

Organizado y financiado por:



OEA | REMJA

FORO HEMISFÉRICO DE COOPERACIÓN INTERNACIONAL CONTRA EL DELITO CIBERNÉTICO

PROGRAMA DE LA CONFERENCIA

SANTO DOMINGO,
5-7 de DICIEMBRE 2017

ESQUEMA

1. ANTECEDENTES

Con la creciente relevancia de las tecnologías de la información y las comunicaciones para las sociedades de todo el mundo y su consiguiente vulnerabilidad a amenazas tales como el delito cibernético, es necesario intensificar la labor de aumento de la capacidad para que las autoridades de la justicia penal puedan investigar, juzgar y dictar sentencia en relación con delitos cometidos contra computadoras o por medio de ellas, así como otros delitos que impliquen pruebas electrónicas.

En vista de la magnitud de este desafío y la escasez de recursos, las organizaciones internacionales deben aunar fuerzas y lograr sinergias para apoyar a los países de una manera uniforme y eficaz.

El Consejo de Europa y la Unión Europea, por ejemplo, proporcionan asistencia a los países por medio de diversos proyectos conjuntos, entre ellos el proyecto de Acción Mundial sobre el Delito Cibernético Extendido (GLACY+). En ambas organizaciones, GLACY+ ayuda a crear la capacidad necesaria para implementar el Convenio de Budapest y cooperar en el ámbito internacional en el marco de este tratado. La República Dominicana, como el primer país de América Latina en convertirse en Parte del Convenio, tiene un rol de país prioritario y de centro de intercambio de experiencias (www.coe.int/cybercrime).

La Unión Europea

La Unión Europea apoya la organización de este Foro Hemisférico de Cooperación Internacional contra el Delito Cibernético por medio del proyecto conjunto de la Unión Europea y el Consejo de Europa de Acción Mundial sobre el Delito Cibernético Extendido (GLACY+), financiado por medio de su Instrumento en pro de la estabilidad y la paz.

La Unión Europea ha tomado medidas energéticas en los últimos años para aumentar la seguridad cibernética y fortalecer la acción de la justicia penal contra la ciberdelincuencia. El aumento de la capacidad es un elemento decisivo de la respuesta mundial de la Unión Europea.

En 1999, la Reunión de Ministros de Justicia u Otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA), celebrada en el marco de la Organización de los Estados Americanos (OEA), estableció el Grupo de Trabajo en Delito Cibernético (“el Grupo de Trabajo”) como el foro principal para la cooperación internacional en la prevención, la investigación y el juzgamiento de delitos cibernéticos. El Grupo de Trabajo tiene también el cometido de facilitar el intercambio de información y experiencias entre sus miembros y formular recomendaciones para mejorar y fortalecer la cooperación entre los Estados Miembros de la OEA y con

organizaciones y mecanismos internacionales. Estados Unidos, por medio de su Departamento de Justicia, preside el Grupo de Trabajo, que cuenta con el apoyo del Departamento de Cooperación Jurídica de la Secretaría de Asuntos Jurídicos de la OEA, en calidad de Secretaría Técnica de la REMJA.

Este Grupo de Trabajo ha asumido el liderazgo en la aplicación de las recomendaciones de la REMJA con respecto al delito cibernético, entre ellas la adhesión al Convenio sobre la Ciberdelincuencia, conocido también como Convenio de Budapest, por los Estados Miembros de la OEA y la adopción de las medidas jurídicas y de otra naturaleza que se requieran para su aplicación. Además, el Departamento de Justicia de Estados Unidos y la Secretaría Técnica han colaborado en más de 34 talleres sobre ciberdelincuencia desde 2004, en los que participaron más de 2.200 jueces, fiscales e investigadores de América Latina y el Caribe.

En 1996, el Departamento de Justicia de Estados Unidos creó la Sección de Delitos Informáticos y Propiedad Intelectual (CCIPS), con cinco fiscales federales. Actualmente, la CCIPS cuenta con 45 fiscales que investigan y juzgan casos que implican exclusivamente pruebas electrónicas. La CCIPS es también el representante de Estados Unidos entre los contactos de la Red 24/7 del G7 para Delitos de Alta Tecnología. Además, el Departamento de Justicia tiene por lo menos un fiscal especializado en piratería informática y propiedad intelectual en cada una de las 96 oficinas federales de todo el país. Cada año, la CCIPS reúne a los fiscales especializados en piratería informática y propiedad intelectual y realiza un curso de una semana sobre los nuevos retos jurídicos y técnicos en el ámbito del delito cibernético. Una parte importante

del trabajo de la CCIPS consiste también en el aumento de la capacidad internacional. Por ejemplo, más de 2.200 jueces, fiscales, e investigadores de América Latina y el Caribe han participado en talleres de tres días sobre el delito cibernético en el marco de un proyecto conjunto del Departamento de Justicia y la Organización de los Estados Americanos. La CCIPS ha ofrecido cursos similares en Asia y África.

La Comunidad del Caribe (CARICOM) es un grupo de veinte países: quince Estados Miembros y cinco Miembros Asociados. CARICOM, el movimiento de integración más antiguo que subsiste en los países en desarrollo, tiene cuatro pilares principales: integración económica, coordinación de la política exterior, desarrollo humano y social, y seguridad.

De acuerdo con el artículo 23 del Tratado Revisado de Chaguaramas, la Secretaría es el principal órgano administrativo de CARICOM y tiene su sede en Georgetown, Guyana.

En la Vigésima Sexta Reunión de la Conferencia de Jefes de Gobierno, celebrada en julio de 2005, se formuló un marco nuevo con los siguientes objetivos: 1) establecer mecanismos en CARICOM para administrar la agenda regional sobre delincuencia y seguridad, y 2) colocar el tema de la delincuencia y la seguridad a la par de otras áreas tales como el comercio, la salud, la agricultura y la educación.

Se propuso también establecer los siguientes órganos:

1. Un Consejo de Ministros encargados de la seguridad nacional y la aplicación de la ley como órgano separado de CARICOM, que rinde cuentas a la Conferencia de Jefes de Gobierno por medio del Primer Ministro, con funciones relativas a la delincuencia y la seguridad; y

2. Una Agencia de Implementación de Seguridad y contra la Delincuencia (IMPACS), el centro neural de este marco de gestión y la institución de CARICOM con la responsabilidad primordial de implementar la agenda regional sobre delincuencia y seguridad, que depende directamente del Consejo de Ministros.

El marco comenzó a funcionar formalmente en marzo de 2006, cuando la Secretaría de CARICOM convocó la primera reunión del Consejo Nacional para la Seguridad y Aplicación de la Ley (CONSLE). En 2006 se puso en marcha el proyecto HIPCAR, en cuyo marco se promulgaron nueve leyes, entre ellas una sobre delitos cibernéticos. La adopción de leyes ha sido lenta debido a numerosas circunstancias atenuantes, pero se planea intensificar esta labor en 2018.

En CARICOM se están llevando a cabo varias actividades en el ámbito del delito cibernético, entre ellas la formulación del Plan de Acción de CARICOM contra el delito cibernético, la Declaración de St. Philip, Barbados, sobre la colaboración en materia de seguridad cibernética en el Caribe, que fue ratificada en 2013, la estrategia de CARICOM para el delito cibernético y la creación de equipos de respuesta a incidentes informáticos (CIRT).

La República Dominicana llevó a cabo su primera “investigación de delitos cibernéticos” a mediados de 2003, que puso de manifiesto la necesidad de leyes que aborden específicamente estos delitos y de una unidad de investigaciones. La primera unidad, la División de Investigaciones de Delitos Informáticos (DIDI), fue creada a fines

de 2003 como dependencia del Departamento Nacional de Investigaciones, cuya misión es proteger al presidente y a los funcionarios electos y ocuparse de la seguridad nacional y el terrorismo. En 2004 se inició la redacción de una ley específicamente sobre ciberdelincuencia, siguiendo las directrices del Convenio de Budapest. En noviembre de 2004 se creó el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) en la Dirección Central de Investigaciones Criminales de la Policía Nacional para abordar todos los aspectos del delito cibernético.

En abril de 2007 se promulgó la Ley 53-07 sobre Delitos de Alta Tecnología, plenamente compatible con el Convenio de Budapest. En 2008, el Consejo de Europa invitó a la República Dominicana a adherirse al Convenio de Budapest, que el país finalmente ratificó en 2013, convirtiéndose de esta forma en el primer país de la región en ser Parte del Convenio. En 2013 se creó la Procuraduría Especializada Contra los Crímenes y Delitos de Alta Tecnología (PEDATEC) como dependencia de la Procuraduría General, que cuenta actualmente con abogados especializados en los 34 distritos judiciales.

La República Dominicana es ahora un país prioritario y un centro regional del proyecto GLACY+ de aumento de la capacidad, y está ayudando a la Oficina del Programa sobre la Ciberdelincuencia (C-PROC) a llegar a todos los países de América Latina y el Caribe.

2. RESULTADOS PREVISTOS

Se prevé obtener los siguientes resultados del foro:

- ✓ Los representantes de los países participantes estarán en mejores condiciones de beneficiarse del apoyo de diferentes organizaciones internacionales para fortalecer su capacidad en el ámbito de la justicia penal en lo que se refiere al delito cibernético y las pruebas electrónicas.
- ✓ Las organizaciones internacionales habrán fortalecido su cooperación y sinergia con miras al apoyo futuro a países de la región. Se prevé que el foro en sí servirá de ejemplo.
- ✓ Los representantes de los países participantes podrán conversar sobre prácticas óptimas y crear una red de contactos que les permita trabajar de manera más eficiente por medio del intercambio de información sobre tareas comunes, fortalecer su capacidad para hacer frente a retos nuevos en las investigaciones penales que tengan un

componente de delito cibernético y evaluación de pruebas electrónicas, promover y mejorar los protocolos de cooperación regional entre proveedores de servicios de internet e investigadores de casos penales y fortalecer los mecanismos regionales en el ámbito penal.

3. PARTICIPANTES

Los gobiernos de países de América Latina y el Caribe han propuesto a funcionarios que trabajan en asuntos relacionados con delitos cibernéticos y pruebas electrónicas, provenientes de las fuerzas del orden, fiscalías, el poder judicial, ministerios pertinentes (como los de Justicia y del Interior), y legisladores. También participarán organizaciones del sector privado.

4. LUGAR

El foro tendrá lugar en el Centro de Convenciones del Ministerio de Relaciones Exteriores (MIREX) en Santo Domingo, República Dominicana, y durará tres días.

PANORAMA DEL PROGRAMA

MAR, 5 DE DICIEMBRE

08h00 – 09h00.

INSCRIPCIÓN Y ACREDITACIÓN DE PARTICIPANTES

SESIÓN PLENARIA

SALA 1

09h00 – 10h00.

CEREMONIA DE APERTURA

(inglés y español)

1. Consejo de Europa
2. Unión Europea
3. Organización de los Estados Americanos
4. Departamento de Justicia de Estados Unidos
5. Secretaría de CARICOM
6. Gobierno de la República Dominicana

10h00 – 10h30.

RECESO

10h30 – 11h45

Aumento de la capacidad para combatir el delito cibernético en las Américas: cómo pueden ayudarle las organizaciones internacionales y regionales y otras autoridades (10 minutos cada uno)

1. Mayor Michael JONES, Jefe de Operaciones, IMPACS
2. Adrián ACOSTA, Oficial de Delitos Digitales, INTERPOL
3. Wouter VENSTRA, Subjefe, Secretaría del Foro Mundial de Competencia Cibernética
4. Capitán (N) Errington R. SHURLAND, Director Ejecutivo, Sistema de Seguridad Regional
5. Álvaro Proaño CARRIÓN, Mayor de Policía, AMERIPOL, Colombia
6. Normand WONG, Asesor Jurídico, Política en materia de Derecho Penal, Departamento de Justicia, Canadá

11h45 – 12h45.

Oradores principales (15 minutos cada uno):

1. Formulación de una estrategia contra la ciberdelincuencia
Alexander SEGER, Consejo de Europa
2. Uso de redes cibernéticas en la lucha contra el delito cibernético
Adrián ACOSTA, Oficial de Delitos Digitales, INTERPOL
3. El proyecto “República Digital” y la política nacional de ciberseguridad
Zoraima CUELLO, Vice-Ministra de la Presidencia de la República Dominicana

12h45 – 13h00.

Información y organización de los talleres

13h00 – 14h00.

ALMUERZO

TALLERES

SALA 1 (Español/Inglés)

SALA 2 (Español/Inglés)

14h00 – 17h30.

**TALLER 1
CONSEJO DE EUROPA**

El aumento de la capacidad y el Convenio de Budapest sobre la Ciberdelincuencia; apoyo a la elaboración de estrategias en materia de delito cibernético y pruebas electrónicas

**TALLER 2
INTERPOL**

El papel de Interpol en la cooperación policial internacional y la coordinación con el sector privado

(Receso de)

15h30 – 16h00.

20h00

CENA SOCIAL OFRECIDA POR EL GOBIERNO DE LA REPÚBLICA DOMINICANA

MIER, 6 DE DICIEMBRE

TALLERES	SALA 1 (Español/Inglés)	SALA 2 (Español/Inglés)
9h30 – 13h00. (Receso de) 10h30-10h45.	TALLER 3 INTERPOL El aumento de la capacidad y la certificación obligatoria de agentes de policía en pruebas digitales e investigaciones de delitos cibernéticos	TALLER 4 OEA/USDoJ Tor, la web oscura y Bitcoin: conocimientos técnicos necesarios y ejemplo de una investigación y un juicio exitosos
13h00 – 14h00.	LUNCH	

TALLERES	SALA 1 (Español/Inglés)	SALA 2 (Español/Inglés)
14h00 – 17h00. (Receso de) 15h30 – 16h00.	TALLER 5 CONSEJO DE EUROPA Acceso a pruebas en la nube	TALLER 6 Otras organizaciones internacionales y regionales y otros países (Parte 1) La comunidad internacional en la lucha contra el delito cibernético

JUE, 7 DE DICIEMBRE

TALLERES	SALA 1 (Español/Inglés)	
9h30 – 13h00. (Receso de) 10h30-11h00.	TALLER 7 OEA/USDoJ Derecho procesal y derecho sustantivo: cómo determinan los tribunales la admisibilidad de las pruebas digitales	TALLER 8 Otras organizaciones internacionales y regionales y otros países (Parte 2) La comunidad internacional en la lucha contra el delito cibernético
13h00 – 14h00.	ALMUERZO	

TALLERES	SALA 1
14h00 – 17h00.	PLENARIA FINAL <ul style="list-style-type: none">• Resultados de los talleres• Intervenciones finales y el camino hacia adelante (CoE, OEA, IMPACS, Secretaría de CARICOM, INTERPOL, Departamento de Justicia de Estados Unidos, Canadá y Unión Europea) CEREMONIA DE CLAUSURA Gobierno de la República Dominicana
17h00.	FIN DE LA CONFERENCIA

PROGRAMA DETALLADO

MAR, 5 DE DICIEMBRE

08h00 – 09h00.

REGISTRO Y ACREDITACIÓN DE PARTICIPANTES

TALLERES

SALA 1 (Español/Inglés)

09h00 – 10h00.

CEREMONIA DE APERTURA

(inglés y español)

1. Consejo de Europa
2. Unión Europea
3. Organización de los Estados Americanos
4. Departamento de Justicia de Estados Unidos
5. Secretaría de CARICOM
6. Gobierno de la República Dominicana

10h00 – 10h30.

RECESO

10h30 – 11h45

Aumento de la capacidad para combatir el delito cibernético en las Américas: cómo pueden ayudarle las organizaciones internacionales y regionales y otras autoridades (10 minutos cada uno)

1. Mayor Michael JONES, Jefe de Operaciones, IMPACS
2. Adrián ACOSTA, Oficial de Delitos Digitales, INTERPOL
3. Wouter VENSTRA, Subjefe, Secretaría del Foro Mundial de Competencia Cibernética
4. Capitán (N) Errington R. SHURLAND, Director Ejecutivo, Sistema de Seguridad Regional
5. Álvaro Proaño CARRIÓN, Mayor de Policía, AMERIPOL, Colombia
6. Normand WONG, Asesor Jurídico, Política en materia de Derecho Penal, Departamento de Justicia, Canadá

11h45 – 12h45.

Oradores principales (15 minutos cada uno):

1. Formulación de una estrategia contra la ciberdelincuencia
Alexander SEGER, Consejo de Europa
2. Uso de redes cibernéticas en la lucha contra el delito cibernético
Adrián ACOSTA, Oficial de Delitos Digitales, INTERPOL
3. El proyecto “República Digital” y la política nacional de ciberseguridad
Zoraima CUELLO, Vice-Ministra de la Presidencia de la República Dominicana

12h45 – 13h00.

Información y organización de los talleres

13h00 – 14h00.

ALMUERZO

TALLERES

SALA 1 (Español/Inglés)

14h00 – 17h30.

(Receso de)

16h00-16h15.

TALLER 1:

CONSEJO DE EUROPA: El aumento de la capacidad y el Convenio de Budapest sobre la Ciberdelincuencia; apoyo a la elaboración de estrategias en materia de delito cibernético y pruebas electrónicas

La “cultura de la seguridad” es el componente fundamental del desarrollo de la capacidad digital de un país. Aborda el nivel en el cual el gobierno y los ciudadanos reconocen los riesgos intrínsecos del espacio cibernético y la forma de manejar esos riesgos con buenas prácticas de seguridad. En este taller, los expertos y los participantes analizarán y llegarán a un acuerdo sobre los elementos principales para elaborar una estrategia cibernética: fundamentos estratégicos, política y gobernanza, asignación de recursos, gestión de riesgos, resiliencia, delitos cibernéticos, alianzas clave, y la cultura de la ciberseguridad y la fuerza laboral.

Otro objetivo de este taller es señalar los elementos principales del Convenio de Budapest en la lucha contra el delito cibernético, incluido el proceso de adhesión y los proyectos de aumento de la capacidad que se están llevando a cabo en la región, así como en el aumento de la capacidad de los fiscales y jueces para combatir el delito cibernético y manejar las pruebas electrónicas.

Moderador: Claudio PEGUERO, General de Brigada, Director de Planificación y Desarrollo de la Policía Nacional y coordinador nacional del proyecto GLACY+, República Dominicana;

Relator: Daniela DUPUY, Fiscal especializada en Delitos Informáticos, Buenos Aires, Argentina

- **Tema :** Cómo reflejar los delitos cibernéticos y las pruebas electrónicas en una estrategia cibernética para los países de América Latina y el Caribe

Orador: Francisco NEIRA BASSO, Responsable Principal de TIC, consultor internacional, experto en ciberdelincuencia, Consejo de Europa (30 min + 30 min para debate)

- **Tema:** Elementos principales del Convenio de Budapest en la lucha contra el delito cibernético

Orador: Betty SHAVE, consultora internacional, experta en ciberdelincuencia, Consejo de Europa (30 min + 30 min para debate)

- **Tema:** Ideas y estrategias para un programa de aumento de la capacidad de los operadores del sistema de justicia penal de los países de América Latina y el Caribe

Orador: Marcos SALT, consultor internacional, experto en ciberdelincuencia, Consejo de Europa (30 min + 30 min para debate)

Conclusiones: Ingredientes del éxito

Orador: Claudio PEGUERO, República Dominicana (15 min)

TALLER

SALA 2 (Español/Inglés)

14h00 – 17h30.

(Receso de)

16h00-16h15.

TALLER 2:

El papel de Interpol en la cooperación policial internacional y la coordinación con el sector privado

La ciberdelincuencia está creciendo con rapidez. Más y más delincuentes están aprovechando la velocidad, la conveniencia y la anonimidad de Internet para llevar a cabo una amplia gama de actividades delictivas que no conocen fronteras físicas o virtuales, que causan graves daños y que plantean amenazas muy reales para sus víctimas en todo el mundo.

La mayoría de los delitos cibernéticos son transnacionales. Por lo tanto, INTERPOL es un aliado natural de cualquier organismo de las fuerzas del orden que quiera investigar estos delitos sobre la base de la cooperación. Al trabajar con el sector privado, INTERPOL puede proporcionar a las fuerzas locales del orden inteligencia cibernética focalizada, derivada de la combinación de insumos a escala mundial.

Speaker: Milos MIJOMANOVIC, Interpol (15 min)

Moderador: Milos MIJOMANOVIC, Oficial de Delitos Digitales, INTERPOL;

Relator: Dong Uk KIM, Gerente de Proyectos, INTERPOL;

- **Tema:** Operaciones coordinadas por Interpol en el ámbito de la ciberdelincuencia: intensificación de las actividades cibernéticas en las Américas

Orador: Adrian ACOSTA (30 min + 30 min para discusión)

- **Tema:** Estudio de Caso

Orador: Victor CHANENKO, Jefe del Departamento de Ciberdelincuencia de la Policía Federal, Argentina y Horacio AZZOLI, titular de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), Argentina (30 min + 30 min for discussion)

- **Tema:** Estudio de Caso

Orador: Edgar Martin VARGAS CARPIO, Policía Nacional, Colombia (30 min + 30 min para debate)

Conclusiones: Ingredientes del éxito

Orador: Milos MIJOMANOVIC, Interpol (15 min)

MIÉRCOLES, 6 DE DICIEMBRE

TALLERES

SALA 1 (Español/Inglés)

09h30 - 13h00

(Receso de)
10h30-10h45.

TALLER 3:

INTERPOL: El aumento de la capacidad y la certificación obligatoria de agentes de policía en pruebas digitales e investigaciones de delitos cibernéticos

La ciberdelincuencia está avanzando con rapidez y está diversificándose debido a su desarrollo técnico y a la sofisticación de las operaciones delictivas. Además, las organizaciones delictivas están recurriendo en medida creciente a Internet para facilitar sus actividades y maximizar sus ganancias en el menor tiempo posible. Los delitos en sí no son necesariamente nuevos (hurto, fraude, juegos de azar ilícitos, venta de medicamentos falsificados), pero están evolucionando a la par de las oportunidades que se presentan en línea y, por lo tanto, están generalizándose y están volviéndose más perniciosos.

La capacitación de la policía desempeña un papel decisivo en la misión general de INTERPOL de promover la cooperación entre las fuerzas policiales nacionales. INTERPOL trabaja para aumentar y certificar la capacidad de la policía de los países miembros participantes, equipándola con los conocimientos teóricos y prácticos que necesita para hacer frente a los retos actuales de la labor policial. Asimismo, ofrece una amplia gama de iniciativas para cerrar la brecha entre la labor policial nacional e internacional.

Moderador: Adrian ACOSTA, INTERPOL;

Relator: Dong Uk KIM, INTERPOL;

- **Tema:** Programa de aumento de la capacidad regional: "Ciberaméricas"

Orador: Milos MIJOMANOVIC, Interpol (30 min + 30 min para debate)

- **Tema:** Conclusión del programa de aumento de la capacidad en materia de delitos informáticos en la República Argentina

Orador: Diosnel ALARCON (30 min + 30 min para debate)

- **Tema:** Ejemplo de país: Aumento de la capacidad y certificación en Guatemala

Orador: Diego TEOS, Jefe de la Unidad contra Delitos Informáticos de la Policía Nacional, Guatemala (30 min + 30 min para debate)

Conclusiones: Ingredientes para el éxito.

Orador: Adrian ACOSTA (15 min)

TALLERES

SALA 2 (Inglés/Español)

09h30 - 13h00

[Receso de]
10h30-10h45.**TALLER 4:****ORGANIZACIÓN DE LOS ESTADOS AMERICANOS AND DEPARTAMENTO DE JUSTICIA DE ESTADOS UNIDOS (OEA/Departamento de Justicia de Estados Unidos): Tor, la web oscura y Bitcoin: conocimientos técnicos necesarios y ejemplo de una investigación y un juicio exitosos**

En la actualidad se pueden cometer delitos en el espacio cibernético con anonimidad, fácilmente y, a veces, sin que las víctimas los detecten. El espacio cibernético permite a los delincuentes extender su accionar a través de fronteras nacionales y absorbe recursos de los fiscales e investigadores. ¿Qué ocurre cuando a esto se le agrega otra capa de anonimidad? En este taller, los expertos hablarán de la red Tor (conocida también como “la cebolla”), la forma de investigar casos en esta red, la web oscura, las herramientas necesarias para rastrear a los delincuentes y la moneda que usan los delincuentes para comprar y vender mercaderías en la red (bitcoin). Los participantes también tendrán la oportunidad de interactuar con un fiscal que formó parte del equipo que investigó y llevó a juicio a Ross Ulbricht, conocido también como “el Temible Pirata Roberts”, creador de Silk Road.

Moderador: Rodolfo ORJALES, Departamento de Justicia de Estados Unidos

Relator: Laura MARTINEZ, OAS;

- **Tema:** La web oscura y Bitcoin

Orador: Licurgo YUNES, Jefe del DICAT, Policía Nacional, República Dominicana
(60 min + 30 min para debate)

- **Tema:** Estudio de caso: Silk Road

Orador: Tim HOWARD, Fiscalía Federal del Distrito Sur de Nueva York (fiscal del caso contra Silk Road)
(60 min + 30 min para debate)

Conclusiones: Ingredientes para el éxito

Orador: Rodolfo ORJALES, USDoJ (15 min)

13h00 – 14h00.

ALMUERZO

TALLERES

SALA 1 (Español/Inglés)

14h00 – 17h30.

[Receso de]
16h00-16h15.**TALLER 5:****CONSEJO DE EUROPA: Acceso a pruebas en la nube**

El Comité del Convenio contra la Ciberdelincuencia, en su 12.ª sesión plenaria (2 y 3 de diciembre de 2014), estableció un grupo de trabajo a fin de buscar soluciones para el acceso a pruebas en la nube para uso de la justicia penal, incluso por medio de la asistencia jurídica mutua (“Grupo T-CY sobre pruebas en la nube”). Esta decisión estuvo motivada por el reconocimiento de que, a la luz de la proliferación de la ciberdelincuencia y otros delitos que implican pruebas electrónicas y en el contexto de los cambios tecnológicos y la incertidumbre con respecto a la jurisdicción, se necesitan otras soluciones para que las autoridades de la justicia penal puedan obtener las pruebas electrónicas especificadas en las investigaciones penales.

En este taller, los participantes abordarán las recomendaciones del Grupo T-CY sobre pruebas en la nube, las dificultades, las limitaciones y también la utilidad de las investigaciones en la “nube”.

Moderador: Alexander SEGER, CoE;

Relator: Betty SHAVE, United States;

- **Tema:** Retos para la justicia penal con respecto al acceso a pruebas en la nube
Orador: Francisco NEIRA BASSO, Responsable Principal de TIC, consultor internacional, experto en ciberdelincuencia, Consejo de Europa (30 min + 30 min para debate)
- **Tema:** Cooperación con proveedores de servicios
Orador: Enrique GUTIÉRREZ, Jefe de Investigaciones en América Latina y el Caribe, Asuntos Jurídicos de Empresas Externas, Microsoft (30 min + 30 min para debate)
- **Tema:** Retos judiciales del acceso transfronterizo a datos alojados en la nube: análisis de caso
Orador: Marcos SALT, Profesor, Universidad de Buenos Aires, Facultad de Derecho, consultor internacional, Consejo de Europa (30 min + 30 min para debate)

Conclusiones: Ingredientes para el éxito.

Orador: Alexander SEGER, CoE (15 min)

TALLERES

SALA 2 (Español/Inglés)

14h00 – 17h30.

(Receso de)
16h00-16h15.

TALLER 6:

La comunidad internacional en la lucha contra el delito cibernético (Parte 1)

De acuerdo con diferentes fuentes de todo el mundo, los delitos cibernéticos están costándole a la economía mundial hasta US\$500.000 millones al año. No obstante, la cooperación internacional entre los distintos agentes internacionales y regionales y con países que tienen la capacidad para tener una influencia positiva sigue siendo peligrosamente insuficiente.

Por lo tanto, es preciso tomar conciencia de la necesidad de cooperar a nivel internacional y nacional para llevar a cabo una acción efectiva. Es necesario reevaluar y renovar en la medida de lo posible los marcos jurídicos internacionales y ofrecer un foro para un diálogo internacional más amplio con miras a intensificar y promover la cooperación policial y judicial entre las autoridades nacionales y entre organizaciones internacionales y regionales. En estos avances se debería considerar la influencia de los asuntos nuevos y emergentes con respecto a la cooperación policial y judicial internacional en asuntos penales, con recomendaciones sobre el aumento de la capacidad, que debería ser igualmente motivo de preocupación con respecto a la situación de los países que se encuentran en distintas etapas de desarrollo a fin de evitar un futuro caótico.

Este taller reúne a países con programas de aumento de la capacidad y organizaciones internacionales y regionales que están aunando fuerzas para mostrar sus áreas de acción y la forma en que pueden beneficiar a los países que necesitan su apoyo.

Moderador: Wayne M. CAINES, Ministro de Seguridad Nacional, Bermudas

Relator: Cesar MOLINE, INDOTEL, República Dominicana

- **Tema:** La ciberseguridad y el ambiente
Orador: Anselm CHARLES, Gerente de TIC (Ag), IMPACS (30 min + 15 min para debate)
- **Tema:** Secretaría de CARICOM
Orador: Jennifer BRITTON, Gerente Adjunto de Programas – ICT4D, Secretaría de CARICOM (30 min + 15 min para debate)
- **Tema:** Cómo equilibrar los poderes policiales con la necesidad de proteger la privacidad en la legislación
Orador: Normand WONG, Asesor Jurídico, Política en materia de Derecho Penal, Departamento de Justicia, Canadá (20 min + 10 min para debate)

- **Tema:** Cómo abordar asuntos de jurisdicción cuando la policía necesita datos que se encuentran en una jurisdicción extranjera

Orador: Normand WONG, Asesor Jurídico, Política en materia de Derecho Penal, Departamento de Justicia, Canadá (20 min + 10 min para debate)

Conclusiones: Ingredientes para el éxito.

Orador: Wayne M. CAINES, Ministro de Seguridad Nacional, Bermudas (15 min)

JUEVES, 7 DE DICIEMBRE

TALLERES

SALA 1 (Español/Inglés)

09h15 - 13h00.

(Receso de)
10h45-11h15.

TALLER 7:

OEA/Departamento de Justicia de Estados Unidos: Derecho procesal y derecho sustantivo: cómo determinan los tribunales la admisibilidad de las pruebas digitales

¿Qué leyes pueden facilitar el juzgamiento de los delitos cibernéticos? ¿Cuáles son los acuerdos y requisitos internacionales para solicitar pruebas de otros países? En este taller se abordarán estas preguntas y los desafíos que enfrentan las fuerzas del orden y los fiscales al presentar pruebas electrónicas a un juez. Además, en el taller se examinará la necesidad de armonizar y actualizar las leyes penales contra los delitos cibernéticos a fin de facilitar la admisibilidad de las pruebas digitales en los tribunales..

Moderador: Rodolfo ORJALES, USDoJ;

Relator: Laura MARTINEZ, OAS;

- **Tema:** Cooperación internacional: maneras formales (tratados bilaterales) e informales de obtener pruebas digitales en Estados Unidos

Orador: Rodolfo ORJALES, Departamento de Justicia, Sección de Delitos Informáticos (60 min + 30 min para debate)

- **Tema:** Derecho procesal

Orador: Marcos SALT, Profesor, Universidad de Buenos Aires, Facultad de Derecho (60 min + 30 min para debate)

Conclusiones: Ingredientes para el éxito.

Orador: Rodolfo ORJALES, USDoJ (15 min)

TALLERES

SALA 2 (Español/Inglés)

09h15 - 13h00.

(Receso de)
10h45-11h15.

TALLER 8:

La comunidad internacional en la lucha contra el delito cibernético (Parte 2)

De acuerdo con diferentes fuentes de todo el mundo, los delitos cibernéticos están costándole a la economía mundial hasta US\$500.000 millones al año. No obstante, la cooperación internacional entre los distintos agentes internacionales y regionales y con países que tienen la capacidad para tener una influencia positiva sigue siendo peligrosamente insuficiente.

Por lo tanto, es preciso tomar conciencia de la necesidad de cooperar a nivel internacional y nacional para llevar a cabo una acción efectiva. Es necesario reevaluar y renovar en la medida de lo posible los marcos jurídicos internacionales, ofrecer un foro para un diálogo internacional más amplio con miras a intensificar y promover la cooperación policial y judicial entre las autoridades nacionales y entre organizaciones internacionales y regionales. En estos avances se debería considerar la influencia de los asuntos nuevos y emergentes con respecto a la cooperación policial y judicial internacional en asuntos penales, con recomendaciones sobre el aumento de la capacidad, que debería ser igualmente motivo de preocupación con respecto a la situación de los países que se encuentran en distintas etapas de desarrollo a fin de evitar un futuro caótico.

Este taller reúne a países con programas de aumento de la capacidad y organizaciones internacionales y regionales que están aunando fuerzas para mostrar sus áreas de acción y la forma en que pueden beneficiar a los países que necesitan su apoyo.

Moderador: Francisco NEIRA BASSO, Consejo de Europa;

Relator: Esther AGELAN, Jueza de la Corte Suprema de la República Dominicana, Santo Domingo

• **Tema:** Global Programme on Cybercrime of the United Nations Office of Drugs and Crime (UNODC), video presentation.

Orador: Neil WALSH, Head of UNODC Global Programme on Cybercrime, Vienna, Austria and Bertha Nayelly LOYA MARIM, Deputy Head of Office for UNODC in El Salvador (15 min)

• **Tema:** Laboratorio Forense Digital del Sistema de Seguridad Regional

Orador: Candacy MAYNARD, Gerente de Laboratorio, Sistema de Seguridad Regional (30 min + 15 min para debate)

• **Tema:** El proyecto GLACY+ del Consejo de Europa (Acción Mundial sobre el Delito Cibernético Extendido) (30 min + 15 min para debate)

Orador: Manuel DE ALMEIDA PEREIRA, Gerente del proyecto GLACY+, Consejo de Europa (por confirmar)

• **Tema:** Aumento de la capacidad cibernética en el Foro Mundial de Competencia Cibernética: aplicación práctica de los principios

Orador: Wouter VENSTRA, Subjefe, Secretaría del Foro Mundial de Competencia Cibernética (30 min + 15 min para debate)

Conclusiones: Ingredientes para el éxito

Orador: Francisco NEIRA BASSO, Consejo de Europa (15 min)

13h00 – 14h00.

ALMUERZO

SESIÓN PLENARIA

SALA 1 (IDIOMAS: INGLÉS/FANCÉS/ESPAÑOL/PORTUGUÉS)

14h00 – 17h00.

(Receso de)

16h00-16h15.

Resultados de los talleres (15 minutos para cada relator – 120 minutos)

T 1: CONSEJO DE EUROPA: Formulación de una estrategia contra la ciberdelincuencia para los países de América Latina y el Caribe; elementos proporcionados por el Convenio de Budapest y aumento de la capacidad en materia de ciberdelincuencia (Relator: Daniela DUPUY).

T 2: INTERPOL: El papel de Interpol en la cooperación policial internacional y la coordinación con el sector privado (Relator: Dong Uk KIM).

T 3: INTERPOL: El aumento de la capacidad y la certificación obligatoria de agentes de policía en pruebas digitales e investigaciones de delitos cibernéticos (Relator: Dong Uk KIM).

T 4: OEA/USDoJ: Tor, la web oscura y Bitcoin: conocimientos técnicos necesarios y ejemplo de una investigación y un juicio exitosos (Relator: Laura MARTÍNEZ).

T 5: CONSEJO DE EUROPA: Acceso a pruebas en la nube (Relator: Betty SHAVE).

T 6: La comunidad internacional en la lucha contra el delito cibernético (Parte 1): Relator: Cesar MOLINE).

T 7: OEA/USDoJ: Derecho procesal y derecho sustantivo: cómo determinan los tribunales la admisibilidad de las pruebas digitales (Relator: Laura MARTÍNEZ).

T 8: La comunidad internacional en la lucha contra el delito cibernético (Parte 2): (Relator: Esther AGELAN).

Alocuciones finales y el camino hacia adelante (CoE, OEA, IMPACS, Secretaría de CARICOM, INTERPOL, Estados Unidos, Canadá y Unión Europea) – 5 minutos cada uno

CEREMONIA DE CLAUSURA

Gobierno de la República Dominicana (15 minutos)

17h00.

FIN DE LA CONFERENCIA

CON EL APOYO DE:

