1. Conservar todos los datos de tráfico nacional
 2. Notificar al país solicitante si el rastreo conduce a otro país
 3. Proporcionar datos suficientes al país solicitante para que pueda solicitar asistencia de otro país
 4. Los países deben ser capaces de hacer esto para otros con rapidez, las 24 horas del día y los 7 días de la semana.

Recolectar y compartir pruebas

- ▶ ¿Qué pruebas se recolectarán en un país que sean admisibles en los tribunales de otros?
- ▶ Posibilidad de problemas probatorios
 - ▶ Recolección de pruebas digitales
 - ▶ Rastreo de comunicaciones electrónicas en todo el mundo
 - ▶ Ciencias forenses de cómputo
- ▶ Los tratados actuales de asistencia legal mutua podrían no incluir pruebas electrónicas

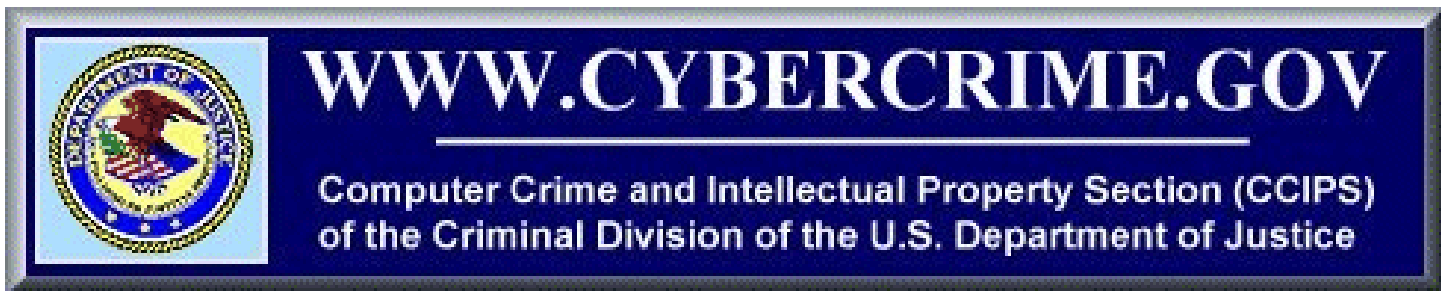
Red de Delincuencia de Alta Tecnología

24/7

- ▶ Un medio para conservar pruebas electrónicas
- ▶ Cincuenta y nueve (59) estados miembro en todo el mundo
- ▶ Todos los estados son invitados a unirse a esta red informal
- ▶ Detalles:
 - ▶ Un procurador o policía en cada estado miembro está disponible en todo momento para responder a solicitudes urgentes de otros estados miembro relacionadas con pruebas electrónicas
 - ▶ Las solicitudes a la red deben comunicarse en inglés
 - ▶ Las partes de la Convención de Budapest están obligadas a tener un punto de contacto y a conservar los datos cuando se les solicite
- ▶ CCIPS es el punto de contacto para Estados Unidos

Información de contacto

- ▶ Bill Hall, Abogado Litigante
- ▶ Correo electrónico: william.a.hall@usdoj.gov
- ▶ Teléfono de CCIPS : +1 202 514 1026 (general/trabajo)
- ▶ CCIPS en Internet:





Workshop on cybercrime legislation in Latin America
Mexico City
31 March (national workshop)
1 - 2 April 2014 (international workshop)

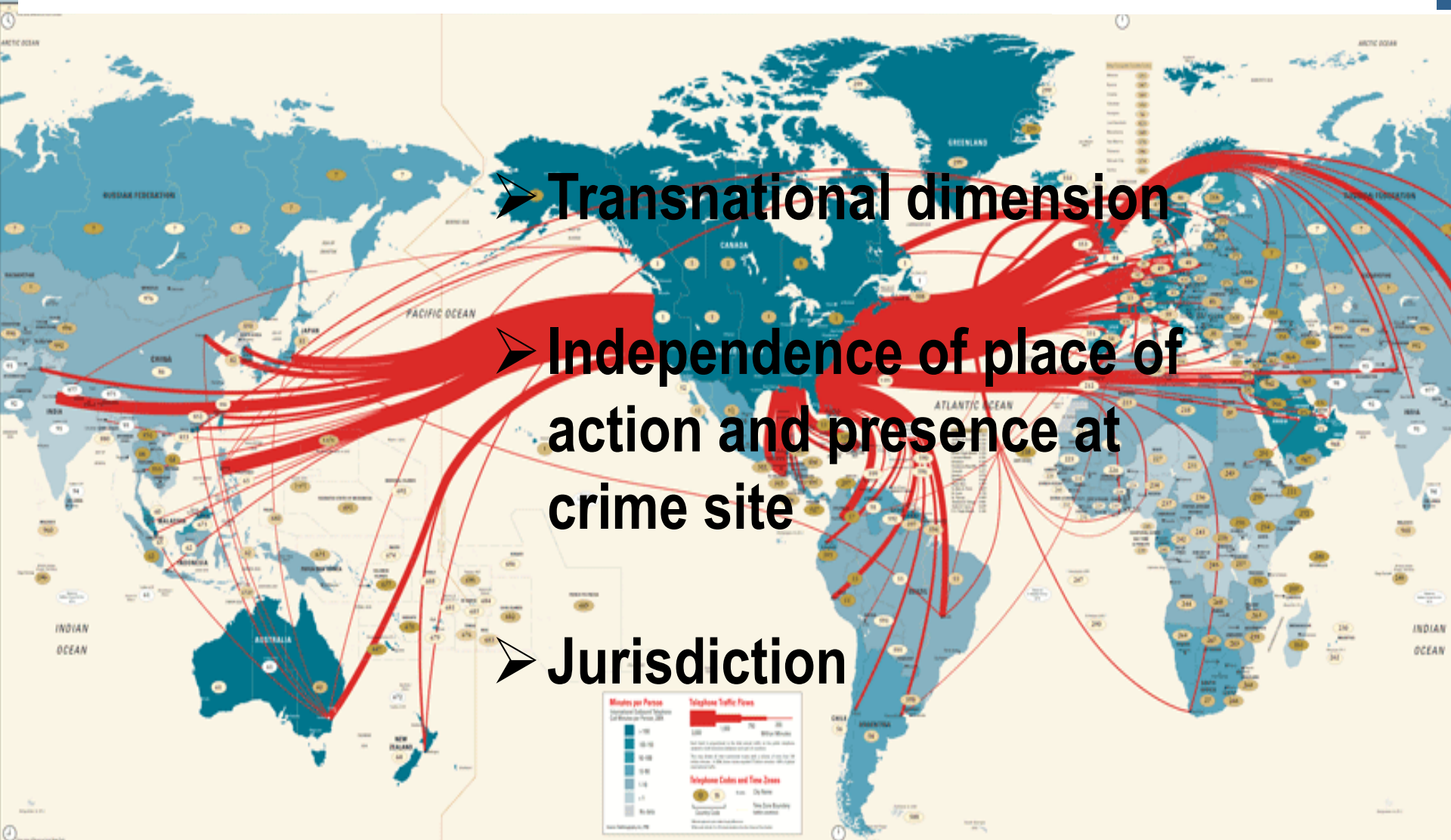
The Budapest Convention on Cybercrime

CONVENIO SOBRE LA CIBERDELINCUENCIA

Alexander.seger@coe.int

www.coe.int/cybercrime



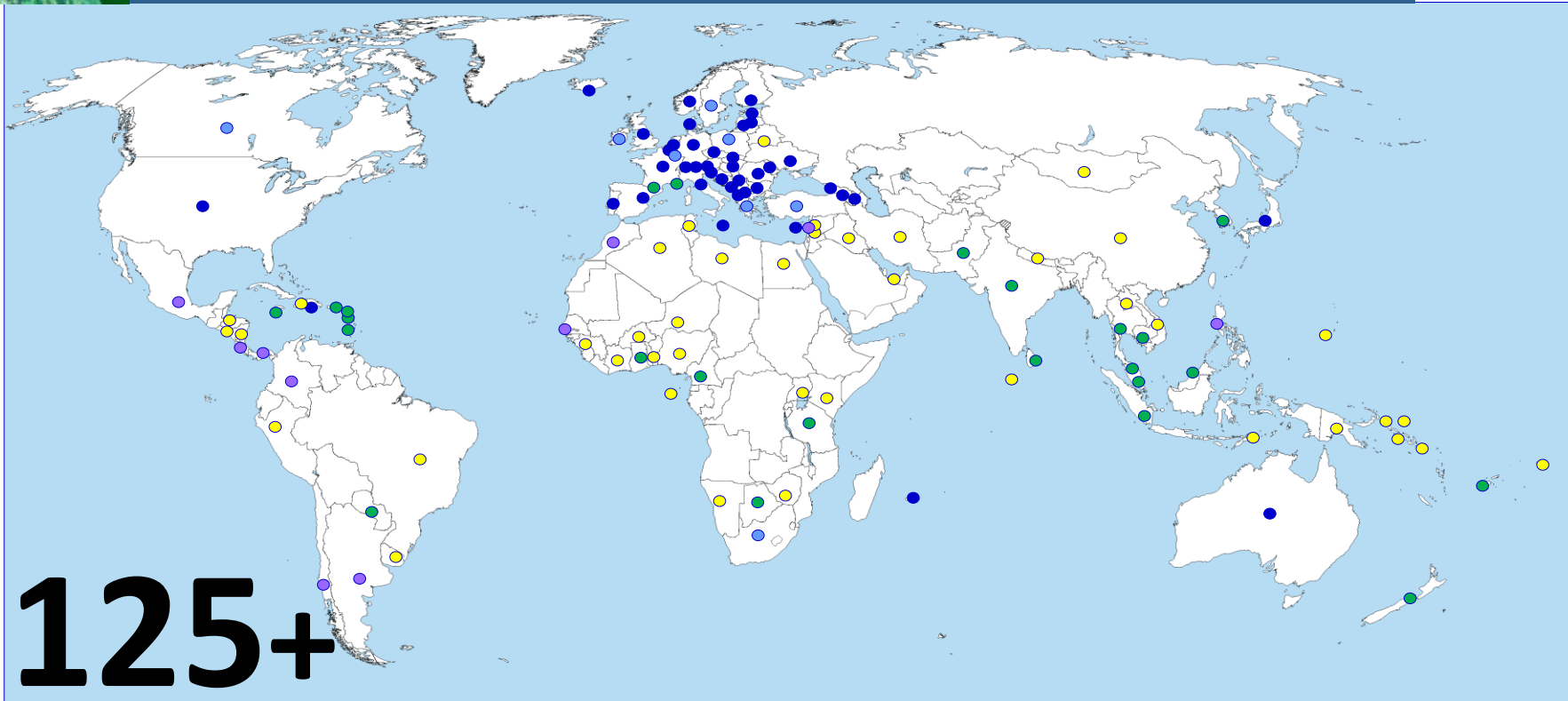


➤ Transnational dimension

➤ Independence of place of action and presence at crime site

➤ Jurisdiction

Reach of Budapest Convention



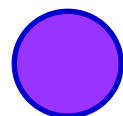
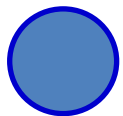
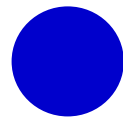
125+

Indicative map only

Ratified/acceded: 42

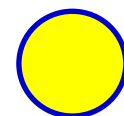
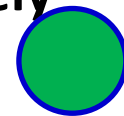
Signed: 11

Invited to accede: 9
= 62



Other States with laws/draft laws largely
in line with Budapest Convention = 20

Further States drawing on Budapest
Convention for legislation = 43+





Handheld Devices



Electronic evidence in relation to ANY crime

Sniffer - Local Ethernet (Line speed at 100 Mbps) - [http-syn-attack.cap : 2712 Ethernet frames]

File Monitor Capture Display Tools Database Window Help

No.	Status	Source Address	Dest Address	Summary
1	R	[10.1.0.8]	[10.1.0.1]	TCP: D=34 S=2360 87W 8EQ=277351 LEN=0 WIN=8192
2		[10.1.0.8]	[10.1.0.1]	TCP: D=38 S=2368 87W 8EQ=277393 LEN=0 WIN=8192
3		[10.1.0.8]	[10.1.0.1]	TCP: D=42 S=2376 87W 8EQ=277418 LEN=0 WIN=8192
4		[10.1.0.8]	[10.1.0.1]	TCP: D=36 S=2362 87W 8EQ=277366 LEN=0 WIN=8192
5		[10.1.0.8]	[10.1.0.1]	TCP: D=39 S=2370 87W 8EQ=277399 LEN=0 WIN=8192
6		[10.1.0.8]	[10.1.0.1]	TCP: D=43 S=2378 87W 8EQ=277426 LEN=0 WIN=8192
7		[10.1.0.8]	[10.1.0.1]	TCP: D=36 S=2364 87W 8EQ=277372 LEN=0 WIN=8192
8		[10.1.0.8]	[10.1.0.1]	TCP: D=40 S=2372 87W 8EQ=277405 LEN=0 WIN=8192
9		[10.1.0.8]	[10.1.0.1]	TCP: D=44 S=2380 87W 8EQ=277432 LEN=0 WIN=8192

Contents of the Budapest Convention

- 1. Derecho penal sustantivo**
- 2. Derecho procesal**
- 3. Cooperación internacional**

Budapest Convention: Derecho penal sustantivo



Article	Budapest Convention	
Art. 1	Definitions	Definiciones
Art. 2	Illegal access	Acceso ilícito
Art. 3	Illegal interception	Interceptación ilícita
Art. 4	Data interference	Ataques a la integridad de los datos
Art. 5	System interference	Ataques a la integridad del sistema
Art. 6	Misuse of devices	Abuso de los dispositivos

Budapest Convention: Derecho penal sustantivo

Article	Budapest Convention	
Art. 7	Computer-related forgery	Falsificación informática
Art. 8	Computer-related fraud	Fraude informático
Art. 9	Child pornography	Delitos relacionados con la pornografía infantil
Art. 10	IPR offences	Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
Art. 11	Attempt, aiding, abetting	Tentativa y complicidad
Art. 12	Corporate liability	Responsabilidad de las personas jurídicas
Art. 13	Sanctions and measures	Sanciones y medidas

Budapest Convention: Derecho procesal

Article	Budapest Convention	
Art. 14	Scope	Ámbito de aplicación de las disposiciones de procedimiento
Art. 15	Conditions and safeguards	Condiciones y salvaguardias
Art. 16	Expedited preservation	Conservación rápida de datos informáticos almacenados
Art. 17	Expedited preservation and partial disclosure of traffic data	Conservación y revelación parcial rápidas de los datos relativos al tráfico
Art. 18	Production order	Orden de presentación
Art. 19	Search and seizure	Registro y confiscación de datos informáticos almacenados
Art. 20	Real-time collection traffic data	Obtención en tiempo real de datos relativos al tráfico
Art. 21	Interception of content data	Interceptación de datos relativos al contenido
Art. 22	Jurisdiction	Jurisdicción

Artículo 15 – Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

Budapest Convention: Cooperación internacional



Article	Budapest Convention	Principios generales
Art. 23	General princip. (subsidiarity)	Principios generales relativos a la cooperación internacional
Art. 24	Extradition	Extradición
Art. 25	General rules	Principios generales relativos a la cooperación
Art. 26	Spontaneous information	Información espontánea
Art. 27	MLA in absence of treaty	Procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable
Art. 28	Confidentiality	Confidencialidad y restricciones de uso

Budapest Convention: Cooperación internacional

Article	Budapest Convention	Disposiciones específicas
Art. 29	Expedited preservation	Conservación inmediata de datos informáticos almacenados
Art. 30	Partial disclosure traffic data	Comunicación inmediata de los datos informáticos conservados
Art. 31	MLA accessing data	Asistencia concerniente al acceso a datos informáticos almacenados
Art. 32	Transborder access	Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso
Art. 33	MLA collection traffic data	Asistencia para la recogida en tiempo real de datos de tráfico
Art. 34	MLA interception content	Asistencia en materia de interceptación de datos relativos al contenido
Art. 35	24/7 point of contact	Red 24/7

Artículo 37 – Adhesión al Convenio

[el] Consejo de Europa podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo de Europa y que no haya participado en su elaboración

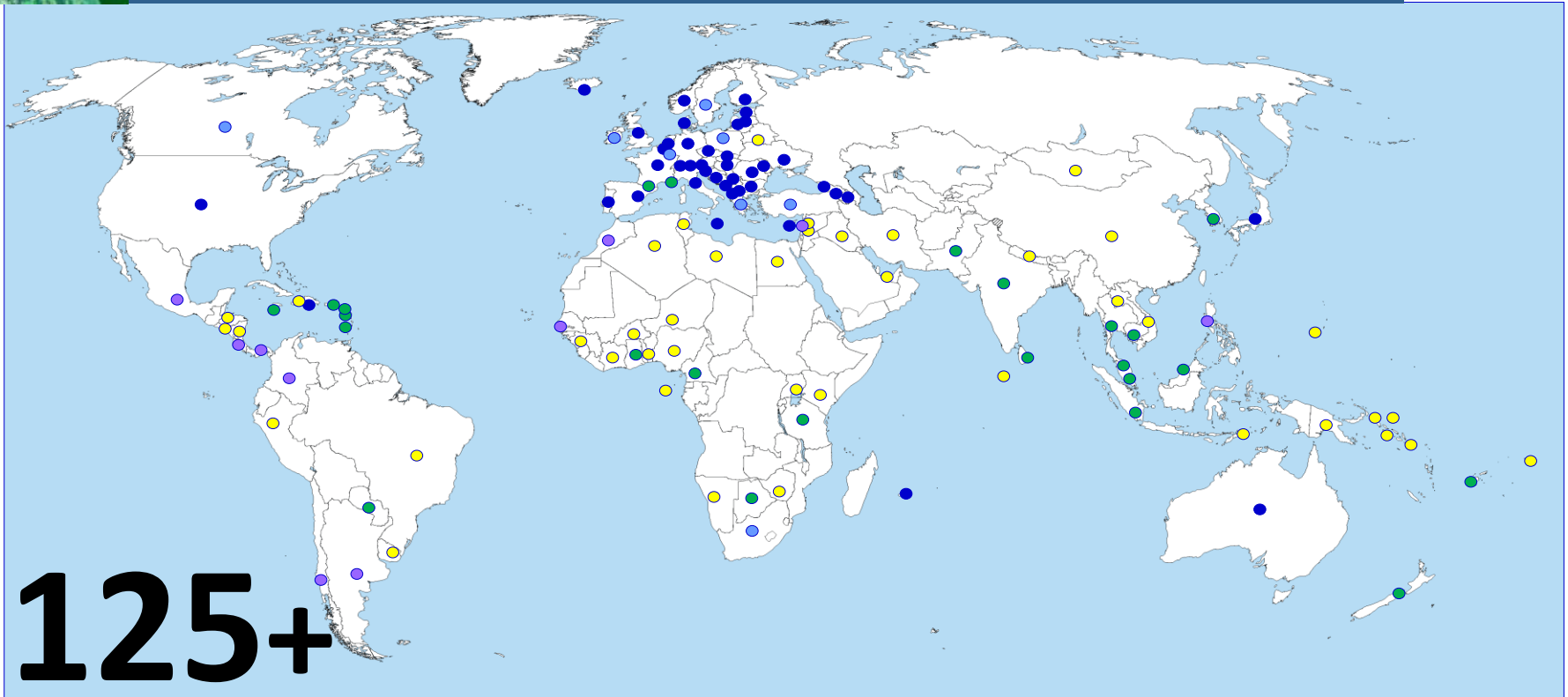
Phase 1:

- A country with legislation in place or advanced stage
- Letter from Government to CoE expressing interest in accession
- Consultations (CoE/Parties) in view of decision to invite
- Invitation to accede

Phase 2:

- Domestic procedure (e.g. decision by national Parliament)
- Deposit of the instrument of accession

Reach of Budapest Convention



125+

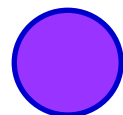
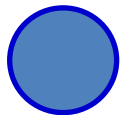
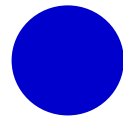
Indicative map only

Ratified/acceded: 42

Signed: 11

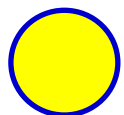
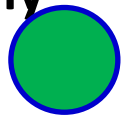
(incl. 5 EU m/s)

**Invited to accede: 9
= 62**



**Other States with laws/draft laws largely
in line with Budapest Convention = 20**

**Further States drawing on Budapest
Convention for legislation = 43+**



Parties/observers of Budapest Convention

Parties:

- **European States**
- **Australia**
- **Dominican Republic**
- **Japan**
- **Mauritius**
- **Panama**
- **USA**

Signed:

- **Canada**
- **South AFRICA**
- **European countries**

Invited to accede:

- **Argentina**
- **Chile**
- **Colombia**
- **Costa Rica**
- **Israel**
- **Mexico**
- **Morocco**
- **Philippines**
- **Senegal**

COE approach on cybercrime

1 Elaborar normas : Convenio de Budapest

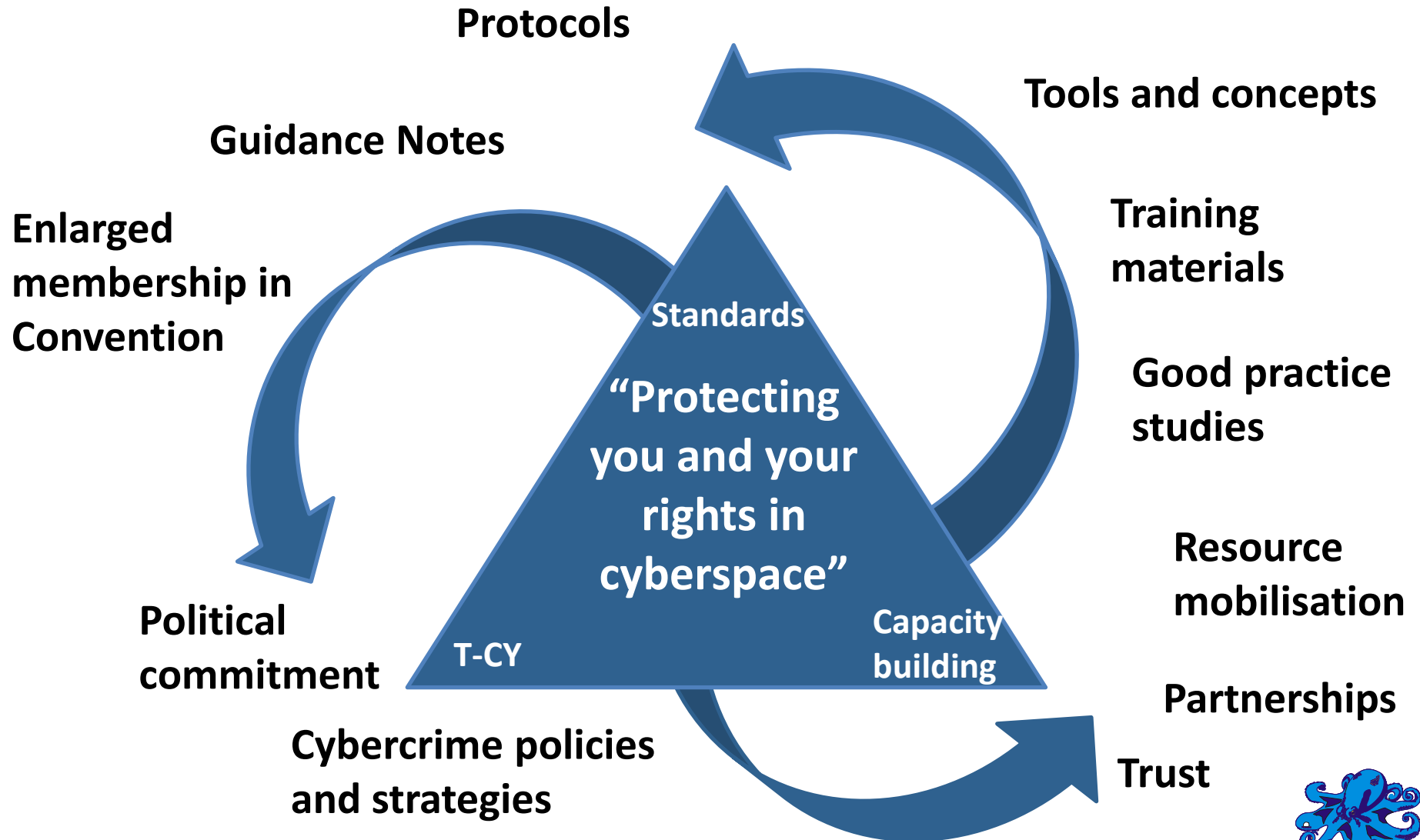
2 Supervisar el cumplimiento:
Cybercrime
Convention
Committee (T-CY)



3 Capacity building:
C-PROC ►

Cooperación técnica

A dynamic approach / un approche dynamique



Established under Article 46 Budapest Convention

Membership

(status March 2014):

- 42 Members (State Parties)
- 20 Observer States
- 10 International organisations (African Union Commission, ENISA, European Union, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

Functions:

- Assessments of the implementation of the Convention by the Parties
- Guidance Notes
- Draft legal instruments
- Etc.

2nd round of T-CY Assessments:

Efficiency of international cooperation provisions:

- **Article 31 on mutual assistance regarding accessing of stored computer data.**
- **And related Articles 23, 25, 26, 27, 28 and 35.**

Aim:

- **Better use of existing provisions**
- **Additional solutions**

Procedure and status:

- **Questionnaire February 2013.**
- **Plenary discussions June 2013 and December 2013.**
- **Revised report to be circulated for comments, consideration and adoption in [June] 2014.**

International requests for data

Types of data requested:

- 1. Subscriber information (80+%?)**
- 2. Traffic data**
- 3. Content data**

Underlying offences

- 1. Fraud and other financial crimes**
- 2. Violent and serious crime (murder, assault, trafficking, child abuse etc.)**
- 3. Offences against computer systems**

Preliminary findings/issues

- Good level of cooperation between Parties
- MLA process considered inefficient
- Insufficient use made of existing opportunities
- Limited cooperation in minor cases
- Possibilit of direct cooperation underused
- Stronger (supportive) role of 24/7 contact points in MLA process
- Cooperation with service providers
- Etc.

26 draft recommendations to be discussed by T-CY in June 2014

Budapest Convention: Impact

- **Process of legislative reforms worldwide**
- **Increased criminal justice measures**
- **Increased trust and cooperation between parties**
- **Global outreach, global impact: 56 countries ratified, signed, invited to accede. Cooperation with at least another 50 countries**
- **Catalyst for capacity building**
- **Increased legal certainty and trust by private sector**
- **An essential element of norms of behaviour for cyberspace**
- **Contribution to human rights and the rule of law in cyberspace**
- **Protecting you and your rights**

Benefits

- ✓ Trusted and efficient cooperation with other Parties
- ✓ Participation in the Cybercrime Convention Committee (T-CY)
- ✓ Participation in future standard setting (Guidance Notes, Protocols and other additions to Budapest Convention)
- ✓ Enhanced trust by private sector
- ✓ Technical assistance and capacity building

“Cost”: Commitment to cooperate

Disadvantages?

Substantive Provisions

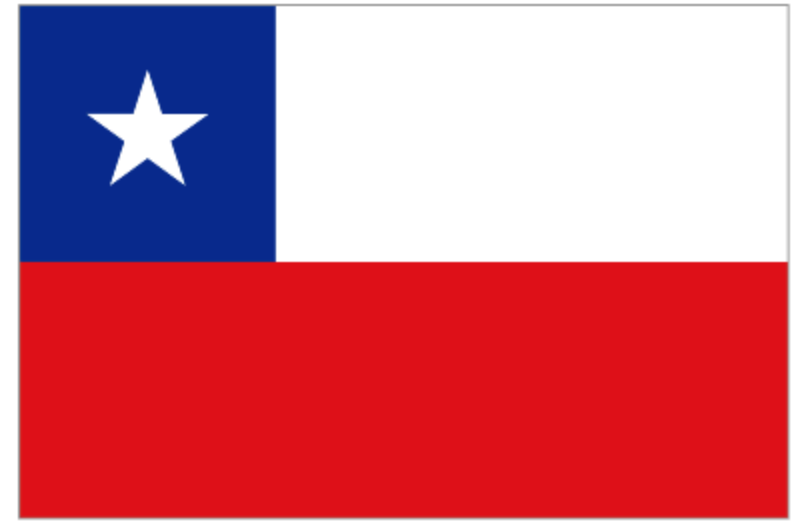
ARGENTINA

- Law 26388 (24 July 2008) - introduced “cybercrimes” in the Penal Code
- Section 128 of the Penal Code - child pornography



CHILE

- Penal Code
- Law 19223 (7 July 1993)



COLOMBIA

- Penal Code
- Law 1273 (5 January 2009) – amendments to the Penal Code
- Law 1336 (21 July 2009) – amendment to the Penal Code



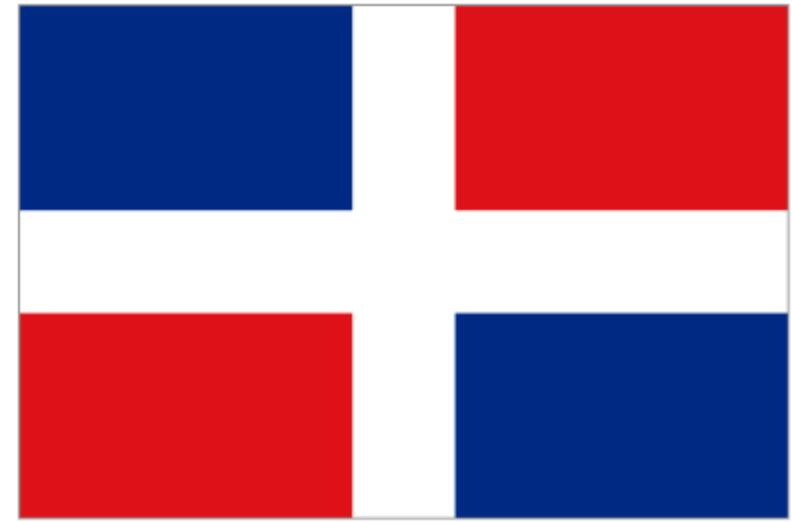
COSTA RICA

- Penal Code
- Law 7899 (3 August 1999)
- Law 8143 (5 November 2001)
- Law 8590 (18 July 2007)
- Law 9048 (10 July 2012)
- Law 9135 (24 April 2013)



DOMINICAN REPUBLIC

- Law 53/07 (16 January 2007)
- *Proyecto de Ley 1668 – spam and other cybercrimes*



MEXICO

- Federal Penal Code
- *Legislative intention on cybercrime and electronic evidence*



PANAMA

- Penal Code
- *Proyecto de Ley 653 (18 September 2013)*



PARAGUAY

- Penal Code
- Law 2861 (17 January 2006)
- Law 4439 (3 October 2011)



PERU

- Law 30096 (22 October 2013)
- Law 30171 (10 March 2014)





micitt

MINISTERIO
DE CIENCIA, TECNOLOGÍA
Y TELECOMUNICACIONES



Estado actual de la política pública y legislación sobre Ciberdelito en Costa Rica

Política, armonización y avances en
Costa Rica





I. Estructura Ministerial

Ministerio de Ciencia, Tecnología y
Telecomunicaciones

Viceministerio de
Telecomunicaciones

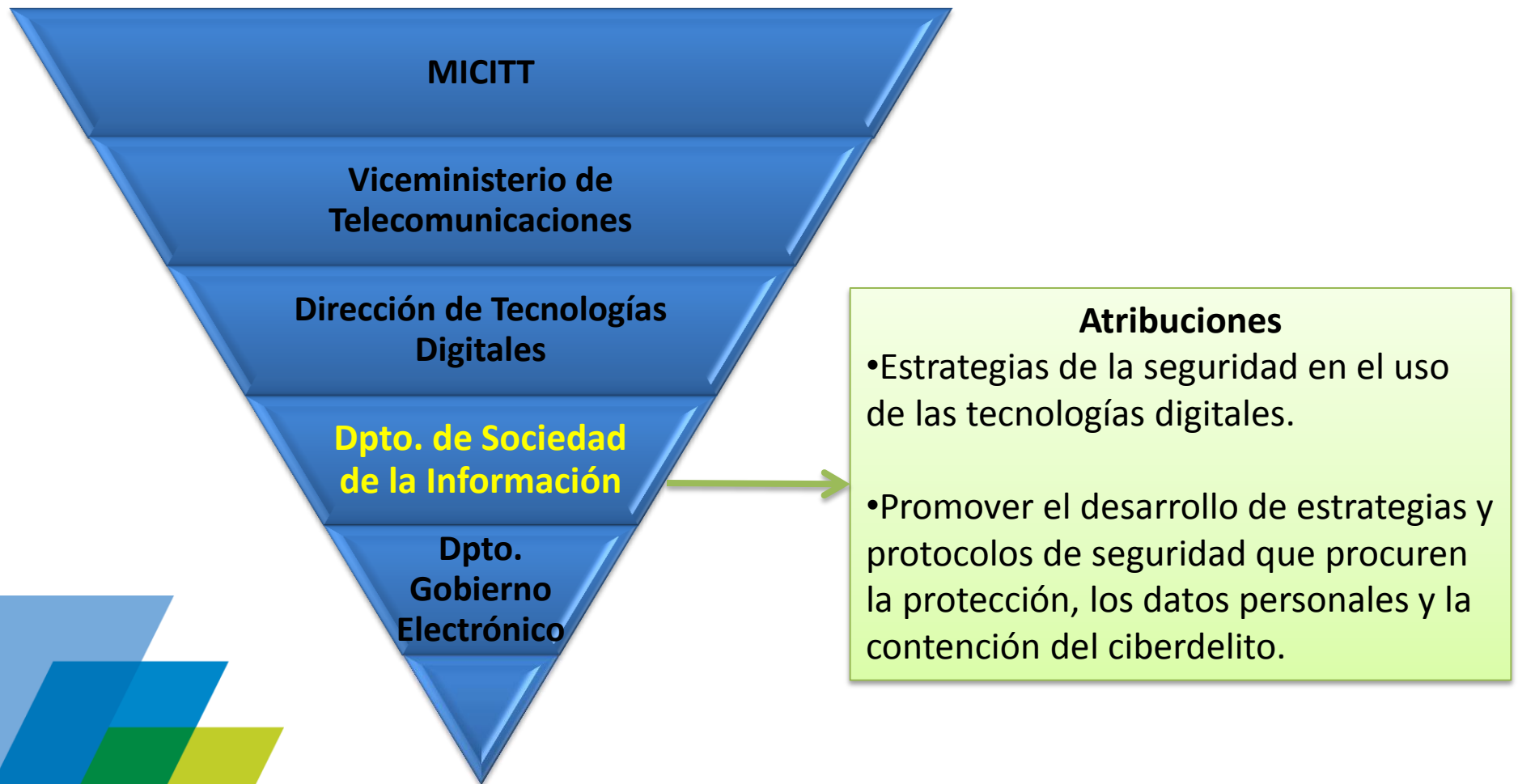


Nueva estructura Ministerial

- **Febrero 2014:** Decreto No. 38166-MICITT. Establece nueva organización del Viceministerio de Telecomunicaciones.
- Se crea la Dirección de Políticas Digitales y los Departamentos de Sociedad de la Información y Gobierno Electrónico.

Organización Ministerial y competencias

2014



Instrumentos de planificación Ministerial

Plan Nacional de Desarrollo



```
graph TD; A[Plan Nacional de Desarrollo] --> B[Plan Nacional de Ciencia, Tecnología e Innovación]; B --> C[Plan Nacional de Desarrollo de las Telecomunicaciones];
```

**Plan Nacional de Ciencia,
Tecnología e Innovación**

**Plan Nacional de Desarrollo de
las Telecomunicaciones**

Plan Nacional de Desarrollo de las Telecomunicaciones

- Establece una línea estratégica de Seguridad.
- **Objetivos:**
 1. Garantizar la seguridad física y lógica de las redes y servicios.
 2. Garantizar continuidad del servicio en casos de emergencia.

Plan Nacional de Desarrollo de las Telecomunicaciones



- **Metas:**

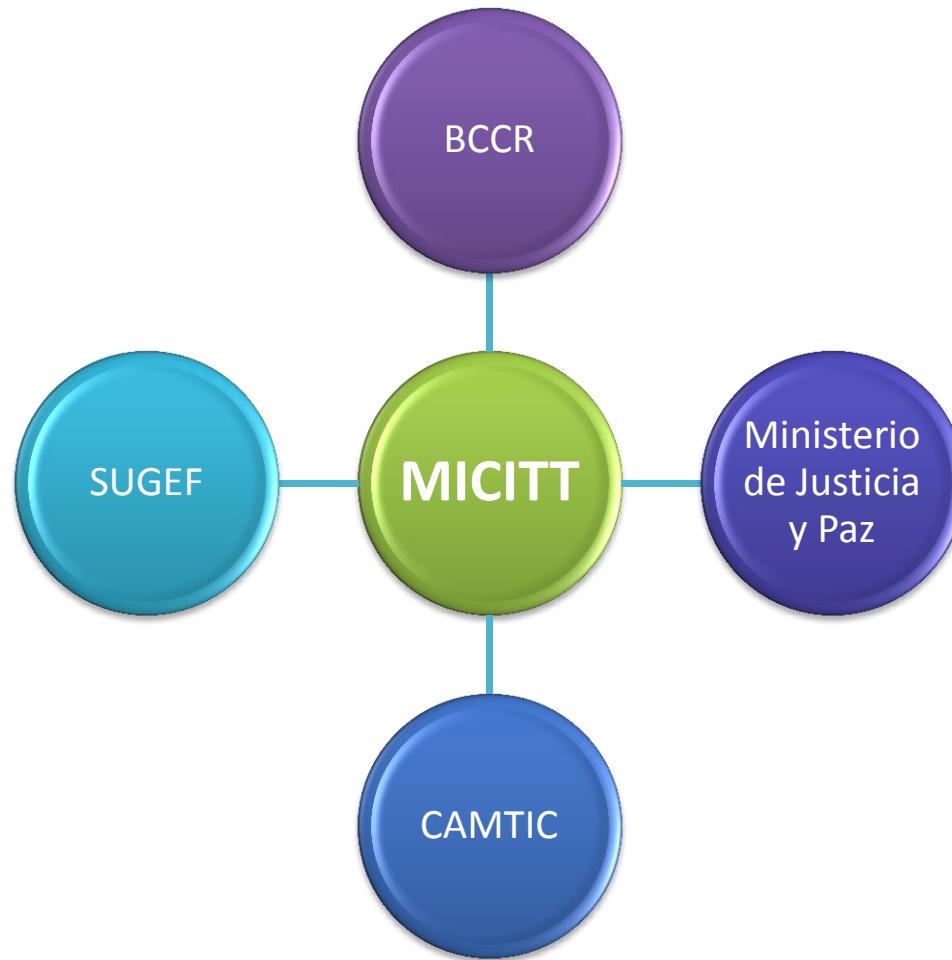
1. Crear un plan de continuidad de las operaciones que dicte medidas de seguridad física y lógica de las redes y servicios.
 2. Elaborar un plan de acción para atender ataques lógicos a la red nacional de internet.
- 



II. Acciones Ministeriales

1. Firma Digital
 2. CSIRT-CR
 3. Legislación vigente
- 

1. Firma Digital



Firma digital

Certificados emitidos:

Cantidad de oficinas	2009	2010	2011	2012	2013	2014*	Total
33	668	6.214	10.516	19.127	24.365	6.130	67.020

Fuente: Banco Central de Costa Rica. 2014.

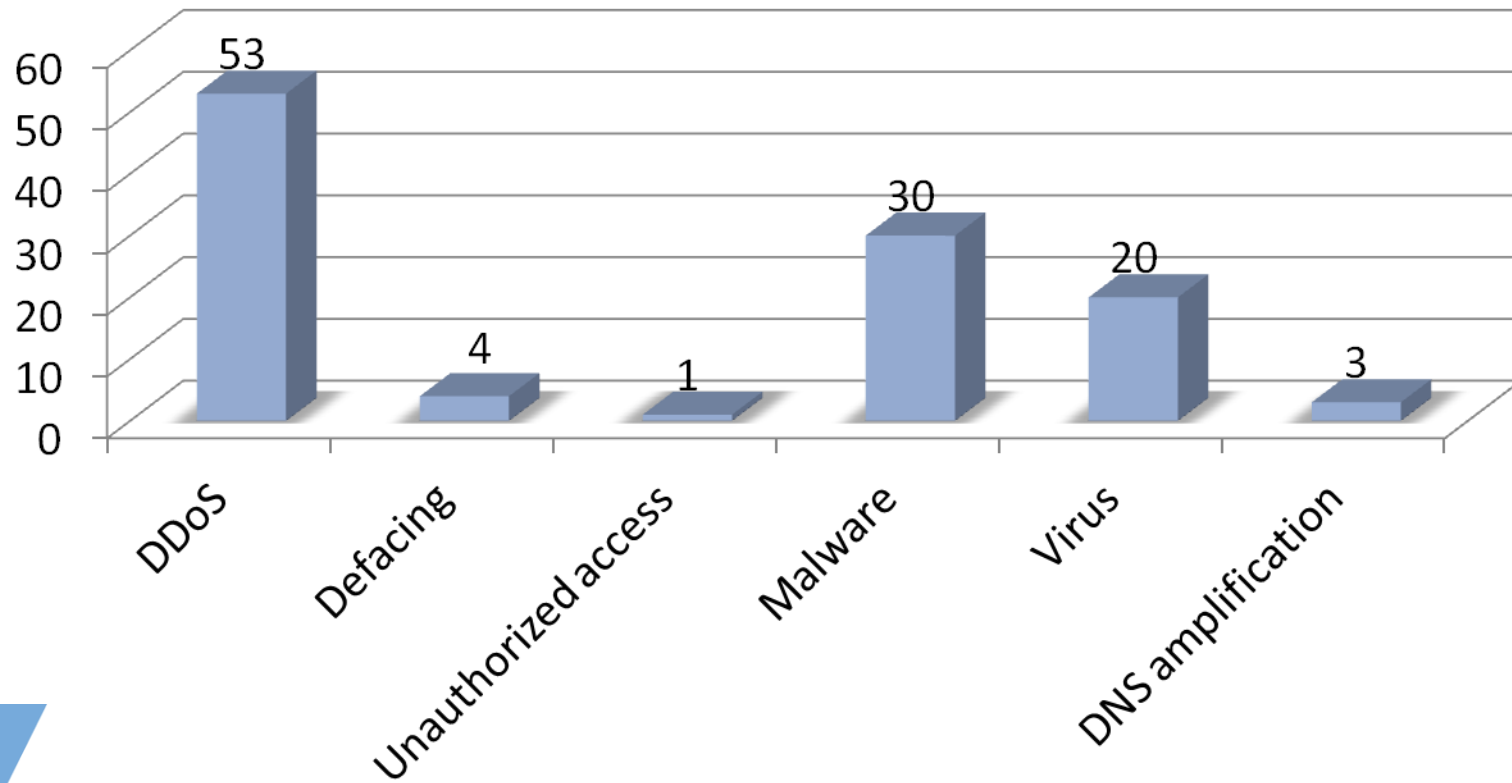
2014*: Datos a febrero del 2014.

2. CSIRT-CR

- **2005:** Adhesión al tratado internacional contra el terrorismo.
- **2008:** Adhesión al tratado internacional contra el cibercrimen.
- **2012:** Creación formal del CSIRT-CR, abril.
 - Primer incidente: 14 de abril.
 - **2012 a La fecha:** Se han creado y establecido protocolos de acción.

CSIRT-CR

Número de incidentes



Fuente: CSIRT-CR 2013.

CSIRT-CR



Principales retos del CSIRT-CR:

- Articular las acciones a partir de la nueva estructura ministerial.
 - Fortalecer el CSIRT-CR y sus protocolos a través de alianzas institucionales.
 - Aumentar el personal dedicado.
 - Definir la ubicación de infraestructura del CSIRT-CR.
- 

3. Legislación vigente de ciberseguridad

- Ley de la Administración Financiera de la República y Presupuestos Públicos (2001).
- Ley de certificados, firmas digitales y documentos electrónicos y su reglamento. (2005).
- Ley de protección de la niñez y la adolescencia frente al contenido nocivo de internet y otros medios electrónicos. (2011).
- Ley de protección de la persona frente al tratamiento de sus datos personales. (2011).

Legislación vigente de ciberseguridad

- **Ley de Delitos Informáticos. (2012).**
Modificación de artículos del código penal.

Tipifica y pena los delitos de:

1. Estafa informática.
2. Daño informático.
3. Suplantación de identidad.
4. Espionaje informático.
5. Suplantación de páginas electrónicas.
6. Suplantación de identidad.

**Penas desde los 3
hasta los 10 años
de prisión.**

Legislación vigente de ciberseguridad

Convenio de Budapest:

- Presentación del proyecto de Ley al Plenario: junio, 2012.
- Primera publicación para consulta pública no vinculante: agosto, 2012.
- Dictaminado por Comisión de Relaciones Internacionales y Comercio Exterior: octubre, 2013.
- Aprobado en primer debate por Plenario: diciembre, 2013.
- Enviado a Comisión, para dictamen definitivo: diciembre, 2013.

Legislación vigente de ciberseguridad



Retos para la aprobación del Convenio de Budapest:

- Aprobación en la presente administración.
(Plazo 31 de abril).
- Liderazgo del MICITT para el posicionamiento, seguimiento y armonización de los alcances del Convenio y la legislación nacional vigente.





III. Otras acciones ministeriales



Otras acciones e iniciativas

- Poder Ejecutivo a través de la Presidenta de la República. Licda. Laura Chinchilla Miranda, se ha comprometido como madrina del Programa Child Online Protection –COP-.
- En setiembre del 2011 se aprueba en la Asamblea Legislativa la Ley No. 8834 “Ley de protección de la niñez y la adolescencia frente al contenido nocivo de internet y otros medios electrónicos”.



Ministerio de Ciencia, Tecnología y Telecomunicaciones

Lic. Jimmy Cruz Jiménez

Viceministerio de Telecomunicaciones

Gerencia de Sociedad de la Información

jimmy.cruz@micit.go.cr

(506) 2211-1241





Medidas sobre Derecho Procesal Convenio de Budapest

**Taller Nacional sobre Legislación en
materia de Ciberdelincuencia
Secretaría de Relaciones Exteriores
México, D.F. 1o de Abril de 2014**

Dr. Cristos Velasco
cristosv@protecciondatos.mx

Medidas sobre Derecho Procesal

Art. 14 – Ámbito de aplicación de las medidas de derecho procesal.

Adoptar medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y procedimientos para la investigación e instauración de procedimientos penales específicos para sancionar las conductas previstas en los Arts. 2 a 11 y la recolección de pruebas electrónicas en cualquier infracción penal.

Medidas sobre Derecho Procesal

Art. 15 – Condiciones y garantías

Establecer garantías en derecho interno para asegurar una protección adecuada de los derechos fundamentales, en particular sobre los derechos derivados de las obligaciones que haya asumido derivado del Convenio para la protección de los derechos humanos y libertades fundamentales del Consejo de Europa (1950) y del **Pacto internacional de derechos civiles y políticos de Naciones Unidas (1966)** o de otros instrumentos internacionales relativos a los derechos del hombre, y que debe integrar el principio de proporcionalidad.

Dichas **condiciones y garantías** incluirán, entre otras, la **supervisión judicial u otras formas de supervisión independiente**, la **motivación justificante de la aplicación**, la **limitación del ámbito de aplicación** y la **duración del poder o del procedimiento en cuestión**.

.....

Medidas sobre Derecho Procesal

Art. 16 – Conservación inmediata de datos informáticos almacenados

Adoptar medidas legislativas o de otro tipo que se estimen necesarias para **permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación inmediata de datos electrónicos especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdida o de modificación.**

2. Adoptar medidas legislativas o de otro tipo que se estimen necesarias para obligar a una persona a conservar y proteger la integridad de los datos – que se encuentran en su poder o bajo su control y respecto de los cuales exista un mandato previo de conservación en aplicación del párrafo precedente – durante el tiempo necesario, hasta un máximo de 90 días, para permitir a las autoridades competentes obtener su comunicación. Los Estados podrán prever que dicho mandato sea renovado posteriormente.

Medidas sobre Derecho Procesal

Art. 16 – Conservación inmediata de datos informáticos almacenados

3. **Adoptar medidas legislativas** o de otro tipo que se estimen necesarias **para obligar** al responsable de los datos o a otra persona encargada de conservarlos **a mantener en secreto la puesta en ejecución de dichos procedimientos durante el tiempo previsto por su derecho interno.**

4. Los **poderes y procedimientos** mencionados en el presente artículo **deben quedar sometidos a los artículos 14 y 15.**

Medidas sobre Derecho Procesal

Art. 17 – Conservación y divulgación inmediata de los datos de tráfico

1. A fin de asegurar la conservación de los datos de tráfico, en aplicación del artículo 16, las Partes **adoptarán las medidas legislativas** o de otro tipo que se estimen necesarias **para:**

a. **procurar la conservación inmediata de los datos de tráfico, cuando uno o más prestadores de servicio hayan participado en la transmisión de dicha comunicación; y**

Medidas sobre Derecho Procesal

Art. 17 – Conservación y divulgación inmediata de los datos de tráfico

b. **asegurar la comunicación inmediata a la autoridad competente del Estado, o a una persona designada por dicha autoridad, de datos de tráfico suficientes para permitir la identificación de los prestadores de servicio y de la vía por la que la comunicación se ha transmitido.**

2. Los **poderes y procedimientos** mencionados en el presente artículo **deben quedar sometidos a los artículos 14 y 15.**

Medidas sobre Derecho Procesal

Art. 18 – Mandato de comunicación

1. Adoptar medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar:

a. a una persona presente en su territorio que comunique los datos informáticos especificados, en posesión o bajo el control de dicha persona, y almacenados en un sistema informático o en un soporte de almacenaje informático; y

b. a un prestador de servicios que ofrezca sus prestaciones en el territorio del Estado firmante, que comunique los datos en su poder o bajo su control relativos a los abonados y que conciernan a tales servicios;

Medidas sobre Derecho Procesal

Art. 18 – Mandato de comunicación

2. Los **poderes y procedimientos** mencionados en el presente artículo **deben quedar sometidos a los artículos 14 y 15.**

3. A los efectos del presente artículo, la expresión **«datos relativos a los abonados»** designa cualquier información, expresada en datos informáticos o de cualquier otro modo, poseída por un prestador de servicio y que se refiere a los abonados de sus servicios, así como a los datos de tráfico o relativos al contenido, y que permite establecer:

a. **el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el tiempo del servicio;**

Medidas sobre Derecho Procesal

Art. 18 – Mandato de comunicación

- b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado o cualquier otro número de acceso, los datos relativos a la facturación y el pago, disponibles por razón de un contrato o de un alquiler de servicio;**
- c. cualquier otra información relativa al lugar donde se ubican los equipos de comunicación, disponible por razón de un contrato o de un alquiler de servicio.**

Medidas sobre Derecho Procesal

Art. 19 – Registro y decomiso de datos informáticos almacenados

1. **Adoptar medidas legislativas** o de otro tipo que se estimen necesarias **a fin de habilitar a sus autoridades competentes para registrar o acceder** de un modo similar:
 - a. **a un sistema informático** o a una parte del mismo, **así como a los datos informáticos que están almacenados**; y
 - b. **a un soporte de almacenamiento** que permita contener **datos informáticos en su territorio**.

Medidas sobre Derecho Procesal

Art. 19 – Registro y decomiso de datos informáticos almacenados

2. Adoptar medidas legislativas o de otro tipo que se estimen necesarias para procurar que, cuando sus autoridades registren o accedan de un modo similar a un sistema informático específico o a una parte del mismo, conforme al párrafo 1 (a), y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son igualmente accesibles a partir del sistema inicial o están disponibles a través de ese primer sistema, dichas autoridades estén en condiciones de ampliar inmediatamente el registro o el acceso y extenderlo al otro sistema.

3. Adoptar medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para decomisar u obtener de un modo similar los datos informáticos cuyo acceso haya sido realizado en aplicación de los párrafos 1 o 2. Estas medidas incluyen las prerrogativas siguientes:

Medidas sobre Derecho Procesal

Art. 19 – Registro y decomiso de datos informáticos almacenados

- a. decomisar u obtener de un modo similar un sistema informático o una parte del mismo o un soporte de almacenaje informático;**
- b. realizar y conservar una copia de esos datos informáticos;**
- c. preservar la integridad de los datos informáticos almacenados pertinentes; y**
- d. hacer inaccesibles o retirar los datos informáticos del sistema informático consultado.**

Medidas sobre Derecho Procesal

Art. 19 – Registro y decomiso de datos informáticos almacenados

4. Adoptar medidas legislativas o de otro tipo que se estimen necesarias **a fin de habilitar a sus autoridades competentes para ordenar a cualquier persona, que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione todas las informaciones razonablemente necesarias**, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.

5. Los **poderes y procedimientos** mencionados en el presente artículo **deben quedar sometidos a los artículos 14 y 15.**

Medidas sobre Derecho Procesal

Art. 20 – Recogida en tiempo real de datos informáticos

1. Adoptar medidas legislativas o de otro tipo que se estimen necesarias **a fin de habilitar a sus autoridades competentes para:**
 - a. **recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio;**
 - b. **obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a**
 - i. **recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o**
 - ii. **prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio a través de un sistema informático.**

Medidas sobre Derecho Procesal

Art. 20 – Recogida en tiempo real de datos informáticos

2. **Cuando un Estado**, en razón de los principios establecidos en su ordenamiento jurídico interno, **no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas** o de otro tipo que estime necesarias **para asegurar la recogida o la grabación en tiempo real de los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.**

3. Adoptar las medidas legislativas o de otro tipo que se estimen necesarias **para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas** previstas en el presente artículo, **así como cualquier información al respecto.**

4. Los **poderes y procedimientos** mencionados en el presente artículo **deben quedar sometidos a los artículos 14 y 15.**

Medidas sobre Derecho Procesal

Art. 21 – Interceptación de datos relativos al contenido

1. Adoptar medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes respecto a infracciones consideradas graves conforme a su derecho interno para:

a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio; y

b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a

i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar,

en tiempo real, los datos relativos al contenido de concretas comunicaciones en su territorio, transmitidas a través de un sistema informático.

Medidas sobre Derecho Procesal

Art. 21 – Interceptación de datos relativos al contenido

2. **Cuando un Estado**, en razón de los principios establecidos en su ordenamiento jurídico interno, **no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos relativos al contenido de concretas comunicaciones transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.**
3. **Adoptar medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.**
4. **Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.**

Medidas sobre Derecho Procesal

Art. 22 – Competencia

1. **Adoptar medidas legislativas o de otro tipo que se estimen necesarias para atribuirse la competencia respecto a cualquier infracción penal establecida en los artículos 2 a 11 del presente Convenio, cuando la infracción se haya cometido:**
 - a. **en su territorio;**
 - b. **a bordo de una nave que ondee pabellón de ese Estado;**
 - c. **a bordo de una aeronave inmatriculada en ese Estado;**
 - d. **por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado.**

Medidas sobre Derecho Procesal

Art. 22 – Competencia

2. **Las Partes podrán reservarse el derecho de no aplicar**, o de aplicar sólo en ciertos casos o condiciones específicas, las reglas de competencia definidas en **los párrafos 1b a 1d** del presente artículo o en cualquiera de las partes de esos párrafos.

3. **Las Partes adoptarán las medidas** que se estimen necesarias **para atribuirse la competencia respecto de cualquier infracción mencionada en el artículo 24, párrafo 1** del presente Convenio, cuando el presunto autor de la misma se halle en su territorio y no pueda ser extraditado a otro Estado por razón de la nacionalidad, después de una demanda de extradición.

4. El presente Convenio no excluye ninguna competencia penal ejercida por un Estado conforme a su derecho interno.

5. **Cuando varios Estados reivindiquen una competencia respecto a una infracción** descrita en el presente Convenio, **los Estados implicados se reunirán, cuando ello sea oportuno, a fin de decidir cuál de ellos está en mejores condiciones para ejercer la persecución.**

Medidas sobre Derecho Procesal

Recomendaciones

- Las medidas sobre derecho procesal deben ser implementadas tomando en cuenta la protección de los derechos fundamentales, consagrados en la Constitución, los tratados internacionales y la jurisprudencia de la SCJN y los Tribunales Federales.
- Son una parte muy importante para poder procesar y castigar conductas cometidas a través de sistemas de cómputo e Internet. Sin esta parte los países se verán imposibilitados de perseguir y procesar conductas a nivel nacional.
- El marco jurídico comparado y las mejores practicas deben ser tomadas en cuenta.



Trabajo con Estados Unidos y sus proveedores



William Hall
Departamento de justicia de Estados Unidos

Conservación y la Red de Delincuencia en Alta Tecnología 24/7

- ▶ La Red es un medio para conservar pruebas electrónicas
- ▶ Cincuenta y nueve (59) estados miembro en todo el mundo
- ▶ Todos los estados son invitados a unirse a esta red informal
- ▶ Detalles:
 - ▶ En cada estado miembro, hay un procurador o policía en todo momento para responder a las solicitudes urgentes de otros estados miembro relacionadas con pruebas electrónicas
 - ▶ Las solicitudes a la red deben comunicarse en inglés
 - ▶ Las partes de la Convención de Budapest están obligadas a tener un punto de contacto y a conservar los datos cuando se les solicite
- ▶ CCIPS es el punto de contacto para Estados Unidos

Cooperación formal

- ▶ Tratados de asistencia legal mutua
- ▶ Convención de Budapest sobre la Ciberdelincuencia
 - ▶ Actúa como un Tratado de Asistencia Legal Mutua cuando los países no cuentan con uno
 - ▶ Las partes aceptan proporcionar asistencia a otros países para obtener y revelar pruebas electrónicas

Cooperación informal: investigaciones conjuntas

- ▶ Punto de contacto con EUA en su país
 - ▶ Agregado Legal del FBI (LEGATT), un agente del FBI
 - ▶ Agregado Legal del Departamento de justicia, un procurador
- ▶ INTERPOL y organizaciones similares

Más información para trabajar con EUA

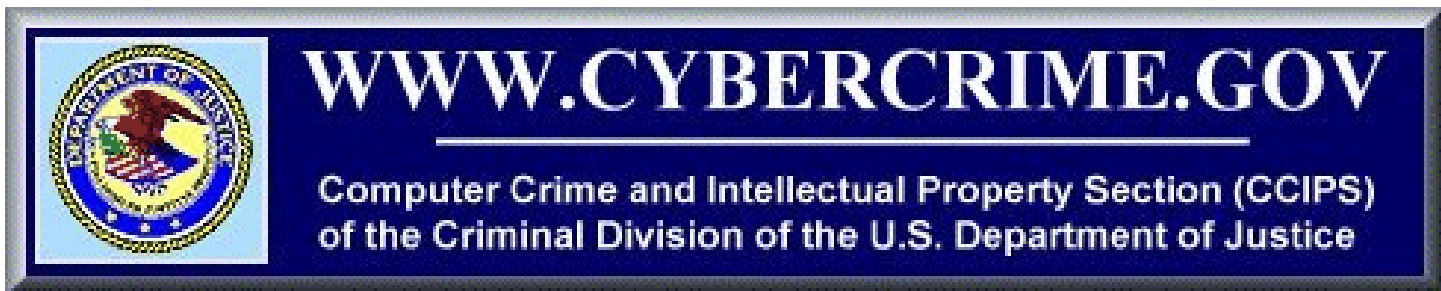
- ▶ Posibilidad de revelar la información de los suscriptores directamente de los proveedores (pero EUA no puede estar involucrado)
- ▶ Revelación de emergencia
- ▶ Las solicitudes de conservación son vitales
 - ▶ EUA no tiene requisitos / leyes para la retención de datos
 - ▶ Usted puede ponerse en contacto con FBI Legat para su país / región
 - ▶ Los miembros de la Red 24/7 pueden usarla para ponerse en contacto con CCIPS
- ▶ Contacto de CCIPS para asistencia: +1 202 514 1026

La Primera Enmienda

- ▶ La Primera Enmienda de la Constitución de Estados Unidos protege el derecho a la libertad de expresión contra interferencia del gobierno
- ▶ La libertad de expresión consiste de los derechos a la libertad de expresión, prensa, reunión y de pedir al gobierno la reparación de daños, y los derechos implícitos de asociación y de creencia
 - ▶ La Suprema Corte interpreta el grado de protección que se otorga a estos derechos

Información de contacto

- ▶ Bill Hall, Abogado Litigante
- ▶ Correo electrónico: william.a.hall@usdoj.gov
- ▶ Teléfono de CCIPS : +1 202 514 1026 (general/trabajo)
- ▶ CCIPS en Internet:





IRIARTE & ASOCIADOS

Protección de Datos Personales, Habeas
Data Y Privacidad en America Latina
Erick Iriarte aka @coyotegris

IRIARTE & ASOCIADO



IRIARTE & ASOCIADOS

Para empezar

Quien nos cuida?

<https://www.youtube.com/watch?v=j-tFoYNHi1w>



IRIARTE & ASOCIADOS

eLAC 2007 / eLAC 2010 / eLAC 2015
Grupo de Trabajo Marco Legal
Capítulo VI. Instrumentos de
Políticas y Estrategias
Coordinación: Perú

Erick Iriarte Ahon



IRIARTE & ASOCIADOS

Cobertura

<http://eclac.cl/socinfo>

Tareas Pendientes eLAC 2007

– Meta 25

Dos temas críticos primarios y dos temas críticos secundarios. Los dos temas críticos primarios son: La regulación en privacidad y de protección de datos en la región y Estado Situacional de la Regulación de Delitos Informáticos en la región. Como temas críticos secundarios son: Uso y aplicación de la firma digital para actividades cotidianas del ciudadano en ambientes gubernamentales para el e-government; y, Soluciones jurídicas y técnicas a la problemática del SPAM.

eLAC2007 - Grupo de Trabajo 25

OBJETIVOS del GRUPO

El grupo tiene como objetivo básico el generar instrumentos de armonización normativa (no normativa armonizada), que permitan la interoperación de regulación en materias de sociedad de la información, entre los países que ya tuvieran regulación, y generar regulación, para aquellos que no la tuvieran.

Lo anterior dicho entendido en el marco de una estrategia política regional de Sociedad de la Información, donde los instrumentos normativos son útiles para lograr los fines de las políticas de desarrollo, en relación a los componentes TIC.



IRIARTE & ASOCIADOS

eLAC2007 - Grupo de Trabajo 25

Protección de Datos Personales

1. *Principio de Legalidad y Licitud*
2. *Principio de Calidad de los Datos de Carácter Personal*
3. *Principio de Seguridad*
4. *Principio de Nivel de Protección Adecuado*

eLAC2007 - Grupo de Trabajo 25

Protección de Datos Personales

9.1. La garantía del cumplimiento de estas directrices deberá quedar sujeto al control de una o varias autoridades de protección de datos. Las autoridades podrán tener personalidad propia o encontrarse integradas en la Administración Pública o en un Organismo Público preexistente. Igualmente podrán tener como función exclusiva el cumplimiento de las normas de protección de datos o ejercer tal competencia junto con otras atribuidas por su legislación.

La organización territorial del Estado no podrá suponer un obstáculo para que las garantías derivadas de la existencia de la o las autoridades de protección de datos sean reales y efectivas en relación con todos los tratamientos llevados a cabo tanto por el sector público como por el privado.



IRIARTE & ASOCIADOS

eLAC2007 - Grupo de Trabajo 25

- 9.2. Las autoridades de protección de datos deberán actuar con plena independencia e imparcialidad, no pudiendo estar sometidas en el ejercicio de sus funciones al mandato de ninguna autoridad pública. Deberán establecerse mecanismos que garanticen la independencia e inamovilidad de las personas a cuyo cargo se encuentre la dirección de dichas autoridades.*
- 9.3 Las autoridades deberá tener como mínimo las siguientes competencias:*
- Conocer de las reclamaciones que les sean dirigidas por los ciudadanos, en particular en cuanto al ejercicio de los derechos a los que se refiere el apartado 5 de estas directrices.*
 - Realizar las averiguaciones e investigaciones que resulten necesarias para el cumplimiento de las directrices, pudiendo acceder a los datos que sean objeto de un tratamiento y recabar toda la información necesaria para el cumplimiento de su misión de control.*
 - Adoptar las medidas que resulten necesarias para evitar la persistencia en el incumplimiento de las directrices.*



IRIARTE & ASOCIADOS

eLAC2007 - Grupo de Trabajo 25

- *Mantener un registro de los tratamientos llevados a cabo por los sectores público y privado, al que puedan acceder los interesados, a fin de poder ejercer los derechos reconocidos en las presentes directrices. La solicitud de inscripción se realizará mediante modelos simplificados y basados en estándares técnicos, respetando el principio de neutralidad tecnológica, utilizándose siempre que ello sea posible técnicas o medios electrónicos.*
- *Autorizar, cuando sea preciso, las transferencias internacionales de datos a Estados cuya legislación no recoja lo dispuesto en las presentes directrices.*
- *Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales que: (i) represente un valor añadido en su contenido respecto de lo dispuesto en las leyes, (ii) contenga o esté acompañado de elementos que permitan medir su nivel de eficacia en cuanto al cumplimiento y el grado de protección de los datos personales y (iii) consagre medidas efectivas en caso de su incumplimiento.*



eLAC2007 - Grupo de Trabajo 25

IRIARTE & ASOCIADOS

- *Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales que: (i) represente un valor añadido en su contenido respecto de lo dispuesto en las leyes, (ii) contenga o esté acompañado de elementos que permitan medir su nivel de eficacia en cuanto al cumplimiento y el grado de protección de los datos personales y (iii) consagre medidas efectivas en caso de su incumplimiento.*
- *Dictaminar los proyectos de disposiciones normativas que puedan afectar al derecho fundamental a la protección de datos personales de los ciudadanos.*
- *Divulgar a los ciudadanos y a los poderes públicos el contenido del derecho fundamental a la protección de datos personales.*
- *Cooperar con las autoridades de protección de datos para el cumplimiento de sus competencias y generar los mecanismos de cooperación bilateral y multilateral para asistirse entre si y prestarse el debido auxilio mutuo cuando se requiera.”*



Tarea Pendiente 1: Fomento de la implementación de Agencias de Protección de Datos (Argentina es el único país que cuenta con este tipo de organización), de un alto nivel en la estructura gubernamental. Estas oficinas deben velar por la adecuada protección de los datos personales, en relación a su uso, manejo, manipulación, traspaso y/o venta. Asimismo debe implementarse una red regional que coordine los esfuerzos de estas Agencias Nacionales. De esta manera es tarea el desarrollo de manuales operativos y de requisitos mínimos para la implementación de dichas oficinas.



Tarea Pendiente 2: Es necesario establecer los mínimos necesarios para una adecuada Política y Regulación en Protección de Datos Personales en todos los ámbitos sociales: política, religiosa, económica, cultural, médica, judicial (siendo de especial interés para el último caso la adhesión abierta y aplicación de los Reglas de Heredia). Estos mínimos deben servir de sustento al desarrollo de políticas y normas de protección de datos ínter operables a nivel de los países región.



Tarea Pendiente 3: Siendo un subtema específico pero que ha desarrollado implicancias comerciales y sociales especiales, la temática del SPAM tiene que ser considerada en el análisis de políticas y normativas, desde las perspectiva técnica, comercial, jurídica y política, siendo una tarea pendiente el establecer un espacio de monitoreo sobre el particular, así como un trabajo en base a la normativa existente y las propuestas que se puedan realizar, para limitar sino eliminar el SPAM.

- *Delitos Informáticos*

Son aquellas conductas ilícitas que afectan el bien jurídico información en formato digital, entendido dichas afectaciones a la confidencialidad, integridad, disponibilidad o uso de la información o de sus sistemas informacionales de soporte.

- *Delitos mediante el uso de las TICs*

Son aquellas conductas ilícitas que empleando TICs, afectan bienes jurídicos previamente reconocidos en la legislación penal vigente, distintos al de la información en formato digital, siempre que el tipo penal lo permita.

La propuesta de regulación va en cuatro vías.

- a. Suscripción y Ratificación de la Convención de Cybercrimen.
- b. Desarrollo de instrumentos para peritaje forense informático
- c. Generación de CERTs, afianzamiento de los instrumentos de Law Enforcement
- d. Desarrollo normativo de tipos penales.

Delitos por medios electrónicos

- *El juez, al dictar sentencia, tendrá en consideración que el uso de las TICs para cometer un delito tipificado, son un agravante de dicho hecho, a parte de las agravantes propias de cada tipo penal.*

Delitos informáticos

- *La adhesión y ratificación del Convenio de Cybercrimen, como instrumento de armonización normativa regional, al presentar los marcos necesarios para dicho proceso.*
- *Tarea Pendiente 1 de Delitos Informáticos, del documento “Estado situacional y perspectivas del derecho informático en América Latina y el Caribe”, que dice: “(...) diseño de una propuesta normativa mínima, basada entre otros en las propuestas del tratado de Cybercrimen, ya existentes”., Siendo así la Convención de Cybercrimen⁵ y su Protocolo Adicional⁶, son la base de esta propuesta.*

78. Renovar el mandato del grupo de trabajo en materia del marco legal de la sociedad de la información para facilitar el diálogo y la coordinación de las diversas iniciativas regulatorias a nivel regional y local que pudieran favorecer la armonización normativa de la región.

81. Invitar a los países a estudiar la posibilidad de ratificar o adherirse al Tratado de Ciberdelitos del Consejo de Europa y su Protocolo adicional, como un instrumento facilitador de nuestra integración y adecuación normativa en esta materia, enmarcados en principios de protección de los derechos de privacidad.



eLAC 2010 – Otras metas

Si bien la tarea indicada para el grupo de trabajo sobre Marco Legal tiene los párrafos anteriores como prioritarios, en diversos capítulos y temas aparece la problemática jurídica de manera relevante para ser analizada.

Es entonces relevante para poder asistir a los otros grupos establecer que la cobertura del presente grupo de trabajo esta relacionada, en la medida de los requerimientos de los coordinadores de dichos grupos, a las tareas que se puedan asignar de manera compartida.



IRIARTE & ASOCIADOS

Tareas Pendientes

*Reporte Final eLAC 2010 –
Metas 78 y 81*



eLAC 2010 - Avances normativos

Tarea Pendiente: desarrollar espacios de dialogo para una opción desarrollada desde la región, que refleje nuestra diversidad cultural, pero que también le permita a los países participar en los espacios de dialogo en un pie de igualdad, con un respeto de los principios de la WSIS de multilateralidad, democracia y transparencia, en un espíritu multi-stakeholder.

Realidad: El problema no es normativo en si mismo, mas alla de la generación de islas regulatorias, sino es un problema de coordinación regional de desarrollos armónicos (no homogéneos)

Realidad. El problema no es normativo, es de desarrollo de capacidades en los actores juridicos para poder utilizar la legislación vigente, sin dejar de enfrentarse a la realidad, de la sociedad de la informacion no hay vuelta atrás.



(Egov) Meta 9: Implementar los cambios normativos necesarios para incrementar la interoperabilidad de los servicios públicos usando estándares abiertos, sin menoscabo de la protección de datos personales y del secreto comercial, la seguridad y la estabilidad de los sistemas de información.

(Entorno Habilitador) Meta 21: Favorecer el diálogo y la cooperación en materia de regulación para la integración a nivel regional, especialmente en materia de protección de datos personales, firma digital y delitos por medios electrónicos.



IRIARTE & ASOCIADOS

 alfa - redi





IRIARTE & ASOCIADOS

Argentina



 alfa - redi

Año	Legislación	Regulación de que se trata	Observaciones
Art. 43 de La Constitución		Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o banco de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.	
2000	Ley 25.326 Ley de Protección de Datos Personales	La ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas...	Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.
2001	Decreto 1558/2001	Reglamentación de la Ley Nº 25.326. Principios generales relativos a la protección de datos. Derechos de los titulares de los datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones.	No es necesario el consentimiento en caso de transferencia de datos desde un registro público que esté legalmente constituido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta.
2002	Dictamen 4/2002	Sobre el nivel de protección de datos personales en Argentina	
2006	Disposicion nº 11/2006	Aprueba las "Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados".	

IRIARTE & ASOCIADOS

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2008	Ley 26.343 Incorporación del art. 47 a la Ley 25.326	Toda persona que considerase que sus obligaciones canceladas o regularizadas están incluidas en lo prescripto en el presente artículo puede hacer uso de los derechos de acceso, rectificación y actualización en relación con lo establecido (en esta norma)...	Una vez obtenida la información, el Banco Central de la República Argentina implementará las medidas necesarias para asegurar que todos aquellos que consultan los datos de su Central de Deudores sean informados de la procedencia e implicancias de lo aquí dispuesto.
	Ley 26.388	Reforma del Código Penal en materia de Delitos Informáticos. Deroga y modifica algunos incisos introducidas por el art. 32 de la Ley 25.326 al Código Penal.	Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;.(...)
	Disposición 10/2008	Se establece que los responsables y usuarios de bancos de datos públicos o privados, deberán incluir en su página web y en toda comunicación o publicidad, en particular, en los formularios utilizados para la recolección de datos personales, información al respecto.	Deberá decir. Leyenda: "El titular de los datos personales tiene la facultad de ejercer el derecho de acceso a los mismos en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto conforme lo establecido en el artículo 14, inciso 3 de la Ley Nº 25.326". "La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, Organo de Control de la Ley Nº 25.326, tiene la atribución de atender las denuncias y reclamos que se interpongan con relación al incumplimiento de las normas sobre protección de datos personales".

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2010	Disposición 7/2010	Se crea el Centro de asistencia a las víctimas de robo de identidad.	Funciones: -Facilitar orientación y asistencia a las personas que hayan sido afectadas por este accionar fraudulento en cualquiera de sus variantes. -Desarrollar información sobre medidas de prevención a adoptar. -Adoptar todas las medidas que considere convenientes, en particular aquellas necesarias para evitar que la acción fraudulenta continúe desarrollándose respecto de la misma persona.
	Disposición 12/2010	Tratamientos de datos personales destinados a difusión pública	Cuando se efectúen tratamientos de datos personales destinados a difusión pública que contengan datos sensibles en los términos de la Ley N° 25.326 o referente a menores, incapaces, asuntos de familia y cualquier otra categoría de datos protegida por ley, deberá observarse la aplicación de procedimientos eficaces de disociación y/o de todo procedimiento riguroso de protección a fin de evitar la identificación del titular del dato, en defensa de sus derechos de intimidad o cualquier otro que se encuentre en juego.





IRIARTE & ASOCIADOS

Bolivia



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
Constitución: Art.21.2, Art. 130 Art.131	2009	21.2 2. A la privacidad, intimidad, honra, honor, propia imagen y dignidad. 130 I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad. II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa. 131 .I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional.	
2004	Ley 2631. Art. 23 363	Artículo 23.I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de Habeas Data ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya.	



IRIARTE & ASOCIADOS



IRIARTE & ASOCIADOS

Brasil



 alfa - redi

Legislación/ N° Normas	Regulación de que se trata	Observaciones
Art. 5 Constitución	X Son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurándose el derecho a indemnización por el daño material o moral derivado de su violación; Se concederá "habeas data": 1. para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; 2. para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo;	
Ley 9.507 (1997)	Regula el derecho de acceso a informaciones y procedimiento de Habeas Data	
Código Civil	Dispone que la divulgación de información sin autorización y con violación al derecho de privacidad es pasible de indemnización por daños materiales o morales, se establece también medidas cautelares para evitar o detener cualquier violación.	
Código de Defensa de Consumidor	Dispone que el consumidor debe ser informado por escrito al respecto de la recolección de sus datos personales para la apertura de formularios y registros, cuando no haya sido solicitada por él.	
Ley de Telecomunicaciones	Garantiza al usuario la protección de su privacidad e intimidad en el uso de sus datos.	
Legislación Bancaria	Establece secreto bancario para las actividades bancarias y de servicios prestados, y trata como delito la violación de la confidencialidad. Algunas situaciones no constituyen violación de la confidencialidad, como el intercambio de información entre las instituciones financieras, el suministro de información a las entidades de protección de crédito y la comunicación a las autoridades de la práctica ilegal.	



IRIARTE & ASOCIADOS



IRIARTE & ASOCIADOS

Chile



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
1999	Ley Núm. 19.628	Sobre Protección de la vida privada	La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.
2000	Decreto No.779/2000	Aprueba el Reglamento del registro de Bancos de Datos Personales a Cargo de Organismos Públicos	Los organismos señalados en el artículo primero de este Reglamento deberán requerir su inscripción en el Registro de Bancos de Datos Personales ante las Oficinas del Servicio de Registro Civil e Identificación habilitadas para estos efectos o en el respectivo sitio en Internet del Servicio, o de cualquier otra forma que el Servicio determine. Las inscripciones que sean requeridas a través del sitio en Internet del Servicio, estarán sujetas a las confirmaciones y medidas de seguridad que la institución determine conforme a las normas legales pertinentes.
2004	TLC con EEUU, firmado en el 2002	Artículo 15.5: Cooperación (...) b. compartir información y experiencias sobre las leyes, regulaciones y programas en el ámbito del comercio electrónico, incluso aquéllas referidas a la privacidad de los datos, confianza de los consumidores, seguridad cibernética, firma electrónica, derechos de propiedad intelectual y formas electrónicas de gobierno;	
	TLC con UE	Art.- 76 (...) 2. Todo intercambio de información estará sujeto a las reglas y normas de confidencialidad que se aplican en el territorio de cada Parte. Ninguna Parte estará obligada a proporcionar información, si ello es contrario a sus leyes sobre divulgación de información. Cada Parte mantendrá la confidencialidad de cualquier información que se le proporcione, en conformidad con las limitaciones de uso que imponga la Parte que entregue la información. Cuando la legislación de una Parte así lo disponga, la información confidencial podrá ser proporcionada a sus respectivos tribunales de justicia.	



IRIARTE & ASOCIADOS

Año	Legislación	Regulación de que se trata	Observaciones
2008	Ley 20.285 Sobre acceso a la información pública	Art.7: Los órganos de la Administración del Estado señalados en el artículo 2°, deberán mantener a disposición permanente del público, a través de sus sitios electrónicos, los siguientes antecedentes actualizados, al menos, una vez al mes: i)además de las nóminas de beneficiarios de los programas sociales en ejecución. No se incluirán en estos antecedentes los datos sensibles, esto es, los datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen social, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.	
2009	Ley 20.406	Ley que permite el acceso a la información bancaria. Se reemplaza el artículo 62 del Código Tributario	Artículo 62.- La Justicia Ordinaria podrá autorizar el examen de información relativa a las operaciones bancarias de personas determinadas, comprendiéndose todas aquellas sometidas a secreto o sujetas a reserva, en el caso de procesos por delitos que digan relación con el cumplimiento de obligaciones tributarias....
	TLC con Australia, firmado en el 2008	Define : (d) datos personales significa la información acerca de un individuo cuya identidad es determinable o que pueda www.bcn.cl - Biblioteca del Congreso Nacional de Chile ser determinada en forma razonable por dicha información;	



Año	Legislación	Regulación de que se trata	Observaciones
Art. 15 Constitución		...En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley...	
2008	Ley 1266,	Ley de habeas Data	Regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de otros países.
2009	Ley 1288 Capítulos IV y V	Establecen las reglas que se deben manejar en las bases de datos y archivos de inteligencia y contrainteligencia, donde se garanticen los procesos de recolección, almacenamiento, producción y difusión de la información	Por la naturaleza de las funciones que cum-plen los organismos que desarrollan actividades de inteligencia y contra inteligencia sus documentos, información y elementos técni-cos, estarán amparados por la reserva legal por un término máximo <i>Ley 1288 de 2009 13/23</i> de 40 años y tendrán carácter de información reservada según el grado de clasificación que les corresponda en cada caso.





Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2009	Ley 1273	Se adiciona al Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos",	269f.- El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique <i>p emplee códigos</i> personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
	Decreto 1727	Se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información	
2010	Proyecto de Ley Estatutaria 46	Por la cual se dictan disposiciones generales para la protección de datos personales	





IRIARTE & ASOCIADOS

Ecuador



 alfa - redi

Año	Legislación	Regulación de que se trata	Observaciones
Constitución Arts.: 23.8 23.13 94	1998	Art. 23.8. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona. Art. 23. 13. La inviolabilidad y el secreto de la correspondencia. Esta sólo podrá ser retenida, abierta y examinada en los casos previstos en la ley. Se guardará el secreto de los asuntos ajenos al hecho que motive su examen. El mismo principio se observará con respecto a cualquier otro tipo o forma de comunicación. Art. 94 ...La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional	
1997	Ley Orgánica de Transparencia y Acceso a la Información Pública.	Art. 6 .- Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes.	
1997	Ley de Control Constitucional	Las personas naturales o jurídicas, nacionales o extranjeras, que deseen tener acceso a documentos, bancos de datos e informes que sobre si mismas o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les esté por dar, podrán interponer el recurso de hábeas data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta Ley, por parte de las personas que posean tales datos o informaciones.	
2002	Ley 2002-63	Artículo 9º. Protección de datos. Para la elaboración, transferencia o utilización de bases de datos(...) La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad (...)	
	Decreto 3496	Artículo 21.- De la seguridad en la prestación de servicios electrónicos.- La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio. (...)	



IRIARTE & ASOCIADOS

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
Constitución. Capítulo III. Art. 40 (1980 Con Reformas en 1996)	Every person in Guyana is entitled to the basic right to a happy, creative and productive life, free from hunger, disease, ignorance and want. That right includes the fundamental rights and freedoms of the individual, that is to say, the right, whatever his race, place of origin, political opinions, colour, creed or sex, but subject to respect for the rights and freedoms of others and for the public interest, to each and all of the following, namely — (...) C. protection for the privacy of his home and other property and from deprivation of property without compensation		
1997	Integrity Comission Act		Se enumeran los funcionarios públicos cuyos datos tienen una menor protección
	MAH Prioridad 3 - Utilizar el conocimiento, la innovación y la educación para establecer una cultura de seguridad y de resiliencia a todo nivel .		
	Data National Authority Act		





IRIARTE & ASOCIADOS

Guayana Francesa



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
1978	Ley 78-17 "informática y Libertades"		
28 de Enero de 1981	Convenio del Consejo de Europa		
2002	Directiva 2002/58/CE (12.06)	Relativa al tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas	
2004	Ley número 2004-801 que aprueba Directiva 95/46 Modifica Ley 78-17	Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (1).	
2006	Directiva 2006/24/CE (15.03)	Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones	Modifica la Directiva 2002/58/CE, del 15 de Marzo de 2006



Legislación aplicable de la UE



IRIARTE & ASOCIADOS

Isla Georgia del Sur



alfa - redi

Año	Legislación	Regulación de que se trata	Observaciones
1984	Data Protection Act		
1995	Directiva 95/46/CE	Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos	
1998	Data Protection Act	Personal information may be kept for no longer than is necessary and must be kept up to date. Personal information may not be sent outside the European Economic Area unless the individual whom it is about has consented or adequate protection is in place, for example by the use of a prescribed form of contract to govern the transmission of the data.	
2000	Freedom of Information Act		
2002	Directiva 2002/58/CE 12.06	Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas	
2005	DECISIÓN MARCO 2005/222/JAI DEL CONSEJO de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información	Artículo 4 . Intromisión ilegal en los datos Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.	
2006	Directiva 2006/24/CE 15.03	Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE	



Legislación aplicable de Reino Unido y UE



IRIARTE & ASOCIADOS

Islas Malvinas alfa - redi

Año	Legislación	Regulación de que se trata	Observaciones
1984	Data Protection Act		
1995	Directiva 95/46/CE	Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos	
1998	Data Protection Act	Personal information may be kept for no longer than is necessary and must be kept up to date. Personal information may not be sent outside the European Economic Area unless the individual whom it is about has consented or adequate protection is in place, for example by the use of a prescribed form of contract to govern the transmission of the data.	
2000	Freedom of Information Act		
2002	Directiva 2002/58/CE 12.07	Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas	
2005	DECISIÓN MARCO 2005/222/JAI DEL CONSEJO de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información	Artículo 4 . Intromisión ilegal en los datos Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.	
2006	Directiva 2006/24/CE 15.03	Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE	



Legislación aplicable de Reino Unido y UE



IRIARTE & ASOCIADOS

México



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
Art.6 y Art. 7 Constitución		Establecen como límite a la manifestación de las ideas y a la libertad de imprenta, el ataque a los derechos de un tercero y el respeto a la vida privada (los datos personales se encuentran dentro de la esfera de la vida privada)	Surge el deber del estado de brindar protección a los datos personales de los ciudadanos
2002 2003	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (Cap. IV)	Toda persona puede solicitar a las instituciones federales cualquier documento que contenga información pública, y obtenerla en forma rápida y sencilla *Se crea el IFAI por Decreto del 24.12.2002 * Reglamento de la Ley -2003	Excepciones de la Ley: La información que posee el Gobierno Federal es reservada cuando su divulgación pone en riesgo la seguridad nacional o la vida de cualquier persona. Asimismo, el concepto de información confidencial se refiere a datos personales cuya divulgación lesionaría el derecho a la privacidad de las personas
2003	Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos. Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección.		

IRIARTE & ASOCIADOS

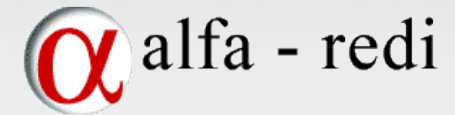


Año	Legislación Nº de Normas	Regulación de que se trata	Observaciones
2004	Lineamientos que deberán observar las dependencias y entidades de la administración pública federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los Particulares.		
2005	Lineamientos de Protección de datos personales	Para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.	Establece las condiciones y requisitos mínimos para el debido manejo y custodia de los sistemas de datos que se encuentran en posesión de la Administración Pública Federal en el ejercicio de sus atribuciones
2007	Decreto de Reforma del art. 6 de la Constitución	Se adiciona un segundo párrafo con siete fracciones al artículo sexto de la constitución política de los estados unidos mexicanos.	Se agrega: Art. 6 ... II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
2008	Lineamientos que deberán observar las dependencias y entidades de la administración pública federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su Corrección.		





IRIARTE & ASOCIADOS



Año	Legislación Nº de Normas	Regulación de que se trata	Observaciones
2010	Ley de Protección de Datos Personales en posesión de los particulares	establece como violatorio que no se cumpla con la solicitud del ciudadano de cancelación u oposición al tratamiento de sus datos personales, así como actuar con negligencia o dolo en la tramitación. También sanciona a quien recabe o transfiera datos personales sin el consentimiento expreso del titular, como con engaño y fraude, y prohíbe la creación de bases de datos en contravención de dicha ley	pretende evitar abusos con el manejo de referencias por parte de empresas de información de clientes, bancos de datos y padrones.



IRIARTE & ASOCIADOS



IRIARTE & ASOCIADOS

Paraguay



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
Arts. 33 y 36 Constitución		Art. 33 La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. Art. 36 ...La ley determinará modalidades especiales para el examen de la contabilidad comercial y de los registros legales obligatorios.	
2001	Ley N° 1.682 Reglamentación de la Información de Caracter Privado	Artículo 4°.- Se prohíbe dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables. Se consideran datos sensibles los referentes a pertenencias raciales o étnicas, preferencias políticas, estado individual de salud, convicciones religiosas, filosóficas o morales; intimidad sexual y, en general, los que fomenten prejuicios y discriminaciones, o afecten la dignidad, la privacidad, la intimidad doméstica y la imagen privada de personas o familias.	Artículo 6°.- Podrán ser publicados y difundidos: a) Los datos que consistan únicamente en nombre y apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional; b) Cuando se trate de datos solicitados por el propio afectado; y, c) Cuando la información sea recabada en el ejercicio de sus funciones, por magistrados judiciales, fiscales, comisiones parlamentarias o por otras autoridades legalmente facultadas para ese efecto.



IRIARTE & ASOCIADOS



IRIARTE & ASOCIADOS

Perú



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
Constitución: Art. 2		Artículo 2°. Toda persona tiene derecho: 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. El secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado. 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.	
2000	Ley N° 27269	Artículo 8 - Confidencialidad de la información La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la presente ley. Asimismo la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital.	
2001	Ley N° 27489.	Ley que regula las centrales privadas de información de riesgos y de protección al titular de la información	
2004	Ley N° 28237	Código Procesal Constitucional. Título IV- Habeas Data	
2005	Ley N° 28493	Ley que regula el uso del correo electrónico comercial no solicitado (SPAM)	



IRIARTE & ASOCIADOS



IRIARTE & ASOCIADOS



 alfa - redi

2009	TLC con Canadá	Entra en vigencia el TLC entre Canadá y Perú, suscrito el 29 de mayo de 2008. En el Capítulo de Comercio Electrónico se incluye el compromiso de contar con legislación y regulación para la protección de la información personal en las transacciones electrónicas, además del compromiso de intercambiar información y experiencias en esta materia.	
2010	Proyecto de Ley N° 0479/2009-PE	Propone la Ley de Protección de Datos Personales	Respeto y control de sus datos personales en posesión actual y futura de sectores públicos y privados. Impedir la intromisión de terceros no autorizados en la información personal de la persona, resguardando la vida privada.



IRIARTE & ASOCIADOS



IRIARTE & ASOCIADOS

Surinam



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
	Constitución Art. 17	Art. 17 .1 Everyone has a right to respect of his privacy, his family life, his home and his honor and good name.	



IRIARTE & ASOCIADOS



IRIARTE & ASOCIADOS

Uruguay



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata		Observaciones
Art. 72 Constitución		La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno.		
1995	Ley Orgánica 10/1995 (23 de Noviembre)	Art. 197. 1 El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.		
2004	Ley 17.838	Protección de datos personales para ser utilizados en informes comerciales y acción de Habeas Data	Regula el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración, y en general, el tratamiento de datos personales asentados en archivos, registros, bases de datos, u otros medios similares autorizados, sean éstos públicos o privados, destinados a brindar informes objetivos de carácter comercial.	
2005	Ley N° 17.930	Ley de aprobación del Presupuesto Nacional.	Todos los órganos u organismos públicos estatales o no estatales, están obligados a aportar, sin contraprestación alguna, los datos que no se encuentren amparados por el secreto bancario o estadístico y que le sean requeridos por escrito por la Dirección General Impositiva (DGI) para el control de los tributos. El Poder Judicial y el Poder Legislativo quedan exceptuados de brindar información, datos o documentos correspondientes a actuaciones de carácter secreto o reservado.	



IRIARTE & ASOCIADOS

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2006	Acordada de la Suprema Corte de Justicia No. 7564	Protección de datos personales y Habeas Data	Respondiendo a la “necesidad de adecuar la reglamentación referente al tratamiento de datos en el ámbito del Poder Judicial a la normativa vigente, a los avances tecnológicos y al estadio actual de la materia”
2008	Ley 18.331 (18 de Agosto) Ley de Protección de Datos y acción de habeas Data	Art. 10 .- Se considera información confidencial: (...) II) Los datos personales que requieran previo consentimiento informado.	
		Artículo 1º. Derecho humano.- El derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República.	El régimen de la presente ley será de aplicación a <i>los datos personales registrados en cualquier soporte</i> que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.





IRIARTE & ASOCIADOS

Venezuela



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2001	Ley Especial sobre Delitos Informáticos Arts. 6, 7, 9, 11, 12, 14, 20, 21, 22	Acceso Indebido, daño a sistemas, Espionaje informático, falsificación documentos, Fraude, Violación privacidad de comunicaciones, datos o información personal,	
2004	Ley de Protección al consumidor y al usuario arts. 37 y 38 Privacidad y selección de información	Regula los intereses de los consumidores y usuarios	
2004	Art. 5 sometimiento de mensajes a privacidad de comunicaciones y acceso a la información personal		



IRIARTE & ASOCIADOS



IRIARTE & ASOCIADOS

 alfa - redi



Año	Legislación Nº Normas	Regulación de que se trata
	E-commerce policy	
2002	Directiva 2002/58/CE (12.06)	Relativa al tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas
2006	Directiva 2006/24/CE (15.03)	Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones

Aplica legislación de UE

Antigua y Barbuda



Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2004	The freedom of Information Act Cap. 26	La parte IV da excepciones al derecho general de acceso a la información las cuales están relacionadas con la privacidad, información comercial confidencial, salud, defensa y seguridad, orden público.	Regula uso de información personal de terceros sin autorización
		Maintenance of 12. (1) Every public authority shall maintain its records in a records manner which facilitates the right of access to information, as provided for in this Act, and in accordance with the Code of Practice issued pursuant to subsection (3). (2) Every public authority shall establish and maintain adequate procedures for the correction of personal information held by it.	





IRIARTE & ASOCIADOS

Antillas



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
1999	Personal Data Protection Act Art. 8,9	Article 8 Personal data may only be processed where: a. the data subject has unambiguously given his consent for the processing; b. the processing is necessary for the performance of a contract to which the data subject is party, or for actions to be carried out at the request of the data subject and which are necessary for the conclusion of a contract; (...)	
2002	Directiva 2002/58/CE 12.07	Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas	
2005	DECISIÓN MARCO 2005/222/JAI DEL CONSEJO de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información	Artículo 4 . Intromisión ilegal en los datos Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.	
2006	Directiva 2006/24/CE 15.03	Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE	



Aplica legislación de Países Bajos



IRIARTE & ASOCIADOS

Aruba



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
1999	Personal Data Protection Act Art. 8,9	Article 8 Personal data may only be processed where: a. the data subject has unambiguously given his consent for the processing; b. the processing is necessary for the performance of a contract to which the data subject is party, or for actions to be carried out at the request of the data subject and which are necessary for the conclusion of a contract; (...)	
2002	Directiva 2002/58/CE 12.07	Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas	
2005	DECISIÓN MARCO 2005/222/JAI DEL CONSEJO de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información	Artículo 4 . Intromisión ilegal en los datos Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.	
2006	Directiva 2006/24/CE 15.03	Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE	



Aplica legislación de Países Bajos



IRIARTE & ASOCIADOS

Bermuda



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
1999	Electronic Transactions Act	Promueve mecanismos de auto-regulación y establecimiento de regulación por el Ministerio en protección datos	



IRIARTE & ASOCIADOS



IRIARTE & ASOCIADOS

Bahamas



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2003	Data Protection Act Policy Statement on E-commerce & digital agenda	Protección de datos, la Agenda establece compromiso de regular protección información personal	



IRIARTE & ASOCIADOS

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2005	Data Protection Act	An Act to provide for <i>(a) the regulation of the collection, keeping, processing, use or dissemination of personal data;</i> <i>(b) the protection of the privacy of individuals in relation to personal data; and</i> <i>(c) related matters related thereto.</i>	The data protection principles referred to under subsection are as follows: <i>(a) First Principle: personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless there is compliance with at least one of the conditions set out in</i> <i>(b) Second Principle: personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;</i> <i>(c) Third Principle: personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;</i> <i>(d) Fourth Principle: personal data shall be accurate and, where necessary, kept up-to-date;</i> <i>(e) Fifth Principle: personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;</i> <i>(f) Sixth Principle: personal data shall be processed in accordance with the rights of data subjects under this Act;</i> <i>(g) Seventh Principle: appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data; and</i> <i>(h) Eighth Principle: personal data shall not be transferred to a country or territory outside Barbados unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.</i>





IRIARTE & ASOCIADOS

Belice



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
	Constitución. II Parte. Art. 14 .1	14.-(1) A person shall not be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. The private and family life, the home and the personal correspondence of every person shall be respected.	
2000 (edición revisada)	Families and Children Act	153.-(1) A court may decide to sit in private for the whole or part of any proceedings in which any power under this Act may be exercised by that court with respect to any child. (2) It shall be an offence for any person to publish any material which is intended, or is likely, to identify - (a) any child as being involved in any proceedings before a court in which any power under this Act may be exercised by the court with respect to that or any other child; or (b) an address or school as being that of a child involved in any such proceedings; or (c) any child involved in any alleged crime, whether as a victim, witness or the accused person. (3) In any proceedings for an offence under this section it shall be a defence for the accused to prove that he did not know, and had no reason to suspect, that the published material was intended, or was likely, to identify the Child	



IRIARTE & ASOCIADOS

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2004	Reglamento Autónomo del servicio para la regulación del correo electrónico masivo o no deseado	Regular la práctica de correo electrónico masivo o no deseado.	
Proyecto de Ley de Habeas Data. Expediente N° 12.827.			





Año	Legislación N° Normas	Regulación de que se trata
1999	Resolución conjunta 1/99	Art. 2.- La protección aquí conferida se extiende a las bases o compilaciones de datos u otros materiales cuya selección o disposición tengan carácter creativo. Dicha protección no abarca los datos o materiales en sí mismos, y es sin perjuicio de cualquier derecho existente respecto de los datos o materiales contenidos en la colección.





IRIARTE & ASOCIADOS

El Salvador



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
Constitución Art. 2		Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen	
1997	Decreto 1030 art. 184	Se sanciona a todo aquél que atente contra la privacidad de la comunicación privada de las personas mediante el apoderamiento de documentación o algún soporte informático.	
2004	Se reconoció, por primera vez y mediante sentencia de la Corte Suprema de Justicia, como derecho fundamental de todos los salvadoreños la protección de datos o autodeterminación informativa, derivado de un proceso de amparo constitucional que el abogado Boris Rubén Solórzano interpuso contra una empresa dedicada a la recopilación y comercialización de información crediticia, DICOM. Por ahora, la figura del hábeas data sólo puede ser analizada por la misma Corte Suprema de Justicia, al no existir una ley especial que regule la protección de datos en El Salvador.		



IRIARTE & ASOCIADOS

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
	Constitución Art. 44 Art. 31	ARTICULO 44.- Derechos inherentes a la persona humana. Los derechos y garantías que otorga la Constitución no excluyen otros que, aunque no figuren expresamente en ella, son inherentes a la persona humana. El interés social prevalece sobre el interés particular. Serán nulas ipso jure las leyes y las disposiciones gubernativas o de cualquier otro orden que disminuyan, restrinjan o tergiversen los derechos que la Constitución garantiza. ARTICULO 31.- Acceso a archivos y registros estatales. Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos.	
2003	Ley de protección integral de la Niñez y Adolescencia	ARTICULO 152. Derecho a la privacidad. Los adolescentes tendrán derecho a que se les respete su vida privada y la de su familia. Consecuentemente, se prohíbe divulgar la identidad de un adolescente sometido a proceso.	



Año	Legislación N° Normas	Regulación de que se trata	Observaciones
Constitución. Art. 40		Article 40 (Right to information) : The State has the obligation to publicize in the oral, written and televised press in the Creole and French languages all laws, orders, decrees, international agreements, treaties, and conventions on everything affecting the national life, except for information concerning national security.	





IRIARTE & ASOCIADOS

Honduras



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2006	DECRETO No. 170-2006	ARTÍCULO 2.- OBJETIVOS DE LA LEY. Son objetivos de esta Ley establecer los mecanismos para: (...) 6) Garantizar la protección, clasificación y seguridad de la información pública y el respeto a las restricciones de acceso en los casos de: (...) c) Los datos personales confidenciales; y, d) La secretividad establecida por Ley.	



IRIARTE & ASOCIADOS



IRIARTE & ASOCIADOS

Isla Dominica



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
No existe norma al respecto.			



IRIARTE & ASOCIADOS



País	Legislación N° Normas	Regulación de que se trata
2002	Directiva 2002/58/CE (12.06)	Relativa al tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas
2006	Directiva 2006/24/CE (15.03)	Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2000	Information & Communications Technology Authority Law (2000) cap. VIII numeral 75	Prohíbe la interceptación de mensajes cap. VIII, el capítulo de sanciones establece sanción administrativa por envío de mensajes contrarios al interés público	
2002	Directiva 2002/58/CE (12.06)	Relativa al tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas	
2006	Directiva 2006/24/CE (15.03)	Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones	
2009	Freedom of Information Regulations Act	Where an information manager intends to give access to a record which he believes contains personal information, he shall, within fourteen calendar days of receipt of the application, send the third party written notice of the application for access.	



Año	Legislación Nº Normas	Regulación de que se trata
2002	Directiva 2002/58/CE (12.06)	Relativa al tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas
2006	Directiva 2006/24/CE (15.03)	Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones



Aplica legislación de UE



IRIARTE & ASOCIADOS

Jamaica



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2002	Interception of Communications Act	5.1.a.communication transmitted by means of a public or private telecommunications network to or from one or more addresses specified in the warrant, being an address or addresses likely to be used for the transmission of communications to or from- Warrant. (i) one particular person specified or described in the warrant; or (ii) one particular set of premises <i>so specified or</i> described; and <i>(b) such other communications (if any) as is necessary to intercept in order to intercept communications falling within paragraph (U).</i>	



IRIARTE & ASOCIADOS



País	Legislación N° Normas	Regulación de que se trata	Observaciones
Constitución Art. 26		Toda persona tiene derecho: 1. A su vida privada y a la de su familia....	
2007	Ley de Acceso a la Información Pública		





IRIARTE & ASOCIADOS

Panamá



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
2002	Ley 6	información confidencial: Todo tipo de información en manos de agentes del estado o de cualquier institución pública que tenga relevancia con respecto a los datos médicos y psicológicos de las persona, la vida íntima de los particulares, incluyendo sus asuntos familiares, actividades maritales u orientación sexual, su historial penal y policivo, su correspondencia y conversaciones telefónicas o aquellas mantenidas por cualquier otro medio audiovisual o electrónico, así como la información pertinente a los menores de edad. También se considera como confidencial la información contenida en los registros individuales o expedientes de personal o de recursos humanos de los funcionarios	
	Ley 24	Regula el servicio de información sobre el historial de crédito de los consumidores o clientes.	
2010	TLC con Canadá	(Cap. XI) 4. Adicionalmente a lo dispuesto por el Artículo 23.02 (Excepciones – Excepciones Generales), una Parte podrá tomar medidas necesarias para: (a) garantizar la seguridad y confidencialidad de los mensajes; o (b) proteger la privacidad de los suscriptores de servicios públicos de transporte de telecomunicaciones.	



IRIARTE & ASOCIADOS



IRIARTE & ASOCIADOS

Puerto Rico



 alfa - redi

Año	Legislación N°/ Normas	Regulación de que se trata	Observaciones
Sección 8 Constitución		Toda persona tiene derecho a protección de ley contra ataques abusivos a su honra, a su reputación y a su vida privada o familiar	
2004	Código Penal. Parte Especial Subtítulo 5- § 4812. Revelación de comunicaciones y datos personales	Toda persona que difunda, publique, revele o ceda a un tercero los datos, comunicaciones o hechos descubiertos o las imágenes captadas a que se refieren las secs. 4810 (Violación de comunicaciones personales) y 4811 (Alteración y uso de datos personales en archivos) de este título, o que estableciere una empresa para distribuir o proveer acceso a información obtenida por otras personas en violación de las referidas secciones, u ofreciere o solicitare tal distribución o acceso en la jurisdicción de Puerto Rico, incurrirá en delito grave de cuarto grado.	
2008	L.P.R.A. Protección de la privacidad de los usuarios. Título XXVII –Parte II .§ 269I (Septiembre 12, 1996, Núm. 213, adicionado como art. III-15 en Agosto 7, 2008, Núm. 198, sec. 1.)	Las compañías de telecomunicaciones y cable adoptarán y presentarán ante la Junta una política de protección de la privacidad de información de sus usuarios. Dicha política deberá ser notificada a los usuarios y deberá describir qué tipo de información del usuario es recopilada y para qué fines y en qué circunstancias está sujeta a ser compartida con otras entidades públicas o privadas.	Salvo que se ordene explícitamente lo contrario la empresa deberá aceptar que el cliente le informe el número sin necesidad de presentar el original o la copia de la tarjeta de Seguro Social original
	L.P.R.A. Confidencialidad y privacidad Título XXIV- Parte VII. § 3535	Toda la información recopilada y analizada pertinente a este capítulo deberá mantenerse confidencial en el sentido de la identidad del paciente y se utilizará únicamente para los propósitos descritos en este capítulo. (a) Los datos obtenidos directamente de los expedientes médicos de un paciente es para el uso exclusivo	(c) El Departamento de Salud podrá publicar resultados de análisis de los reportes para propósitos científicos o de salud pública, asegurando que la identificación de los individuos esté debidamente protegida.



IRIARTE & ASOCIADOS



IRIARTE & ASOCIADOS

República Dominicana



Año	Legislación N° Normas	Regulación de que se trata	Observaciones
Art. 44 .2 Constitución		Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos...	
2004	Ley General de Libre Acceso a la Información Pública	Art. 20 Cuando no se trate de datos personales, especialmente protegido por derecho a la autodeterminación informativa del ciudadano, las administraciones indicadas en el Artículo 1 de esa Ley podrán permitir el acceso directo a las informaciones reservadas, recopiladas en sus acervos, siempre y cuando sean utilizadas para el giro normal de las competencias de los entes y órganos solicitantes y se respete, en consecuencia, el principio de adecuación al fin público que dio sentido a la entrega de la información.	



IRIARTE & ASOCIADOS

Año	Legislación N° Normas	Regulación de que se trata Observaciones
Constitucion Art. 10.1		Except with his own consent, a person shall not be hindered in the enjoyment of his freedom of expression, including freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons and freedom from interference with his correspondence.





IRIARTE & ASOCIADOS

Santa Lucía



 alfa - redi

Año	Legislación N° Normas	Regulación de que se trata	Observaciones
	Capitulo I , Constitución	c) protection for his family life, his personal privacy, the privacy of his home and other property and from deprivation of property without compensation,	
2007	Collective agreement Between the Government of Saint Lucia and the St. Lucia Police welfare association	Article 28 PERSONAL FILE 28.1 Before a confidential or adverse report is placed on a Police Officer's personal file, this report must be discussed with the employee concerned. 28.2 Members shall have the right to object or comment on any clause, which he or she thinks is unfair to him or her.	Por el periodo: Abril 1 de 2007 a Marzo 31 de 2010



IRIARTE & ASOCIADOS



Año	Legislación N° Normas	Regulación de que se trata	Observaciones
1999	Integrity in the Public Life Act	Se enumeran los funcionarios públicos cuyos datos personales tienen una menor protección	
1999	Freedom of Information Act	Prohíbe a las entidades públicas divulgar documentos con información personal de gobernados	Incluye cierta protección para las personas muertas





IRIARTE & ASOCIADOS

Para empezar

Y si aun asi no sabemos que hacer?

<http://vimeo.com/3462928>



**Taller sobre legislación en materia de ciberdelincuencia en América Latina
México, D.F.**

**31 de marzo (taller nacional)
1 y 2 de abril de 2014 (taller internacional)**

CONVENCIÓN SOBRE LA CIBERDELINCUENCIA:

Condiciones y salvaguardias

Alexander.seger@coe.int

www.coe.int/cybercrime

www.coe.int

**para
promover**

**La democracia
El Estado de
derecho
Los derechos
humanos**



**Medidas contra la
ciberdelincuencia**

Convención de Budapest: Derecho procesal

Artículo	Convención de Budapest	
Art. 14	Scope	Ámbito de aplicación de las disposiciones de procedimiento
Art. 15	Conditions and safeguards	Condiciones y salvaguardias
Art. 16	Expedited preservation	Conservación rápida de datos informáticos almacenados
Art. 17	Expedited preservation and partial disclosure of traffic data	Conservación y revelación parcial rápidas de los datos relativos al tráfico
Art. 18	Production order	Orden de presentación
Art. 19	Search and seizure	Registro y confiscación de datos informáticos almacenados
Art. 20	Real-time collection traffic data	Obtención en tiempo real de datos relativos al tráfico
Art. 21	Interception of content data	Interceptación de datos relativos al contenido
Art. 22	Jurisdiction	Jurisdicción

Artículo 15 – Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

Requisitos del estado de derecho

En términos generales, se esperaría que el Estado cumpla con los requisitos del estado de derecho como:

- **No habrá castigo sin una ley**
- **Todos tienen el derecho a un juicio justo, incluyendo la presunción de inocencia**
- **Interferencia con los derechos de las personas únicamente de acuerdo con la ley y con base en el interés público – incluyendo la prevención del delito – o la protección de los derechos de los demás. Las medidas de investigación deben ser prescritas por la ley**
- **Cualquier persona a quien se hayan violado sus derechos debe tener el derecho a un recurso efectivo**
- **Los Estados instituirán un marco que permita conciliar los intereses diferentes que deberán ser protegidos**
- **Obligación positiva de los estados de proteger los derechos de las personas. Esto puede incluir el derecho penal y la aplicación efectiva para llevar a los delincuentes ante la justicia**

Requisitos y principios del estado de derecho en relación con los poderes procesales de la Convención de Budapest

- **Principio de proporcionalidad**, con el significado específico de que “el poder o procedimiento será proporcional a la naturaleza y circunstancias del delito”. Por ejemplo, las medidas especialmente invasivas, como la interceptación, deberán limitarse a los delitos graves
- **Supervisión judicial u otra supervisión independiente**
- **Fundamentos que justifiquen la aplicación del poder o procedimiento y la limitación en alcance o duración**
- **Los poderes y procedimientos deben ser razonables y “considerar el impacto en los derechos, responsabilidades e intereses legítimos de terceros”**

Evaluación del artículo 15

Para propósitos prácticos, una evaluación del Artículo 15 podría incluir:

- Un inventario de los tratados internacionales de derechos humanos de los que el Estado es una parte
- Un panorama de cómo los requisitos anteriores se reflejan en la constitución de un Estado
- Un análisis de cómo los requisitos anteriores se reflejan en el derecho penal de un Estado en general
- Un análisis más específico de cómo se aplican estos requisitos cuando las medidas de los Artículos 16 (conservación rápida) al 21 (interceptación) se aplican a nivel nacional

¿Por qué es importante la protección de los datos?

- ▶ La protección / confidencialidad de los datos es un derecho fundamental
- ▶ Condición para los derechos humanos, democracia y estado de derecho
- ▶ Condición para la cooperación en aplicación de justicia
- ▶ Condición para la tercerización (*off-shoring*)
- ▶ Ayuda a proteger la confidencialidad, integridad y disponibilidad de datos y sistemas

Los “datos personales” es cualquier información personal que puede producir la identificación de alguna persona

Normas para la protección de datos del Consejo de Europa

“Convención 108 para la Protección de Datos”

Convención para la Protección de las Personas con respecto al Procesamiento Automatizado de sus Datos Personales (28 de enero de 1981)

“Protocolo 181 para la Protección de Datos”

Protocolo Adicional a la Convención 108 “relacionado con las autoridades de supervisión y los flujos transfronterizos” (2001)

Recomendaciones de leyes blandas (14)

Rec(1987)15 Uso de datos personales en el sector policíaco

Rec(2010)13 Procesamiento de datos personales para perfilamiento

Futuro de la Convención 108

Abierta para adhesión por estados no miembros

- Uruguay se integró en 2013
- Marruecos fue invitado a acceder
- La adhesión en proceso de consideración en otros países

Modernización de la Convención 108

Modernización en proceso para

- Enfrentar los desafíos nuevos de las tecnologías de información y comunicación
- Considerar un mecanismo de seguimiento (monitoreo)
- Negociaciones en marcha en el Comité CAHDATA

Conclusión

- ▶ **Obligación positiva de proteger a las personas contra delitos**
- ▶ **Condiciones que deben cumplirse cuando se interfiere con los derechos**
- ▶ **Artículo 115 de la Convención de Budapest**
- ▶ **Convención 108 para la protección de datos**
- ▶ **Justicia penal contra seguridad nacional**

La interferencia en los derechos fundamentales:

- **debe se prescrita por la ley y ser precisa, clara, accesible y previsible**
- **debe buscar un objetivo legítimo**
- **debe ser necesaria, esto es, debe responder a una necesidad social apremiante en una sociedad democrática y, por lo tanto, ser proporcional**
- **debe considerar recursos efectivos**
- **debe estar sujeta a garantías contra el abuso.**

Palabras para la clausura del Taller sobre Legislación en Materia de Ciberdelincuencia en América

Agradecimientos

- A la **Mtra. Mariana Benítez Tiburcio**, Subprocuradora Jurídica y de Asuntos Internacionales de la Procuraduría General de la República; al **Emb. Juan Manuel Gómez–Robledo Verduzco**, Subsecretario para Asuntos Multilaterales y Derechos Humanos de la Secretaría de Relaciones Exteriores, por la cooperación para el desarrollo del Taller, así como a la **Secretaría de Gobernación**, quien colaboró a través de la **Comisión Nacional de Seguridad**.
- Al **Sr. Alexander Seger**, Secretario Ejecutivo del Comité del Convenio sobre la Ciberdelincuencia, por el patrocinio y participación del Consejo de Europa.
- A los **Senadores y Diputados Federales** que nos acompañaron a lo largo del taller, y al **Diputado Héctor Gutiérrez de la Garza** por estar aquí hoy.
- Al **Magistrado Luis Fernando Angulo Jacobo**, Secretario Ejecutivo, Secretaría General de la Presidencia del Consejo de la Judicatura Federal, representante del Poder Judicial Federal.
- Al **Poder Judicial del DF**.
- A los **representantes de los ministerios de justicia y de relaciones exteriores de la región de América Latina**.
- La participación del **sector privado, de la Academia y de la sociedad civil**.

Buenas tardes.

Quiero resaltar el **hecho inédito** de la asistencia y participación activa de representantes de los tres Poderes de la Unión a este taller que ha sido un espacio de discusión sobre un asunto que nos toca enfrentar a todos: la ciberdelincuencia. Me da mucho gusto que estemos de acuerdo en la necesidad de hacer un frente común.

En un mundo como en el que vivimos, **es una prioridad la adaptación de las leyes y de las autoridades a un entorno que cambia todos los días, incluso cada hora.** El objetivo debe ser generar un **marco de confianza y seguridad para la ciudadanía**, adoptando las mejores prácticas a nivel internacional, como es el caso del Convenio 185 del Consejo de Europa, el “Convenio de Budapest”, y que ha sido el motivo que nos convocó a este Taller.

Durante estos tres días, pudimos ver un ejercicio de análisis y reflexión dividido en tres jornadas: la primera, dedicada al ámbito nacional y las otras dos orientadas al ámbito internacional. El objetivo fue **sensibilizar a los participantes, así como compartir experiencias sobre el fenómeno creciente de la ciberdelincuencia y los graves daños que ocasiona a la sociedad, ya sea sobre el patrimonio o la integridad de las personas y de las empresas y gobiernos.**

Desde la Coordinación de Estrategia Digital Nacional de la Oficina de la Presidencia de la República, se han abierto espacios de diálogo para que todos los involucrados en el tema puedan aportar ideas, compartir experiencias y propuestas.

La Estrategia Digital Nacional necesita, para lograr poner la tecnología al servicio de las grandes metas de desarrollo del país, **de un entorno seguro donde las personas puedan desarrollarse en el mundo digital e incorporarlo a sus actividades diarias.**

Los delitos cometidos por medios digitales afectan a todos y dificultan que se aprovechen los beneficios de la digitalización.

De diciembre de 2012 a febrero de 2014, según la información que presentó la Comisión Nacional de Seguridad, se han presentado **21 mil denuncias por ciberdelitos**, pero esta cifra puede aún ser lejana al número real de delitos cometidos, ya que no todos son denunciados.

El impacto económico es alto, pero es aún más cuando se considera la desconfianza que genera en la población. Para el año 2012 en México, el 36% de las personas señalaron que no realizaron compras en Internet por **miedo a proporcionar los datos de su Tarjeta de Crédito y que estos pudieran ser robados.**

Como ya lo mencionó la Subprocuradora Mariana Benítez en la inauguración del Taller, **se estima que la ciberdelincuencia en México cuesta alrededor de 39 mil millones de pesos a la economía**, cifra cercana a la que nos compartió el presidente de AMIPCI.

Por esto, la Estrategia Digital Nacional contempla en el habilitador de Marco Jurídico realizar adecuaciones jurídicas que permitan generar un entorno de certeza digital.

Aunque la mayoría de los cibercrimenes son formas más sofisticadas de otros tipos de crímenes que ya existían en el mundo offline, la ciberdelincuencia presenta retos novedosos a las autoridades, ya que los delincuentes han aprendido a utilizar las tecnologías para aumentar su alcance y mantenerse en el anonimato. **El Estado tiene la obligación de ser mejor en adoptar tecnologías para combatir este tipo de delitos.**

Para esto, es indispensable la colaboración de todas las autoridades dentro de México, y también, que las naciones tiendan líneas de comunicación que nos permitan compartir experiencia y combatir estas actividades más allá de forma internacional, ya que el ciberespacio no tiene fronteras.

Por ello, me da mucho gusto la valiosa participación de todos ustedes; de los ponentes internacionales que se dieron cita para aportar sus experiencias y compartir sus procesos de adhesión al Convenio.

A partir de lo discutido en el taller, quiero destacar las siguientes ideas en torno al tema:

Primero.- Sabemos que el impacto económico del cibercrimen es muy alto, pero existe un **costo social** aún mayor por el daño que ocasiona a ciertos sectores de la población.

Segundo.- Se requiere trabajar en la **generación de estadísticas** que permitan entender la magnitud de este fenómeno para poder contar con mejores políticas públicas para combatirlo;

Tercero.- Todos coincidimos en que es indispensable fomentar la **denuncia de los ciberdelitos**;

Cuarto.- El Cibercrimen es un fenómeno global, complejo y transfronterizo, por lo que es urgente continuar trabajando en los esquemas de cooperación internacional y con los diversos órdenes de gobierno para combatir el cibercrimen;

Quinto.- Es indispensable **adecuar nuestra legislación** para que las autoridades puedan combatir el cibercrimen de manera efectiva y oportuna.

Estoy convencida de que somos más los que queremos un México Digital con un entorno seguro y confiable. Sabemos que México todavía tiene bastante camino por recorrer, ya que es necesario tener mayor capacitación a nivel técnico, realizar la armonización legislativa en la materia, aumentar la coordinación con otros países, e incrementar la inversión tecnológica en seguridad.

Sin embargo, nos damos cuenta que existe la coincidencia de los tres poderes de la unión en hacer frente al fenómeno del Cibercrimen y en la necesidad de que se estrechen labores de colaboración, y que juntos emprendamos soluciones **para que Internet sea un espacio para la libertad de expresión y no un medio para el desarrollo del crimen.**

Después de tres productivos días en este Taller, invito a todos los sectores a colaborar y cooperar en el combate contra la ciberdelincuencia.

Ahora procederé a la **clausura**:

Siendo las __ horas del día 2 de abril del 2014, doy por concluido el Taller sobre la Legislación en Materia de Ciberdelincuencia en América Latina.

¡Muchas gracias a todos por su participación y buen regreso a casa!

TALLER SOBRE LEGISLACIÓN EN MATERIA DE CIBERDELINCUENCIA EN AMÉRICA LATINA

Jueves 03.04.14 | México, D. F. | Comunicado Conjunto Presidencia de la República-SRE-PGR

Del 31 de marzo al 2 de abril de 2014, con el co-auspicio del Gobierno de la República y del Consejo de Europa, se llevó a cabo en la sede de la Cancillería el “Taller sobre Legislación en materia de Ciberdelincuencia en América Latina”. Entre los temas abordados en el Taller se subrayó la necesidad de generar avances en el derecho penal sustantivo y procesal en materia de ciberdelito, la preservación de información digital, los mecanismos para agilizar la cooperación internacional entre gobiernos y con los prestadores de servicios de internet, las salvaguardias de los derechos humanos y la protección de datos en el internet, así como los procedimientos y opciones para culminar los procesos de adhesión de México y otros países de la región al Convenio de Budapest y de armonización de la legislación interna con el mismo.

La primera jornada, dedicada al ámbito nacional, fue inaugurada por la Subprocuradora Jurídica y de Asuntos Internacionales de la Procuraduría General de la República, Mtra. Mariana Benítez Tiburcio, quien manifestó que la adhesión de nuestro país a dicho instrumento, aunado a la aprobación de las reformas necesarias para actualizar nuestro marco jurídico, permitirán a México colocarse a la vanguardia, a fin de responder a las necesidades de la sociedad y convertirse en un líder en la zona en el combate a la ciberdelincuencia.

La inauguración del segmento internacional del Taller, el 1 de abril, correspondió al Emb. Juan Manuel Gómez – Robledo Verduzco, Subsecretario para Asuntos Multilaterales y Derechos Humanos de la Cancillería. En este segmento se sumaron representantes de Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú y República Dominicana, así como expertos del Consejo de Europa, de la Organización de los Estados Americanos y de los Estados Unidos.

Acompañaron al Subsecretario las senadoras Diva Hadamira Gastelum Bajo, integrante de la delegación mexicana ante la Asamblea Parlamentaria del Consejo de Europa y promovente de un punto de acuerdo para la adhesión de México al Convenio de Budapest, y Laura Angélica Rojas Hernández, Presidenta de la Comisión de Relaciones Exteriores – Organismos Internacionales de la Cámara Alta, al igual que el Sr. Alexander Seger, Secretario Ejecutivo del Convenio sobre la Ciberdelincuencia, del Consejo Europa, también conocido como Convenio de Budapest.

“Para México el Convenio de Budapest representa un referente obligado en los esfuerzos de la comunidad internacional en pro del fortalecimiento del Estado de derecho en el ciberespacio”, señaló el Emb. Gómez – Robledo, al tiempo de agregar que “sobre la base de la reforma constitucional en materia de telecomunicaciones y del lanzamiento presidencial de la Estrategia Digital Nacional”, el proceso de adhesión de México al citado convenio “representa, además, una oportunidad de evaluar y sintonizar la normatividad interna con las tendencias internacionales, tanto como de compartir nuestras mejores prácticas en este ámbito”.

La clausura, 2 de abril, estuvo a cargo de la Lic. Alejandra Lagunes Soto Ruíz, Coordinadora de Estrategia Digital Nacional de la Presidencia de la República, quien fue acompañada por el Mtro. Ignacio Ernesto Vásquez Chavolla, Oficial Mayor de la Cancillería; por el Diputado Héctor Humberto Gutiérrez de la Garza, Presidente de la Comisión de Comunicaciones de la Cámara de Diputados; y por el Lic. Ulises Gómez

Nolasco, Coordinador de Asuntos Internacionales y Agregadurías de la Procuraduría General de la República.

La Lic. Lagunes subrayó que la Estrategia Digital Nacional contempla como uno de sus habilitadores el Marco Jurídico que busca realizar adecuaciones jurídicas que permitan generar un entorno de certeza para los usuarios de Tecnologías de la Información. Mencionó que “el ciberespacio debe permanecer como una herramienta que potencie el ejercicio de la libertad de expresión y no un medio para el desarrollo del crimen”, y destacó la necesidad de generar estadísticas sobre este fenómeno que contribuyan a establecer las políticas públicas pertinentes, así como fortalecer los esquemas de cooperación internacional de la mano con los diversos órdenes de gobierno.

En lo que respecta a México, los representantes de los tres Poderes de la Unión coincidieron en que existen las condiciones políticas y jurídicas para que a más tardar el próximo periodo legislativo se aprueben las medidas antes señaladas. El Secretario Seger y los participantes agradecieron al Gobierno de México la organización del evento y coincidieron en que la concurrencia de los tres Poderes del Estado Mexicano, sector privado y academia en este Taller, es inédita, y refleja el compromiso de cada uno de ellos en su ámbito, por lo que será un referente para la celebración de otros a nivel internacional.

Promueven en México Convenio europeo sobre cibercrimen

El Consejo de Europa busca incorporar a México y a otros países a un convenio que tiene como fin reforzar la cooperación para atacar ese delito

31/03/2014 07:31 EFE

ESTRASBURGO (Francia), 31 de marzo.- El **Consejo de Europa** organiza martes y miércoles, junto con el gobierno mexicano, un taller sobre **legislación en materia de ciberdelincuencia** en **América Latina**, con participantes de países de la región interesados en adherirse al convenio europeo sobre el asunto.

En la reunión, prevista en la Ciudad de México, participarán parlamentarios y representantes de los Ministerios de Justicia y Exteriores de los países invitados por la organización paneuropea a sumarse al también llamado **Convenio de Budapest**: Argentina, Chile, Colombia, Costa Rica y México.

El taller estudiará asuntos como la amenaza del cibercrimen, la persecución de los delitos informáticos y la protección de menores “online”

Además, estarán presentes representantes de la República Dominicana y Panamá, únicos Estados de la región que son parte del citado convenio, y de Paraguay y Perú, que ya han mostrado su interés en incorporarse.

El máximo responsable del Comité del Convenio sobre cibercrimen, **Alexander Seger**, aseguró a Efe que su incorporación les permitirá “participar en una **cooperación internacional efectiva**”, ya que “el **cibercrimen** y las pruebas del **delito electrónico** son transnacionales”.

Además, la reforma de las legislaciones nacionales para adecuarlas al también conocido como **Convenio de Budapest** les proporcionará “una amplia base jurídica coherente con la de otros países y con los principios del Estado de derecho”.

El taller estudiará asuntos como la amenaza del cibercrimen, la persecución de los **delitos informáticos** y la protección de menores “online”.

Para Seger, el **abuso sexual a niños en la red es un ciberdelito “muy serio y generalizado”**, del que también se ocupa el **Convenio de Lanzarote**, centrado en la protección de menores contra la explotación y el **abuso sexual**.

La organización paneuropea de 47 Estados miembros anima a sus integrantes a implementar ambos para “permitir que las operaciones policiales nacionales e internacionales rescaten a las víctimas menores de edad y lleven a los delincuentes ante la justicia”.

De esos 47 miembros, han ratificado el Convenio sobre cibercrimen 36, aparte de Estados Unidos, Japón, Australia y Mauricio, mientras que Sudáfrica y Canadá lo han firmado.

dgp

Excelsior, disponible en
<http://www.excelsior.com.mx/hacker/2014/03/31/951462>

Gastélum pide suscribir Convenio de Budapest contra ciberdelincuencia



Por NTX | Notimex – mar, 1 abr 2014

México, 1 Abr. (Notimex).- La senadora priista Diva Gastélum urgió a que México suscriba el Convenio de Budapest y así se sume a la lucha contra la ciberdelincuencia, que es uno de los delitos más impunes.

Al señalar que ya está en comisiones del Senado un punto de acuerdo para que México suscriba este convenio, que habla del marco regulatorio que se debe tener contra la ciberdelincuencia, confió en que en breve se subirá al pleno dicha propuesta, del cual ella es autora, para su discusión.

Explicó que al no existir una regulación en este tema, en el anonimato se hacen muchísimas transgresiones a la ley: se destruyen nombres, hay pornografía infantil y se roban datos, entre otros delitos.

En conferencia de prensa, Gastélum Bajo explicó que la ciberdelincuencia es un tema que al presidente Enrique Peña Nieto y al Partido Revolucionario Institucional (PRI) les importa mucho, por lo cual ha iniciado una lucha que ya empieza a dar resultados en el país.

“Hoy nos dieron la grata noticia que el presidente de la República, a través de la cancillería, está haciendo todas las diligencias para que México suscriba el Convenio de Budapest”, externó.

La legisladora priista señaló que se requiere una reforma regulatoria, que va a llevar mucho tiempo, pero es momento de que México inicie esta gran tarea para controlar y sancionar uno de los delitos más impunes que se tienen no sólo en este país, sino en todo el continente.

La también titular del Organismo Nacional de Mujeres Priistas (ONMPRI) reveló además que están “muy metidos” en la reconstitución de esta organización.

Recordó que otras agrupaciones del partido como la Unidad Revolucionaria y el Frente Juvenil Revolucionario ya pasaron por su refundación, y ahora le corresponde a la ONMPRI.

“Estamos casi listas para entregar nuestros estatutos con un nuevo eslogan de nuestra organización, con una nueva imagen y con un espíritu muy renovado”, explicó.

Una de las reformas más importantes que se tuvieron en la XXI Asamblea Nacional del PRI, celebrada el año pasado, es que el instituto político garantizará la paridad de género en los cargos de elección popular.

Diva Gastélum añadió que hay reformas muy importantes en las que “se nos reconoce personalidad jurídica propia, patrimonio propio y presupuesto propio”.

NTX/MAH/CHA

Disponible en: <https://mx.noticias.yahoo.com/gast%C3%A9lum-pide-suscribir-convenio-budapest-ciberdelincuencia-181836258.html>

México se adhiere a Convenio de Budapest

Este tratado internacional, también conocido como Convenio sobre cibercriminalidad, busca combatir delitos en internet mediante la armonización de leyes nacionales.

JOSÉ ANTONIO BELMONT 03/04/2014 04:30 PM

Ciudad de México

El gobierno federal anunció la adhesión de México al Convenio de Budapest, el cual busca combatir delitos en internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y la coordinación entre las naciones incluidas en el mismo.

La subprocuradora Jurídica y de Asuntos Internacionales de la PGR, Mariana Benítez, destacó que la unión del país a dicho instrumento, aunado a la aprobación de las reformas "necesarias" para actualizar el marco jurídico, permitirán a México convertirse en un líder en la zona en el combate a la ciberdelincuencia.

Por su parte, el subsecretario para Asuntos Multilaterales y Derechos Humanos de la Secretaría de Relaciones Exteriores, Juan Manuel Gómez-Robledo aseguró que "para México el Convenio de Budapest representa un referente obligado en los esfuerzos de la comunidad internacional en pro del fortalecimiento del Estado de derecho en el ciberespacio".

"Sobre la base de la reforma constitucional en materia de telecomunicaciones y del lanzamiento presidencial de la Estrategia Digital Nacional", el proceso de adhesión de México a dicho convenio "representa, además, una oportunidad de evaluar y sintonizar la normatividad interna con las tendencias internacionales, tanto como de compartir nuestras mejores prácticas en este ámbito", destacó.

Dicho documento fue elaborado por el Consejo de Europa en Estrasburgo.

Disponible en http://www.milenio.com/policia/Cibercriminalidad-Mexico-adhiere-Convenio_de_Budapest-PGR-delitos_informaticos-delitos_en_internet_0_274173006.html