Conferencia Octopus 2023

13-15 de diciembre de 2023 - Bucarest, Rumanía

Programa de la Conferencia - Panorama general

Versión del 9 de octubre de 2023

MIÉRCOLES, 13 DE DICIEMBRE DE 2023			
8:30-9:30	*Café de bienvenida e inscripción*		
9:30-11:00	**Sesión plenaria de apertura** EN/FR/ES ► Apertura ► Escenario: retos		
11:00-11:30	*Pausa café*		
11:30-13:00	**Sesión plenaria** [continuación] EN/FR/ES ► Escenario: soluciones		
13:00-14:30	*Foto de grupo y pausa para comer*		
14:30-16:00	**Taller 1** EN/FR/ES/RO ► Situación mundial de la legislación sobre ciberdelincuencia	**Taller 2** EN/FR/ES/RO ► Intercambio espontáneo de información	**Taller 3** EN/FR/ES ► Detección automática de material de explotación y abuso sexual infantil
16:00-16:30	*Pausa café*		
16:30-18:00	**Taller 4** EN/FR/ES/RO ► Sinergias entre los Convenios de Budapest, Lanzarote, Estambul y el Convenio sobre la trata de seres humanos	**Taller 5** EN/FR/ES/RO ► La interacción de la ciberdelincuencia y las investigaciones financieras	**Taller 6** EN/FR/ES ► Inteligencia artificial generativa: amenazas y ventajas para la justicia penal
18:00-20:00	*Evento social*		

<table>
<tr><th colspan="4">JUEVES, 14 DE DICIEMBRE</th></tr>
<tr><td>9:30-13:00

[pausa-café 11:00-11:30]</td><td rowspan="3">Evento del proyecto:
EN

► De CyberEAST a CyberEast+</td><td>Evento del proyecto:
EN

► De iPROCEEDS-2 a CyberSEET</td><td rowspan="4">Evento del proyecto:
EN/FR/ES

► De GLACY+ a GLACY-e</td></tr>
<tr><td>13:00-14:30

Pausa para comer</td><td></td></tr>
<tr><td>14:30-18:00</td><td rowspan="3">Evento del proyecto:
EN/FR

► De CyberSouth a CyberSouth+</td></tr>
<tr><td>15:30-16:00</td><td>Pausa café</td></tr>
<tr><td>16:30-18:00</td><td>Charlas relámpago
EN/FR/ES/RO</td></tr>
<tr><th colspan="4">VIERNES 15 DE DICIEMBRE</th></tr>
<tr><td>9:30-11:00</td><td>Taller 7
EN

► Taller regional para Asia</td><td>Taller 8
EN

► Taller regional para el Pacífico</td><td>Taller 9
EN/FR

► Taller regional para África</td><td>Taller 10
EN/ES

► Taller regional para América Latina y el Caribe</td></tr>
<tr><td>11:00-11:30</td><td colspan="3">Pausa café</td></tr>
<tr><td>11:30-13:00</td><td>Taller 11
EN/FR/ES/RO

► El desarrollo de capacidades como factor de cambio: ¿qué marca la diferencia?</td><td>Taller 12
EN/FR/ES/RO

► Xenofobia y racismo en línea frente a libertad de expresión</td><td>Taller 13
EN/FR/ES

► Refuerzo de los puntos de contacto permanente 24/7</td><td>Taller 14
EN/FR/ES/RO

► La interacción entre ciberseguridad y ciberdelincuencia</td></tr>
<tr><td>13:00-14:30</td><td colspan="3">► Evento especial: La cooperación entre Rumanía y el Consejo de Europa en materia de ciberdelincuencia

► Ceremonia del Tratado

Pausa para comer</td></tr>
<tr><td>14:30-16:30</td><td colspan="3">Sesión plenaria de clausura y conclusiones
EN/FR/ES

► Principales conclusiones de los talleres
► Perspectivas para 2024
► Conclusiones de la conferencia</td></tr>
<tr><td>16:30-17:00</td><td colspan="3">Café - intercambio de contactos</td></tr>
<tr><td>18:00</td><td colspan="3">Fin de la conferencia</td></tr>
</table>

Programa detallado

MIÉRCOLES, 13 DE DICIEMBRE DE 2023	
9:30-13:00 Pausa café *11:00-11:30*	**Sesión plenaria de apertura** Idiomas: EN/FR/ES Objetivo: Esta sesión plenaria tiene por objeto preparar el terreno para las sesiones posteriores de la conferencia y los intercambios entre los participantes. Cada uno de los "retos" y "soluciones" será presentado por uno o dos ponentes y vendrá seguido de breves debates. ► **Apertura** ► **Escenario: retos y soluciones** – El *ransomware* y la Iniciativa contra el *ransomware* – OSINT y las pruebas electrónicas de crímenes de guerra: Lecciones aprendidas de la agresión rusa contra Ucrania – Ciberdelincuencia frente a libertad de expresión – Marcos jurídicos: el Convenio sobre la Ciberdelincuencia y sus Protocolos – Desarrollo de capacidades: 10 años de la Oficina del Programa contra la Ciberdelincuencia del Consejo de Europa (C-PROC)
14:30-16:00	**Taller 1 - Estado mundial de la legislación sobre ciberdelincuencia** 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 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. ► **Introducción y objetivo del taller** ► **De 2013 a 2023: Diez años de avances en la legislación sobre ciberdelincuencia y pruebas electrónicas** ► **Ejemplos de reformas recientes** ► **Retos y riesgos** ► **Conclusiones**
14:30-16:00	**Taller 2 - Intercambio espontáneo de información** Idiomas: EN/FR/ES 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": *"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 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. ► **Introducción y objetivo del taller** ► **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** ► **Mesa redonda sobre la utilización del artículo 26 del Convenio por las Partes que facilitan información: ¿cuáles son los procedimientos y las condiciones?** ► **Mesa redonda sobre la recepción de información espontánea: ¿Cómo puede utilizarse como prueba?** ► **Conclusiones**
14:30-16:00	**Taller 3 - Detección automática de material de explotación y abuso sexual infantil** Idiomas: EN/FR/ES 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. 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. ► **Introducción y objetivo del taller** ► **Avances en detección automatizada y optimización de informes** ► **Aumentar las obligaciones y superar los retos** ► **Soluciones de colaboración y aplicación de políticas** ► **Conclusiones**
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/RO 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) ► **Introducción y objetivo del taller** ► **Acción penal: necesidad de colmar las lagunas antes de buscar las sinergias** ► **Prevención y protección: una perspectiva diferente** ► **Lucha contra la ciberviolencia: posibles sinergias** ► **Conclusiones**

16:30-18:00	**Taller 5 - La interacción de la ciberdelincuencia y las investigaciones financieras** Idiomas: EN 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. ► **Introducción y objetivo del taller** ► **Flujo de dinero de la delincuencia en línea y tipologías de blanqueo de capitales** ► **Cooperación en la búsqueda, incautación y decomiso de los productos del delito en línea** ► **Nuevas herramientas y técnicas de investigación financiera en casos de ciberdelincuencia** ► **Conclusiones**
16:30-18:00	**Taller 6 - Inteligencia artificial generativa: amenazas y beneficios para la justicia penal** Idiomas: EN/FR/ES 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 *deep fake*) 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. ► **Introducción y objetivo del taller** ► **Ciberdelincuencia e IA generativa: amenazas y oportunidades** ► **Abordar las pruebas electrónicas de IA generativa: cuestiones clave, amenazas y beneficios** ► **Conclusiones**
JUEVES, 14 DE DICIEMBRE	
9:30-16:30	**Evento del proyecto: De CyberEAST a CyberEast+**

Pausa café *11:00-11:30* *Pausa para comer* *13:00-14:30*	Idiomas: EN 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. ► **Sesión inaugural** ► **Cierre del proyecto CyberEast** ► **Debate sobre el proyecto CyberEast+** ► **Reunión de responsables políticos sobre políticas de ciberdelincuencia en la región de la Asociación Oriental**
9:30-16:30 *Pausa café* *11:00-11:30* *Pausa para comer* *13:00-14:30*	**Evento del proyecto: De iPROCEEDS-2 a CyberSEE** Idiomas: EN 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. ► **Sesión inaugural** ► **Acto de clausura del proyecto iPROCEEDS-2** ► **Hacia el proyecto CyberSEE: reunión regional** ► **Aspectos esenciales del nuevo proyecto**
9:30-18:00	**Evento del proyecto: De GLACY+ a GLACY-e**

Pausa café *11:00-11:30* *Pausa para comer* *13:00-14:30* *Pausa café* *15:30-16:00*	Idiomas: EN/FR/PT/ES 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 reforza el papel de liderazgo de los 8 países centrales en el programa de desarrollo de capacidades en sus respectivas regiones. ► **Sesión inaugural** ► **Lecciones aprendidas de GLACY+** ► **¿Qué podemos esperar ahora?** ► **Adopción de la declaración de principios para los polos regionales** ► **Observaciones finales**
14:30-18:00 *Pausa café* *15:30-16:00*	**Evento del proyecto: Del CyberSouth al CyberSouth+** Idiomas: EN/FR 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. ► **Sesión inaugural** ► **Evaluación de CyberSouth: evaluación de los cinco resultados del proyecto** ► **Buenas prácticas y revisión de las modalidades de ejecución de los proyectos** ► **Prioridades de la región MENA en la cooperación sobre ciberdelincuencia 2024-2026** ► **Observaciones finales**
16:30-18:00	**Charlas relámpago** Idiomas: EN/FR/ES/RO 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. 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. Nos esforzamos por garantizar un equilibrio adecuado entre regiones, profesiones y relevancia de los temas de debate. Los ponentes que utilicen este formato tendrán un límite estricto de cinco minutos, con cuatro minutos para preguntas. A mediados de noviembre se le comunicará si su propuesta ha sido seleccionada. ► **Introducción y objetivo de la sesión** ► **Charlas relámpago** ► **Conclusiones**
VIERNES 15 DE DICIEMBRE	
9:30-11:00	**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** Idiomas: EN 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 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. ► **Introducción y objetivo del taller** ► **Salvaguardias de protección de datos en el Segundo Protocolo Adicional: ¿por qué las necesitamos?** ► **La protección de datos, piedra angular de la cooperación policial internacional** ► **Protección de datos: testimonios de países** ► **La obligación del Estado de proteger frente a los delitos y el derecho a la intimidad: ¿cómo encontrar el equilibrio adecuado?**

	► **Conclusiones**
9:30-11:00	**Taller 8 - Taller regional para el Pacífico: Desafíos en la aplicación de las leyes sobre ciberdelincuencia en las pequeñas jurisdicciones del Pacífico** Idiomas: EN 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. 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 técnicos específicos. El objetivo del taller es identificar esos retos y las posibles soluciones basadas en prácticas exitosas en la región. ► **Introducción y objetivo del taller** ► **¿En qué consiste un marco jurídico eficaz contra la ciberdelincuencia, adaptado a las necesidades de los Estados insulares del Pacífico?** ► **Hacer que las leyes sean pertinentes: ¿qué retos afrontan los Estados insulares del Pacífico cuando trabajan en su reforma legislativa?** ► **Conclusiones**
9:30-11:00	**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** Idiomas: EN/FR 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 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. ► **Introducción y objetivo del taller - ¿Por qué los países africanos deberían considerar el Convenio sobre la Ciberdelincuencia y sus Protocolos?** ► **Herramientas reforzadas para la cooperación internacional: ¿qué cambios aporta el Segundo Protocolo Adicional?** ► **Llevar la teoría a la práctica: caminos hacia una cooperación internacional más eficaz - historias de éxito y retos en la región** ► **Conclusiones**
9:30-11:00	**Taller 10 - Taller regional para América Latina y el Caribe: Cooperación interinstitucional en materia de pruebas electrónicas** Idiomas: EN/ES 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 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. ► **Introducción y objetivo del taller** ► **Unidades forenses digitales: ¿cuáles son las prácticas de investigación y las capacidades organizativas actuales y cuáles son sus limitaciones?** ► **Vías de cooperación interinstitucional** ► **Conclusiones**
11:30-13:00	**Taller 11 - El desarrollo de capacidades como factor de cambio: ¿qué marca la diferencia?** Idiomas: EN/FR/ES 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. ► **Introducción y objetivo del taller** ► **Mesa redonda: qué ha funcionado bien y qué menos** ► **Conclusiones**
11:30-13:00	**Taller 12 - Xenofobia y racismo en línea frente a la libertad de expresión** Idiomas: EN/FR/ES/RO 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 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. ► **Introducción y objetivo del taller** ► **Conclusiones del estudio sobre buenas prácticas** ► **Desafíos de la lucha contra la xenofobia y el racismo en línea** ► **Determinar los límites entre la incitación al odio y la libertad de expresión** ► **Conclusiones**
11:30-13:00	**Taller 13 - Reforzar los puntos de contacto permanentes 24/7** Idiomas: EN/FR/ES 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. ► **Introducción y objetivo del taller**

	► **Ejemplos de cooperación internacional facilitada por la Red** ► **Aplicación nacional de las nuevas responsabilidades de los puntos de contacto permanentes 24/7** ► **Promoción de la red a escala nacional e internacional** ► **Conclusiones**
11:30-13:00	**Taller 14 - Interacción entre ciberseguridad y ciberdelincuencia** Idiomas: EN/FR/ES/RO 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. ► **Introducción y objetivo del taller** ► **Riesgos y amenazas comunes: comprender el panorama de la cooperación** ► **Protección de infraestructuras críticas: responsabilidad conjunta** ► **Desarrollo de capacidades para mejorar la seguridad y la resistencia** ► **Opciones para mejorar la cooperación entre las fuerzas del orden y los CSIRT** ► **Conclusiones**
13:00 - 14:00	**Evento especial: La cooperación entre Rumanía y el Consejo de Europa en materia de ciberdelincuencia** Idiomas: EN/RO Objetivo: Este acto especial tiene por objeto reflexionar sobre la larga asociación entre Rumanía y el Consejo de Europa para fomentar la cooperación mundial en materia de lucha contra la ciberdelincuencia. Hace treinta años, en octubre de 1993, Rumanía ingresó en el Consejo de Europa. Durante unos veinte años, Rumanía ha sido un socio fuerte del Consejo de Europa en asuntos relacionados con la ciberdelincuencia, como Parte en el Convenio de Budapest (desde 2004), aportando expertos y contribuyendo y presidiendo el Comité del Convenio sobre la Ciberdelincuencia (T-CY). Hace diez años, en 2013, esta cooperación se elevó a otro nivel: en octubre de 2013, el Gobierno de Rumanía y el Consejo de Europa celebraron un memorando de entendimiento sobre el establecimiento de la Oficina del Programa contra la Ciberdelincuencia del Consejo de Europa (C-PROC) en Bucarest. El C-PROC ha prestado apoyo a más de 100 países a través de más de 2000 actividades de desarrollo de capacidades desde que empezó a funcionar en abril de 2014.

14:00 - 14:30	**Ceremonia del Tratado** ► **Firmas, ratificaciones o adhesiones al Convenio de Budapest y sus Protocolos**
14:30-17:00	**Sesión plenaria de clausura y conclusiones** Idiomas: EN/FR/ES ► **Principales conclusiones de los talleres** ► **Perspectivas para 2024** ► **Conclusiones**