



# Conferencia Octopus 2023

13-15 de diciembre de 2023 - Bucarest, Rumanía

## Programa general de la Conferencia

Versión del 28 de noviembre de 2023

<b>MIÉRCOLES 13 DE DICIEMBRE DE 2023</b>			
8:30-9:30	<i>Café de bienvenida y registro</i>		
9:30-13:00	<b>Sesión plenaria de apertura</b> EN/FR/ES/RO <ul style="list-style-type: none"> <li>▶ Ciberdelincuencia y pruebas electrónicas: perspectivas mundiales</li> <li>▶ Ciberdelincuencia y pruebas electrónicas de crímenes de guerra: ¿qué nos ha enseñado la agresión rusa contra Ucrania?</li> <li>▶ Ciberdelincuencia frente a libertad de expresión</li> <li>▶ El marco del Convenio sobre la Ciberdelincuencia: actualización</li> </ul>		
Pausa café 10:30-11:00			
13:00-14:30	<i>Foto de grupo y pausa para comer</i>		
14:30-16:00	<b>Taller 1</b> EN/FR/ES/RO <ul style="list-style-type: none"> <li>▶ Situación mundial de la legislación en materia de ciberdelincuencia</li> </ul>	<b>Taller 2</b> EN/FR/ES/RO <ul style="list-style-type: none"> <li>▶ Intercambio espontáneo de información</li> </ul>	<b>Taller 3</b> EN/FR/ES/RO <ul style="list-style-type: none"> <li>▶ Detección automática de material de explotación y abuso sexual infantil</li> </ul>
16:00-16:30	<i>Pausa café</i>		
16:30-18:00	<b>Taller 4</b> EN/FR/ES <ul style="list-style-type: none"> <li>▶ Sinergias entre los Convenios de Budapest, Lanzarote, Estambul y el Convenio sobre la trata de seres humanos</li> </ul>	<b>Taller 5</b> EN/FR/ES <ul style="list-style-type: none"> <li>▶ La interacción de la ciberdelincuencia y las investigaciones financieras</li> </ul>	<b>Taller 6</b> EN/FR/ES <ul style="list-style-type: none"> <li>▶ Ciberdelincuencia e inteligencia artificial</li> </ul>
18:00-20:00	<i>Evento social</i>		

<b>JUEVES 14 DE DICIEMBRE</b>				
9:30-13:00 Pausa-café 11:00-11:30	<b>Evento del proyecto:</b> EN ▶ <a href="#">De CyberEAST a CyberEast+</a>	<b>Evento del proyecto:</b> EN ▶ <a href="#">De iPROCEEDS-2 a CyberSEE</a>	<b>Evento del proyecto:</b> EN/FR/ES/PT ▶ <a href="#">De GLACY+ a GLACY-e</a>	
13:00-14:30 Pausa para comer				
14:30-15:30		<b>Evento del proyecto:</b> EN/FR ▶ <a href="#">De CyberSouth a CyberSouth+</a>		
15:30-16:00	<i>Pausa café</i>			
16:30-18:00	<b>Charlas relámpago</b> EN/FR/ES/RO			
<b>VIERNES 15 DE DICIEMBRE</b>				
9:30-11:00	<b>Taller 7</b> EN ▶ Taller regional para Asia	<b>Taller 8</b> EN ▶ Taller regional para el Pacífico	<b>Taller 9</b> EN/FR/PT ▶ Taller regional para África	<b>Taller 10</b> EN/ES ▶ Taller regional para América Latina y el Caribe
11:00-11:30	<i>Pausa café</i>			
11:30-13:00	<b>Taller 11</b> EN/FR/ES ▶ El desarrollo de capacidades como factor de cambio: ¿qué marca la diferencia?	<b>Taller 12</b> EN/FR/ES ▶ Xenofobia y racismo en línea frente a libertad de expresión	<b>Taller 13</b> EN/FR/ES ▶ Refuerzo de los puntos de contacto permanente 24/7	<b>Taller 14</b> EN/FR/ES ▶ La interacción entre ciberseguridad y ciberdelincuencia
13:00-14:30	<i>Pausa para comer</i>			
14:00-14:30	<b>Ceremonia del Tratado</b> ▶ Firmas, ratificaciones o adhesiones al Convenio de Budapest y sus Protocolos			
14:30-17:00	<b>Sesión plenaria de clausura y conclusiones</b> EN/FR/ES/RO ▶ Principales conclusiones de los talleres ▶ Lecciones extraídas en el décimo aniversario de la Oficina del Programa de lucha contra la Ciberdelincuencia del Consejo de Europa (C-PROC) ▶ Perspectivas para 2024 y conclusiones			
18:00	<i>Fin de la conferencia</i>			

# Programa detallado

MIÉRCOLES 13 DE DICIEMBRE DE 2023	
9:30-13:00	<b>Sesión plenaria de apertura</b>  Idiomas: EN/FR/ES  Moderador: Alexander Seger, Jefe de la División de Ciberdelincuencia, Consejo de Europa  Secretaría: Nina Lichtner, Directora del Proyecto Octopus, Consejo de Europa  <b>► Apertura [9:30-9:45]</b> <ul style="list-style-type: none"><li>– Ministro del Interior de Rumanía</li><li>– Dmytro Verbytsky, Fiscal General Adjunto, Ucrania</li><li>– Patrick Penninckx, Jefe del Departamento de Sociedad de la Información, Consejo de Europa</li></ul> <b>► Ciberdelincuencia y pruebas electrónicas: perspectivas globales [9:45-10:30]</b> <ul style="list-style-type: none"><li>– Erica O'Neill, CCIPS, Departamento de Justicia de EE.UU.</li><li>– Carlos Díaz, Fiscal General, Costa Rica</li><li>– Linda S Folaumoetu'I, Fiscal General, Tonga</li><li>– Pedro Verdelho, Presidente del Comité del Convenio sobre la Ciberdelincuencia, Portugal</li><li>– Jamila Akaaga Ade, Counter Ransomware Initiative (CRI), Jefa de la Unidad de Ciberdelincuencia, Ministerio Federal de Justicia, Nigeria</li><li>– Claudio Peguero, Ciberembajador, República Dominicana</li></ul> <b>► Ciberdelincuencia y pruebas electrónicas de crímenes de guerra: ¿Qué nos ha enseñado la agresión rusa contra Ucrania? [11:00-11:45]</b> <ul style="list-style-type: none"><li>– Dmytro Verbytsky, Fiscal General Adjunto, Ucrania</li><li>– Aisling Kelly, Consejera General Adjunta, Aplicación de la Ley y Seguridad Nacional, Europa, Microsoft</li><li>– CCI (POR CONFIRMAR)</li><li>– EUROJUST (POR CONFIRMAR)</li></ul> <b>► Ciberdelincuencia frente a libertad de expresión [11:45-12:30]</b> <ul style="list-style-type: none"><li>– Introducción</li><li>– Panel: Ponentes del Tribunal Europeo de Derechos Humanos, África, América y Asia</li></ul> <b>► El marco del Convenio sobre la Ciberdelincuencia: Actualización [12:30-13:00]</b> <ul style="list-style-type: none"><li>– Alexander Seger, Consejo de Europa</li></ul>
Pausa café 10:30-11:00	
14:30-16:00	<b>Taller 1 - Estado mundial de la legislación sobre ciberdelincuencia</b>  Idiomas: EN/FR/ES  Objetivo: La legislación es la base de la acción de la justicia penal en materia de ciberdelincuencia y pruebas electrónicas. Muchos gobiernos de todo el mundo han emprendido reformas legales, a menudo utilizando como directriz el Convenio de Budapest sobre la Ciberdelincuencia. Sin

	<p>embargo, la legislación sobre ciberdelincuencia también debe cumplir los requisitos en materia de derechos humanos y Estado de Derecho para evitar su uso indebido. El objetivo de este taller es examinar los progresos realizados en todo el mundo en materia de legislación sobre ciberdelincuencia e identificar posibles riesgos y retos.</p> <p>Moderador: Zahid Jamil, Abogado, Jamil &amp; Jamil, Pakistán</p> <p>Ponente: Fernanda Teixeira Domingos, Fiscalía, Brasil</p> <p>Secretaría: Giorgi Jokhadze / Tatiana Bastrighin</p> <ul style="list-style-type: none"> <li>▶ <b>Introducción y objetivo del taller [5 min]</b> <ul style="list-style-type: none"> <li>— Apuntes del moderador</li> <li>— Secretaría</li> </ul> </li> <li>▶ <b>De 2013 a 2023: Diez años de avances en la legislación sobre ciberdelincuencia y pruebas electrónicas [10 min]</b> <ul style="list-style-type: none"> <li>— Resultados de una encuesta de la Oficina del Programa de lucha contra la Ciberdelincuencia del Consejo de Europa (Giorgi Jokhadze, C-PROC)</li> </ul> </li> <li>▶ <b>Ejemplos de reformas recientes [30 min]</b> <ul style="list-style-type: none"> <li>— Ejemplos de buenas prácticas y reformas recientes (Convenio de Budapest): <ul style="list-style-type: none"> <li>- Jamila Ade, Nigeria</li> <li>- Germán Ortega, Ecuador</li> <li>- Glenys E. Andrews, Fiyi</li> </ul> </li> </ul> </li> <li>▶ <b>Retos y riesgos [40 min]</b> <ul style="list-style-type: none"> <li>— Segundo Protocolo Adicional: legislación de aplicación (Ioana Albani)</li> <li>— Garantías de los derechos humanos/libertad de expresión (Jan Kralik)</li> <li>— Debate: lo que se debe y lo que no se debe hacer en materia de legislación sobre ciberdelincuencia y pruebas electrónicas (debate abierto y ejemplos)</li> </ul> </li> <li>▶ <b>Conclusiones [5 min]</b></li> </ul>
14:30-16:00	<p><b>Taller 2 - Intercambio espontáneo de información</b></p> <p>Idiomas: EN/FR/ES/PT (pasivo)</p> <p>Objetivo: Las autoridades de justicia penal poseen a menudo información valiosa que consideran que puede ayudar a las autoridades de otro país en una investigación penal, pero de la que estas otras autoridades no tienen conocimiento. Las Partes en el Convenio de Budapest pueden compartir este tipo de información a través del artículo 26 sobre "información espontánea":</p> <p><i>"Dentro de los límites de su derecho interno y sin que exista demanda previa, una Parte podrá comunicar a otra Parte información obtenida de sus propias investigaciones si considera que ello puede ayudar a la Parte destinataria a iniciar o a concluir investigaciones o</i></p>

*procedimientos en relación con delitos previstos de conformidad con el presente Convenio, o cuando dicha información pueda conducir a una petición de cooperación de dicha Parte en virtud del presente Capítulo."*

La relevancia del artículo 26 ha ido aumentando con el tiempo, incluso en el contexto de casos relacionados con la *dark web* o con el intercambio de datos obtenidos de comunicaciones cifradas.

El objetivo del taller es identificar las prácticas actuales de utilización del artículo 26 del Convenio sobre la Ciberdelincuencia.

Moderadores: Jan Jerkhofs, Magistrado Federal, Jefe de la Unidad Cibernética, Fiscalía Federal, Bélgica

Antonio Segovia, Profesor de Derecho Penal Transnacional, Universidad UAI, Chile

Ponentes: Jorge Espina, Presidente del Equipo de Ciberdelincuencia, Miembro Nacional Adjunto por España, EUROJUST

Catalina Stroe, Directora de Programa, Oficina del Programa de lucha contra la Ciberdelincuencia, Consejo de Europa

Secretaría: Equipo GLACY+

► **Introducción y objetivo del taller [5 min]**

- Jan Jerkhofs, Magistrado Federal, Jefe de la Unidad Cibernética, Fiscalía Federal, Bélgica

► **Aplicación e interpretación del concepto de intercambio espontáneo de información entre las autoridades judiciales de los Estados miembros de la UE y los países con Fiscal de Enlace presente en EUROJUST [10 min]**

- Sofia Mirandola, Asesora de Cooperación Judicial en la Unidad de Casework, Departamento de Operaciones, EUROJUST

► **Mesa redonda sobre la utilización del artículo 26 del Convenio por las Partes que facilitan información: ¿cuáles son los procedimientos y las condiciones? [35 min]**

- Benjamin Fitzpatric, Consejero Principal, Sección de Delitos Informáticos y Propiedad Intelectual, División Penal, Departamento de Justicia de los Estados Unidos
- Debates abiertos - moderados por Jan Jerkhofs

► **Mesa redonda sobre la recepción de información espontánea: ¿Cómo puede utilizarse como prueba? [35 min] - moderada por Antonio Segovia**

- Anastasiia Ponarina, Oficial Superior de Cooperación Internacional, Departamento de Ciberseguridad, Servicio de Seguridad del Estado, Ucrania
- Esteban Aquilar Vargas, Fiscal, Coordinador de la Unidad de Ciberdelincuencia, Ministerio Público, Costa Rica
- Filipinas (por confirmar)
- Debates abiertos - moderados por Antonio Segovia

► **Conclusiones de los ponentes [10 min]**

- Jorge Espina, Presidente del Equipo de Ciberdelincuencia, Miembro

	<p>Nacional Adjunto por España, EUROJUST</p> <p>— Catalina Stroe, Directora de Programa, Oficina del Programa de lucha contra la Ciberdelincuencia, Consejo de Europa</p>
14:30-16:00	<p><b>Taller 3 - Detección automática de material de explotación y abuso sexual infantil</b></p> <p>Idiomas: EN/FR/ES/RO</p> <p>Objetivo: En la última década, los proveedores de servicios multinacionales han desplegado tecnología para la detección automatizada de material de abuso sexual infantil (CSAM) cargado o difundido a través de sus servicios. Decenas de millones de CSAM han sido identificadas y denunciadas de este modo, y en muchos casos han ayudado a rescatar a víctimas y a identificar y procesar a delincuentes en todo el mundo. Al mismo tiempo, el uso de estas técnicas ha suscitado inquietudes en relación con el Estado de Derecho y los derechos humanos, por ejemplo, pues interfieren en la privacidad de las comunicaciones o implican la transferencia transfronteriza de datos personales o violan las garantías procesales.</p> <p>El objetivo del taller es continuar la búsqueda de soluciones que permitan a los gobiernos cumplir con su obligación positiva de proteger a los niños contra la violencia sexual en línea y permitir a los proveedores de servicios utilizar tecnologías automatizadas para identificar y denunciar CSAM con las salvaguardias necesarias de privacidad, protección de datos y estado de derecho.</p> <p>Moderadora: Maria José Costello-Branco, Presidenta de Mesa, Oficina del Comité de Lanzarote</p> <p>Ponente: Jean-Christophe le Toquin</p> <p>Secretaría: Naomi Trewinnard, Asesora Jurídica, Secretaría del Comité de Lanzarote</p> <p>Nina Lichtner, Directora de Programas, Proyecto Octopus, Consejo de Europa</p> <ul style="list-style-type: none"> <li>▶ <b>Introducción y objetivo del taller [5 min]</b> <ul style="list-style-type: none"> <li>- Reflexiones y avances tras el taller de la Conferencia Octopus 2021</li> </ul> </li> <li>▶ <b>Avances en detección automática y optimización de informes</b> <ul style="list-style-type: none"> <li>- INTERPOL (por confirmar)</li> <li>- Susanna Pettersson, ECPAT Suecia</li> </ul> </li> <li>▶ <b>Aumentar las obligaciones y superar los retos</b> <ul style="list-style-type: none"> <li>- Debate con el público</li> </ul> </li> <li>▶ <b>Soluciones de colaboración y aplicación de políticas</b> <ul style="list-style-type: none"> <li>- Debate con el público</li> </ul> </li> <li>▶ <b>Conclusiones [10 min]</b></li> </ul>

16:30-18:00

#### **Taller 4 - Sinergias entre los Convenios de Budapest, Lanzarote, Estambul y el Convenio sobre la trata de seres humanos para un ciberespacio más seguro**

Idiomas: EN/FR/ES

Objetivo: Las normas de los Convenios mantenidos por el Consejo de Europa en los ámbitos de la ciberdelincuencia, la protección de los niños contra los abusos sexuales, la trata de seres humanos y la violencia contra las mujeres no son simplemente complementarias, sino que tienen por objeto fomentar el trabajo entre las autoridades de justicia penal, los responsables de la protección y los responsables políticos para garantizar una mejor justicia penal y las medidas conexas en estos ámbitos. Los delitos de derecho sustantivo, el uso de herramientas procesales para la investigación y el trabajo preventivo/protector con víctimas y testigos son sólo ejemplos en los que la armonización sería clave, mientras que conceptos como la acción sobre la ciberviolencia podrían servir para indicar dónde y cómo deberían funcionar tales sinergias.

El objetivo de este taller es potenciar las sinergias entre cuatro Convenios diferentes, pero interconectados:

- ▶ Convenio sobre la Ciberdelincuencia ([STE nº 185](#))
- ▶ Convenio del Consejo de Europa sobre la protección de los niños contra la explotación y los abusos sexuales ([STCE nº 201](#))
- ▶ Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica ([STCE nº 210](#))
- ▶ Convenio del Consejo de Europa sobre la lucha contra la trata de seres humanos ([STCE nº 197](#))

Moderadora: Miriam Bahamonde Blanco, Ministerio de Justicia, España

Ponente: Ovidiu Majina, División de Infancia, Consejo de Europa

Secretaría: Giorgi Jokhadze / Ana Vlad

▶ **Introducción y objetivo del taller [5 min]**

- Apuntes de la moderadora
- Secretaría

▶ **Acción penal: hay que colmar las lagunas antes de buscar las sinergias [40 min]**

Intervenciones de:

- Estudio del Consejo de Europa sobre los aspectos de derecho sustantivo de los tres Convenios: Budapest, Estambul, Lanzarote (Betty Shave, consultora T-CY)
- Perspectiva estadounidense: hacer que las normas funcionen juntas (Nate Brooks, ICHIP Zagreb, USDOJ)

Puntos de vista de la comisión:

- Judith Herrnfeld, Oficina T-CY
- Naomi Trewinnard, Comité del Convenio de Lanzarote
- María Rún Bjarnadóttir, GREVIO (en línea)
- GRETA

	<p>► <b>Trabajo de prevención y protección: una perspectiva diferente [30 min]</b></p> <p>Ejemplos de buenas (y malas) prácticas/intervenciones de los paneles:</p> <ul style="list-style-type: none"> <li>- Judith Herrnfeld, Oficina T-CY</li> <li>- Naomi Trewinnard, Comité del Convenio de Lanzarote</li> <li>- María Rún Bjarnadóttir, GREVIO (en línea)</li> <li>- GRETA</li> <li>- Ejemplos</li> </ul> <p>► <b>Lucha contra la ciberviolencia: potencial de sinergias [10 min]</b></p> <ul style="list-style-type: none"> <li>– El concepto de ciberviolencia: ¿un "puente" entre estos tratados?</li> <li>– Debate y ejemplos: opiniones de las comisiones presentes</li> </ul> <p>► <b>Conclusiones [5 min]</b></p>
16:30-18:00	<p><b>Taller 5 - La interacción de la ciberdelincuencia y las investigaciones financieras</b></p> <p>Idiomas: EN</p> <p>Objetivo: Establecer una colaboración eficaz entre las autoridades de justicia penal que investigan la ciberdelincuencia y las instituciones responsables de las investigaciones financieras es vital para proteger a las sociedades contra las actividades delictivas. El objetivo del taller es determinar prácticas de colaboración y fomentar la cooperación nacional e internacional, modelos eficaces de trabajo en equipo entre organismos y principios que rijan el intercambio de información y pruebas entre expertos en delitos financieros y ciberdelincuencia.</p> <p>Moderador: Robert Golobinek, Ministerio de Justicia de Eslovenia</p> <p>Ponente: Goran Jankoski, Banco Nacional de la República de Macedonia del Norte</p> <p>Secretaría: Daniel Cuciurianu, Director de Programa, Consejo de Europa / Equipo iPROCEEDS-2</p> <p>► <b>Introducción y objetivo del taller [5 min]</b></p> <ul style="list-style-type: none"> <li>– Apuntes del moderador</li> <li>– Secretaría</li> </ul> <p>► <b>Flujo de dinero de la delincuencia en línea y tipologías de blanqueo de capitales [20 min]</b></p> <ul style="list-style-type: none"> <li>– Camelia López, Abogada Asesora, ICHIP Global, Dark Web y Criptodivisas, US DOJ</li> <li>– Max Braun, Director, Fiscalía General, UIF Luxemburgo</li> </ul> <p>► <b>Cooperación en la búsqueda, incautación y decomiso de los productos del delito en línea [20 min]</b></p> <ul style="list-style-type: none"> <li>– Max Braun, Director, Fiscalía General, UIF Luxemburgo</li> <li>– Camelia López, Abogada Asesora, ICHIP Global, Dark Web y Criptodivisas, US DOJ</li> </ul> <p>► <b>Nuevas herramientas y técnicas de investigación financiera en casos</b></p>

	<p><b>de ciberdelincuencia [35 min]</b></p> <ul style="list-style-type: none"> <li>— Kārlis Pūce, analista jefe, FIU Letonia</li> <li>— Horacio J. Azzolin, Fiscal, Unidad Especializada en Ciberdelincuencia UFECI, Argentina</li> </ul> <p>► <b>Conclusiones del ponente [10 min]</b></p> <ul style="list-style-type: none"> <li>— Goran Jankoski, Banco Nacional de la República de Macedonia del Norte</li> </ul>
16:30-18:00	<p><b>Taller 6 - Inteligencia artificial generativa: amenazas y beneficios para la justicia penal</b></p> <p>Idiomas: EN/FR/ES</p> <p>Objetivo: La Inteligencia Artificial en el sector de la justicia penal puede tanto representar una grave amenaza como mejorar la lucha contra la ciberdelincuencia. La IA generativa puede proporcionar medios eficaces para detectar delitos o prestar asistencia en la investigación mediante el análisis de grandes cantidades de datos, pero también puede utilizarse indebidamente con fines delictivos. Los datos falsificados (como las falsificaciones profundas o <i>deep fake</i>) pueden incluso presentarse como pruebas ante un tribunal. El objetivo de este taller es examinar (a) las amenazas criminales que la IA generativa puede plantear para el sector de la justicia penal, (b) su papel en la lucha contra la ciberdelincuencia, y (c) las cuestiones clave que deben tenerse en cuenta en la evaluación de las pruebas electrónicas generadas por la IA.</p> <p>Moderador/es: Patrick Penninckx, Jefe del Departamento de Sociedad de la Información, Consejo de Europa</p> <p>Ponente: Por confirmar</p> <p>Secretaría: Jan Kralik, Director de Programa, Secretaría T-CY, Consejo de Europa</p> <p>► <b>Introducción y objetivo del taller [5 min]</b></p> <ul style="list-style-type: none"> <li>— Patrick Penninckx, Jefe del Departamento de Sociedad de la Información, Consejo de Europa</li> </ul> <p>► <b>Ciberdelincuencia e IA generativa: amenazas y oportunidades [40 min]</b></p> <ul style="list-style-type: none"> <li>— Emmanuel Kessler, Jefe de Equipo - Prevención/Difusión, EUROPOL</li> <li>— Secretaría de la CAI (por confirmar)</li> <li>— Sabine Gless, ponente de la CDPC sobre Inteligencia Artificial y Derecho Penal, Profesora de Derecho Penal y Procesal Penal, Universidad de Basilea, Suiza.</li> <li>— Debate</li> </ul> <p>► <b>Abordar las pruebas electrónicas de IA generativa: cuestiones clave, amenazas y beneficios [35 min]</b></p> <ul style="list-style-type: none"> <li>— Krešimir Kamber, Asesor del Presidente y del Secretario del Tribunal Europeo de Derechos Humanos</li> <li>— Centro de Innovación de INTERPOL (por confirmar)</li> <li>— Mario Lara Orellana, Director del Departamento de Desarrollo Institucional de la Rama Administrativa del Poder Judicial de Chile</li> <li>— Debate</li> </ul>

	<p>► <b>Conclusiones [10 min]</b></p>
<p><b>JUEVES 14 DE DICIEMBRE</b></p>	
<p>9:30-15:30</p> <p><i>Pausa café</i> 11:00-11:30</p> <p><i>Pausa para comer</i> 13:00-14:30</p>	<p><b>Evento del proyecto: De CyberEAST a CyberEast+</b></p> <p>Idiomas: EN</p> <p>Objetivo: Este acto servirá de conferencia de clausura del proyecto CyberEast y allanará el camino a su continuación, el proyecto CyberEast+. El evento recorrerá los temas del proyecto: legislación y políticas, desarrollo de capacidades y cooperación; y contará la historia de CyberEast desde la perspectiva de los socios nacionales, demostrando el impacto y la relevancia del proyecto para mejorar sus capacidades en materia de ciberdelincuencia y pruebas electrónicas. La Comisión Europea y el Consejo de Europa evaluarán y completarán formalmente el proyecto y lanzarán una nueva acción regional sobre ciberdelincuencia y pruebas electrónicas en la región a través del nuevo proyecto CyberEast+. En el taller también se debatirá con vistas a la adopción de una nueva Declaración sobre Prioridades Estratégicas para la región de la Asociación Oriental con los principales socios del proyecto, que servirá de inspiración para las políticas y el desarrollo de capacidades en los países de la región.</p> <p>Moderador/es: Giorgi Jokhadze / Equipo CyberEast</p> <p>Ponente: Equipo CyberEast</p> <p>Secretaría: Giorgi Jokhadze / Equipo CyberEast</p> <p>► <b>Sesión inaugural [20 min]</b></p> <ul style="list-style-type: none"> <li>— Representante de la Comisión Europea</li> <li>— Representante del Consejo de Europa</li> <li>— Presentación de los equipos nacionales del proyecto</li> <li>— Lead-in: orden del día de la reunión (Oficina del Programa de lucha contra la Ciberdelincuencia)</li> </ul> <p>► <b>Clausura del proyecto CyberEast [70 min]</b></p> <ul style="list-style-type: none"> <li>— Prioridades y logros del país en materia de legislación y políticas (representante nacional del proyecto)</li> <li>— Desarrollo de capacidades: necesidades e impacto (representante nacional del proyecto)</li> <li>— Cooperación: puesta en práctica de las normas (representante nacional del proyecto)</li> </ul> <p>Pausa café [30 min]</p> <p>► <b>Debate sobre el proyecto CyberEast+ [90 min]</b></p> <ul style="list-style-type: none"> <li>— Nuevas prioridades y orientaciones de actuación (Comisión Europea)</li> <li>— Equipos nacionales (Oficina del Programa de lucha contra la Ciberdelincuencia)</li> <li>— Plan de actividades (Oficina del Programa de lucha contra la Ciberdelincuencia)</li> </ul> <p>Pausa para el almuerzo [90 min]</p>

	<ul style="list-style-type: none"> <li>▶ <b>Reunión de responsables políticos sobre políticas de ciberdelincuencia en la región de la Asociación Oriental [120 min]</b> <ul style="list-style-type: none"> <li>— Presentación y análisis comparativo de la Declaración previa (2013) (experto invitado)</li> <li>— Declaración de prioridades estratégicas para la Asociación Oriental 2023 (Secretaría)</li> <li>— Intervención y evaluación de la Comisión Europea</li> <li>— Intervenciones y evaluaciones de cada uno de los países de la Asociación Oriental</li> <li>— Recapitulación y adopción de la Declaración de Prioridades Estratégicas 2023</li> </ul> </li> </ul>
<p>9:30-16:30</p> <p><i>Pausa café</i> 11:00-11:30</p> <p><i>Pausa para comer</i> 13:00-14:30</p>	<p><b>Evento del proyecto: De iPROCEEDS-2 a CyberSEE</b></p> <p>Idiomas: EN</p> <p>Objetivo: Esta conferencia de clausura del proyecto iPROCEEDS-2 evaluará los principales objetivos del proyecto, incluida la legislación y los enfoques estratégicos, los mecanismos de denuncia, la mejora de la capacidad en materia de ciberdelincuencia, la formación de la judicatura y el fomento de la colaboración entre los sectores público y privado, así como la cooperación internacional. La atención se centrará en la presentación por parte de los socios nacionales de la diferencia que ha supuesto el proyecto para mejorar la competencia de sus organismos en el tratamiento de la ciberdelincuencia y las pruebas electrónicas. El acto marcará la evaluación formal y el cierre del proyecto. También preparará el terreno para una nueva acción regional dirigida a la ciberdelincuencia y las pruebas electrónicas en Europa Sudoriental y Turquía: la nueva iniciativa "CyberSEE" será emprendida conjuntamente por la Comisión Europea y el Consejo de Europa de 2024 a 2027.</p> <p>Moderador: Daniel Cuciurianu / Equipo iPROCEEDS-2</p> <p>Ponente: Daniel Cuciurianu / Equipo iPROCEEDS-2</p> <p>Secretaría: Daniel Cuciurianu / Equipo iPROCEEDS-2</p> <ul style="list-style-type: none"> <li>▶ <b>Sesión inaugural [20 min]</b> <ul style="list-style-type: none"> <li>— Representante de la Comisión Europea</li> <li>— Representante del Consejo de Europa</li> <li>— Presentación del objetivo y del orden del día de la reunión</li> <li>— Presentación de los equipos nacionales del proyecto</li> </ul> </li> <li>▶ <b>Acto de clausura del proyecto iPROCEEDS-2 [70 min]</b> <ul style="list-style-type: none"> <li>— Logros de los países/zonas en materia de legislación, políticas y estrategias</li> <li>— Capacidades de los países/zonas en materia de investigación de la ciberdelincuencia, búsqueda, incautación y confiscación de los productos del delito en línea y obtención de pruebas electrónicas</li> <li>— Resultados de la formación judicial: objetivo más destacado del proyecto</li> <li>— Progresos realizados en la cooperación público-privada e internacional</li> </ul> </li> </ul>

	<p>Pausa café [30 min]</p> <ul style="list-style-type: none"> <li>▶ <b>Hacia el proyecto CyberSEE: reunión regional [90 min]</b> <ul style="list-style-type: none"> <li>– Prioridades estratégicas y nuevas orientaciones de actuación (Comisión Europea)</li> <li>– Plan de actividades (Oficina del Programa de lucha contra la Ciberdelincuencia)</li> <li>– Necesidades actuales, prioridades nacionales y regionales (Equipos nacionales)</li> </ul> </li> </ul> <p>Pausa para el almuerzo [90 min]</p> <ul style="list-style-type: none"> <li>▶ <b>Aspectos esenciales del nuevo proyecto [120 min]</b> <ul style="list-style-type: none"> <li>– Formación sostenible sobre ciberdelincuencia y pruebas electrónicas en las Academias de Justicia, las Academias de Policía y otras instituciones de formación.</li> <li>– Mayor atención a las amenazas de ataques de <i>ransomware</i> y OCSEA</li> <li>– Cooperación entre instituciones de ciberdelincuencia y ciberseguridad</li> <li>– Complementariedad de las actividades nacionales y regionales</li> </ul> </li> </ul>
<p>9:30-18:00</p> <p><i>Repaso a los logros de GLACY+</i></p> <p><i>Pausa café 11:00-11:30</i></p>	<p><b>Evento del proyecto: De GLACY+ a GLACY-e</b></p> <p>Idiomas: EN/FR/PT/ES</p> <p>Objetivo: Esta sesión es el acto de clausura del proyecto GLACY+. Brindará la oportunidad de revisar el impacto del proyecto GLACY+ y de compartir las lecciones aprendidas. Basándose en los resultados positivos de GLACY+, se está iniciando ahora una continuación, consolidación y expansión con la "Acción Mundial contra la Ciberdelincuencia Mejorada" (GLACY-e), un nuevo proyecto conjunto UE-CdE. GLACY-e ampliará la experiencia del proyecto GLACY+ apoyando a nuevos países seleccionados de África, Asia-Pacífico y América Latina, además de refuerza el papel de liderazgo de los 8 países centrales en el programa de desarrollo de capacidades en sus respectivas regiones.</p> <p>Moderador/es: Catalina Stroe, Responsable de los proyectos GLACY+/-e</p> <p>Secretaría: Proyecto GLACY+</p> <ul style="list-style-type: none"> <li>▶ <b>Sesión inaugural [30 min]</b> <ul style="list-style-type: none"> <li>– Unión Europea</li> <li>– Interpol</li> <li>– Consejo de Europa</li> </ul> </li> <li>▶ <b>Panorama general e impacto de GLACY+ [30 min]</b> <ul style="list-style-type: none"> <li>– Catalina Stroe y Dong uK Kim, presentación introductoria</li> </ul> </li> <li>▶ <b>Enseñanzas extraídas de GLACY+ [150 min].</b> <ul style="list-style-type: none"> <li>– Coordinadores nacionales, logros nacionales, impacto a nivel nacional e historias menos exitosas [5 min por intervención]</li> </ul> </li> <li>▶ <b>¿Qué podemos esperar ahora? [30 min]</b> <ul style="list-style-type: none"> <li>– Presentación del proyecto GLACY-e, Catalina Stroe</li> </ul> </li> </ul>

<p><i>Perspectivas de futuro: GLACY-e</i></p> <p><i>Pausa para comer 13:00-14:30</i></p> <p><i>Pausa café 16:00-16:30</i></p>	<ul style="list-style-type: none"> <li>▶ <b>Presentación de los países seleccionados [60 min]</b> <ul style="list-style-type: none"> <li>– Representantes de los países, presentación de los países seleccionados [7 min cada uno]</li> </ul> </li> <li>▶ <b>Plan de trabajo GLACY-e para el primer trimestre de 2024 [30 min].</b> <ul style="list-style-type: none"> <li>– Catalina Stroe y Dong uK Kim, presentación del plan de trabajo y debates abiertos</li> </ul> </li> <li>▶ <b>Sostenibilidad por diseño y por defecto: prioridades estratégicas para los países centrales [45 min]</b> <ul style="list-style-type: none"> <li>– Presentación de las prioridades y agendas regionales por parte de los países centrales</li> </ul> </li> <li>▶ <b>Observaciones finales [10 min]</b> <ul style="list-style-type: none"> <li>– Unión Europea</li> <li>– Interpol</li> <li>– Consejo de Europa</li> </ul> </li> </ul>
<p>14:30-18:00</p> <p><i>Pausa café 15:30-16:00</i></p>	<p><b>Evento del proyecto: De CyberSouth a CyberSouth+</b></p> <p>Idiomas: EN/FR</p> <p>Objetivo: El objetivo de la conferencia final es revisar y validar conjuntamente los avances en la lucha contra la ciberdelincuencia en la región MENA durante el período 2018 - 2023; evaluar el impacto del proyecto CyberSouth en cinco áreas principales relacionadas con los resultados del proyecto (legislación, trabajo de la policía, trabajo del poder judicial, cooperación internacional, estrategias nacionales) y evaluar conjuntamente lo que ha funcionado bien (mejores prácticas) y lo que se puede mejorar en la siguiente fase.</p> <p>Moderadora: Denise Mazzolani, Directora del Programa CyberSouth, Consejo de Europa</p> <p>Secretaría: Equipo CyberSouth</p> <ul style="list-style-type: none"> <li>▶ <b>Sesión inaugural (10 min)</b> <ul style="list-style-type: none"> <li>– Stefano Dotto, Jefe de Equipo – División de Buena Gobernanza y Seguridad, DG NEAR B2, Comisión Europea</li> <li>– Denise Mazzolani, Directora del Programa CyberSouth, Consejo de Europa</li> </ul> </li> <li>▶ <b>Evaluación de CyberSouth: evaluación de los cinco resultados del proyecto (50 min)</b> <ul style="list-style-type: none"> <li>– Resumen del informe de evaluación final</li> <li>– Aportaciones de los países prioritarios</li> <li>– Debate</li> </ul> </li> <li>▶ <b>Buenas prácticas y revisión de las modalidades de ejecución de los proyectos (60 min)</b> <ul style="list-style-type: none"> <li>– Presentación del equipo del proyecto CyberSouth</li> <li>– Aportaciones de los países prioritarios</li> <li>– Debate</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>▶ <b>Prioridades de la región MENA en la cooperación sobre ciberdelincuencia 2024-2026 (50 min)</b> <ul style="list-style-type: none"> <li>– Presentación por países prioritarios</li> <li>– Política Europea de Vecindad: prioridades para la región MENA</li> <li>– Introducción al proyecto CyberSouth+: principales componentes y fase inicial</li> </ul> </li> <li>▶ <b>Observaciones finales (10 min)</b></li> </ul>
16:30-18:00	<p><b>Charlas relámpago</b></p> <p>Idiomas: EN/FR/ES/RO</p> <p>Objetivo: Por tercera vez, el Consejo de Europa ofrecerá sesiones de Charlas relámpago, durante las cuales los ponentes presentarán brevemente ideas innovadoras en el ámbito de la ciberdelincuencia. Una charla relámpago es una presentación muy breve que dura sólo unos minutos. Por lo general, varios oradores pronunciarán varias charlas relámpago en una misma sesión.</p> <p>Le invitamos a presentar su propuesta de una idea innovadora importante que esté dispuesto a compartir con más de 500 participantes de todo el mundo, que se reunirán en la Conferencia Octopus de Bucarest. Se seleccionarán 10 propuestas en función de la diversidad de temas y ponentes.</p> <p>Moderador: por confirmar</p> <p>Secretaría: Equipo Octopus</p> <ul style="list-style-type: none"> <li>▶ <b>Introducción y objetivo de la sesión</b></li> <li>▶ <b>Charlas relámpago</b></li> <li>▶ <b>Conclusiones</b></li> </ul>
<b>VIERNES 15 DE DICIEMBRE</b>	
9:30-11:00	<p><b>Taller 7 - Taller regional para Asia: La protección de datos como facilitadora de la investigación y la resolución de casos de ciberdelincuencia y casos que implican pruebas electrónicas</b></p> <p>Idiomas: EN</p> <p>Objetivo: Con la creciente dependencia de la tecnología impulsada por la información y el crecimiento exponencial de la cantidad de datos creados e intercambiados cada día por usuarios y organizaciones, el derecho a la protección de los datos personales se enfrenta a grandes retos. Esto también es cierto para las autoridades de justicia penal, que necesitan conciliar medidas eficaces para obtener, procesar y compartir datos personales que son necesarios en investigaciones y procedimientos penales con los requisitos de protección de datos. Cuando estos requisitos se cumplen, facilitan el intercambio de datos personales también a través de las fronteras y con proveedores de servicios y otras entidades del sector privado. Esta es la razón por la que el artículo 14 sobre la protección de</p>

	<p>datos personales se incluyó en el Segundo Protocolo del Convenio de Budapest. El objetivo de este taller es compartir experiencias -y debatir los retos- para los países de Asia en el establecimiento de marcos de protección de datos que permitan una respuesta más eficaz de la justicia penal a la ciberdelincuencia.</p> <p>Moderador: Peter Kimpian, Director de Programa, Unidad de Protección de Datos del Consejo de Europa</p> <p>Ponente: por confirmar</p> <p>Secretaría: Proyecto GLACY+</p> <ul style="list-style-type: none"> <li>▶ <b>Introducción y objetivo del taller [5 min]</b> <ul style="list-style-type: none"> <li>– Peter Kimpian, Director de Programa, Unidad de Protección de Datos del Consejo de Europa</li> </ul> </li> <li>▶ <b>Salvaguardias de protección de datos en el Segundo Protocolo Adicional: ¿por qué las necesitamos? [10 minutos]</b></li> <li>▶ <b>La protección de datos como piedra angular de la cooperación policial internacional [10 min]</b> <ul style="list-style-type: none"> <li>– Caroline Goemans-Dorny, Oficial de Protección de Datos de INTERPOL</li> </ul> </li> <li>▶ <b>Abordar la protección de datos: testimonios de países [10 min].</b></li> <li>▶ <b>La obligación del Estado de proteger frente a los delitos y el derecho a la intimidad: ¿cómo encontrar el equilibrio adecuado? [50 min]</b> <ul style="list-style-type: none"> <li>– Debate moderado por Jayantha Fernando, Director de la Autoridad de Protección de Datos y Director de la Junta Directiva del CERT de Sri Lanka</li> </ul> </li> <li>▶ <b>Conclusiones del ponente [5 min]</b></li> </ul>
9:30-11:00	<p><b>Taller 8 - Taller regional para el Pacífico: Desafíos en la aplicación de las leyes sobre ciberdelincuencia en las pequeñas jurisdicciones del Pacífico</b></p> <p>Idiomas: EN</p> <p>Objetivo: Unos marcos jurídicos sólidos en materia de ciberdelincuencia y pruebas electrónicas son la piedra angular del éxito de las investigaciones y los procesos penales. Las normas internacionales, como el Convenio de Budapest, proporcionan un marco para la coherencia de las definiciones y la tipificación, la normalización de las competencias procesales y los mecanismos de cooperación internacional. La ausencia de transposición de tales medidas a las legislaciones nacionales socava la capacidad de un país para investigar, procesar y juzgar casos relacionados con pruebas electrónicas y para participar en los esfuerzos mundiales por responder eficazmente a los nuevos retos que plantea la ciberdelincuencia.</p> <p>Las jurisdicciones pequeñas, como los Estados insulares del Pacífico, pueden encontrar retos adicionales a la hora de adoptar y adaptar leyes adecuadas, teniendo en cuenta sus contextos jurídicos, administrativos y</p>

	<p>técnicos específicos. El objetivo del taller es identificar esos retos y las posibles soluciones basadas en prácticas exitosas en la región.</p> <p>Moderadora: Linda Folaumoetu'I, Fiscal General de Tonga y Presidenta del Grupo de Trabajo sobre Ciberdelincuencia de PILON</p> <p>Ponente: Jamie Crawford, Senior Crown Counsel, Crown Law Office of the Cook Islands, en representación de PILON.</p> <p>Secretaría: Proyecto GLACY+</p> <p>► <b>Introducción y objetivo del taller [10 min]</b></p> <ul style="list-style-type: none"> <li>– Linda Folaumoetu'I, Fiscal General de Tonga y Presidenta del Grupo de Trabajo sobre Ciberdelincuencia de PILON</li> </ul> <p>► <b>¿En qué consiste un marco jurídico eficaz contra la ciberdelincuencia, adaptado a las necesidades de los Estados insulares del Pacífico, y cuáles son los retos a los que se enfrentan cuando trabajan en su reforma legislativa? [35 minutos]</b></p> <ul style="list-style-type: none"> <li>– Glenys Andrews, Directora Jurídica y Oficial (Redacción), Oficina del Fiscal General, Fiyi</li> <li>– Andrew Ega Kelesi, Director de la Fiscalía, Oficina del Director de la Fiscalía, Islas Salomón</li> <li>– Debates moderados por Noumea Loretta Afamasaga-Teueli, Jefa de Redacción Legislativa, Oficina del Director de la Fiscalía Pública, Nauru</li> </ul> <p>► <b>Perspectivas del Pacífico en materia de aplicación: ¿cuáles son los ingredientes clave para una aplicación efectiva? [40 min]</b></p> <ul style="list-style-type: none"> <li>– Domingo Kabunare, Oficina de Transformación Digital, Ministerio de Información, Comunicaciones y Transportes, Kiribati</li> <li>– John Graham Jack, CIO Oficina del Gobierno, Gabinete del Primer Ministro, Vanuatu</li> <li>– Debates moderados por Matthew Blackwood, ICHIP, Departamento de Justicia de EE.UU.</li> </ul> <p>► <b>Conclusiones por parte del ponente</b></p>
<p>9:30-11:00</p>	<p><b>Taller 9 - Taller regional para África: El Convenio sobre la Ciberdelincuencia y el Segundo Protocolo - claves para la cooperación internacional en materia de pruebas electrónicas</b></p> <p>Idiomas: EN/FR (PT pasivo)</p> <p>Objetivo: Aunque las pruebas electrónicas son cada vez más importantes para las investigaciones y procedimientos penales también en África, los procedimientos para obtener dichas pruebas de otras jurisdicciones suelen ser largos y poco eficaces. El Segundo Protocolo del Convenio de Budapest (abierto a la firma en 2022) proporciona herramientas para mejorar la cooperación y la divulgación de pruebas electrónicas, como la cooperación directa con los proveedores de servicios y los registradores, medios eficaces para obtener información sobre abonados y datos de tráfico, cooperación inmediata en situaciones de emergencia o investigaciones conjuntas, al tiempo que garantiza un sólido sistema de salvaguardias de los derechos humanos y del Estado de Derecho, especialmente en lo que</p>

	<p>se refiere a la protección de los datos personales. Casi una cuarta parte de los países africanos son Partes o han sido invitados a adherirse al Convenio de Budapest. Utilizar las herramientas del Segundo Protocolo es, pues, una opción para África. Cabo Verde, Ghana, Marruecos y Mauricio figuran entre los países signatarios hasta la fecha. El taller tiene por objeto mostrar la pertinencia y conveniencia de las herramientas de cooperación previstas en el Protocolo, así como debatir los posibles retos que plantea su aplicación en la región africana.</p> <p>Moderador: Hein Dries, Experto clave en ciberdelincuencia, proyecto OCWAR-C</p> <p>Ponente: Abdul-Hakeem Ajjola, Presidente del Grupo de Expertos en Ciberseguridad de la Unión Africana</p> <p>Secretaría: Proyecto GLACY+</p> <p>► <b>Introducción y objetivo del taller - ¿Por qué los países africanos deberían considerar el Convenio sobre la Ciberdelincuencia y sus Protocolos? [15 minutos]</b></p> <ul style="list-style-type: none"> <li>— Erica O'neil, Directora Adjunta, Sección de Delitos Informáticos y Propiedad Intelectual, Departamento de Justicia de EE.UU.</li> <li>— Dr. Albert Antwi-Boasiako, Director General de la Autoridad de Ciberseguridad de Ghana</li> <li>— Alassane Ndiaye, Magistrado, Director Adjunto de la Dirección de Asuntos Penales e Indultos, Senegal</li> </ul> <p>► <b>Herramientas reforzadas para la cooperación internacional: ¿qué cambios aporta el Segundo Protocolo Adicional? [25 min]</b></p> <ul style="list-style-type: none"> <li>— Angela Cristina Marques Rodrigues, Magistrada Judicial del Tribunal de Praia, Consejo Superior del Poder Judicial, Cabo Verde</li> <li>— Moulay-Ahmed Tahiri-Alaoui, Jefe de la Unidad de Ciberdelincuencia, Ministerio Fiscal, Marruecos</li> <li>— Debates moderados</li> </ul> <p>► <b>Llevar la teoría a la práctica: vías hacia una cooperación internacional más eficaz - buenas historias y desafíos en la región [45 min]</b></p> <ul style="list-style-type: none"> <li>— Jamila Akaaga Ade, Directora Adjunta, Jefa de la Unidad de Ciberdelincuencia, Departamento de la Fiscalía Pública, Ministerio Federal de Justicia de Nigeria</li> <li>— Jacqueline De Lange, Jefa de la Sección de Ciberdelincuencia Comercial y Financiera, OCN de INTERPOL PRETORIA, Sudáfrica</li> <li>— Debates moderados</li> </ul> <p>► <b>Conclusiones [5 min]</b></p>
9:30-11:00	<p><b>Taller 10 - Taller regional para América Latina y el Caribe: Cooperación interinstitucional en materia de pruebas electrónicas</b></p> <p>Idiomas: EN/ES</p> <p>Objetivo: Muchos países de ALC se han esforzado en los últimos años por crear unidades especializadas en ciberdelincuencia a nivel de los servicios policiales y fiscales, así como unidades encargadas de la investigación forense digital. Sin embargo, la estructura organizativa y las funciones de dichas unidades siguen evolucionando y no siempre se basan en las buenas prácticas internacionales. Además, la cooperación</p>

	<p>interinstitucional entre las unidades especializadas en ciberdelincuencia y otros servicios para garantizar que las pruebas electrónicas sean admisibles en los tribunales, sigue siendo un reto. El taller tiene como objetivo identificar las buenas prácticas de creación de unidades forenses en la policía o la fiscalía, cómo garantizar la cooperación interinstitucional y cómo evitar conflictos de competencias en el ámbito de la investigación forense digital.</p> <p>Moderador: Bruno Fabio, AD, Innovación Aplicada, pro tempore, Innovación Aplicada, INTERPOL</p> <p>Ponente: Sonia Jiménez, OEA</p> <p>Secretaría: Equipo GLACY+, INTERPOL</p> <ul style="list-style-type: none"> <li>▶ <b>Introducción y objetivo del taller [10 min]</b> <ul style="list-style-type: none"> <li>— INTERPOL</li> </ul> </li> <li>▶ <b>Unidades forenses digitales: ¿cuáles son las prácticas de investigación y las capacidades organizativas actuales y cuáles son sus limitaciones? [35 min]</b> <ul style="list-style-type: none"> <li>— Luciano Kuppens, Consejo Nacional de Justicia Federal, Brasil</li> <li>— Mauricio Fernández, Director de la Unidad de Ciberdelincuencia, Ministerio Público, Chile</li> <li>— Armando José Díaz, Jefe del Departamento de Ciberseguridad y Miembro de la Unidad de Punto de Contacto Permanente 24/7, República Dominicana</li> <li>— Debates abiertos basados en preguntas preparadas de antemano y compartidas con el público.</li> </ul> </li> <li>▶ <b>Vías de cooperación interinstitucional en materia de investigación forense digital [40 min]</b> <ul style="list-style-type: none"> <li>— Debates moderados por Bruno Fabio, AD, Innovación Aplicada, pro tempore, Innovación Aplicada, INTERPOL</li> <li>— Preguntas orientativas para compartir previamente con la audiencia</li> </ul> </li> <li>▶ <b>Conclusiones por parte de la ponente [5 min]</b></li> </ul>
11:30-13:00	<p><b>Taller 11 - El desarrollo de capacidades como factor de cambio: ¿qué marca la diferencia?</b></p> <p>Idiomas: EN/FR/ES</p> <p>Objetivo: El objetivo del taller es identificar ejemplos de esfuerzos de desarrollo de capacidades que hayan marcado una diferencia real a la hora de permitir cambios sostenibles en los sistemas de justicia penal y de aumentar la eficacia de las herramientas contra la ciberdelincuencia. En la última década, los gobiernos, las organizaciones internacionales, el sector privado y las organizaciones de la sociedad civil han puesto en marcha numerosos proyectos para hacer frente a la ciberdelincuencia a escala nacional, regional e internacional. Algunas acciones tuvieron más éxito que otras. Es importante capitalizar aquellas experiencias que tuvieron un impacto y ayudaron a las autoridades de justicia penal y a las sociedades a abordar la ciberdelincuencia de manera más eficaz.</p> <p>Moderador/es: por confirmar</p>

	<p>Ponente: Vouter Wenstra, Director de Divulgación y Asociaciones Globales – Foro Global de Ciberexperiencia (GFCE)</p> <p>Secretaría: Equipo CyberSouth</p> <p>► <b>Introducción y objetivo del taller [5 min]</b></p> <p>► <b>Mesa redonda: qué funcionó bien y qué menos</b> Ejemplos de esfuerzos nacionales e internacionales de capacitación que han dado lugar a cambios sistemáticos, así como de acciones que no produjeron los resultados esperados. El moderador dirigirá preguntas a los miembros del panel y abrirá un turno de intervenciones sobre las prácticas y casos compartidos:</p> <p><b>La experiencia nacional (40 min)</b></p> <ul style="list-style-type: none"> <li>– <b>Chile</b> (Mauricio Fernández Montalbán, Director, Unidad Especializada en Ciberdelincuencia y Blanqueo de Capitales, Fiscalía Nacional)</li> <li>– <b>Ghana</b> (Albert Antwi-Boasiako, Director General de la Autoridad de Ciberseguridad)</li> <li>– <b>Corea del Sur</b> (por confirmar)</li> <li>– <b>Marruecos</b> (Ahmed Tahiri Alaoui, Jefe de la Unidad de Ciberdelincuencia de la Fiscalía)</li> <li>– <b>Sri-Lanka</b> (Wasantha Perera, Secretario, Ministerio de Justicia)</li> </ul> <p><b>La experiencia internacional (40 min)</b></p> <ul style="list-style-type: none"> <li>– <b>GFCE</b> (Vouter Wenstra, Director de Divulgación y Asociaciones Mundiales)</li> <li>– <b>GIZ</b> (por confirmar)</li> <li>– <b>INTERPOL</b> (Dong Uk Kim, funcionario especializado en ciberdelincuencia)</li> <li>– <b>ICHIP</b> (Anand Ramaswamy, International Computer Hacking and Intellectual Property, Addis Abeba, USDOJ)</li> <li>– <b>OEA</b></li> <li>– <b>OSCE</b> (Martha Stickings, Jefa Adjunta y Asesora sobre Ciberdelincuencia, Unidad de Estrategia Policial)</li> <li>– <b>UNODC</b> (Mustafa Erten, Centro Regional para la Ciberdelincuencia)</li> <li>– <b>Banco Mundial</b> (Keongmin Yoon, Consejero)</li> <li>– <b>Consejo de Europa</b> (Denise Mazzolani, Directora del Proyecto CyberSouth)</li> </ul> <p>► <b>Sesión de preguntas y respuestas</b></p> <p>► <b>Conclusiones [10 min]</b></p>
11:30-13:00	<p><b>Taller 12 - Xenofobia y racismo en línea frente a libertad de expresión</b></p> <p>Idiomas: EN/FR/ES/RO</p> <p>Objetivo: Ante el aumento de la incitación al odio en línea, incluidos el racismo y la xenofobia, las sociedades se esfuerzan por dar una respuesta eficaz que respete también el derecho fundamental a la libertad de expresión. Se puede adoptar una amplia gama de medidas para hacer frente a la incitación al odio en línea (véase la Recomendación del Consejo de Europa sobre la incitación al odio adoptada en 2022). En este espectro de</p>

	<p>medidas, el derecho penal es un importante último recurso. En 2003, se abrió a la firma el primer Protocolo del Convenio sobre la Ciberdelincuencia, que aborda la "penalización de los actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos" (STE nº 189). Con motivo del vigésimo aniversario de este Protocolo, se realizó un estudio de buenas prácticas sobre la experiencia de este tratado. El taller tiene por objeto presentar las conclusiones de este estudio, proporcionar nuevas orientaciones y debatir los retos que plantea la lucha contra la xenofobia y el racismo cometidos en línea, respetando al mismo tiempo el derecho a la libertad de expresión.</p> <p>Moderadora: Jamila Akaaga Ade, Subdirectora Jefa de la Unidad de Ciberdelincuencia, Ministerio Federal de Justicia, Nigeria</p> <p>Ponente: por confirmar</p> <p>Secretaría: Jan Kralik, División de lucha contra la Ciberdelincuencia, Consejo de Europa</p> <ul style="list-style-type: none"> <li>▶ <b>Introducción y objetivo del taller</b> <ul style="list-style-type: none"> <li>— Jamila Akaaga Ade</li> </ul> </li> <li>▶ <b>Retos de la lucha contra la xenofobia y el racismo en línea</b> <ul style="list-style-type: none"> <li>— Fernanda Teixeira Souza, Fiscal del Circuito Federal en Brasilia, Coordinadora del Grupo Asesor sobre Ciberdelincuencia del Ministerio Público Federal, Brasil</li> </ul> </li> <li>▶ <b>Conclusiones del estudio sobre buenas prácticas</b> <ul style="list-style-type: none"> <li>— Jan Kralik, División de lucha contra la Ciberdelincuencia, Consejo de Europa</li> </ul> </li> <li>▶ <b>Determinar los límites entre la incitación al odio y la libertad de expresión</b> <ul style="list-style-type: none"> <li>— Representantes de los tribunales regionales (por confirmar)</li> </ul> </li> <li>▶ <b>Conclusiones</b></li> </ul>
11:30-13:00	<p><b>Taller 13 - Reforzar los puntos de contacto permanentes 24/7</b></p> <p>Idiomas: EN/FR/ES</p> <p>Objetivo: El taller tiene por objeto seguir explorando modalidades para reforzar el funcionamiento de la Red 24/7 de puntos de contacto permanentes en el marco del Convenio de Budapest: compartir buenas prácticas para la tramitación eficaz de las solicitudes recibidas; identificar formas adicionales de aumentar la operatividad de la Red; comprender las funciones y responsabilidades de la Red en relación con las nuevas herramientas del Segundo Protocolo del Convenio de Budapest.</p> <p>Moderador: por confirmar</p> <p>Ponente: por confirmar</p> <p>Secretaría: Daniel Cuciurianu / Equipo iPROCEEDS-2</p> <ul style="list-style-type: none"> <li>▶ <b>Introducción y objetivo del taller [5 min]</b></li> </ul>

	<ul style="list-style-type: none"> <li>– Notas del moderador</li> <li>– Secretaría</li> </ul> <ul style="list-style-type: none"> <li>▶ <b>Ejemplos de cooperación internacional facilitada por la Red [35 min]</b> <ul style="list-style-type: none"> <li>– Erica O'Neil, Directora Adjunta, Sección de Delitos Informáticos y Propiedad Intelectual, Departamento de Justicia de EE.UU.</li> <li>– Nenad Bogunović, Servicio de Lucha contra la Ciberdelincuencia, Serbia</li> </ul> </li> <li>▶ <b>Aplicación a nivel nacional de las nuevas responsabilidades de los puntos de contacto 24/7 [25 min]</b> <ul style="list-style-type: none"> <li>– Antonio Segovia Arancibia, Profesor de Derecho penal transnacional, Universidad UAI, Chile</li> </ul> </li> <li>▶ <b>Promoción de la red a nivel nacional e internacional [15 min].</b></li> <li>▶ <b>Conclusiones por parte del ponente [10 min]</b></li> </ul>
11:30-13:00	<p><b>Taller 14 - Interacción entre ciberseguridad y ciberdelincuencia</b></p> <p>Idiomas: EN/FR/ES/RO</p> <p>Objetivo: Este taller explora los vínculos entre la ciberseguridad y la prevención y el control de la ciberdelincuencia. Se examinará en particular la cooperación entre las autoridades de justicia penal y los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT). El objetivo de esta sesión es determinar las formas en que podría mejorarse la cooperación entre las autoridades de justicia penal y los actores de la ciberseguridad, en particular mediante la acción conjunta contra las amenazas comunes, la protección de las infraestructuras críticas y el desarrollo de capacidades.</p> <p>Moderador: Matteo Lucchetti, Director, Cyber 4.0, Italia</p> <p>Ponente: Cecilia Popa, EU CyberNet</p> <p>Secretaría: Giorgi Jokhadze / Andrei Enachi</p> <ul style="list-style-type: none"> <li>▶ <b>Introducción y objetivo del taller [5 min]</b> <ul style="list-style-type: none"> <li>– Apuntes del moderador</li> <li>– Secretaría</li> </ul> </li> <li>▶ <b>Riesgos y amenazas comunes: comprender el panorama de la cooperación [15 min]</b> <ul style="list-style-type: none"> <li>– Perspectiva del sector privado (Aisling Kelly, Microsoft)</li> <li>– Debate</li> </ul> </li> <li>▶ <b>Protección de infraestructuras críticas: responsabilidad conjunta [30 min]</b> <ul style="list-style-type: none"> <li>– Ucrania (Anatasiia Ponarina, Servicio de Seguridad del Estado)</li> <li>– Sudáfrica: reformas en curso (Jacqueline Fick)</li> <li>– Debate</li> </ul> </li> <li>▶ <b>Desarrollo de capacidades para mejorar la seguridad y la resiliencia [20 min]</b></li> </ul>

	<ul style="list-style-type: none"> <li>— Cesar Moilne, EU CyberNet LAC4, Centro de Competencia Cibernética para América Latina y el Caribe</li> <li>▶ <b>Opciones para mejorar la cooperación entre las fuerzas del orden y los CSIRT [15 min]</b> <ul style="list-style-type: none"> <li>— Debate: ejemplos operativos y sugerencias de los países y organizaciones participantes</li> </ul> </li> <li>▶ <b>Conclusiones [5 min]</b></li> </ul>
14:00 - 14:30	<p><b>Ceremonia del Tratado</b></p> <ul style="list-style-type: none"> <li>▶ <b>Firmas, ratificaciones o adhesiones al Convenio de Budapest y sus Protocolos</b></li> </ul>
14:30-17:00	<p><b>Sesión plenaria de clausura y conclusiones</b></p> <p>Idiomas: EN/FR/ES</p> <ul style="list-style-type: none"> <li>▶ <b>Principales conclusiones de los talleres [14:30-15:15]</b> <ul style="list-style-type: none"> <li>— Resumen de los talleres (2-3 min por taller)</li> </ul> </li> <li>▶ <b>Lecciones en el décimo aniversario de la Oficina del Programa de lucha contra la Ciberdelincuencia del Consejo de Europa (C-PROC) [15:15-16:15]</b> <ul style="list-style-type: none"> <li>— Moderador: Virgil Spiridon, Jefe Adjunto de la Policía Nacional Rumana</li> <li>— Ponencias: <ul style="list-style-type: none"> <li>- Traian Hristea, Secretario de Estado, Ministerio de Asuntos Exteriores, Rumanía</li> <li>- Bjorn Berge, Secretario General Adjunto, Consejo de Europa</li> </ul> </li> <li>— Panel de responsables de proyecto sobre el impacto de C-PROC hasta la fecha, el camino por recorrer y las conclusiones de los eventos paralelos: <ul style="list-style-type: none"> <li>- Catalina Stroe, Responsable del proyecto GLACY+</li> <li>- Giorgi Jokhadze, Responsable del proyecto CyberEast</li> <li>- Nina Lichtner, Responsable del proyecto Octopus</li> <li>- Dan Cuciurianu, Responsable del proyecto iPROCEEDS-2</li> <li>- Denise Mazzolani, Responsable del proyecto CyberSouth</li> </ul> </li> </ul> </li> <li>▶ <b>Perspectivas para 2024 y conclusiones [16:15-17:00]</b> <ul style="list-style-type: none"> <li>— Panel final</li> <li>— Mensajes clave de la Conferencia Octopus</li> </ul> </li> </ul>