CONFERENCIA INTERNACIONAL

Y

SEGUNDA REUNIÓN de

CiberRed/*CiberRede*

(25 y 26 de junio de 2019)

CONCLUSIONES DE LA COORDINACIÓN

MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

AIAMP
Asociación Ibero Americana de Ministerios Públicos

CONFERENCIA INTERNACIONAL Y SEGUNDA REUNIÓN DE CiberRed/*CiberRede*

CONCLUSIONES DE LA COORDINACIÓN

A – LA REUNIÓN

1. El 26 de junio de 2019, se celebró en Santiago, Chile, la segunda reunión de CiberRed/*CiberRede*, la Red Iberoamericana de Ministerios Públicos Especializados en Ciberdelincuencia. Junto con ella, los días 25 y 26, se realizó una conferencia internacional sobre ciberdelito y obtención de prueba digital, dirigida a los puntos de contacto de la red. Asistieron 27 participantes, en representación de 15 de los países de la AIAMP[1]. Apenas no estuvieron representados Honduras, El Salvador, Ecuador, Nicaragua, Uruguay[2] y Venezuela. Se incluye en el Anexo A la lista de participantes y en el Anexo B la agenda de la reunión.

2. CiberRed/*CiberRede* se constituyó por deliberación de la XXIV Asamblea General de la Asociación Iberoamericana de Ministerios Públicos - AIAMP (celebrada en Lisboa, en octubre de 2016). Actualmente incluye puntos de contacto de 19 de los 21 Ministerios Públicos miembros de la AIAMP. Se trata de una red de fiscales especializados en ciberdelincuencia cuyo objetivo es promover y mejorar la información disponible sobre los diferentes sistemas jurídicos iberoamericanos en el campo del ciberdelito, para fomentar el intercambio de experiencias y conocimientos necesarios para resolver los numerosos problemas que surgen en esta área, crear y difundir buenas prácticas entre sus miembros y optimizar y acelerar la cooperación institucional y las solicitudes de cooperación internacional entre los distintos países.

La XXIV Asamblea General de la AIAMP también decidió que esta red sería un foro para el contacto y el intercambio sobre las tendencias del ciberdelito y la obtención de evidencia digital y, por lo tanto, debería celebrar una reunión anual de sus puntos de contacto.

3. Este fue el contexto de la segunda reunión de *CiberRed*/ CiberRede y también fue en este contexto que se eligieron los temas de discusión de la conferencia internacional, que buscaban explorar el tema estratégico del ciberdelito en el espacio iberoamericano (fenómenos criminales y legislación), así como la reacción de los Ministerios Públicos y Fiscalías para enfrentar este desafío.

[1] Argentina, Brasil, Chile, Colombia, Costa Rica, Cuba, España, Guatemala, México, Panamá, Paraguay, Perú, Portugal y República Dominicana.
[2] En cuanto al representante uruguayo, no pudo asistir por motivos de salud graves y de última hora.

4. Se dejan de seguida, las conclusiones que la Coordinación de la red, a cargo de Portugal, obtuvo de la reunión.

B – LAS NORMAS DEL CIBERDELITO EN EL ESPACIO IBEROAMERICANO

5. Una de las conclusiones más visibles de la reunión fue la existencia de algunos marcos regulatorios en temas de ciberdelito en los países iberoamericanos. En este sentido, de la reunión surgió que algunos de los países ya tienen marcos regulatorios específicos al respecto (ya sea llamándolos delito informático, delito cibernético, ciberdelito o cibercrimen).

Sin embargo, este no es todavía el caso de un número significativo de países, que solo tienen previsiones de delitos de ámbito más genérico, aunque susceptibles de ser cometidos en las redes. Estos últimos no siempre se adaptan a las nuevas realidades, por lo que se necesitaría cierta innovación legislativa o al menos algún ajuste legal. En la mayoría de estos casos, existe la efectiva necesidad de una introducción legislativa de delitos informáticos o ciberdelitos propiamente dichos. Algunos de estos países ya están dando pasos en esta dirección, basándose tanto en el Convenio de Budapest como en la legislación de otros países de región.

C - NORMAS RELATIVAS A LA EVIDENCIA DIGITAL EN LA REGIÓN IBEROAMERICANA

6. La conclusión es más pesimista con respecto a los estándares para obtener evidencia digital: solo un pequeño número de países iberoamericanos tienen normas de procedimiento específicamente destinadas a obtener prueba digital. En algunos casos, los marcos regulatorios generales se aplican al entorno digital, aunque de forma inadecuada.

En este sentido, además de la falta normativa, también se identificó la necesidad de una mayor discusión e identificación de las lagunas en cada país.

7. El Anexo C proporciona un resumen de los marcos regulatorios de los distintos países presentes en la reunión.

D – REQUISITOS ESPECIFICOS DE ESPECIALIZACIÓN Y CAPACITACIÓN

8. En otra vertiente, se podría concluir que, de manera uniforme en los distintos países, los delitos en las redes de comunicaciones se están expandiendo rápidamente. Debido a su complejidad, requieren conocimientos especializados y medios específicos de investigación. La necesidad generalizada de

capacitación de fiscales se hizo evidente. También se afirmó en repetidas ocasiones la necesidad de una actualización frecuente de esta capacitación, tal vez mediante el intercambio de conocimientos y buenas prácticas entre los fiscales, o tal vez mediante la discusión de casos prácticos.

9. Por otro lado, se destacó la necesidad de especialización de los fiscales en esta área como una de las conclusiones más claras de la reunión. Sin embargo, la forma en que los distintos países enfrentan esta necesidad es disonante, el panorama es muy diferente y hay varios modelos. En algunos de los países iberoamericanos, esta especialización, que ya existe, se ha afirmado insistentemente como una necesidad inevitable porque no es posible investigar el ciberdelito de otra manera.

10. La comparación de los distintos modelos, con la recopilación de sus ventajas, permitió el intercambio de experiencias para proporcionar a los participantes pistas para la evolución interna, en cada país, en el futuro. Entre los países representados, se concluyó que, en general, se sigue uno de los siguientes distintos modelos:

1. unidades de investigación centralizadas nacionales especializadas;
2. unidades de coordinación nacional, con descentralización de la investigación en puntos focales;
3. unidades nacionales de coordinación (centradas específicamente en la capacitación y el apoyo a distancia) y dispersión de la investigación;
4. unidades nacionales de investigación (no específicamente especializadas);
5. unidades nacionales de apoyo técnico, con dispersión de la investigación y
6. inexistencia de especialización.

D. 1) UNIDADES DE INVESTIGACIÓN CENTRALIZADAS NACIONALES ESPECIALIZADAS

11. En algunos de los Ministerios Públicos o Fiscalías se decidió concentrar las investigaciones en una estructura de alcance y competencia nacional. En dicha estructura, de manera centralizada, las investigaciones son desarrolladas por un cuerpo especializado de fiscales. Este ha sido el caso, por ejemplo, de República Dominicana, desde 2013, cuando se creó una Unidad Especializada de Ciberdelito. Paraguay, que adoptó un modelo similar, también creó una unidad especializada en Asunción, la capital del país, aunque en este caso también tiene funciones de apoyo técnico.

D. 2) UNIDADES DE COORDINACIÓN NACIONAL, CON DESCENTRALIZACIÓN DE LA INVESTIGACIÓN EN PUNTOS FOCALES

12. En otros casos, aunque el Ministerio Público o Fiscalía hayan establecido una unidad de coordinación centralizada, han decidido asignar las investigaciones concretas descentralizadas a las autoridades de todo el territorio, aunque con especialización. Por lo tanto, la unidad central asume predominantemente funciones de garantizar la unidad de acción en todo el país y de una acción coordinada.

Este fue el modelo adoptado en España y Portugal. Ambos países tienen una unidad nacional que coordina, pero las investigaciones concretas se distribuyen a puntos de contacto especializados dispersos por todo el territorio. Algunos de estos puntos de contacto trabajan exclusivamente en investigaciones en esta área, mientras que otros, a pesar de la especialización, también asumen otras funciones (de acuerdo con las características específicas del área territorial a la que están adscritos).

En cuanto a la coordinación concreta, el modelo portugués está más orientado a los métodos, mientras que el modelo español también se centra en la coordinación operativa y jerárquica de los puntos de contacto.

D. 3) UNIDADES NACIONALES DE COORDINACIÓN (CENTRADAS ESPECÍFICAMENTE EN LA FORMACIÓN Y EL APOYO A DISTANCIA) Y DISPERSIÓN DE LA INVESTIGACIÓN

13. En otros casos, el modelo de coordinación nacional está más orientado al apoyo remoto y la capacitación de fiscales. Es decir, la unidad nacional establecida tiene como vocación, sobre todo, implementar la capacitación de los investigadores, quienes, de manera especializada o no, dependiendo de la opción local, asumen la investigación de manera dispersa.

Se registra que este fue el modelo adoptado por países con estructura federal, como Brasil y Argentina, que se suman a la existencia de un Ministerio Público Federal y, en paralelo, a fiscales estatales o provinciales. En ambos casos, hay enfoques de especialización en algunas circunscripciones, pero no en otras, en las que la investigación se realiza de manera dispersa por los distintos fiscales.

En el caso de Chile, la situación se mitiga: existe una coordinación nacional y una estructura de apoyo centrada en cuestiones de ciberdelito que incorpora componentes técnicos, que son responsables de apoyar a los fiscales de todo el país en investigaciones concretas. Pero junto con esto, existe experiencia a nivel local en temas de ciberdelito: hay fiscales específicos asignados a investigaciones en esta área (ciberdelito y otros delitos relacionados con tarjetas bancarias), aunque también tienen otras competencias funcionales.

D. 4) UNIDADES NACIONALES DE INVESTIGACIÓN (NO ESPECÍFICAMENTE ESPECIALIZADAS)

14. En otros casos, los temas de ciberdelito son abordados por unidades nacionales especializadas, pero no específicamente en cibercrimen, sino en temas más amplios y abarcadores como el crimen organizado, el crimen grave o incluso algún más específico.

En general, estas unidades nacionales se crearon para tratar problemas específicos relevantes en el contexto local, y luego, con el surgimiento del ciberdelito, también le fue asignado este tema y pasaron a investigar tales casos.

Este es el caso de Costa Rica, que tiene una Fiscalía Nacional especializada en fraude y que también investiga casos de delitos informáticos. Esta unidad nacional, que tiene una gama más amplia de competencias, también se dedica al apoyo y a la capacitación en temas ciberdelito.

Pero también es el caso de Colombia, que agregó la investigación de algunos casos de delito cibernético a una unidad nacional especializada en la investigación del crimen organizado. Sin embargo, la competencia de esta unidad nacional no es exclusiva, y hay investigaciones de casos de delitos cibernéticos dispersos por las distintas unidades territoriales del país.

En Panamá, la situación es similar: hay una unidad especializada en delitos de derechos de autor que tiene jurisdicción para investigar algunos casos de ciberdelito, aunque la investigación de tales casos esté igualmente dispersa entre otros departamentos del Ministerio Público.

D. 5) UNIDADES NACIONALES DE APOYO TÉCNICO, CON DISPERSIÓN DE LA INVESTIGACIÓN

15. Algunos países han optado por establecer unidades nacionales con más vocación de apoyo técnico (tecnológico), descentralizando la investigación penal en sí.

Este fue el caso de México, que creó una unidad nacional de apoyo puramente técnico, permitiendo que la investigación criminal se llevara a cabo de manera dispersa en los distintos departamentos del territorio. La función de esta unidad nacional es simplemente brindar apoyo técnico a los investigadores, y no ser la responsable de las funciones específicas de investigación y enjuiciamiento, ni de coordinar estas investigaciones.

La situación en Guatemala está cerca de esta, aunque la estructura nacional especializada creada, si bien incluye esta valencia, no está orientada exclusivamente al delito cibernético.

D. 6) INEXISTENCIA DE ESPECIALIZACIÓN

16. Finalmente, algunos de los países aún no han establecido ninguna forma de especialización de las Fiscalías o del Ministerio Público en este sentido. De esta forma, las investigaciones concretas están dispersas en las circunscripciones territoriales. Este es particularmente el caso de Perú y Cuba.

E – CiberRed/*CiberRede*

17. Por otro lado, en cuanto a CiberRed/*CiberRede* en sí misma y su funcionamiento y potencialidades, también se formularon conclusiones.

E. 1) LA IMPORTANCIA DE LA RED

18. Entre los participantes, se reforzó la convicción del valor agregado de la red y de sus reuniones, ya que constituye un foro permanente y especializado que facilita el intercambio de experiencias y buenas prácticas entre fiscales. En este sentido, los participantes expresaron que hay una gran utilidad en la celebración de reuniones presenciales, pero también sería una ventaja permitir el contacto permanente a través de una plataforma segura de comunicaciones electrónicas. Dicha plataforma permitiría el intercambio permanente de información no sensible entre puntos de contacto: se mencionó la posibilidad de utilizar la plataforma existente Iber@, administrada por IberRed.

Una plataforma de comunicaciones, por ejemplo, podría proporcionar aclaraciones temáticas y específicas de otros colegas en casos específicos. O conseguir elementos de trabajo. O compartir iniciativas de capacitación.

Dado que todavía no se dispone de una plataforma segura para el intercambio de información, se creó un grupo de Whatsapp como medio para garantizar provisionalmente un contacto expedito, en el se incluyendo todos los puntos de contacto disponibles para este fin.

E. 2) COMPARTIR EXPERIENCIAS Y BUENAS PRÁCTICAS

19. Durante la reunión, se compartieron casos concretos de iniciativas de algunos de los países representados (algunos de los cuales se describen de seguida), lo que demuestra el potencial de este intercambio de experiencias y buenas prácticas.

La República Dominicana, que se ha encontrado con numerosos casos de estafas de *Business Email Compromisse* (que en Europa es mejor conocida como *CEO Fraud*), ha decidido crear un manual para combatir este crimen, que prevé la creación de un portal web en el Ministerio Público, que centraliza la información en tiempo real sobre este tipo de casos: este método ha permitido la identificación de las

"*money mules*". También de esta manera, se proporciona información a las víctimas sobre la mejor manera de responder cuando se produce este tipo de delito. Esta experiencia se puede mejorar si se comparte con otros fiscales.
También la República Dominicana, compartió un "*Protocolo de investigación y procesamiento de casos de explotación sexual en línea de niños, niñas y adolescentes*", un manual que tiene como objetivo ayudar a todos los fiscales en la investigación de delitos de explotación sexual de niños y jóvenes.
Por su parte, Brasil compartió que organizó un "*Roteiro de investigação de crimes cibernéticos*", que se tradujo al español y, por lo tanto, podría utilizarse en toda Iberoamérica.
Finalmente, a modo de ejemplo, México ha producido y compartido una "*Guia Técnica de Cadena de Custodia de Evidencia Digital*", un manual técnico para respaldar las investigaciones sobre la recopilación de prueba digital.

20. De las discusiones quedó claro que habría una ventaja en dinamizar un espacio dedicado a esta red en el sitio *web* de la AIAMP. Dicho espacio debe usarse para revelar la existencia y el potencial de *CiberRed*/CiberRede, pero también de otra información pública o publicable, como manuales de buenas prácticas o jurisprudencia sobre cibercrimen y evidencia digital.

E. 3) INTERCAMBIO DE INFORMACIÓN OPERATIVA

21. Según se dice, se presentará muy pronto en una próxima reunión de COMJIB (Conferencia de Ministros de Iberoamérica), un proyecto de tratado internacional para regular la transmisión electrónica de solicitudes de asistencia mutua entre los estados de COMJIB.
Sin embargo, en la actualidad, dentro del área AIAMP, todavía no existe un marco legal que permita el intercambio de solicitudes de cooperación internacional en materia penal por medios electrónicos. Por lo tanto, el método de uso de las cartas o comisiones rogativas clásicas, transmitidas en papel, entre las Autoridades Centrales de cooperación internacional, todavía está en vigor.

22. No obstante, CiberRed/*CiberRede* puede utilizarse ya, ahora y en el contexto actual, como modo de apoyo técnico entre los diversos puntos de contacto, así como para intercambios informales, al margen de las solicitudes formales de cooperación.
En este sentido, al proporcionar información operativa, se subrayó la utilidad del Acuerdo de Cooperación Interinstitucional celebrado en la Asamblea General de la IAAMP de México en 2018.
Además, también se subrayó que CiberRed/*CiberRede* es el foro apropiado para el debate sobre la posibilidad de crear herramientas de cooperación internacional específicas para la evidencia digital en el futuro.

E. 4) CONSOLIDACIÓN DE PUNTOS DE CONTACTO

23. Como se mencionó, CiberRed/*CiberRede* tiene puntos de contacto que representan a 19 de los 21 países miembros de la AIAMP. Es decir, todavía hay dos Ministerios Públicos de la AIAMP[3] que no nominaron a sus representantes como puntos de contacto.

A la primera reunión de la red, en Lisboa, asistieron representantes de 18 países miembros. La segunda reunión solo tuvo representantes de 15 países miembros. Se concluyó que, entre la primera y la segunda reunión, algunos de los puntos de contacto fueron asignados a posiciones funcionales distintas de las que tenían antes, y ya no funcionan como puntos de contacto. Muchos de ellos no reportaron este facto a la Coordinación de la red, por lo que fue necesario solicitar su reemplazo en un momento muy cercano a la reunión. Además, con respeto a algunos de los puntos de contacto, ni siquiera fue posible establecer una comunicación efectiva sobre la reunión.

Por lo tanto, sería importante crear conciencia, en la próxima reunión Asamblea General de la AIAMP, del creciente papel y la relevancia de esta red y la importancia de consolidar las funciones de los puntos de contacto.

E. 5) MARCOS NORMATIVOS EN EL ÁREA DEL CIBERDELITO Y DE LA PRUEBA DIGITAL

24. Desde el principio, CiberRed/*CiberRede* ha asumido que uno de los vectores más importantes para facilitar la cooperación internacional es la armonización de las distintas leyes nacionales. Por esta razón, el intercambio de puntos de vista sobre los marcos regulatorios de diferentes países sobre ciberdelito y pruebas digitales se ha incluido en las discusiones. Solo conociendo el marco regulatorio de aquellos países con los que se coopera será posible maximizar las herramientas de cooperación internacional.

Los participantes en la reunión, por lo tanto, indicaron que es importante, para intensificar su conocimiento de las leyes de otros países, desarrollar un breve estudio comparativo del ciberdelito y la prueba digital. Tal estudio puede llevarse a cabo en base a cuestionarios que se distribuirán a los puntos de contacto.

E. 6) SOSTENIBILIDAD DE LA RED

25. Las dos reuniones de los puntos de contacto CiberRed/*CiberRede* (celebradas en Lisboa en febrero de 2018 y Santiago, Chile en junio de 2019) contaron con el apoyo del programa GLACY + del Consejo de Europa. El apoyo de este programa, financiado por la Unión Europea, ha permitido cubrir los viajes de los puntos de contacto, así como su alojamiento y alimentación. También fue este programa el que, en el caso de Santiago, financió los gastos con la sala de la reunión (que, en el caso de la reunión de Lisboa, fue proporcionada por la Procuraduría-General de la República de Portugal).

Con los apoyos referidos fue posible celebrar ambas reuniones sin asumir ninguna carga financiera para los participantes o para los Ministerios Públicos de Iberoamérica.

Sin embargo, sería importante considerar soluciones de sostenibilidad de la red, buscando otras fuentes de financiación que garanticen su continuidad y la autonomía.

8 de octubre de 2019

[3] Nicaragua y Venezuela.

ANEXO A

Conferencia Internacional y 2ª Reunión Anual de CiberRed

RED IBEROAMERICANA DE FISCALES ESPECIALIZADOS EN CIBERDELINCUENCIA

Conferência Internacional e 2ª Reunião Anual da CiberRede

REDE IBERO-AMERICANA DE MINISTÉRIOS PÚBLICOS ESPECIALIZADOS EM CIBERCRIME

Santiago de Chile, 25 e 26 de Júnio de 2019
Santiago do Chile, 25 e 26 de junho de 2019

LISTA DE PARTICIPANTES

País	Nome	Cargo
ARGENTINA	**Horacio Azzolín**	*Unidad Especializada en Ciberdelincuencia*
BRASIL	**Fernanda Domingos**	Grupo de Trabalho sobre Crimes Cibernéticos
BRASIL	**Neide de Oliveira**	Coordenadora do Grupo de Trabalho sobre Crimes Cibernéticos
CHILE	**Antonio Segovia Arancibia**	*Fiscalía Nacional - Director – Unidad de Cooperación Internacional y Extradiciones*
CHILE	**Camila Bosch**	*Fiscalía Nacional - Unidad de Cooperación Internacional y Extradiciones*
CHILE	**Constanza Encina**	*Fiscalía Regional Oriente Alta Complejidad*
CHILE	**Eduardo Baeza**	*Fiscal adjunto*
CHILE	**Giovanna Herrera**	*Fiscal adjunto*
CHILE	**Luis Herrera**	*Fiscalía Regional Sur Puente Alto*
CHILE	**Mauricio Fernández Montalbán**	*Director-Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado (Fiscalía Nacional)*
CHILE	**Monserrat Ramirez**	*Fiscalía Nacional - Unidad de Cooperación Internacional y Extradiciones*
COLOMBIA	**Luis Orlando Paloma Parra**	*Fiscal del eje de cibercriminalidad de la Dirección contra las organizaciones criminales*
COSTA RICA	**Carlos Castro Sojo**	*Fiscal – Unidad Ciberdelito – Oficina de Fraudes*
CUBA	**Dimas Herrera Gandol**	*Secretaria del Fiscal General*
ESPAÑA	**Ana Maria Martín**	*Fiscal de Criminalidad Informática*
ESPAÑA	**Elvira Tejada**	*Fiscal de Sala de Criminalidad Informática*

GUATEMALA	**Andrea Lisbeth Mejia Mendez**	*Departamento de Ciber Delito*
GUATEMALA	**María Elena Galvez Rafael**	*Jefa del Departamento de Ciber Delito*
MÉXICO	**Marco Mecalco Raya**	*Unidad de Investigaciones Cibernéticas*
PANAMÁ	**Martín Oscar Rodriguez Lezcano**	*Fiscal Especializado en Delitos Contra la Propiedad Intelectual y Seguridad Informática*
PARAGUAY	**María Soledad Machuca Vidal**	*Fiscal Adjunta encargada de la Unidad Especializada de Delitos Informáticos del Ministerio Público*
PERÚ	**Ángela Olivia Arévalo Vásquez**	*Fiscal - Unidad de Cooperación Judicial Internacional y Extradiciones de la Fiscalía de la Nación*
PORTUGAL	**Pedro Verdelho**	Coordenador do Gabinete Cibercrime
REPÚBLICA DOMINICANA	**Iván Féliz Vargas**	*Procurador General de Corte, Titular de la Procuraduría Especializada para Delitos de Alta Tecnología*
COUNCIL OF EUROPE	**Manuel de Almeida Pereira**	*Project Manager* *Cybercrime Programme Office (C-PROC)*
COUNCIL OF EUROPE	**Andrei-Stefan Candrea**	*Project Assistant* *Cybercrime Programme Office (C-PROC)*

ANEXO B

Conferencia Internacional y 2ª Reunión Anual de CiberRed

RED IBEROAMERICANA DE FISCALES ESPECIALIZADOS EN CIBERDELINCUENCIA

Conferência Internacional e 2ª Reunião Anual da CiberRede

REDE IBERO-AMERICANA DE MINISTÉRIOS PÚBLICOS ESPECIALIZADOS EM CIBERCRIME

Santiago de Chile, 25 e 26 de Júnio de 2019
Santiago do Chile, 25 e 26 de junho de 2019

CONFERENCIA INTERNACIONAL 25 DE JUNIO	CONFERÊNCIA INTERNACIONAL 25 DE JUNHO
10:00 – Inauguración *Representante del Ministerio Público de Chile* *Representante del Consejo de Europa* *Representante de Unión Europea*	**10:00 – Abertura** *Representante do Ministério Público do Chile* *Representante do Conselho de Europa* *Representante da União Europeia*
SESIÓN 1 – EL CIBERDELITO EN EL ESPACIO IBEROAMERICANO **10:15 – El marco internacional de la ciberdelincuencia: la Convención de Budapest – *Pedro Verdelho - Portugal* (***Breve presentación e intervención de los participantes)*** **11:00** – Pausa **11:15 - El panorama legislativo en el ámbito del ciberdelito y de la obtención de prueba digital, en los países miembros de AIAMP** *Sesión con intervención de los participantes* **13:00** – Pausa	**SESSÃO 1 – O CIBERCRIME NO ESPAÇO IBEROAMERICANO** **10:15 – Enquadramento internacional do cibercrime: a Convenção de Budapeste – *Pedro Verdelho - Portugal* (***Breve apresentação e intervenção dos participantes)*** **11:00** – Pausa **11:15 – O panorama legislativo na área do cibercrime e da obtenção de prova digital, nos países membros da AIAMP** *Sessão com intervenção dos participantes* **13:00** – Pausa
SESIÓN 2 – COOPERACIÓN EN LA OBTENCIÓN DE PRUEBA DIGITAL **14:30 – La Convención de Budapest: instrumentos específicos y la rede 24/7 – *Elvira Tejada - España*** *(Breve presentación e intervención de los participantes)* **15:30** – Pausa **15:45 – Experiencias y buenas prácticas:** **a) cooperación con operadores de comunicaciones nacionales y**	**SESSÃO 2 – COOPERAÇÃO NA OBTENÇÃO DE PROVA DIGITAL** **14:30 – A Convenção de Budapeste: instrumentos específicos e a rede 24/7 – *Elvira Tejada - Espanha*** *(Breve apresentação e intervenção dos participantes)* **15:15** – Pausa **15:30 – Experiências e boas práticas:** **a) cooperação com operadores de telecomunicações nacionais e**

globales - ***Neide de Oliveira e Fernanda Domingos - Brasil*** b) equipos conjuntos de investigación ***-Ana María Martin - España*** *Breves presentaciones e intervención de los participantes* **17:30** - cierre del día	globais - ***Neide de Oliveira e Fernanda Domingos - Brasil*** b) equipas conjuntas de investigação - ***Ana Maria Martin - Espanha*** *Breves apresentações e intervenção dos participantes* **17:30** – encerramento do dia
CONFERENCIA INTERNACIONAL 26 DE JUNIO	**CONFERÊNCIA INTERNACIONAL 26 DE JUNHO**
SESIÓN 3 - EL MINISTERIO PÚBLICO Y LAS EXIGENCIAS DEL CIBERDELITO **10:00 - Estructuras especializadas del Ministerio Público, en el área del Ciberdelito** *Sesión con intervención de los participantes* **11:30 –** Pausa **11:45 – Cooperación Internacional de los Ministerios Públicos y Fiscalías de Iberoamérica - *António Segovia - Chile*** **12:30 – El Ministerio Público e el desafío del ciberdelito - *Pedro Verdelho - Portugal*** **13:00** – Cierre	**SESSÃO 3 – O MINISTÉRIO PÚBLICO E AS EXIGÊNCIAS DO CIBERCRIME** **10:00 – Estruturas especializadas do Ministério Público, na área do Cibercrime** *Sessão com intervenção dos participantes* **11:30** – Pausa **11:45 – Cooperação Internacional dos Ministérios Públicos e *Fiscalías* da Ibero-América – *António Segovia – Chile*** **12:30 - O Ministério Público e o desafio do cibercrime - *Pedro Verdelho - Portugal*** **13:00** – Encerramento
2ª REUNIÓN ANUAL DE CIBERRED 26 DE JUNIO	**2ª REUNIÃO ANUAL DA CIBERREDE 26 DE JUNHO**
14:30 – Inauguración **TEMA GENERAL: *CiberRed* EN EL PRÓXIMO TRIENIO: DESAFÍOS** **14:35 – Objetivos estratégicos de *CiberRed* para el próximo trienio** *Intervención de los participantes* **15:00 - Necesidades de formación especializada** *Intervención de los participantes* **15:30 – La próxima reunión de CiberRed: tema y formato** *Intervención de los participantes* **16:00** – Conclusiones y cierre	**14:30 – Abertura** **TEMA GERAL:– A *CiberRede* NO PRÓXIMO TRIÉNIO: DESAFIOS** **14:35 – Objetivos estratégicos da *CiberRede* para o próximo triénio** *Intervenção dos participantes* **15:00 – Necessidades de formação especializada** *Intervenção dos participantes* **15:30 – A próxima reunião da *CiberRede*: tema e formato** *Intervenção dos participantes* **16:00 – Conclusões e encerramento**

ANEXO C

CIBERCRIME E PROVA DIGITAL

SÚMULA DOS QUADROS NORMATIVOS

	NORMAS EM VIGOR	PROJETOS LEGISLATIVOS
ARGENTINA	O *Código Penal*, por via da *Ley 26388* (http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm) e da *Ley 26904* (http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm) inclui a maior parte dos tipos de crime da Convenção de Budapeste. Foi recentemente introduzida legislação interna que incrimina a mera posse de pornografia infantil. Não existem normas específicas sobre prova digital, uma vez que o Código Procesal Penal, alterado pela Ley 27063 (http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239340/norma.htm#28), apenas inclui, nos artigos 143 e 144, a interceção de comunicações e a apreensão de dados.	Existe um projeto de alteração do *Código Penal*, para passar a incluir novas condutas (como por exemplo a *revenge porn* e o uso de identidade falsa na Internet – existem muitos casos de uma e outra situação). Existem planos para ajustar o *Código Procesal Penal*.
BOLIVIA	Não existem tipos específicos de crimes neste campo – apenas, no Código Penal, um crime de manipulação informática de dados e de alteração, acesso e uso indevido de dados. Não existem normas específicas sobre prova digital – aplicam-se, dentro do possível, as normas gerais.	*OBS: informação recolhida na primeira reunião da CiberRede*
BRASIL	A Lei 12737 (https://www.jusbrasil.com.br/topicos/10605134/artigo-266-do-decreto-lei-n-2848-de-24-de-fevereiro-de-1891) introduziu no Código Penal (Artigos 154-A, 154-B, 266 e 313-A) os crimes de acesso ilegítimo, difusão ilícita de dispositivos e ataques de denegação de	Está pendente no Senado o Projeto de Lei PL 236/2012 (projeto de novo Código Penal), que prevê os crimes da Convenção de Budapeste (https://www25.senado.leg.br/web/atividade/materias/-/materia/106404/pdf).

	serviço. Ainda criminalizou a falsificação de cartões de crédito. Recentemente foi introduzido no Código Penal o Artigo 218º-C (pornografia de vingança), que já está em vigor. O Estatuto da Criança e Adolescente (https://presrepublica.jusbrasil.com.br/legislacao/91764/estatuto-da-crianca-e-do-adolescente-lei-8069-90#art-240), nos artigos 240, 241-A, 241-B, 241-C e 241-E, prevê a punição de pornografia infantil. Não existem normas específicas sobre prova digital. Foi publicada, entretanto, a Lei de Proteção de Dados, a qual entrará em vigor no ano de 2020.	
CHILE	A Lei Nº 19.223, de 1993 (http://bcn.cl/1uw5c), tipifica figuras penais relativas à informática. O Código de Processo Penal tem algumas normas aplicáveis à obtenção de prova digital (nos Artigos 222 a 226bis), designadamente sobre interceção de comunicações.	Está presentemente em discussão no Senado um projeto de lei de alteração do quadro penal substantivo, que tem em vista adotar todas as normas previstas na Convenção de Budapeste (*Boletín Nº* 10145-07 - http://www.senado.cl/appsenado/templates/tramitacion/index.php). Está igualmente em discussão um projeto de lei de revisão da Lei 20.009 (o seu processo está mais avançado e mais próximo do seu final) que, além de norma processuais respeitantes a prova digital, incorpora também normas substantivas referentes a ilícitos relacionados com cartões de crédito.
COLOMBIA	O Código Penal (alterado pela Lei 1273, de 5 de janeiro de 2009, também chamada Lei de Delitos Informáticos,) inclui nove delitos informáticos puros e outros mistos. Não existem na lei normas específicas sobre prova digital.	Está em discussão um projeto de lei de alteração do Código Penal, que introduzirá a burla informática – como um crime cometido no meio informático (*Projecto Lei 60/2018* da Câmara e *Projecto Lei 74/2018* do Senado). Este projeto vai incluir uma circunstância agravante no tipo de crime da burla, como forma de passar a incriminar-se a burla informática. Também inclui normas que punem o *sexting* e a *sextortion* (por via de uma circunstância agravante do crime de extorsão) e outras que punem o mero

		uso de *malware* – que presentemente não é punido. Foi aprovada a Lei 19/28, de adesão à Convenção de Budapeste e a Corte Constitucional já deu voto de exequibilidade desta lei, permitindo assim que o país venha a depositar o seu instrumento de ratificação da Convenção – o que será feito em breve.
COSTA RICA	O Código Penal contém uma secção específica que inclui delitos informáticos e conexos. Não há normas processuais específicas a este propósito, mas o princípio de liberdade probatória permite a obtenção de prova digital – com limites no acesso a certo tipo de prova, como por exemplo a interceção de comunicações.	Está pendente na Assembleia Legislativa um projeto de lei que visa rever os tipos de crime existentes, ao encontro das previsões da Convenção de Budapeste.
CUBA	Não existem tipos específicos de crimes neste domínio (o Código Penal data de 1980). Não existem normas específicas sobre prova digital (o Código de Processo Penal data de 1977).	Estão em fase de estudo, ainda não público, novos códigos Penal e de Processo Penal que irão incluir aspetos relacionados com as tecnologias. Após a revisão constitucional de abril de 2019, foi estipulado o prazo de 18 meses para a revisão daqueles dois diplomas. Por outro lado, está igualmente em estudo um diploma normativo que visa regular a informatização da sociedade, que vai igualmente impulsionar aquelas revisões.
EL SALVADOR	A Lei Especial Contra Delitos Informáticos e Conexos (Decreto 260, de 2016) inclui muitos tipos de ilícito – e também todos os previstos na Convenção de Budapeste. Existem diversas normas respeitantes a obtenção de prova digital, no Código Processual Penal (Decreto 733 de 2009), e em leis especiais: Decreto 953, de 2015 (lei especial contra a extorsão), Decreto 108, de 2006 (terrorismo) e Lei Especial para as Interceções Telefónicas.	*OBS: informação recolhida na primeira reunião da CiberRede*
ESPANHA	O *Código Penal Español* transpõe as normas penais substantivas previstas na Convenção de Budapeste.	Está pendente no parlamento uma proposta legislativa de incriminação da *suplantación de identidad*.

	A *Ley de Enjuiciamiento Criminal*, após a alteração da LO 13/2015, de 5 de outubro por sua vez, transpõe as normas processuais da Convenção.	Está também em análise uma nova lei integral da proteção da infância e da adolescência, que inclui normas respeitantes à proteção de menores nas redes (por exemplo, respeitantes ao incitamento ao suicídio ou à auto mutilação, através da rede). Existe um outro projeto legislativo em estudo, destinado a regular a retirada de conteúdos ilícitos nas redes (bloqueio de conteúdos, interrupção de serviços ou retirada de conteúdos *online*).
GUATEMALA	Não existem ainda tipos específicos de crimes neste campo. Também não existem normas específicas sobre prova digital.	Está pendente, no Congresso, um projeto legislativo com o específico propósito de transpor a Convenção de Budapeste. Aguarda a passagem do corrente período eleitoral.
HONDURAS	Não existem específicos crimes neste campo, no Código Penal - apenas crimes respeitantes à segurança das redes. Não existem normas específicas sobre prova digital.	*OBS: informação recolhida na primeira reunião da CiberRede*
MÉXICO	Existe um Código Penal Federal e diversos Códigos Penais dos Estados (um para cada Estado), que incluem normas na área do cibercrime. Apesar de haver um único código processual penal, a nível nacional, não existem normas específicas sobre prova digital.	
PANAMÁ	Ainda não existem um corpo consolidado de tipos específicos. Não existem normas específicas sobre prova digital.	Existe um projeto legislativo que visa adequar a legislação nacional à Convenção de Budapeste. Foi introduzido no Congresso em 2017.
PARAGUAY	Lei 4439, de 2011, consagra já algumas normas penais de acordo com a Convenção de Budapeste.	

	Não existem normas específicas sobre prova digital.	
PERÚ	A lei interna (Lei 80086) cobre todas as normas substantivas da Convenção de Budapeste e, bem assim, todas as suas normas processuais.	A Resolução Legislativa 30913, de fevereiro de 2019, aprovou a adesão à Convenção de Budapeste, sendo seguida, em Março de 2019, pela ratificação do executivo.
PORTUGAL	A Lei do Cibercrime (Lei 109/2009) transpõe todas as normas da Convenção de Budapeste – substantivas, processuais e de cooperação internacional.	
REPÚBLICA DOMINICANA	A lei interna (Lei 5307), transpõe todas as normas substantivas e processuais da Convenção de Budapeste.	Está em análise no Congresso, em sede de comissão especializada, um projeto de modernização da lei vigente.
URUGUAY	Não existem tipos específicos de crimes neste campo. Não existem na lei normas específicas sobre prova digital - apenas se prevê, em termos gerais, no Código de Processo Penal, a interceção de comunicações.	Existe um projeto legislativo que introduzirá alguns dos crimes descritos na Convenção de Budapeste (acesso não autorizado, dano informático e burla informática). Este projeto está ainda em fase de aprovação pelo poder executivo, somente sendo depois disso submetido ao Congresso. *OBS: informação recolhida na primeira reunião da CiberRede*