

XXXIV

TECMUN Jr.

Organización Internacional de
Policía Criminal

XXXIV TECMUN Jr.
Horario de sesiones

Miércoles 11 de noviembre

Registro	8:00 – 9:00 h.
Ceremonia de Inauguración	9:00 – 10:00 h.
Receso	10:00 – 10:30 h.
Primera Sesión	10:30 – 12:30 h.
Receso	12:30 – 13:00 h.
Segunda Sesión	13:00 – 15:00 h.
Comida	15:00 – 16:00 h.
Tercera Sesión	16:00 – 18:00 h.

Jueves 12 de noviembre

Conferencia Magistral	8:30 – 9:30 h
Receso	9:30 – 10:00 h..
Cuarta Sesión	10:00 – 12:30 h.
Receso	12:30 – 13:00 h.
Quinta Sesión	13:00 – 15:00 h.
Comida	15:00 – 16:00 h.
Sexta Sesión	16:00 – 18:00 h.

Viernes 13 de noviembre

Séptima Sesión	8:00 – 9:30 h
Receso	9:30 – 10:00 h
Octava Sesión	10:00 – 12:00 h
Receso	12:00 – 12:30 h
Novena Sesión	12:30 – 14:40 h
Comida	14:40 – 16:00 h
Ceremonia de Clausura	16:00 – 18:00 h

XXXIV TECMUN Jr.
Agenda General

Secretario General: David Trujillo Loza

COORDINACIÓN GENERAL

Subsecretaria de Coordinación General: Alexa Esmeralda Rivera Jiménez
Supervisoras de Coordinación General para Secretario Co: Ana Sofía Parra Meza y
Narda Regina Rentería Martínez

General Assembly

Subsecretario General: Diego Alejandro Salazar Náfate
Supervisora de Coordinación: María Fernanda Granados Martínez

Plenary Session for the General Assembly

President: Andrea Teresa Romero Bravo

Topic A) Strategies to address the transnational financing networks and arms smuggling mechanisms sustaining the operations of Al-Shabaab in the Horn of Africa.

Topic B) Addressing Cross-Border protection measures and legal frameworks for climate displaced populations especially in the Bay of Bengal and South Asia.

First Committee on Disarmament and International Security

President: Marco Omar Montemurro Spano

Topic A) Measures to restore military transparency and reduce the operational preparation of nuclear arsenals between the Russian Federation and the United States of America.

Topic B) Strategies to confront the illicit trafficking of commercial explosives and military grade weaponry within South America, with emphasis on regional cooperation, stockpile security and the logistical capabilities of transnational criminal networks.

United Nations Office on Drugs and Crime

President: Jeshua Isaí Jordan López

Topic A) Measures to address human trafficking for forced criminality in scam compounds across the Mekong sub-region, with emphasis on transnational cooperation and the protection of trafficking victims.

Topic B) Strategies to dismantle the laundering of drug trafficking profits enabled by corruption in the Sahel region, with emphasis on the cocaine route between South America and Europe.

Comisión del Derecho Internacional
Presidenta: Alexa Ortiz Van Der Graaff

Tópico A) Estrategias para abordar la difusión transfronteriza de contenido sintético generado por inteligencia artificial, que compromete la integridad electoral y la estabilidad diplomática internacional.

Tópico B) Medidas para fortalecer la protección jurídica internacional de personas desplazadas por desastres naturales y crisis climáticas en regiones vulnerables del Sudeste Asiático y el Pacífico.

Haut Commissariat des Nations Unies Pour les Réfugiés
President: Mauricio Antillón Mota

Sujet A) Actions visant à renforcer l'accès aux services essentiels dans les camps de réfugiés rohingyas situés en République Populaire du Bangladesh, en mettant particulièrement l'accent sur les défis climatiques.

Sujet B) Stratégies pour renforcer l'assistance humanitaire destinée aux personnes déplacées internes en République du Soudan, dans le contexte du conflit armé entre les Forces armées soudanaises et les Forces de soutien rapide.

Fondo de las Naciones Unidas para el Desarrollo de la Infancia
Presidenta: Andrea Hernández Caballero

Tópico A) Estrategias para abordar la desinformación en línea y la amplificación algorítmica de contenido dañino que socava el acceso de los niños a información confiable en entornos digitales en Latinoamérica y el Caribe.

Tópico B) Estrategias para garantizar el acceso humanitario infantil en la Franja de Gaza durante los conflictos armados.

International Maritime Organization
President: Isabella Buendía Ramírez

Topic A) Mechanisms to strengthen international regulatory frameworks addressing the deployment of autonomous and AI-assisted maritime systems and their implications for maritime safety, accountability and international coordination.

Topic B) Measures to strengthen occupational safety and environmental sustainability in international ship recycling practices.

Special Political and Decolonization Committee
President: Ariadna Joseline Pacheco Spirina

Topic A) Measures to strengthen international cooperation for environmental remediation and humanitarian assistance in territories affected by the legacy of nuclear testing in the Pacific and Central Asia.

Topic B) Measures to address the legal and political implications of climate-induced territorial loss affecting Low-Lying Non-Self-Governing Territories.

Sixth Legal Committee

President: Diane González Martínez

Topic A) Measures to strengthen international cooperation for environmental remediation and humanitarian assistance in territories affected by the legacy of nuclear testing in the Pacific and Central Asia.

Topic B) Measures to address the legal and political implications of climate-induced territorial loss affecting Low-Lying Non-Self-Governing Territories.

CONSEJO ECONÓMICO Y SOCIAL

Subsecretario General: María Fernanda Domínguez Heredia

Supervisora de Coordinación General: Aitana Rodríguez Hernández

Organización Internacional de la Policía Criminal

Presidenta: Andrea Guadalupe Zaldívar Escamilla

Tópico A) Acciones para fortalecer la cooperación policial internacional en la identificación y desarticulación de organizaciones criminales transnacionales responsables de ataques de ransomware contra infraestructuras críticas en Europa, con énfasis en el Reino Unido de Gran Bretaña e Irlanda del norte .

Tópico B) Mecanismos para fortalecer la cooperación policial internacional en la identificación y desarticulación de redes criminales transnacionales dedicadas al tráfico ilícito de migrantes a través de rutas terrestres irregulares entre América Latina y América del Norte.

United Nations Interregional Crime and Justice Research Institute

President: Sara Vázquez Zamora

Topic A) Actions for enhancing multilateral efluencia to address human trafficking and cross border fraud and cybercrime with emphasis in the Republic of the Union of Myanmar.

Topic B) Measures to address the use of cryptocurrencies in the laundering of criminal proceeds conductas by drug cartels in Latin America with an emphasis in the United Mexican States

Comité de los Derechos del Niño

Presidenta: Camila Aimee Castañeda Espinoza

Tópico A) Medidas internacionales para prevenir el reclutamiento forzado de menores por grupos armados en la República de Haití frente al aumento de violencia de pandillas y crisis institucional.

Tópico B) Estrategias regionales para proteger a menores migrantes no acompañados en la frontera entre los Estados Unidos Mexicanos y los Estados Unidos de América frente al tráfico humano y la violencia del crimen organizado.

Entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de las Mujeres

Presidenta: Danna Valeria Márquez Mejía

Tópico A) Estrategias para fomentar el empoderamiento económico y la inclusión laboral de las mujeres migrantes y refugiadas por motivos de violencia sistemática en América Latina.

Tópico B) Medidas para garantizar la igualdad económica y el derecho a la propiedad de tierras de las mujeres en la reconstrucción de zonas post-conflicto en África, con énfasis en la República Democrática del Congo.

United Nations Institute for Disarmament Research

President: Emiliano Sánchez Dorantes

Topic A) Security risks associated with the transfer, proliferation, and regulation of military artificial intelligence systems in the Indo-Pacific Region.

Topic B) Counterspace capabilities, including cyberattacks and jamming against satellite networks, and their impact on communications, navigation, and strategic systems in Eastern Europe.

Consejo de Derechos Humanos

Presidenta: Andrea Meza Hernández

Tópico A) Medidas para garantizar la protección de periodistas y el acceso libre a la información en situaciones de conflicto armado, con énfasis en la región de Oriente Medio.

Tópico B) Acciones para garantizar la protección de las infancias y adolescencias frente al reclutamiento forzado y las violaciones a los derechos humanos en la región del Sahel ante la expansión de grupos extremistas.

Comité de Expertos de las Naciones Unidas sobre la Gestión Global de la Información Geospacial

Presidenta: Regina Hernández Caballero

Tópico A) Reducción de la brecha tecnológica geoespacial en los Estados Insulares del Pacífico.

Tópico B) Fortalecimiento de la gobernanza ética de datos en sistemas de prevención y respuesta ante desastres naturales en Estados insulares del Caribe.

Food and Agriculture Organization

President: Mariana Jiménez Zamudio

Topic A) Strategies to address bioprospecting and genetic patenting inciting biopiracy that undermines traditional agricultural knowledge and smallholder seed sovereignty in Southern Asia.

Topic B) Confronting the causes of child labour and exploitative practices within West African cocoa supply chains with emphasis in the Republic of Côte d'Ivoire.

Historical Commission on Crime Prevention and Criminal Justice

President: Sofía López Rodríguez

Topic A) Mechanisms to counter the transnational growth of the Primeiro Comando da Capital while addressing the systemic prison crisis in the Federative Republic of Brazil (1993-2016).

Topic B) Mechanisms to combat the transnational trafficking of women and sexual exploitation networks operated by the Russian Mafia (Bratva) in Post-Soviet states (1991-2005).

AGENCIAS ESPECIALIZADAS Y ORGANISMOS REGIONALES

Subsecretario General: Miguel Ander Hernández Aguilar

Supervisora de Coordinación General: Romina Valle Velázquez

Organización del Tratado del Atlántico Norte

Presidente: Emilio Gutierrez

Tópico A) Medidas para enfrentar las crecientes tensiones internacionales, así como la amenaza de un posible conflicto bélico en la región del Medio Oriente, con énfasis en el crecimiento del programa nuclear de la República Islámica de Irán y sus posibles implicaciones para la seguridad global

Tópico B) Medidas para responder al incremento de las tensiones en Europa Oriental, así como a sus posibles repercusiones en la seguridad y estabilidad de la República de Polonia y la República de Lituania, con especial énfasis en la militarización del enclave de Kaliningrado por parte de la Federación de Rusia.

Organización Mundial de la Salud

Presidente: Javier Gil Rodríguez

Tópico A) Acciones para fortalecer la vigilancia, prescripción responsable y acceso regulado a fármacos antimicrobianos en los centros hospitalarios de la Unión Europea, con énfasis en la resistencia bacteriana a los antibióticos, el uso inadecuado de fármacos y las fallas estructurales asociadas.

Tópico B) Medidas para apoyar la recuperación de la infraestructura sanitaria y reforzar la protección del personal de salud en zonas de conflicto armado, con un enfoque crítico en la desnutrición aguda infantil en la República de Sudán.

Consejo de Seguridad

Presidente: Joaquín Pérez y Rodríguez

Tópico A) Estrategias para contrarrestar el conflicto armado en Sudán, haciendo énfasis en el genocidio y los crímenes de guerra cometidos en Darfur y las amenazas que representa para la estabilidad del África Oriental.

Tópico B) Medidas para frenar los ataques militares de los Estados Unidos de América y el Estado de Israel contra el territorio de la República Islámica de Irán, poniendo especial atención en el riesgo de escalada a un conflicto armado generalizado en Medio Oriente.

Fondo Monetario Internacional

Presidente: Daniel Emiliano Morales Ramírez

Tópico A) Estrategias para mitigar el impacto económico global causado por el conflicto en el estrecho de Ormuz tras las tensiones en Oriente Medio,

Tópico B) Mecanismos para enfrentar las repercusiones de las políticas arancelarias de Estados Unidos de América en las economías comerciales asociadas.

Organización Internacional de Energía Atómica

Presidenta: Natalia García Olmos

Tópico A) Reforzamiento de los mecanismos internacionales de verificación y no proliferación en relación con el programa nuclear de la República Islámica de Irán.

Tópico B) Fortalecimiento de las medidas y mecanismos internacionales para mitigar los riesgos ambientales, garantizar la seguridad nuclear y reforzar la protección tecnológica de las instalaciones nucleares en Ucrania.

Counter-Terrorism Committee

President: Santiago Castañeda Castro

Topic A) Measures to address the humanitarian and security crisis in Cabo Delgado, with emphasis on the violent campaign of Ahlu Sunnah Wa-Jamo (ASWJ) and extremist recruitment prevention.

Topic B) Mechanisms to eradicate the security vacuum in Somalia as a consequence of the transition from ATMIS, in the context of the operational resurgence of Al-Shabaab.

Organization for the Prohibition of Chemical Weapons

President: Mauricio Alejandro Salazar López

Topic A) Measures to address the threat of undeclared chemical weapons stockpiles and the proliferation of dual-use chemical substances in the Syrian Arab Republic after the fall of the Assad government.

Topic B) Measures to strengthen international emergency response and assistance mechanisms in relation to alleged chemical weapons incidents in the Republic of the Sudan.

Organización de los Estados Americanos

Presidenta: Andrea Vázquez Zamora

Tópico A) Mecanismos para la supervisión del uso de vehículos aéreos no tripulados en zonas con altas tasas de crimen organizado en Latinoamérica con énfasis en la República de Haití.

Tópico B) Medidas para la regulación del uso de Inteligencia Artificial (IA) enfocado en la manipulación de procesos electorales en Latinoamérica con énfasis en la República Federativa de Brasil.

International Criminal Court

President: Marco Bourget Alvarez

Case A) The Prosecutor v Rodrigo Roa Duterte for alleged crimes against humanity in the Republic of the Philippines.

Case B) 2017 Clearance Operations in the Republic of the Union of Myanmar, with emphasis on the application for a warrant of arrest against Min Aung Hlaing, Commander-in-Chief of the Myanmar Defence Services at the time of the operations, for alleged crimes against humanity.

“The world offers you comfort. But you were not made for comfort, you were made for greatness”

- Joseph Ratzinger

Querido lector,

Hace cinco años comencé este proyecto sin saber en lo que se convertiría. Llegué a TECMUN pensando en que solo era un evento académico; tres días después, esa percepción había cambiado por completo, y ocho modelos más tarde me hicieron ver que el sentido que le veía no se acerca a lo que hoy veo que es y a lo que en realidad es. Al igual que muchos, inicié con el pensamiento de que TECMUN era un modelo de agentes que buscan cambiar y resolver problemáticas que se desarrollan en nuestro mundo. Sin embargo, la diplomacia y la comunicación son apenas un ínfimo en lo que se ocupa y en lo que te da este modelo para salir y cambiar de verdad.

El problema en nuestros días no radica en el poco conocimiento que tenemos de ellos, sino en la poca voluntad de las personas que saben y no actúan. El miedo humano por intentar aquello que sabemos que incomoda supera el deseo que tenemos de realizarlo y, en un intento por cambiar esa mentalidad, entró TECMUN a moldear y cambiar a aquellos que dudan en actuar por temor a trascender y afrontar realidades. Los agentes de cambio que pensaban que se formaban con formalidad, en realidad se estaban formando con adversidades y tropiezos, con gente dispuesta a abrazar lo difícil, gente dispuesta a vaciarse de aquello en lo que abunda y llenarse de aquello en lo que carece.

Entendiendo esto, te invito a ti, delegado, asesor y secretariado, a vaciarte de lo sencillo y llenarte de lo complejo. Te invito a dejar el conformismo y optar por la trascendencia durante tres días. Porque si anhelas el cambio tanto como yo, no hay mejor iniciativa que empezar por uno mismo. De esta forma, muchos Modelos de Naciones Unidas te pueden enseñar comunicación y diplomacia, pero pocos buscan una transición como lo hace TECMUN. Ama el cambio y trabaja con amor por ello, porque solo así ganará la grandeza sobre el conformismo.

David Trujillo Loza
Secretario General para el
XXXIV TECMUN Jr.

"Every great dream begins with a dreamer. Always remember, you have within you the strength, the patience, and the passion to reach for the stars to change the world."

- Harriet Tubman.

Querido soñador:

Siempre he pensado que cada uno de nosotros llegó a este universo con un mismo propósito: cambiar el mundo. Estoy segura de que debes tener miles de sueños y metas que anhelas cumplir en un futuro; yo vengo a pedirte que nunca te rindas. Hoy en día el mundo está lleno de noticias sobre cómo la humanidad está siendo gobernada por el poder y la ambición, y yo sé que eso puede llegar a desanimar e incluso desviar nuestros propósitos, pero, por favor, nunca dejes que los retrocesos sean una razón para dejar de intentar; al contrario, que se conviertan en el porqué de tus pasos hacia el cambio.

Hace algunos años mis sueños seguían borrosos, no era muy consciente de mis alrededores y tampoco tenía herramientas para comprenderlo del todo, pero el día que entré a Tecmun fue como si hubiera visto con lentes por primera vez. Tecmun me ha enseñado que el primer paso para el cambio es el volvernos conscientes; con esto me refiero a no hundirnos en la ignorancia y empezar a ver el mundo desde cualquier perspectiva posible, empezar a investigar sobre todo lo bueno y lo malo y formar un criterio de ello.

Si me preguntaran cómo describiría a Tecmun, diría que es un espacio para descubrir; dentro de este eres capaz de pensar más allá e intentar buscar soluciones para problemáticas que gente real vive día con día. No solo analizas, te vuelves un poquito más empático con cada propuesta que realizas. Tecmun es un lugar para soñadores; está basado en un modelo de naciones que surgió para evitar futuros conflictos, pero yo considero que Tecmun es aún más que eso.

Para mí, Tecmun se ha convertido en los tres días que espero con ansias cada semestre. El motivo eres tú; trabajar durante todo el semestre para llegar al modelo y poder verte list@ para adentrarte en un mundo lleno de ideas y soluciones, de creatividad y pasión, hace que todo mi esfuerzo valga la pena. Mi propósito es que te enamores de Tecmun al igual que yo lo hice; busco transmitirte mi pasión y hacerte ver este proyecto como lo hago yo, como el lugar en el que los sueños se hacen realidad.

Como jóvenes debemos luchar por un mundo mejor; somos el futuro de nuestra sociedad y debemos actuar como tal. Nuestro deber como estudiantes es querer ser mejor cada día, pero no por los demás, sino porque esa alma soñadora que tenemos en nuestros corazones nos vea triunfar y ser la persona más feliz del mundo, siempre apegada a nuestros valores, siempre perseverante, siempre libre. Luchemos por tener un mundo mejor, pensemos en grande y no dejemos que nunca nadie nos quite lo más importante que poseemos, nuestra humanidad. Gracias por estar aquí, por hacer el cambio, por no rendirte.

Alexa Esmeralda Rivera Jiménez
Subsecretaría de Coordinación para el
XXXIV TECMUN Jr.

"Just because you have rights today does not mean you will have rights tomorrow"

- Sheryl Lee Ralph

Queridos visionarios:

Seamos honestos: las problemáticas globales que están frente a nosotros no son sólo simulaciones; son un reflejo de la fricción exacta que define nuestro presente. Deben considerarse afortunados de poder tener una voz con la cual expresar sus ideas, opiniones y descontentos. Sean mentes revolucionarias y recuerden que el simple hecho de cuestionarse el mundo en el que viven es un acto puro de rebeldía. Vivimos en un mundo donde cada vez nos preocupamos menos por el de al lado, y ustedes son quienes deben recordar que, al estar aquí, participando en este modelo, han adquirido un compromiso con la transformación social.

Desde que empecé mi camino en TECMUN, nunca me hubiera imaginado ser la persona que soy ahora. Ser parte de este modelo te lleva a lugares increíbles, pero lo más importante son las cosas que te llevas de él. El hecho de que la mayoría de nuestra sociedad no se preocupe por lo que pasa al otro lado del mundo, mientras que ustedes tienen la oportunidad no solo de conocer estas problemáticas, sino también de buscarles solución, habla muy bien de lo valientes que pueden llegar a ser. Una vida puede cambiar si tan solo se decide actuar. Por eso, el consejo más valioso que puedo darles es que no tengan miedo de expresarse ni de alzar la voz, porque no saben el poder que tienen. Luchen y hablen por las personas que hoy no pueden hacerlo o a quienes su voz les fue arrebatada. Puede que sean pequeños, pero no dejen que eso los defina y, mucho menos, que se convierta en un limitante para soñar en grande.

Les deseo mucha suerte en este modelo y espero que salgan de cada sesión satisfechos y felices de sí mismos. No vean desde el privilegio, atrévanse a más y recuerden que el verdadero cambio empieza aquí y empieza en ustedes.

María Fernanda Domínguez Heredia
Subsecretaría para el Consejo Económico y Social para el
XXXIV TECMUN Jr.

“Lograrlo con miedo es lograrlo dos veces”

Querido delegado,

En la actualidad nos enfrentamos a un mundo lleno de desafíos, desigualdades e inseguridades, que en ocasiones, pueden parecer demasiado grandes para nosotros, sin embargo el cambio comienza cuando decides alzar la voz, porque ningún cambio se hace desde la comodidad.

A lo largo de mi experiencia en TECMUN he aprendido que el modelo va mucho más allá de debatir y representar un país, es un espacio que nos reta a entender nuestra realidad, escuchar perspectivas distintas pero sobretodo nos motiva a hacer un cambio, cada debate y propuesta representan una oportunidad para solucionar los problemas a los que nos enfrentamos.

Cuestiona y sostén aquello en lo que crees. Nunca tengas miedo de defender lo que consideras justo. Cada decisión, palabra y acción pueden marcar una diferencia, por más pequeña que sea. Confía en sus ideas, escuchen a quienes piensan diferente y nunca pierdas la curiosidad por comprender los problemas que te rodean, eso es lo que marcará el cambio.

Espero que al terminar esta experiencia no solamente te lleves nuevos conocimientos, sino también la certeza de que tu voz sí importa y de que, desde cualquier espacio en él que te encuentres, tienes la capacidad de contribuir a construir un mundo mejor. Espero tengas el mejor modelo. ¡Suerte!

Andrea Guadalupe Zaldívar Escamilla
Presidenta de la Organización Internacional de Policía Criminal para el
XXXIV TECMUN Jr.

Antecedentes

La Organización internacional de Policía Criminal (INTERPOL) fue creada como respuesta a la necesidad de fortalecer la cooperación internacional frente al aumento del crimen transnacional durante el siglo XX. Fundada en 1923 en Viena, Austria, con el propósito de facilitar la comunicación y la colaboración entre las autoridades policiales de distintos países. Actualmente cuenta con 196 países miembros, cada uno de los cuales posee una Oficina Central Nacional (OCN) de INTERPOL, con la finalidad de tener contacto entre la secretaría general y otras OCN; siendo Lyon, Francia su sede principal. Durante los años, INTERPOL ha evolucionado para adaptarse a las nuevas amenazas derivadas de la globalización y los avances tecnológicos, centrándose en el combate de delitos como extremismo, narcotráfico, trata de personas, lavado de activos, tráfico de armas y cibercrimen. Coordina los sistemas de notificación y bases de datos internacionales mediante el sistema I-24/7 permitiendo el intercambio de información criminal, la localización de fugitivos y el fortalecimiento de la seguridad global.

Facultades

La Organización Internacional de Policía Criminal con el objetivo de desarrollar estrategias internacionales en función de crear soluciones para las amenazas actuales, tiene la capacidad de:

- Gestionar mecanismos de cooperación internacional entre los Estados miembros para fortalecer el combate y prevención del crimen organizado transnacional;
- Facilitar el intercambio de información, inteligencia criminal y evidencias mediante el sistema de comunicación I 24/7 y bases de datos especializadas de la organización;

- Emitir y coordinar notificaciones internacionales para apoyar la localización, identificación y detención provisional de individuos buscados por delitos graves, en petición de un país miembro bajo sus leyes;
- Organizar operativos conjuntos y brindar soporte logístico para investigaciones internacionales relacionadas con delitos y extremismos violentos;
- Proporcionar asistencia técnica, capacitación especializada y apoyo operativo a las autoridades policiales nacionales;
- Diseñar estrategias de prevención, respuesta y cooperación internacional frente a crisis de seguridad y amenazas del crimen organizado.

Tópico A

Acciones para fortalecer la cooperación policial internacional en la identificación y desarticulación de organizaciones criminales transnacionales responsables de ataques de ransomware contra infraestructuras críticas en Europa, con énfasis en el Reino Unido de Gran Bretaña e Irlanda del Norte

Introducción

Los ataques provocados por ransomware se han consolidado como una de las principales amenazas del crimen organizado transnacional durante el siglo XXI. Este tipo de ciberdelincuencia consiste en el acceso ilícito a sistemas informáticos con el objetivo de bloquear, cifrar o restringir información crítica; posteriormente, se exige una petición de rescate financiero a cambio de restablecer el acceso a la información afectada (IBM, 2024). Paralelamente, el crecimiento de la digitalización en sectores estratégicos ha aumentado de manera acelerada, provocando una mayor dependencia de gobiernos, empresas y organismos públicos respecto a los sistemas informáticos utilizados para sus operaciones diarias. Esta vulnerabilidad estructural no solo compromete la continuidad operativa de las instituciones afectadas, sino que también pone en riesgo la seguridad nacional y la estabilidad económica global al paralizar servicios esenciales.

El efecto provocado por el ransomware supera las pérdidas económicas asociadas a las transacciones de rescate. La interrupción de servicios hospitalarios, sistemas energéticos, redes de transporte o plataformas gubernamentales, constituyen un impacto que ha afectado directamente la vida de millones de personas. Debido a la importancia que tienen estos sectores, los grupos criminales los seleccionan como objetivos prioritarios con el fin de generar mayor presión sobre las víctimas y aumentar sus probabilidades de obtener recursos de sus rescates. Esta situación ha generado preocupación en diversos Estados estén comenzando a considerar el ransomware como una amenaza para la seguridad nacional y no únicamente una modalidad de la delincuencia informática.

La preocupación internacional frente a esta problemática ha aumentado debido a que los grupos responsables distribuyen sus operaciones entre distintas *jurisdicciones*¹, lo que dificulta su identificación, persecución y desarticulación por parte de las autoridades

¹ **Jurisdicciones:** Territorios o sistemas legales en los que un Estado o autoridad tiene competencia para investigar, juzgar y sancionar conductas delictivas. (Naciones Unidas, 2004).

nacionales. En la mayoría de los casos, los responsables pueden encontrarse en un país distinto al de la víctima y hacer uso de servicios ubicados en diversas ubicaciones con la finalidad de recibir transacciones monetarias de rescate mediante sistemas financieros difíciles de rastrear. Esta situación limita la capacidad de respuesta individual de los Estados y evidencia la necesidad de fortalecer los mecanismos de cooperación policial internacional. Ante este escenario, organismos como La Organización Internacional de Policía Criminal (INTERPOL) desempeñan un papel fundamental en la coordinación de investigaciones y en el fortalecimiento del intercambio de inteligencia entre las autoridades policiales.

Especialmente en Europa, los ataques de ransomware han afectado de manera constante a infraestructuras críticas vinculadas a los sectores de salud, energía, telecomunicaciones y administración pública. Particularmente, el Reino Unido de Gran Bretaña e Irlanda del Norte se ha convertido en uno de los países más afectados por esta problemática debido a diversos incidentes que han comprometido el funcionamiento de servicios esenciales. La magnitud que han alcanzado este tipo de ataques ha impulsado a los gobiernos y a las organizaciones internacionales a reforzar sus capacidades de ciberseguridad y cooperación internacional. Esto ha derivado a la identificación y desarticulación de organizaciones criminales dedicadas a los ataques de ransomware sean consideradas actualmente una prioridad dentro de la agenda de seguridad internacional.

Antecedentes

Durante las últimas décadas, Europa se ha consolidado como una de las regiones más afectadas por los ataques de ransomware debido a su elevado nivel de digitalización y a la relevancia estratégica de sus infraestructuras críticas. De acuerdo con la Agencia de la Unión Europea para la Ciberseguridad (ENISA), las infraestructuras críticas europeas siguen siendo uno de los principales objetivos de las organizaciones criminales enfocadas al ransomware. (ENISA, 2020). Regiones como el Reino Unido de Gran Bretaña e Irlanda del Norte,

República Federal de Alemania, República Francesa, República Italiana y el Reino de España son algunos de los países más afectados. Organismos gubernamentales, redes de telecomunicaciones y hospitales comenzaron a depender cada vez más de plataformas digitales para almacenar información, gestionar operaciones y garantizar la continuidad de sus actividades. Mientras aumentaba la dependencia de estos sistemas, también creció el interés de grupos criminales por explotar sus debilidades. Este tipo de ciberdelincuencia comenzó a finales de la década de 1980 y principios de los años 2000. Uno de sus primeros antecedentes globales data de la Conferencia Mundial sobre el Sida de la Organización Mundial de la Salud (OMS) en 1989 se basó en la distribución de disquetes que contenían el virus *Síndrome de Inmunodeficiencia Adquirida (SIDA)*², el cual bloqueaba el acceso a determinados archivos y exigía una transacción de activos por correo postal dirigido a un apartado internacional con gestión remota. Posteriormente, durante los años 2000 y 2010, surgieron los denominados bloqueadores, cuya función consistía en impedir el uso del sistema operativo mediante el bloqueo de la pantalla, mientras que los pagos eran exigidos a través de Servicio de Mensajes Cortos (SMS) o monederos electrónicos.

Con la llegada de las criptomonedas, los ciberdelincuentes adoptaron nuevas modalidades de extorsión basadas en el cifrado masivo de archivos para dificultar el rastreo financiero. Uno de los casos más significativos fue WannaCry, un programa malicioso de tipo ransomware con comportamiento de gusano informático que paralizó a más de 200,000 computadoras en 150 países durante mayo de 2017. Este *malware*³ cifraba archivos y exigía rescates en bitcoins para su liberación, siendo especialmente visible su impacto en Reino Unido de Gran Bretaña e Irlanda del Norte, donde el National Health Service (NHS) sufrió interrupciones en hospitales y centros médicos que afectaron a la atención sanitaria de miles

² **Síndrome de Inmunodeficiencia Adquirida (SIDA):** Etapa avanzada de la infección por el Virus de la Inmunodeficiencia Humana (VIH), que debilita gravemente el sistema inmunológico. (Organización Mundial de la Salud, 2024).

³ **Malware:** Software malicioso que daña o compromete sistemas informáticos. (Oxford Dictionary of Computing, 2023)

de pacientes. WannaCry es considerado uno de los ejemplos más representativos de la vulnerabilidad de las infraestructuras críticas europeas ante los ataques de ransomware.

Desde el 2017, el modelo de negocio *Ransomware como Servicio (RaaS)*⁴ se ha consolidado firmemente dentro del entorno delictivo digital. Actualmente, grupos de sabotadores informáticos como Sodinokibi o Akira no solo cifran equipos, sino que también extraen información confidencial y amenazan con publicar en la *web oscura*⁵, si no se realiza una transacción rescate. La evolución constante de las organizaciones criminales, junto con el carácter transnacional de sus operaciones, ha evidenciado las limitaciones de las respuestas nacionales frente a amenazas que rebasan las fronteras estatales. Esto ha generado que los Estados europeos fortalezcan sus mecanismos de cooperación policial e intercambio de información para poder frenar de manera conjunta, los desafíos ocasionados por el ransomware.

La evolución del ransomware y nuevos desafíos para la seguridad europea

Actualmente, las organizaciones criminales responsables de los ataques de ransomware han incrementado significativamente su capacidad operativa mediante la incorporación de tecnologías emergentes que les han permitido ejecutar campañas más complejas y difíciles de detectar. Entre estas herramientas destaca el uso de inteligencia artificial para automatizar procesos de reconocimiento de vulnerabilidades, enviar correos electrónicos de suplantación de identidad personalizados y desarrollar códigos maliciosos con capacidad de adaptarse a distintos entornos digitales. Esta evolución tecnológica ha reducido los recursos necesarios para ejecutar ataques complejos, permitiendo que grupos criminales de menor tamaño accedan a capacidades que, en años anteriores, se encontraban limitadas a organizaciones más

⁴ **Ransomware como Servicio (Raas):** Modelo criminal que permite a terceros utilizar ransomware a cambio de una comisión. (ENISA, 2020)

⁵ **Web oscura:** Parte de Internet accesible únicamente mediante software especializado. (RAE, 2024)

avanzadas. Como resultado, la amenaza del ransomware se ha expandido a un ritmo superior al de las capacidades de respuesta de las distintas instituciones públicas y privadas.

Uno de los desafíos más importantes ha radicado en la dependencia constante de proveedores tecnológicos externos. En los últimos años, distintas organizaciones criminales han aprovechado vulnerabilidades presentes en empresas encargadas de proporcionar servicios digitales a diversos clientes para extender el alcance de sus ataques. Como resultado, una sola intrusión puede afectar simultáneamente a cientos de instituciones conectadas a la misma red de servicios. Esta situación ha provocado interrupciones en aeropuertos, sistemas de transporte y otras infraestructuras estratégicas, demostrando que el elemento más débil dentro de una cadena tecnológica puede comprometer la seguridad de sectores completos. El Reino Unido de Gran Bretaña e Irlanda del Norte continúa figurando entre los países europeos más afectados por los ataques de ransomware debido al nivel elevado de digitalización de sus servicios públicos y privados, por lo que se ha impulsado el fortalecimiento de sus estrategias nacionales de ciberseguridad y cooperación internacional.

Ante este panorama, la cooperación internacional en materia de ciberseguridad ha adquirido una relevancia sin precedentes. Organismos como la Agencia de Ciberseguridad de la Unión Europea (ENISA) han impulsado el fortalecimiento de marcos normativos con la finalidad de mejorar la protección de infraestructuras críticas frente a las amenazas digitales. Entre estas iniciativas destaca la Directiva NIS2, instrumento normativo de la Unión Europea cuyo objetivo es establecer estándares comunes de ciberseguridad para los sectores esenciales y reforzar los mecanismos de prevención, respuesta y recuperación frente a incidentes informáticos. Sin embargo, las diferencias en capacidades tecnológicas, legislaciones nacionales y niveles de preparación institucional han evidenciado importantes desafíos para la construcción de una respuesta coordinada frente a organizaciones criminales transnacionales que continúan operando en el entorno digital.

Limitaciones jurídicas para la persecución de organizaciones criminales transnacionales dedicadas al ransomware

La persecución penal de las organizaciones criminales dedicadas al ransomware enfrenta importantes limitantes relacionadas con la soberanía de los Estados y la fragmentación del marco jurídico internacional. En la mayoría de los casos, los responsables operan sus campañas desde países sin tratados de asistencia jurídica mutua (UNODC, 2024), lo que genera limitaciones en la investigación, identificación y detención de los atacantes. Asimismo, al no contar con una autoridad judicial global en el ciberespacio, se impide que las órdenes de aprehensión tengan efecto pleno. De esta manera, la soberanía legal de algunas naciones se ha convertido en un espacio de refugio para las organizaciones criminales.

Bajo este panorama de impunidad, han surgido complicaciones debido a lo complejo que suelen ser los procesos de extradición internacional, los cuales, en su mayoría, dependen de trámites largos y decisiones políticas entre países. A esto se suma que no todos los Estados tienen las mismas leyes para castigar el ransomware o la extorsión digital; como consecuencia, se generan vacíos legales significativos. Además, algunos gobiernos no siempre están dispuestos a extraditar a sus ciudadanos, lo que dificulta aún más la cooperación. Un ejemplo de ello es la Federación de Rusia, cuya legislación impide la extradición de nacionales, situación que ha obstaculizado los procesos judiciales contra presuntos integrantes de grupos de ransomware como REvil y LockBit. Como resultado, acciones que en el Reino Unido de Gran Bretaña e Irlanda del Norte son consideradas como delitos graves pueden no ser reconocidas o no contar con penalizaciones en otros países, lo que termina favoreciendo a la impunidad y exige reforzar la cooperación internacional y la armonización de las leyes.

El uso de activos virtuales se ha consolidado como el mecanismo financiero preferido por las organizaciones criminales. En sus comienzos, las transacciones mediante *bitcoin*⁶ tenían cierto grado de rastreo debido a la naturaleza pública que mantenían; no obstante, con el paso del tiempo los grupos delictivos han sofisticado sus métodos, evolucionado hacia el uso de criptomonedas enfocadas en la privacidad absoluta, como *Monero*⁷. Estas plataformas mantienen en privado la identidad de los usuarios, así como las cifras reales transferidas en la red. Como resultado, esta evolución financiera ha limitado la efectividad de las herramientas tradicionales de *auditoría forense*⁸ con las que cuentan las agencias de seguridad.

La cooperación entre las agencias policiales y empresas privadas en la respuesta a ataques de ransomware

La naturaleza tecnológica del ransomware ha provocado que las agencias policiales dependan en gran medida de las capacidades técnicas del sector privado. Corporaciones globales como Microsoft y firmas especializadas como CrowdStrike cuentan con infraestructuras de monitoreo altamente desarrolladas. El intercambio de dicha información con INTERPOL resulta indispensable para la emisión de alertas tempranas a sectores vulnerables. De esta manera, la alianza entre el sector público y las empresas privadas se ha convertido en una defensa clave.

Sin embargo, la consolidación de esta cooperación ha enfrentado diversos obstáculos logísticos vinculados con la confidencialidad de la información. Las empresas de telecomunicaciones mantienen una postura reservada al momento del intercambio de datos sobre incidentes informáticos debido al temor de afectar su reputación comercial o incumplir las leyes de protección de datos personales. Por ello, se vuelve imperativo diseñar protocolos

⁶ **Bitcoin:** Criptomoneda descentralizada que permite realizar transacciones digitales sin intermediarios financieros. (*Oxford Dictionary of Computing*, 2023).

⁷ **Monero:** Criptomoneda enfocada en la privacidad que oculta la identidad de los usuarios y los detalles de las transacciones. (*Monero Project*, 2024).

⁸ **Auditoría forense:** Análisis técnico de sistemas para obtener y preservar evidencia digital con fines de investigación. (*NIST*, 2024).

estandarizados de clasificación y anonimización de la información, así como procedimientos de intercambio seguro mediante plataformas cifradas como I-24/7 de INTERPOL o SIENA de Europol, que faciliten un flujo confidencial y oportuno de inteligencia criminal.

Cooperación internacional contra el ransomware

La Organización Internacional de Policía Criminal (INTERPOL) y *Europol*⁹ colaboran de manera conjunta a través de acuerdos operativos para combatir el crimen transnacional. Mientras que Europol concentra sus esfuerzos analíticos en la Unión Europea, INTERPOL aporta una red de comunicación policía con alcance global. Ambas instituciones conectan sus canales seguros con el propósito de intercambiar datos críticos y alertas sobre grupos delictivos. Tras el Brexit, el cual fue el proceso donde el Reino Unido de Gran Bretaña e Irlanda del Norte decidió salir de la Unión Europea oficialmente en 2020, el país mantiene su cooperación con Europol mediante un estatus de *Estado de alta prioridad*¹⁰. Esta alianza estratégica permite enlazar la inteligencia regional europea con los mecanismos de localización internacional administrados por INTERPOL.

Europol aporta a esta estrategia las capacidades especializadas de su Centro Europeo de Ciberdelincuencia (EC3) investigando muestras de malware, identificar indicadores de compromiso (IoC) y coordinar investigaciones técnicas entre los Estados miembros. Por su parte, INTERPOL coordina a las Oficinas Centrales Nacionales (OCN) mediante la red segura I-24/7, a través de la cual las autoridades intercambian en tiempo real direcciones IP, dominios maliciosos, firmas de malware, billeteras de criptomonedas, información sobre servidores ilícitos y datos de sospechosos. La Agencia Nacional contra el Crimen (NCA) alimenta constantemente bases de datos compartidas para sustentar las investigaciones. El

⁹ **Europol:** Agencia de la Unión Europea para la Cooperación Policial, encargada de apoyar a los Estados miembros en la prevención, investigación y combate de la delincuencia grave, el terrorismo y el crimen organizado transnacional mediante el intercambio de inteligencia y la coordinación de operaciones. (Europol, 2024).

¹⁰ **Estado de alta prioridad:** País identificado como prioritario para la aplicación de medidas de seguridad y cooperación internacional. (INTERPOL, 2024)

Reino Unido de Gran Bretaña e Irlanda del Norte mantiene una política de tolerancia cero al pago de rescates y fortalece la cooperación con la National Crime Agency (NCA). En la Unión Europea, la República Francesa, la República Federal de Alemania, el Reino de España y la República Italiana promueven la armonización legislativa y sanciones coordinadas bajo marcos como la Directiva NIS2, junto con el Convenio de Budapest como base de cooperación jurídica internacional (Consejo de Europa, 2001). Los países mantienen cooperación limitada, lo que dificulta la persecución transnacional del ransomware y genera vacíos de aplicación legal señalados en reportes internacionales (UNODC, 2024). Mientras tanto, países de América Latina como los Estados Unidos Mexicanos, la República Federativa del Brasil, la República de Colombia y la República de Chile, así como países africanos como la República de Sudáfrica, la República Federal de Nigeria y la República de Kenia, enfrentan restricciones económicas, tecnológicas e institucionales que limitan la protección de infraestructuras críticas e incrementan su vulnerabilidad frente a ataques de ransomware. Esta desigualdad refuerza la necesidad de fortalecer la cooperación técnica internacional, reducir las brechas operativas y ampliar los mecanismos de asistencia en materia de ciberseguridad (UNODC, 2024).

Referencias

1. Analysis of ransomware court cases and trends: Jan 2020 – Dec 2024 - Cybersecurity report from ENISA. (s. f.). ENISA. Recuperado el 17 de junio de 2026, de <https://www.enisa.europa.eu/publications/reports/ransomware-current-threats-and-trends/>
2. BBC News Mundo. (2019). *Qué es el Brexit y qué cambia ahora que Reino Unido abandonó la Unión Europea*. BBC. Recuperado el 19 de junio de 2026, de <https://www.bbc.com/mundo/noticias-internacional-50821557>
3. Chainalysis Team. (2025). *Organized crime shows high level of professionalization, low level of crypto sophistication*. Chainalysis. Recuperado el 17 de junio de 2026, de <https://www.chainalysis.com/blog/organized-crime-crypto/>
4. Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia (Convenio de Budapest)*. Serie de Tratados del Consejo de Europa. Recuperado el 10 de junio de 2026, de <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
5. CrowdStrike Intelligence. (2024). *Global Threat Report: Cybercrime tactics and ransomware evolution*. CrowdStrike. Recuperado el 19 de junio de 2026, de <https://www.crowdstrike.com/global-threat-report/>
6. European Union Agency for Cybersecurity (ENISA). (2024). *ENISA Threat Landscape for Ransomware Attacks*. ENISA. Recuperado el 17 de junio de 2026, de <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
7. Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Centro Europeo de Ciberdelincuencia (EC3). Recuperado el 19 de junio de 2026, de <https://www.europol.europa.eu/publications-events/publications/internet-organised-crime-threat-assessment-iocta-2024>

8. Financial Action Task Force (FATF). (2023). *Money laundering risks from virtual assets and anonymity-enhancing coins*. FATF-GAFI. Recuperado el 17 de junio de 2026, de <https://www.fatf-gafi.org/en/publications/Methodsandtrends/virtual-assets-anonymity-enhancing-coins.html>
9. IBM Security. (2024). *X-Force Threat Intelligence Index 2024: Ransomware and critical infrastructure targeting*. IBM. Recuperado el 20 de junio de 2026, de <https://www.ibm.com/reports/threat-intelligence>
10. INTERPOL. (2024). *Ciberdelincuencia: Amenazas globales y operaciones policiales transnacionales*. Organización Internacional de Policía Criminal. Recuperado el 20 de junio de 2026, de <https://www.interpol.int/es/Delitos/Ciberdelincuencia>
11. INTERPOL. (2024). *Cybercrime: How law enforcement tackles the Ransomware-as-a-Service model*. Organización Internacional de Policía Criminal. Recuperado el 17 de junio de 2026, de <https://www.interpol.int/en/Crimes/Cybercrime>
12. INTERPOL. (2024). *Respuesta a las ciberamenazas y coordinación con las Oficinas Centrales Nacionales (OCN)*. Organización Internacional de Policía Criminal. Recuperado el 17 de junio de 2026, de <https://www.interpol.int/es/Delitos/Ciberdelincuencia/Respuesta-a-las-ciberamenazas>
13. Microsoft Security. (2024). *Microsoft Digital Defense Report 2024: The state of the Ransomware-as-a-Service ecosystem*. Microsoft. Recuperado el 17 de junio de 2026, de <https://www.microsoft.com/en-us/security/blog/microsoft-digital-defense-report-2024/>
14. National Cyber Crime Unit (NCCU). (2024). *Strategic assessment of serious cyber threats to the United Kingdom*. National Crime Agency. Recuperado el 17 de junio de

2026, de

<https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime>

15. National Cyber Security Centre (NCSC). (2024). *The cyber threat to UK critical national infrastructure: A joint analysis*. NCSC. Recuperado el 17 de junio de 2026, de <https://www.ncsc.gov.uk/report/cni-threat-assessment-2024>
16. National Health Service (NHS). (2017). *Lessons learned review of the WannaCry ransomware cyber attack on healthcare delivery*. NHS England. Recuperado el 17 de junio de 2026, de <https://www.england.nhs.uk/publication/lessons-learned-review-wannacry/>
17. National Institutes of Health (NIH). (2023). *Trends in ransomware attacks on US hospitals, clinics, and other health care delivery systems*. PubMed Central. Recuperado el 17 de junio de 2026, de <https://pmc.ncbi.nlm.nih.gov/articles/PMC1072214/>
18. Organización Mundial de la Salud (OMS). (1989). *Report on the World AIDS Conference: International technical and health-related incidents*. OMS. Recuperado el 17 de junio de 2026, de <https://www.who.int/publications/historical-archives>
19. Parlamento Europeo y el Consejo de la Unión Europea. (2022). *Directiva (UE) 2022/2555 relativa a medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2)*. Diario Oficial de la Unión Europea. Recuperado el 17 de junio de 2026, de <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022L2555>
20. United Nations Office on Drugs and Crime (UNODC). (2024). *Global Report on Cybercrime: Legal fragmentation and jurisdictional challenges*. UNODC. Recuperado el 17 de junio de 2026, de <https://www.unodc.org/unodc/en/cybercrime/global-report-202>

Tópico B

Mecanismos para fortalecer la cooperación policial internacional en la identificación y desarticulación de redes criminales transnacionales dedicadas al tráfico ilícito de migrantes a través de rutas terrestres irregulares entre América Latina y América del Norte

Por: Andrea Guadalupe Zaldívar Escamilla, Santiago Rodríguez Olivares, Kaori Mar

Aguilar, Sofía Vázquez González

Introducción

El tráfico ilícito de migrantes se ha establecido como una de las principales amenazas del crimen organizado transnacional del siglo XXI. Este delito radica en facilitar el ingreso ilegal de una persona a un Estado del cual no sea nacional o residente permanente, con la finalidad de obtener un beneficio financiero o material (UNODC, 2000). Se caracteriza por el consentimiento inicial del migrante para su traslado irregular; sin embargo, durante el trayecto muchas víctimas son sometidas a violencia, explotación o abusos contra sus derechos humanos. Factores como la falta de recursos, la violencia, la inestabilidad económica, los desastres naturales y la falta de oportunidades económicas han impulsado a las personas a abandonar su país de origen en búsqueda de mejores condiciones de vida. En años recientes, el aumento de los flujos migratorios en América Latina y América del Norte ha favorecido el fortalecimiento de las organizaciones criminales dedicadas al transporte ilícito de personas.

La preocupación internacional frente a esta problemática ha aumentado debido a que los grupos responsables distribuyen sus operaciones entre distintas *jurisdicciones*¹¹, utilizando intermediarios y documentación falsificada en diversos países, lo que obstaculiza su identificación y persecución por parte de las autoridades nacionales. Esta situación limita la capacidad de respuesta individual de los Estados y evidencia la necesidad de optimizar los mecanismos de cooperación policial internacional. Bajo este panorama, la Organización Internacional de Policía Criminal (INTERPOL) ejerce un papel fundamental en la coordinación de investigaciones, el intercambio de inteligencia criminal entre las autoridades policiales y el fortalecimiento de la cooperación entre las Oficinas Centrales Nacionales (OCN) de sus países miembros. Asimismo, la naturaleza transnacional de este delito exige

¹¹ **Jurisdicciones:** Territorio o ámbito en el que una autoridad tiene la facultad legal de ejercer sus funciones y aplicar la ley. (RAE, 2024)

mecanismos permanentes de intercambio de información e inteligencia criminal que permitan una respuesta coordinada frente a estas organizaciones.

Con el fin de combatir eficazmente las redes criminales dedicadas al tráfico ilícito de migrantes, resulta imperativo fortalecer la cooperación policial internacional mediante estrategias conjuntas y coordinadas. El alcance que han adquirido estos flujos clandestinos ha impulsado a los gobiernos y a las organizaciones internacionales a reforzar sus mecanismos de seguridad fronteriza y cooperación judicial internacional. Entre las principales iniciativas destacan el Protocolo contra el Tráfico Ilícito de Migrantes por Tierra, Mar y Aire (2000), que establece un marco común para prevenir y sancionar este delito. Bajo este panorama, herramientas como el sistema mundial de comunicación policial segura I-24/7 han fortalecido el intercambio de información entre las autoridades, al facilitar la comunicación segura y el acceso en tiempo real a bases de datos policiales compartidas entre los Estados miembros, contribuyendo a la identificación y desarticulación de redes criminales. El diseño de un frente normativo común resulta indispensable para armonizar los criterios de persecución penal y ampliar la coordinación entre los Estados.

Antecedentes

En las últimas décadas, el hemisferio occidental se ha establecido como una de las regiones más afectadas por el tráfico ilícito de migrantes debido a las desigualdades económicas, la inestabilidad política y la relevancia estratégica de sus *corredores fronterizos*¹². De acuerdo con la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), las principales rutas terrestres que traspasan América Latina y América del Norte son utilizadas de manera frecuente por organizaciones criminales transnacionales con el fin de facilitar el traslado irregular de personas. Las regiones que abarcan desde el *istmo*¹³ centroamericano hasta la

¹² **Corredores fronterizos:** Zonas de tránsito utilizadas para el desplazamiento de personas y mercancías entre dos o más Estados. (OIM, 2019).

¹³ **Istmo:** Franja estrecha de tierra que une dos grandes extensiones terrestres y separa dos mares. (RAE, 2024).

frontera entre los Estados Unidos de América y los Estados Unidos Mexicanos concentran una parte significativa de estas actividades ilícitas. Como respuesta ante este panorama, las autoridades migratorias y los organismos responsables de la seguridad fronteriza han fortalecido sus mecanismos de vigilancia, intercambio de información y cooperación internacional para mejorar la identificación y desarticulación de redes criminales. Sin embargo, la constante adaptación de estas organizaciones a los métodos de control continúa representando un desafío para los Estados de la región.

La expansión del tráfico ilícito de migrantes comenzó a intensificarse aceleradamente durante las últimas décadas del siglo XX, en contraste con el incremento de los flujos migratorios irregulares y el fortalecimiento de las políticas de control fronterizo. Uno de los principales antecedentes jurídicos internacionales fue la adopción de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y de su Protocolo contra el Tráfico Ilícito de Migrantes por Tierra, Mar y Aire, aprobados en el año 2000, los cuales establecieron un marco jurídico común con el objetivo de prevenir, investigar y sancionar este delito mediante la cooperación internacional. Posteriormente, entre los años 2000 y 2010, las organizaciones criminales desarrollaron redes logísticas cada vez más complejas, incorporando intermediarios, guías locales, documentación de identidad falsificada y facilitadores distribuidos en distintos países. A medida que aumentó el uso de teléfonos inteligentes, redes sociales y sistemas de posicionamiento global (GPS), los grupos criminales incorporaron nuevas herramientas tecnológicas para coordinar rutas, monitorear el movimiento de las autoridades, contactar migrantes y mejorar su capacidad operativa a nivel transnacional.

La crisis migratoria regional de 2014 representó uno de los episodios más significativos en la evolución del tráfico ilícito de migrantes en América Latina y América del Norte. Durante este periodo se registró un incremento histórico en el flujo de niñas, niños,

adolescentes y mujeres no acompañados, así como de unidades familiares originarias principalmente del Triángulo Norte de Centroamérica, con el propósito de llegar a los Estados Unidos de América. Esta situación de extrema vulnerabilidad humanitaria fue aprovechada por organizaciones criminales transnacionales, las cuales ampliaron y consolidaron sus redes logísticas para facilitar el traslado irregular de personas. De este modo, los grupos delictivos consolidaron su presencia mediante el uso de intermediarios logísticos, documentación falsificada, corrupción de funcionarios públicos y rutas terrestres clandestinas.

Desde 2017, estos grupos delictivos han incrementado su grado de organización mediante la adopción de estructuras criminales descentralizadas distribuidas en múltiples jurisdicciones. Los grupos delictivos han incorporado herramientas tecnológicas avanzadas, sistemas de comunicación cifrada y mecanismos de coordinación transfronteriza que les permiten adaptar constantemente sus métodos de operación frente al reforzamiento de los controles fronterizos estatales (Europol, 2024). De igual manera, diversos grupos criminales han recurrido a la extorsión sistemática, el secuestro y la violencia física contra los migrantes para aumentar sus ganancias y consolidar el control sobre las principales rutas de tránsito terrestre. Como resultado, los Estados del hemisferio han fortalecido el intercambio de inteligencia criminal, la cooperación policial y las investigaciones conjuntas con el propósito de identificar y desarticular estas redes delictivas.

La evolución del tráfico irregular y nuevos desafíos para la seguridad hemisférica

En la actualidad, el tráfico ilícito de migrantes representa una de las principales amenazas para la seguridad regional en América Latina y América del Norte, constituyendo un mercado ilegal que genera importantes ganancias para las organizaciones criminales. Aunque los controles fronterizos han sido fortalecidos, no han reducido significativamente la actividad de estas redes. En consecuencia, las organizaciones criminales han desplazado sus rutas hacia

corredores terrestres irregulares. Según datos de la Organización Internacional para las Migraciones (OIM, 2024), durante 2023 más de 500,000 personas cruzaron de manera irregular el Parque Nacional Darién, lo que evidencia la magnitud de los flujos migratorios por esta ruta.

La cooperación policial internacional constituye uno de los principales mecanismos para consolidar la respuesta de los Estados frente al tráfico ilícito de migrantes. A través de INTERPOL, las Oficinas Centrales Nacionales (OCN), la Organización Internacional para las Migraciones (OIM) y la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), los países impulsan el intercambio de inteligencia criminal, la coordinación de investigaciones conjuntas y la ejecución de operativos transfronterizos dirigidos a identificar y desarticular estas redes criminales. No obstante, las diferencias en recursos tecnológicos, capacidades operativas y marcos jurídicos continúan limitando la eficacia de las investigaciones y los operativos conjuntos. En consecuencia, el fortalecimiento de los mecanismos de cooperación policial internacional, la homologación de criterios de actuación y el intercambio oportuno de información constituyen algunos de los principales desafíos que deberán abordar los Estados para enfrentar eficazmente esta amenaza.

Organizaciones criminales transnacionales dedicadas al tráfico ilícito de migrantes

En la actualidad, las organizaciones criminales dedicadas al tráfico ilícito de migrantes operan mediante estructuras transnacionales que distribuyen sus actividades entre distintas jurisdicciones geográficas. Estas redes suelen involucrar a coordinadores, reclutadores, transportistas, guías, falsificadores de documentos y diversos facilitadores que participan de manera especializada en las diferentes etapas del traslado irregular de personas (UNODC, 2023). Este reparto fragmentado de funciones permite que los grupos mantengan la continuidad de sus operaciones operativas incluso tras la detención de actores secundarios en el terreno. En consecuencia, la atomización del proceso dificulta considerablemente que las

autoridades identifiquen, investiguen y sancionen a los verdaderos líderes encargados de la coordinación logística e intelectual desde los niveles superiores.

En América Latina y América del Norte, el tráfico ilícito de migrantes se ha complementado con otras actividades ilícitas, como el narcotráfico, la trata de personas, el tráfico de armas y el lavado de activos, mediante la participación de diversos grupos criminales. Organizaciones vinculadas al Cártel Jalisco Nueva Generación (CJNG), así como otras redes criminales dedicadas al tráfico de migrantes, han sido señaladas por su participación en actividades ilícitas relacionadas con el traslado irregular de personas. Estas organizaciones han establecido alianzas con facilitadores locales distribuidos a lo largo de las rutas migratorias, permitiendo la continuidad de sus operaciones y adaptándose al reforzamiento de los controles fronterizos. La diversidad de actores involucrados dificulta determinar una estructura única de mando y favorece la reorganización de las redes cuando alguno de sus integrantes es detenido.

Redes logísticas y mecanismos utilizados para facilitar el tráfico ilícito de migrantes

Las organizaciones criminales sostienen sus operaciones a través de sofisticadas redes logísticas que les permiten coordinar el traslado irregular de personas a través de múltiples Estados sin depender de un mando centralizado. De acuerdo con la Europol, estas redes comprenden sistemas de transporte terrestre, casas de seguridad, documentación de identidad falsificada, facilitadores locales, operadores financieros y mecanismos de comunicación que garantizan la continuidad del recorrido desde los países de origen hasta el destino final. Asimismo, la Organización Internacional para las Migraciones (OIM) señala que la utilización simultánea de estos recursos incrementa significativamente la capacidad adaptativa de las organizaciones y dificulta la identificación de sus responsables por parte de las autoridades. Esta diversificación logística genera una marcada asimetría entre la agilidad

operativa del crimen organizado y la capacidad de respuesta de los mecanismos de control fronterizo estatales.

En los últimos años, el desarrollo tecnológico ha transformado la forma en que estas redes coordinan sus actividades. Aplicaciones de mensajería cifrada, sistemas de posicionamiento global (GPS), redes sociales y plataformas digitales permiten modificar rutas en tiempo real y mantener comunicación entre los distintos integrantes de la organización. Estas herramientas han facilitado la coordinación de pagos y la alerta sobre operativos policiales. Al mismo tiempo, el uso de mecanismos de corrupción, documentación falsificada e identidades falsas simplifica el tránsito irregular por diferentes fronteras y limita la eficacia de los mecanismos tradicionales de vigilancia migratoria.

Los Estados enfrentan el desafío de identificar los patrones logísticos utilizados por las organizaciones criminales antes de que modifiquen sus métodos de operación. La coordinación entre las Oficinas Centrales Nacionales (OCN) permite fortalecer la cooperación internacional frente al tráfico ilícito de migrantes. El intercambio oportuno de inteligencia criminal y el análisis conjunto de información favorece las investigaciones transnacionales y la identificación de los patrones delictivos. Estas acciones pueden contribuir a reducir la capacidad operativa de las organizaciones criminales dedicadas a este delito.

Cooperación policial internacional e intercambio de inteligencia criminal

La naturaleza transnacional del tráfico ilícito de migrantes exige mecanismos permanentes de cooperación entre las autoridades policiales de los Estados afectados. INTERPOL coordina esta colaboración mediante las Oficinas Centrales Nacionales (OCN) y la red mundial segura I-24/7, una plataforma que permite intercambiar en tiempo real información relacionada con personas buscadas, documentos de viaje robados o falsificados, vehículos, rutas utilizadas por organizaciones criminales, notificaciones internacionales y otros elementos relevantes para

las investigaciones, de acuerdo con los informes del 2024 de INTERPOL. Este intercambio inmediato de inteligencia criminal fortalece la coordinación de operativos conjuntos, permite identificar conexiones entre investigaciones desarrolladas en distintas jurisdicciones y facilita la detección de redes dedicadas al tráfico ilícito de migrantes. Además, el análisis conjunto de esta información permite anticipar movimientos de las organizaciones criminales, mejorar la respuesta de las autoridades y fortalecer la cooperación internacional para desarticular sus estructuras y reducir su capacidad de operación.

Organismos como la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), la Organización Internacional para las Migraciones (OIM), Ameripol y Europol han consolidado las capacidades de los Estados por medio de programas de asistencia técnica, capacitación especializada, intercambio de inteligencia y coordinación de investigaciones transfronterizas. Estas instituciones complementan los esfuerzos de INTERPOL al proporcionar herramientas y conocimientos especializados para enfrentar las distintas modalidades del tráfico ilícito de migrantes. Sus iniciativas permiten identificar patrones de operación comunes, fortalecer las capacidades institucionales y facilitar la ejecución simultánea de operativos dirigidos contra organizaciones criminales que operan en múltiples países (Europol, 2024; UNODC, 2024). Asimismo, la cooperación entre estas organizaciones favorece la prevención del delito, el intercambio de buenas prácticas y una respuesta coordinada que permita desarticular redes criminales y proteger a las personas migrantes frente a situaciones de explotación y abuso.

No obstante, la diversidad de marcos jurídicos, las limitaciones tecnológicas y las diferencias en los protocolos para compartir información reducen la eficacia de la cooperación internacional. Estas diferencias dificultan el intercambio de inteligencia, retrasan investigaciones y permiten que las organizaciones criminales aprovechen las brechas entre los Estados. Por ello, fortalecer el intercambio seguro de inteligencia, armonizar los

procedimientos y consolidar la coordinación policial son desafíos prioritarios. De igual manera, mejorar la compatibilidad tecnológica, establecer protocolos comunes y capacitar a las autoridades permitirá una respuesta más rápida y coordinada frente al tráfico ilícito de migrantes.

Desafíos actuales para la cooperación policial internacional contra el tráfico ilícito de migrantes

La fragmentación de las investigaciones entre distintas jurisdicciones, la corrupción de funcionarios públicos y el uso de identidades falsas dificultan la integración de evidencia suficiente para procesar judicialmente a los principales responsables de acuerdo con los informes de UNODC. La constante modificación de las rutas migratorias también dificulta el seguimiento de las operaciones y la identificación de sus responsables. Como consecuencia, las organizaciones criminales mantienen una elevada capacidad para reestructurar sus operaciones y sustituir rápidamente a los integrantes detenidos. Las diferentes prioridades nacionales representan otro obstáculo para la cooperación internacional. Mientras los Estados Unidos de América y Canadá priorizan el fortalecimiento de la seguridad fronteriza, el intercambio inmediato de información biométrica y la detección temprana de amenazas, diversos Estados de América Latina sostienen que una respuesta integral también debe considerar los factores económicos, sociales y humanitarios que impulsan la migración irregular. (IOM, 2024)

Los desafíos radican en las diferencias existentes entre los Estados respecto al intercambio de información sensible. Algunos países mantienen restringido el uso compartido de datos biométricos y personales debido a sus legislaciones nacionales sobre privacidad y protección de datos, mientras que otros consideran indispensable ampliar el acceso a esta información para fortalecer las investigaciones transnacionales y la identificación de

organizaciones criminales. En consecuencia, se solicita el fortalecer la cooperación policial mediante protocolos comunes para el intercambio seguro de información y la coordinación de investigaciones transfronterizas, del mismo modo, la mejora de cooperación tecnológica y operativa entre respectivas instituciones con el fin facilitar la identificación de las redes criminales. Estas medidas permitirán establecer una respuesta regional coordinada para prevenir y desarticular las organizaciones dedicadas al tráfico ilícito de migrantes.

Referencias

1. Ameripol. (2023). Informe sobre delincuencia organizada transnacional y redes de tráfico en las Américas. Comunidad de Policías de América. Recuperado el 14 de julio de 2026, de <https://www.ameripol.org/informes/delincuencia-organizada-2023>
2. Organización Internacional de Policía Criminal. (s. f.). El sistema de comunicación policial segura I-24/7. Secretaría General de INTERPOL. Recuperado el 16 de junio de 2026, de <https://www.interpol.int/es/Como-trabajamos/Servicios-de-comunicacion-policial/I-24-7>
3. Organización Internacional de Policía Criminal. (2024). Operación Turquesa: Operativos globales contra el tráfico ilícito de migrantes y la trata de personas. Secretaría General de INTERPOL. Recuperado el 14 de julio de 2026, de <https://www.interpol.int/es/Delitos/Trafico-de-personas-y-migrantes/Operacion-Turquesa>
4. Organización Internacional para las Migraciones. (2023). Gestión integrada de fronteras y cooperación policial en corredores terrestres irregulares. OIM. Recuperado el 16 de junio de 2026, de <https://www.iom.int/es/gestion-fronteriza-cooperacion>
5. United Nations Office on Drugs and Crime. (2022). Abordaje del tráfico ilícito de migrantes desde la perspectiva de las finanzas criminales e inteligencia policial. UNODC. Recuperado el 14 de julio de 2026, de <https://www.unodc.org/unodc/es/money-laundering/smuggling-migrants-finance.html>
6. U.S. Department of the Treasury. (2025). Treasury Sanctions Mexico-Based Transnational Criminal Organization Smuggling Migrants into the United States.

Office of Foreign Assets Control. Recuperado el 30 de agosto de 2026, de

<https://home.treasury.gov/news/press-releases/sb0296>

7. Chainalysis Team. (2025). Organized crime shows a high level of professionalization, low level of crypto sophistication. Chainalysis. Recuperado el 14 de julio de 2026, de <https://www.chainalysis.com/blog/organized-crime-crypto/>
8. Europol. (2024). Tackling threats, addressing challenges: Europol's response to migrant smuggling and trafficking in human beings. European Migrant Smuggling Centre (EMSC). Recuperado el 14 de julio de 2026, de <https://www.europol.europa.eu/publications-events/publications/emsc-report-tackling-threats-addressing-challenges>
9. International Organization for Migration. (s. f.). Understanding the Smuggling of Migrants Protocol. Recuperado el 16 de junio de 2026, de <https://www.iom.int/sites/g/files/tmzbd1486/files/iscm/materials/understandingthesmugglingofmigrantsprotocol.pdf>
10. Oficina de las Naciones Unidas contra la Droga y el Delito. (s. f.). Smuggling of migrants. Recuperado el 14 de julio de 2026, de <https://www.unodc.org/toc/en/crimes/migrant-smuggling.html>
11. Oficina de las Naciones Unidas contra la Droga y el Delito. (s. f.). Tráfico ilícito de migrantes: la dura búsqueda de una vida mejor. Recuperado el 16 de junio de 2026, de <https://www.unodc.org/toc/es/crimes/migrant-smuggling.html>
12. Oficina de las Naciones Unidas contra la Droga y el Delito. (2019). Módulo 5: Tráfico ilícito de migrantes. Recuperado el 14 de julio de 2026, de https://www.unodc.org/documents/e4j/tip-som/Module_5_-_E4J_SOM_ES_FINAL.pdf

13. Organización de las Naciones Unidas. (2000). Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos. Oficina de Asuntos Jurídicos. Recuperado el 16 de junio de 2026, de <https://www.unodc.org/toc/es/documents.html>
14. Organización Internacional para las Migraciones. (2024). Movilidad humana y migración en las Américas: tendencias y desafíos. Organización Internacional para las Migraciones. Recuperado el 14 de julio de 2026, de <https://www.iom.int/es>
15. United Nations Office on Drugs and Crime. (2000). Protocolo contra el Tráfico Ilícito de Migrantes por Tierra, Mar y Aire, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. Oficina de Asuntos Jurídicos. Recuperado el 16 de junio de 2026, de <https://www.unodc.org/toc/es/documents.html>
16. United Nations Office on Drugs and Crime. (2023). Global study on smuggling of migrants 2023. Recuperado el 14 de julio de 2026, de <https://www.unodc.org/unodc/en/data-and-analysis/glosom.html>
17. United Nations Office on Drugs and Crime. (2024). Global Report on Smuggling of Migrants: Transnational networks and financial flows. UNODC. Recuperado el 16 de junio de 2026, de <https://www.unodc.org/unodc/en/data-and-analysis/glosom.html>

XXXIV TECMUN Jr.
Glosario de Palabras Prohibidas

Palabras prohibidas

Definidas por las Naciones Unidas, son términos no diplomáticos que los participantes deben evitar mencionar en sus discursos durante el debate y en la redacción de proyectos de resolución.

Palabras prohibidas

Equivalentes permitidos

Países de primer mundo

Países desarrollados

Países de tercer mundo

Países en desarrollo

Gay

Miembro de la comunidad LGBTIQ+

Guerra¹⁴

Conflicto bélico

Violación

Acoso sexual

Terrorista

Extremista

Matar o asesinar

Despojar a alguien de su vida

Muerte

Deceso o fallecimiento

Asesinato

Homicidio

Ejército

Fuerzas militares

Dinero

Recursos económicos

Pobre

Falta de recursos

Okey

Sí o de acuerdo

Negro¹⁵

Afroamericano

¹⁴ La palabra guerra puede ser utilizada en referencia a contextos históricos, tales como Guerra Fría o Primera Guerra Mundial, etc. Esta palabra solo puede mencionarse en Security Council.

¹⁵ La palabra Negro, en referencia a raza, no está prohibida pero se recomienda limitar su uso y referirse a este sector como afroamericanos o afrodescendientes.

XXXIV TECMUN Jr.
Glosario para proyectos de resolución

Cláusulas preambulatorias

Se utilizan al inicio de toda Hoja de Resolución con el motivo de brindar contexto sobre la razón por la que se está resolviendo el tópico debatido. Dichas cláusulas deben ir con formato de itálicas seguidas por oración que aporte dicho contexto. Para cada hoja de resolución debe haber cinco oraciones que comiencen con cláusulas preambulatorias.

Además lamentando	Declarando	Notando con satisfacción
Además recordando	Desaprobando	Preocupado por
Advirtiendo además	Deseando	Plenamente alarmado
Advirtiendo con aprobación	Destacando	Plenamente consciente de
Advirtiendo con pesar	Enfatizando	Profundamente convencido
Afirmando	Esperando	Profundamente molesto
Alarmado por	Expresando su aprecio	Profundamente perturbado
Buscando	Guiados por	Profundamente preocupado
Preocupado	Habiendo adoptado	Reafirmando
Conscientes de	Habiendo considerando	Reconociendo
Considerando	Habiendo estudiado	Recordando
Contemplando que	Habiendo examinado	Refiriéndose
Convencidos	Habiendo prestado atención	Teniendo en cuenta que

XXXIV TECMUN Jr.
Glosario para proyectos de resolución

Cláusulas Operativas

Se utilizan para iniciar toda resolución que plantee soluciones al tópico debatido. Su formato debe ser en itálicas y negritas.

Acepta	Confirma	Ha resuelto
Además invita	Considera	Insta
Además proclama	Decide	Invita
Además recomienda	Declara	Lamenta
Además recuerda	Define	Llama
Además resuelve	Declara prudente	Pide
Acoge con beneplácito	Deplora	Proclama
Afirma	Designa	Reafirma
Alienta	Enfatiza	Recomienda
Apoya	Exhorta	Recuerda
Aprueba	Expresa su aprecio	Resuelve
Autoriza	Expresa su deseo	Solemnemente afirma
Celebra	Expresa su esperanza	Solicita
Condena	Finalmente condena	Urge

[illegible]

