

REVISTA OFICIAL



Poder Judicial del Perú
Corte Superior de Justicia de Lima

SERVIR ES NUESTRA MISIÓN
LA JUSTICIA CON ROSTRO HUMANO
NUESTRO OBJETIVO

PRIMER CONGRESO INTERNACIONAL

“CIBERCRIMEN, INTELIGENCIA ARTIFICIAL Y NUEVAS FIGURAS DELICTIVAS”



Del 26 al 28 de noviembre



14 EXPOSITORES INTERNACIONALES



9 EXPOSITORES NACIONALES



46 PANELISTAS

AUSPICIADO Y PATROCINADO POR



PRIMER CONGRESO INTERNACIONAL DE CIBER CRIMEN – NOVIEMBRE 2025.

CONSEJO DIRECTIVO

Dra. MILUSKA CANO LOPEZ, Presidenta de la Corte Superior de Justicia de Lima.

Dr. Bonifacio Meneses Gonzáles - Juez Superior Titular, coordinador del Congreso Internacional de Ciber Crimen
Dr. Jaime Zevallos Gonzales, Juez Superior Titular.

Josefa Yzaga Pelegrini, Juez Superior Provisional.

CONSEJO CONSULTIVO

Dr. Gustavo Jalkh Roben - Presidente del Instituto Iberoamericano de Justicia.

Dr. Manuel Lazaro Pulido - Catedrático Principal de la Pontificia Unmivesidad de Salamanca - España.

Catalina Stroe - Coordinadora del Consejo de Europa para Glacy e

Lourdes Gutierrez Ortiz Monasterio - Secretaria de las Naciones Unidas contra el ciber crimen para Centro America y el Caribe.

Cristos Velasco San Martin - Catedratico de la Universidad de Manheim Alemania.

David Gutierrez Castaño - Director de la Escuela de Pos grado de la Universidad de Medellin - Colombia.

Luis Jorge Gamboa Olea - Magistrado ex Presidente del Tribunal Superior Justicia de Morelos - Mexico.

Antoni Bosch Pujol - director general del Institute of Audit & IT-Governance.

Coordinadores

Roberto Jesus Paredes Delgado

Jair Benavides Lanchipa

Gustavo Alzamora Alata

Beatriz Vizcarra Bermudez

Alexander Niño Espinoza

Paola Erika Rosado German

Diagramación – Edición

Área de Informática & Sistemas – Corte Superior de Justicia de Lima.

Colaboración

- Administración Corte Superior de Justicia de Lima, aérea Penal.

Edición **NOVIEMBRE 2025**

Año 1 – Nº 1



INDICE

Presentación -----	Pág. 4
Resolución de la secretaria general del Ministerio de Relaciones Exteriores -----	Pág. 6
Resolución Administrativa N° 867-2025-P-CSJLI-PJ -----	Pág.8
Resolución Administrativa N° 624-2025-P-CSJLI-PJ -----	Pág. 11
Declaración de Lima -----	Pág. 15
Introducción -----	Pág. 18
Finalidad -----	Pág. 20

PRIMER DIA

Palabras de bienvenida y presentación -----	Pág. 22
Palabras inaugurales -----	Pág. 23
Preservación y protección de datos ante el cibercrimen -----	Pág. 25
El Pacto (Europa Latinoamérica Programa de Asistencia contra el crimen transnacional Organizado) Delitos asistidos mediante la IA -----	Pág. 27
La complejidad para investigar los ciberdelitos – El delicado aporte a la fiscalía para su investigación -----	Pág. 29
Inteligencia artificial – Detección y control de Amenazas emergentes -----	Pág. 31
Modalidad del Cibercrimen: Ataques contra datos y sistemas informáticos -----	Pág. 33
Inteligencia artificial – retos de la diligencia organizada – delitos del amor -----	Pág. 35
La importancia de la protección de datos personales para la prevención de delitos cibernéticos -----	Pág. 37

SEGUNDO DIA

De la curiosidad tecnológica a la responsabilidad penal – menores e inteligencia artificial en el cibercrimen -----	Pág. 40
El agente encubierto online en la investigación del cibercrimen -----	Pág. 42
La Causalidad, correspondencia o autopuesta en peligro en los ciberdelitos -----	Pág. 44
Cibercrimen y la acción de extinción de dominio del derecho de dominio – visión Colombiana y Perú -----	Pág. 46
Ministerio Público en el Perú ante la ciberdelincuencia -----	Pág. 48
Del ciberespacio al tribunal: investigación y persecución del cibercrimen -----	Pág. 50

TERCER DIA

Criminalidad organizada, economías ilegales y lavados de activos en el Perú: impacto en la cifra negra -----	Pág. 53
Convenio de Naciones Unidas contra la ciberdelincuencia -----	Pág. 55
Razonamiento probatorio en las conductas de cibercriminalidad -----	Pág. 57
Cibercriminalidad: ciberataques, análisis y consecuencias punitivas -----	Pág. 59
Los delitos informáticos – óptica de la justicia Ecuatoriana frente al pluriofensivo Ciberdelito -----	Pág. 61
Alternativas de prevención del cibercrimen: privacidad, IA, Open Banking -----	Pág. 63
Sociedad de la información, ciberdelincuencia y organismos internacionales -----	Pág. 65
Palabras de clausura del Ministro de Justicia y Derechos Humanos -----	Pág. 67

}

SEMBLANZAS DEL EVENTO

Programa del Primer Congreso Internacional de Cibercrimen	Pág. 68
Fotografías del Primer Congreso Internacional de Cibercrimen	Pág. 75
Capacitaciones previas al Congreso Internacional de Cibercrimen	Pág. 87
Palabras de los patrocinadores	Pág. 92

PRESENTACION

Es un honor presentar la Revista del Primer Congreso Internacional de Cibercrimen, publicación oficial que recopila las conferencias, materiales y aportes académicos expuestos durante tres jornadas dedicadas al análisis profundo de los desafíos actuales en materia de criminalidad informática.

El Congreso fue inaugurado por el Juez Supremo Titular Víctor Roberto Prado Saldarriaga, destacada figura del Derecho peruano, cuya participación honró y dio realce institucional al evento. Asimismo, la clausura estuvo a cargo del Ministro de Justicia, en representación del Presidente de la República, reafirmando el respaldo estatal a la lucha integral contra el delito informático.

Este importante esfuerzo académico y judicial fue posible gracias al apoyo de instituciones internacionales y académicas de prestigio, entre ellas:

- Consejo de Europa a través del Proyecto Glacy e*
- Secretaría de Cibercrimen de las Naciones Unidas (ONU)
- Pontificia Universidad de Salamanca
- Instituto Iberoamericano de Justicia
- Universidad Austral de Argentina
- Universidad de Medellín
- Universidad de San Martín de Porres
- Observatorio de Cibercrimen de Argentina
- Academia Peruana de Ciberseguridad y Derecho Penal Informático.

A todas estas instituciones extendemos nuestro reconocimiento por su colaboración, su confianza y su compromiso con el fortalecimiento de la justicia digital en la región.

De manera especial, expresamos un cordial saludo y agradecimiento al Señor Rector de la Universidad de San Martín de Porres, cuya apertura y respaldo académico contribuyeron al éxito del Congreso y a la difusión del conocimiento especializado.

Asimismo, expreso mi reconocimiento a los expositores nacionales e internacionales, quienes compartieron con rigor técnico y claridad pedagógica sus investigaciones, experiencias y propuestas. Todas sus ponencias, materiales y conferencias se incluyen íntegramente en esta revista para consulta permanente de la comunidad jurídica, técnica y académica del país.

Un homenaje particular merece el Juez Bonifacio Meneses, responsable de la conducción y moderación general del Congreso, cuya labor ordenada, precisa y altamente profesional permitió una articulación impecable de cada jornada de trabajo.

Esta revista busca preservar el conocimiento generado en este encuentro, servir como

herramienta de capacitación y promover la articulación interinstitucional frente a los desafíos crecientes del cibercrimen, siempre en pleno respeto de los principios constitucionales, la legalidad y los derechos fundamentales.

Invito a todos los lectores a recorrer estas páginas con interés y reflexión, seguros de que su contenido contribuirá significativamente a la consolidación de un sistema de justicia moderno, especializado y preparado para enfrentar los retos del entorno digital.

Dra. Miluska Cano López
Presidenta
Corte Superior de Justicia de Lima

Resolución Secretaría General

Lima, 25 NOV. 2025

VISTOS:

El Oficio N° 4173-2025-JUS/SG, de 17 de noviembre de 2025, del Ministerio de Justicia y Derechos Humanos; el Memorandum N° DGM024972025, de 24 de noviembre de 2025, de la Dirección General para Asuntos Multilaterales y Globales; el Memorandum N° LEG024782025, de 25 de noviembre de 2025, de la Oficina General de Asuntos Legales; y,

CONSIDERANDO:

Que, conforme al numeral 8 del artículo 6 de la Ley N° 29357, Ley de Organización y Funciones del Ministerio de Relaciones Exteriores, dicho Ministerio tiene como función específica otorgar el carácter internacional a las asambleas, congresos, conferencias o seminarios que se realicen en el territorio de la República en que participan delegaciones extranjeras;

Que, mediante Decreto Supremo N° 001-2001-RE, modificado por Decreto Supremo N° 083-2016-RE, se establecen disposiciones para el otorgamiento de carácter internacional a eventos que se realicen en el país con la participación de delegaciones extranjeras, cuyo artículo 2 establece que los interesados en la realización de un evento internacional en el Perú dirigirán una solicitud para su oficialización al sector del Gobierno Central al que corresponda el carácter de la reunión. Si este sector considera que la realización del evento implica un aporte a los intereses del Estado, transmitirá la solicitud al Ministerio de Relaciones Exteriores, el cual, de considerarlo conveniente, oficializará el carácter internacional del evento mediante Resolución Ministerial o resolución emitida por el órgano a quien se delegue dicha facultad;

Que, mediante Resolución Ministerial N° 0303-2017-RE se aprobó la Directiva N° 004-2017 MIN/RE "Disposiciones para Oficializar Eventos Internacionales", el cual tiene por finalidad establecer disposiciones y procedimientos para que el Ministerio de Relaciones Exteriores otorgue el carácter internacional a los eventos desarrollados en el territorio nacional. Asimismo, establece que la Secretaría General evalúa los documentos y la opinión técnica cuando corresponda; y, tras verificar las características del evento internacional, elabora el proyecto de resolución para oficializar el evento internacional;

Que, mediante Ley N° 30096, se aprobó la Ley de Delitos Informáticos, cuyo objeto es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia;

Que, a través del Oficio N° 4173-2025-JUS/SG, de 17 de noviembre de 2025, el Ministerio de Justicia y Derechos Humanos solicitó al Secretario General del Ministerio de Relaciones Exteriores la oficialización del evento denominado "Congreso Internacional de Cibercrimen", presentado por la Presidencia de la Corte Superior de Justicia de Lima como fenómeno delictivo en una nueva era digital-tipologías, modalidades, nuevas figuras delictivas, estructuras delictivas-cibercriminalidad y seguridad ciudadana;

Que, asimismo, la Dirección General de Asuntos Criminológicos y la Oficina General de Asesoría Jurídica del Ministerio de Justicia y Derechos Humanos, a través del Informe N° 000463-2025-JUS/DGAC y Memorandum N° 916-2025-JUS/OGAJ, respectivamente, brindan opinión favorable a la oficialización del referido evento, al ser un espacio académico destinado a la actualización sobre los avances de la cibercriminalidad, fomentando así las capacidades de los funcionarios vinculados a la administración de justicia;

0 6 6 5

Resolución Secretaría General

Que, a través del Memorándum N° DGM024972025, de 24 de noviembre de 2025, la Dirección General para Asuntos Multilaterales y Globales del Ministerio de Relaciones Exteriores, estima que el mencionado Congreso contribuirá a consolidar la posición del Perú como un actor comprometido con la gobernanza digital y la lucha contra la ciberdelincuencia, en línea con los compromisos internacionales que el país ha asumido como Estado Parte del Convenio de Budapest, así como con el respaldo político expresado mediante la suscripción de instrumentos que aún no generan obligaciones jurídicas —como el Segundo Protocolo Adicional al Convenio de Budapest y la Convención de las Naciones Unidas contra la Ciberdelincuencia— pero que reflejan la voluntad del Perú de alinearse con sus estándares y avanzar hacia su futura implementación;

Que, mediante Resolución Ministerial N° 1012-2024-RE y modificatorias, se delegan facultades al titular de la Secretaría General, entre otros, para oficializar mediante resolución, el carácter internacional de eventos que se realicen en el territorio de la República en que participen delegaciones extranjeras, cuyo requerimiento provenga de entidades de la Administración Pública, incluyendo el Ministerio de Relaciones Exteriores;

Con los visados de la Dirección General para Asuntos Multilaterales y Globales y de la Oficina General de Asuntos Legales;

De conformidad con lo establecido en el numeral 8 del artículo 6 de la Ley N° 29357, Ley de Organización y Funciones del Ministerio de Relaciones Exteriores; el Decreto Supremo N° 001-2001-RE, modificado por Decreto Supremo N° 083-2016-RE, que establece disposiciones para el otorgamiento de carácter internacional a eventos que se realicen en el país con la participación de delegaciones extranjeras; el Texto Integrado del Reglamento de Organización y Funciones del Ministerio de Relaciones Exteriores, aprobado por Resolución Ministerial N° 0516-2025-RE; la Resolución Ministerial N° 0303-2017-RE, que aprueba la Directiva N° 004-2017-MIN-RE "Disposiciones para Oficializar Eventos Internacionales"; y, la Resolución Ministerial N° 1012-2024-RE y modificatorias;

SE RESUELVE:

Artículo 1.- Oficialización

Se oficializa el carácter internacional del evento denominado "Congreso Internacional de Cibercrimen", a realizarse en Lima, del 26 al 28 de noviembre de 2025, conforme los fundamentos expuestos en la parte considerativa de la presente resolución.

Artículo 2.- Financiamiento

La presente resolución no irroga gasto alguno al Pliego Presupuestal del Ministerio de Relaciones Exteriores.

Artículo 3.- Publicación

Se dispone la publicación de la presente resolución en la sede digital del Ministerio de Relaciones Exteriores de la Plataforma Digital Única del Estado Peruano (www.gob.pe/ree), para su difusión y cumplimiento.

Regístrese y comuníquese.

Eric Anderson Machado
Embajador
Secretario General
Ministerio de Relaciones Exteriores





Presidencia de la Corte Superior de Justicia de Lima

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la recuperación y consolidación de la economía peruana"

Lima, 21 de Octubre del 2025

RESOLUCION ADMINISTRATIVA N° 000867-2025-P-CSJLI-PJ



Firmado digitalmente por GAND
LOPEZ Miska Giovanna FAU
20546303651 soft
Cargo: Presidente De La Csj Lima
Motivo: Soy el autor del documento
Fecha: 21.10.2025 18:46:43 -05:00

VISTO:

El Oficio N.° 002-2025-SSPA-CSJL-PJ, de fecha 20 de octubre de 2025, cursado por el Presidente de la Séptima Sala de Apelaciones de esta Corte Superior de Justicia mediante el cual solicita se autorice la realización del "Congreso Internacional de Cibercrimen: *Nuevas figuras Delictivas – Procesamiento en Flagrancia*" documento ingresado el Sistema de Gestión Documental con número de Expediente N.° 45027; y,

CONSIDERANDO:

Primero. Es atribución de la presidencia de la Corte Superior de Justicia, dirigir la política interna de su distrito judicial de acuerdo a la política institucional en coordinación con el Consejo Ejecutivo del Poder Judicial, cautelar la pronta administración de justicia dictando para ello las medidas pertinentes para el adecuado funcionamiento de los órganos jurisdiccionales y administrativos de la Corte Superior de Justicia, así como ejercer las demás atribuciones que le confieren las leyes y los reglamentos, entre otras obligaciones, ello con la finalidad de brindar un eficiente servicio de administración de justicia en beneficio de los usuarios, tal como se encuentra previsto en el artículo 90 del Texto Único Ordenado de la Ley Orgánica del Poder Judicial.

Segundo. Que el Poder Judicial, en el marco de su política de gestión del conocimiento, promueve la organización de eventos académicos, congresos, seminarios, talleres y conferencias orientados al fortalecimiento de las competencias profesionales de magistrados, personal jurisdiccional y administrativo, contribuyendo con la mejora continua del servicio de justicia.

Tercero. En atención a la situación actual del país, considerando que el Perú ocupa el cuarto lugar entre los países de Latinoamérica que más ciberataques recibieron durante el año 2024, y ante la proyección de un incremento sostenido en el año 2025 y los siguientes años, este Distrito Judicial debe orientar sus capacitaciones hacia los desafíos que plantea esta nueva realidad social y tecnológica.

Cuarto. Mediante el Oficio de visto, el Presidente de la Séptima Sala de Apelaciones solicita a esta Presidencia la autorización para la realización del "*Congreso Internacional de Cibercrimen: Nuevas figuras Delictivas – Procesamiento en Flagrancia*" a efectuarse los días 26, 27 y 28 de noviembre del presente año, en la modalidad presencial en las instalaciones del edificio Carlos Zavala Loayza. Dicha actividad académica cuenta con el patrocinio del Consejo de Europa – *Global Action on Cybercrimen*, la Universidad Pontificia de Salamanca y el Instituto Iberoamericano de Justicia.





Presidencia de la Corte Superior de Justicia de Lima

Quinto. Que, de la revisión del Programa del "Congreso Internacional de Cibercrimen" elevado a esta Presidencia, se aprecia que el evento académico contará con la participación de dieciséis (16) expositores internacionales, nueve (9) expositores nacionales, así como diversos jueces, fiscales y catedráticos en calidad de panelistas, cuyas fechas, temas generales y horarios se detallan a continuación:

FECHAS	TEMAS GENERALES	HORARIOS
DÍA 1: Miércoles 26 de noviembre	"Cibercriminalidad como fenómeno delictivo de una nueva era digital"	8:30 am – 17:15 pm
DÍA 2: Jueves 27 de noviembre	"Tipologías, modalidades y estructuras delictivas"	8:30 am – 18:15 pm
DÍA 3: Viernes 28 de noviembre	"Cibercriminalidad y seguridad ciudadana"	8:30 am – 18:15 pm

Sexto. Que, el objetivo principal del Congreso Internacional es promover la prevención y el tratamiento especializado de la ciberdelincuencia, fomentar el análisis de nuevas figuras delictivas y contribuir a la formación y capacitación de jueces, juezas y servidores jurisdiccionales para fortalecer la respuesta institucional frente a la ciberdelincuencia. Así mismo, debido a la alta incidencia delictiva, esta requiere una mayor especialización en nuestra institución judicial, así como un mejor lineamiento y coordinación frente a esta serie de delitos que efectivice la persecución y sanción de los ciberdelitos, ello para garantizar la protección y seguridad ciudadana a través del Estado de Derecho.

Séptimo. Que, en concordancia con la política de esta Presidencia, se promueve la constante capacitación de los magistrados, personal jurisdiccional y administrativo de esta Corte Superior de Justicia en diversas áreas del conocimiento jurídico, técnico y ético, en coordinación con organismos nacionales e internacionales.

Octavo. Cabe señalar que una de las acciones estratégicas contempladas en el Plan de Trabajo de la presente gestión es promover una mejor y mayor capacitación de los magistrados y auxiliares jurisdiccionales de esta Corte Superior de Justicia. En ese sentido y atendiendo al programa del Congreso Internacional de Cibercrimen corresponde emitir el acto administrativo pertinente, garantizando en todo momento la continuidad del servicio de justicia en los órganos jurisdiccionales involucrados.

Por lo expuesto, en uso de las facultades conferidas por los incisos 1), 3) y 4) del artículo 90 del Texto Único Ordenado de la Ley Orgánica del Poder Judicial; y, por lo tanto:





Presidencia de la Corte Superior de Justicia de Lima

SE RESUELVE:

Artículo Primero. AUTORIZAR el "Congreso Internacional de Cibercrimen: Nuevas figuras Delictivas – Procesamiento en Flagrancia" a efectuarse los días 26, 27 y 28 de noviembre del presente año, en la modalidad presencial en las instalaciones del edificio Carlos Zavala Loayza.

Artículo Segundo. OTORGAR CARÁCTER OFICIAL al citado evento académico, disponiéndose su publicación en la página web institucional de esta Corte Superior de Justicia y en los demás medios de difusión correspondientes.

Artículo Tercero. DISPONER que la Gerencia de Administración Distrital de esta Corte Superior de Justicia brinde apoyo logístico necesario para la realización del referido evento.

Artículo Cuarto. PÓNGASE en conocimiento de la Gerencia de Administración Distrital, la Oficina de Imagen y Comunicaciones, al Presidente de la Séptima Sala de Apelaciones, de la Secretaría General y a las demás áreas interesadas.

Regístrese, comuníquese y cúmplase.

Documento firmado digitalmente

MILUSKA GIOVANNA CANO LOPEZ
Presidente de la CSJ Lima
Presidencia de la Corte Superior de Justicia de Lima

MCL/jpc





Presidencia de la Corte Superior de Justicia de Lima

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la recuperación y consolidación de la economía peruana"

Lima, 18 de Agosto del 2025



Firmado digitalmente por CANO
LOPEZ Miska Giovanna FAU
20546303951 soft
Cargo: Presidenta De La Csj Lima
Metodo: Soy el autor del documento
Fecha: 18.08.2025 15:51:51 -05:00

RESOLUCION ADMINISTRATIVA N° 000624-2025-P-CSJLI-PJ

VISTO:

El Informe de fecha 11 de junio de 2025 emitido por el Señor Juez Superior Bonifacio Meneses Gonzales – Presidente de la Séptima Sala Penal de Apelaciones de Lima; el Oficio Nro. 001325-2025-UPD-GAD-CSJLI-PJ, de fecha 5 de agosto de 2025, emitido por la Unidad de Planeamiento y Desarrollo; el Oficio S/N-2025-7SPA-CSJLI/PJ de fecha 11 de agosto de 2025, emitido por la Coordinación de las Salas Penales del Subsistema de Corrupción de Funcionarios de la Corte Superior de Justicia de Lima; y,

CONSIDERANDO:

Primero. Mediante Informe S/N-2025-ADM-UAF-GAD-CSJLI-PJ, de fecha 11 de junio de 2025, el Juez Superior Bonifacio Meneses Gonzales – Presidente de la Séptima Sala Penal de Apelaciones de Lima, concluyó, entre otros, que la implementación de órganos especializados en cibercrimen es imprescindible para afrontar eficazmente los delitos informáticos, garantizar la seguridad jurídica, eficiencia y legitimidad del sistema judicial, además de contribuir a la protección de derechos en el ciberespacio. En tal sentido, recomendó, entre otros, crear órganos especializados en cibercriminalidad y ciberdelitos, iniciando por Lima Metropolitana.

Segundo. Asimismo, a través del Oficio S/N-2025-7SPA-CSJLI/PJ de fecha 11 de agosto de 2025, la Coordinación de las Salas Penales del Subsistema de Corrupción de Funcionarios de la Corte Superior de Justicia de Lima, presidida por el Juez Superior Bonifacio Meneses Gonzales, solicitó la conformación de la comisión de implementación de los Juzgado Penales con Subespecialidad en Ciberdelitos, con la propuesta de posibles integrantes:

- Juez Superior Titular Bonifacio Meneses Gonzales – Presidente
- Jueza Superior Titular Aissa Rosa Mendoza Retamozo
- Juez Superior Titular Manuel Antonio Chuyo Zavaleta
- Juez Superior Titular Robinson Ezequiel Lozada Rivera
- Jueza Superior Titular Lisdey Magaly Bueno Flores
- Servidora Haydee Luisa Barreto Polo – Secretaria Técnica

Tercero. Mediante Oficio Nro. 001325-2025-UPD-GAD-CSJLI-PJ, de fecha 5 de agosto de 2025, la Unidad de Planeamiento y Desarrollo manifestó la necesidad de incorporar a dicha unidad y a la Coordinación de Estudios y Proyectos dentro de la referida Comisión, a fin de asegurar un adecuado soporte técnico y administrativo para el diseño y puesta en marcha de los órganos jurisdiccionales especializados.





Presidencia de la Corte Superior de Justicia de Lima

Cuarto. El vertiginoso avance de las tecnologías de la información y comunicación ha generado nuevas formas de criminalidad que trascienden las fronteras físicas, constituyendo los llamados delitos informáticos o ciberdelitos. Estos delitos atentan afectan gravemente bienes jurídicos protegidos como la intimidad, el patrimonio, la seguridad pública y el correcto funcionamiento de las instituciones.

Quinto. El informe citado advierte las carencias del sistema de justicia frente a la cibercriminalidad, lo que genera riesgos de impunidad, sobrecarga procesal y desprotección de derechos fundamentales, siendo urgente la implementación de órganos jurisdiccionales especializados capaces de aplicar con eficacia las herramientas procesales disponibles para enfrentar la creciente sofisticación de los ataques informáticos.

Sexto. Los datos estadísticos en el Perú evidencian un incremento sostenido de la ciberdelincuencia, lo que ocasiona un impacto negativo en la seguridad ciudadana y sobrecarga en el sistema penal. La falta de jueces capacitados y de un marco normativo integral en materia de ciberseguridad contribuye a la impunidad, al archivo prematuro de procesos y a la falta de un seguimiento adecuado de las investigaciones fiscales.

Séptimo. A diferencia de otros países de la región, el Perú carece de protocolos y estrategias judiciales específicas frente a la ciberdelincuencia, lo cual limita la coordinación interinstitucional con la Policía Nacional del Perú y el Ministerio Público, que ya cuentan con unidades especializadas en investigación de ciberdelitos.

Octavo. Informes técnicos y encuestas realizadas a fiscales han puesto en evidencia las dificultades del sistema de justicia para procesar eficazmente los delitos informáticos, debido principalmente a la insuficiente capacitación de magistrados, lo cual obstaculiza la admisión y valoración de pruebas digitales y afecta la legitimidad del sistema penal frente a estos fenómenos criminales.

Noveno. En ese contexto, la implementación de órganos jurisdiccionales especializados en ciberdelitos permitirá:

- Elevar el estándar de capacitación técnica y jurídica de los magistrados y personal jurisdiccional.
- Garantizar una adecuada coordinación con las unidades de investigación de la Policía Nacional del Perú, el Ministerio Público y organismos internacionales especializados en criminalidad informática.
- Homogeneizar criterios jurisprudenciales que fortalezcan la seguridad jurídica y la tutela efectiva de los derechos fundamentales en el entorno digital.
- Responder a la creciente demanda ciudadana de un Poder Judicial moderno, capaz de enfrentar los desafíos de la era digital con eficacia y transparencia.

Décimo. De acuerdo con el artículo 72 y los incisos 1), 3) y 4) del artículo 90 del Texto Único Ordenado de la Ley Orgánica del Poder Judicial, así como con los artículos 8 y 9 del Reglamento de Organización y Funciones de las Cortes Superiores de Justicia que





Presidencia de la Corte Superior de Justicia de Lima

operan como Unidades Ejecutoras, aprobado por Resolución Administrativa Nro. 090-2018-CE-PJ, corresponde al Presidente de la Corte Superior de Justicia dirigir y representar al Distrito Judicial, así como adoptar las medidas necesarias para garantizar un adecuado servicio de administración de justicia.

Décimo primero. Consecuentemente, la Presidencia de la Corte Superior de Justicia de Lima, en su calidad de máxima autoridad administrativa, dirige la política interna de esta Corte Superior de Justicia con el objetivo de brindar un eficiente servicio de administración de justicia en beneficio de los justiciables, encontrándose facultada para adoptar las medidas de orden administrativo correspondientes en aras de mejorar y optimizar su funcionamiento.

Por lo expuesto, en uso de las facultades conferidas por los incisos 1) 3), 4) y 9) del artículo 90 del Texto Único Ordenado de la Ley Orgánica del Poder Judicial:

SE RESUELVE:

Artículo Primero: CONFORMAR la Comisión de Implementación de los Juzgado Penales con Subespecialidad en Ciberdelitos de la Corte Superior de Justicia de Lima, la misma que estará integrada por:

1. Juez Superior Titular Bonifacio Meneses Gonzales – Presidente
2. Jueza Superior Titular Aissa Rosa Mendoza Retamozo
3. Juez Superior Titular Manuel Antonio Chuyo Zavaleta
4. Juez Superior Titular Robinson Ezequiel Lozada Rivera
5. Jueza Superior Titular Lisdey Magaly Bueno Flores
6. Jefe de la Unidad de Planeamiento y Desarrollo
7. Coordinador(a) de Estudios y Proyectos
8. Servidora Haydee Luisa Barreto Polo – Secretaria Técnica

Artículo Segundo: DISPONER que la referida Comisión conjuntamente con la Jefatura de la Unidad de Planeamiento y Desarrollo de la Corte, elaboren en un plazo máximo de siete (07) días útiles, el Plan de Implementación de los Juzgados Penales con Subespecialidad en Ciberdelitos, que deberá incluir: diagnóstico situacional, justificación técnica, propuesta de estructura orgánica, requerimiento de recursos humanos y tecnológicos, cronograma de ejecución, así como estimación presupuestal, a fin de que esta Presidencia apruebe oportunamente dicho Plan, así como efectúe las gestiones correspondientes ante el Consejo Ejecutivo del Poder Judicial y demás instancias competentes, orientadas a viabilizar la creación y puesta en funcionamiento de los referidos órganos jurisdiccionales.

Artículo Tercero: AUTORIZAR a la Comisión para coordinar con las áreas y dependencias que resulten competentes, a efectos de adoptar las acciones administrativas y técnicas orientadas a viabilizar la creación de los referidos órganos jurisdiccionales.





Presidencia de la Corte Superior de Justicia de Lima

Artículo Cuarto: DISPONER que la Unidad de Planeamiento y Desarrollo, a través de la Coordinación de Estudios y Proyectos, brinde el apoyo técnico a la referida comisión para posibilitar la ejecución de la mencionada implementación.

Artículo Quinto: PONER la presente resolución administrativa en conocimiento del Consejo Ejecutivo del Poder Judicial, Oficina Descentralizada de la Autoridad Nacional de Control de Lima, la Gerencia de Administración Distrital, la Unidad de Planeamiento y Desarrollo, la Coordinación de Estudios y Proyectos, a los magistrados involucrados, para los fines pertinentes.

Regístrese, publíquese, comuníquese y cúmplase.

Documento firmado digitalmente

MILUSKA GIOVANNA CANO LOPEZ

Presidenta de la CSJ Lima

Presidencia de la Corte Superior de Justicia de Lima

MCL/smv



DECLARACION DE LIMA

Primer Congreso Internacional de Cibercrimen, Inteligencia Artificial y nuevas figuras delictivas.

Nosotros, los expositores, investigadores, operadores de justicia, académicos y profesionales asistentes al **Primer Congreso Internacional de Cibercrimen**, reunidos en la ciudad de Lima entre los días 26 y 28 de noviembre, declaramos lo siguiente:

PRIMERO.

Reconocemos la creciente complejidad, transnacionalidad y acelerada evolución del cibercrimen, fenómeno que exige respuestas jurídicas, técnicas y operativas integrales, coordinadas y basadas en evidencia científica.

SEGUNDO.

Afirmamos la importancia de fortalecer las capacidades institucionales del sistema de justicia, la Policía Nacional, el Ministerio Público, el Poder Judicial y todos los organismos vinculados, para enfrentar eficazmente los delitos informáticos mediante investigación avanzada, ciberinteligencia y técnicas forenses especializadas.

TERCERO.

Declaramos que la cooperación internacional es un pilar esencial para la persecución del cibercrimen. Los Estados deben promover acuerdos, mecanismos de asistencia mutua, intercambio de información y protocolos de actuación conjunta.

CUARTO.

Ratificamos nuestro compromiso con la protección del ciudadano digital, la defensa de los derechos fundamentales, la privacidad, la seguridad de los datos personales y el fortalecimiento de la confianza en los entornos tecnológicos.

QUINTO.

Promovemos la armonización normativa en materia de delitos informáticos, inspirada en buenas prácticas regionales y en estándares internacionales, como el Convenio de Budapest y otros instrumentos que permitan mejorar la seguridad jurídica en el ciberespacio.

SEXTO.

Reafirmamos la importancia de la capacitación continua, la investigación científica, la

difusión del conocimiento técnico y la creación de redes multidisciplinarias que integren a jueces, fiscales, policías, peritos, académicos y sector privado.

SÉPTIMO.

Reconocemos el esfuerzo de las instituciones organizadoras y anfitrionas, cuya labor permitió el diálogo abierto, el intercambio de experiencias y la construcción de consensos para enfrentar de manera conjunta los retos del cibercrimen.

OCTAVO.

Invocamos al Poder Legislativo y Poder Ejecutivo del Perú, la conformación e implementación de los Juzgados de Ciber Crimen a nivel nacional, que se unan al esfuerzo de la Dirección de la Policía Nacional del Perú de Ciber Crimen y la Fiscalía Especializada en Ciber Criminalidad.

Por todo lo expresado, emitimos la presente **DECLARACIÓN DE LIMA**, como compromiso y hoja de ruta para avanzar hacia un país y una región más segura, resiliente y preparada ante las amenazas digitales.

Lima, 28 de noviembre.

VICTOR ROBERTO PRADO SALDARRIAGA – Juez Supremo Titular

MILUSKA CANO LOPEZ – Presidenta de la Corte Superior de Justicia de Lima.

BONIFACIO MENESES GONZALES – Juez Superior.

AURORA REMEDIOS FATIMA CASTILLO FUERMAN – Fiscal Superior

DINO CARLOS CARO CORIA – Jurista Especialista en ciber crimen

RICARDO ELIAS PUELLES – Jurista Especialista en ciber crimen

MARIO YUNIS ARROYO – Ing. Especialista en ciberseguridad e IA

CRISTOS VELAZCO SAN MARTIN. ALEMANIA

MARÍA DE LOURDES GUTIÉRREZ ORTIZ MONASTERIO - ONU

ROSA MARIA TOME GARCIA – ESPAÑA.

ANTONI BOSCH PUJOL – ESPAÑA.

LUIS CARLOS CABALLERO CABALLERO – ESPAÑA.

CARLOS TOMAS ALVEAR PEÑA. – ECUADOR.

JULIO AGUAYO URGILES – ECUADOR.

DANIELA SILVIA DUPUY – ARGENTINA.

JUAN CARLOS CARRETERO – ARGENTINA.

MAURICIO GARRO GUILLEN - COSTA RICA.

LUIS JORGE GAMBOA OLEA - MEXICO.

DAVID GUTIERREZ CASTAÑO - COLOMBIA.

JAIME VERA VEGA - CHILE.

LAURA MAYER LUX - CHILE.

INTRODUCCION

Las conductas cometidas a través de la tecnología, sistemas informáticos y comunicaciones como amenazas a través del ciberespacio es una conminación de un peligro constante y creciente que se encuentra bajo una tenaz y prolongada evolución, siendo el Perú un país que posee distintas tipologías criminológicas en cibercrimen, por lo tanto se encuentra ubicado en el cuarto país de Latinoamérica que más ciberataques recibieron durante el año 2024, con dirección a un consistente crecimiento en el año 2025 y próximos años, donde las autoridades cuentan con la tarea de responder a las demandas de los ciudadanos frente a estas nuevas figuras delictivas.

Es así que, el avance de la ciencia y nuevas tecnologías ha originado el estallido de nuevas conductas y modalidades criminales, por cuanto resulta necesario realizar una formación, estudio y tratamiento situacional multisectorial, con la finalidad de entender los factores que facilitan e impulsan la comisión de este tipo de delitos.

Ante la búsqueda de hacer frente a los delitos informáticos el estado peruano adecuo y adopto de forma progresiva el tratado de Budapest a la Ley 30096, como garantía de los derechos del ciudadano contra las actividades delictivas en línea que acarrea una implementación de normas, métodos, herramientas y procedimientos para garantizar el estado de derecho; empero, en el Perú existe una gran cantidad de delitos informáticos denunciados ascendiente a 19651 denuncias de enero a junio de 2025, siendo el 75% por fraude informático, 13% por suplantación de identidad, 6% por delitos contra datos y sistemas informático y 6% ciberviolencia, lo que demuestra el crecimiento constante y exorbitante de hechos ilícitos cometidos en el ciberespacio; sin contar con la cantidad de delitos que no son denunciados debido a la intemporalidad, territorialidad, fatal de confianza en las autoridades que persiguen el delito, imagen hacia el público (cuando hablamos de empresas o corporaciones) -a la que llamamos cifra negra-.

Asimismo, a pesar de contar con adecuadas técnicas de investigación realizadas entre la DIVINDAT y la Fiscalía Especializada en Cibercrimen, para prevenir, contrarrestar y combatir el impacto de la criminalidad, existen limitaciones por el servicio de administración de justicia -Poder Judicial-; respecto al análisis típico, confundido e interpretativo del hecho factico y jurídico, cuyo resultado demuestra que la Corte Superior de Justicia de Lima conforme al cuadro estadístico del módulo penal cuenta 4968 expedientes, de las cuales 1954 están archivadas por desconocimiento de conductas enmarcadas en delitos informáticos.

En esa misma línea, urge una respuesta especializada, técnica, preparada y rápida del sistema de justicia peruano, que genere el mejoramiento y correcto análisis de conductas enmarcadas en la delincuencia informática, ya que no se viene llevando a cabo una correcta formación para contar con jueces preparados en uso y manejo de información, generando así una deficiencia operativa sobre el manejo de información que hace que se dificulte las acciones preventivas y de sanción.

Es de poner en contexto, que el creciente beneficio de uso de la tecnología de la información y sus comunicaciones ha generado una dependencia de los ciudadanos, instituciones publica, empresas privadas y servicios públicos que vienen siendo víctimas de perpetradores informáticos que se han logrando filtrar de sistemas de defensa nacional,

exponiendo al estado peruano a amenazas internacionales, pudiéndonos referir a las siguientes: ataques a las páginas web y sistemas informáticos de instituciones públicas (Poder Judicial – Presidencia de la Republica – Ministerio Publico - Ministerio de Trabajo y Promoción del Empleo – Essalud – entre otras).

Ello refiere, que el Sistema de Administración de Justicia cuenta con dificultades obstructivas que complica la investigación y enjuiciamiento de este tipo de delitos ya que la falta de capacitación de jueces genera una negativa ante la tipificación del delito, medidas cautelares, medios probatorios ante un debate judicial; por lo tanto, para mejorar su respuesta existe la necesidad inmediata de creación de juzgados especializados en cibercrimen.

No podemos dejar de agradecer el apoyo de distinguidos Magistrados que no obstante que para su realización no tuvimos el apoyo interno a fin de concretizar como evento de raigambre mundial, pusieron el coto y sensibilidad académica que en efecto pudimos advertir la realización de tan memorable Congreso Internacional, reconocido por las instituciones internacionales como el mejor certamen de ciber crimen en el año 2025.

Por ello mas que un saludo un homenaje por el desprendimiento y apoyo a las Magistradas:

Aissa Rosa Mendoza Retamozo
María de los Ángeles Álvarez Camacho
Loretta Monzón Valencia
Glenda Morella Zegarra Bravo
Carmen Castañeda Pacheco
Rocio Quilca Molina
Yesica Lourdes Bahamondes Hernández.
Lisdey Magaly Bueno Flores.

A todo el personal jurisdiccional de la Séptima Sala Penal de Apelaciones de la Corte Superior de Justicia de Lima.

FINALIDAD

Es generar la prevención idónea ante los avances de la cibercriminalidad, para proponer un cambio y contribución en la materia con la formación y capacitación de jueces y personalidad jurisdiccional para el tratamiento de la ciberdelincuencia, ante tal gran cantidad de delitos informáticos archivados por diferentes motivos que generan un paraíso de impunidad, lo que nos hace llegar a la conclusión que los jueces especializados en delitos comunes no se encuentran suficientemente formados para luchar contra este nuevo tipo de criminalidad; motivo por el cual, genera una brecha que limita la capacidad de resolver los casos con eficiencia, genera sobrecarga, conduce a decisiones injustas o erróneas, sobre lineamientos de una nueva era digital – seguridad ciudadana y ciberespacio.

Además, respecto a los estudios criminológicos de la actividad delictiva en delitos informáticos, existe una gran problemática que genera que el cibercrimen sea tan tentador en el Perú, considerando que existen factores que permiten facilitar la comisión del delito, ello nos lleva a falta de conocimiento sobre determinados temas que genera la existencia de una o varias posibilidades que puedan ser aprovechadas por los ciberdelincuentes con la finalidad de generar un provecho ante la mala interpretación de la norma.

Por cuanto, la alta incidencia delictiva, esta requiere una mayor especialización en nuestra institución judicial, así como un mejor lineamiento y coordinación frente a esta serie de delitos que efectivice la persecución y sanción de los ciberdelitos, ello para garantizar la protección y seguridad ciudadana a través del estado de derecho.



PRIMER DIA

“PALABRAS DE BIENVENIDA Y PRESENTACION AL PRIMER CONGRESO INTERNACIONAL DE CIBERCRIMEN”

Dra. MILUSKA GIOVANNA CANO LÓPEZ
Presidenta de la Corte Superior de Justicia de Lima



Brinda sus respetuosos saludos al señor Dr. Víctor Roberto Prado Saldarriaga Juez Supremo de la Republica, al señor Dr. Bonifacio Meneses Gonzales Presidente de la Comisión del Congreso Internacional de Cibercrimen así como a todas las autoridades que han concurrido de manera presencial y virtual ante tan magno evento; en esa misma línea, saluda a cada uno de los expositores ilustres y juristas de distintos países hermanos como Alemania – España – México – Argentina – Ecuador – Colombia – Panamá – Chile – Costa Rica; de igual modo a nuestros expositores y panelistas nacionales quienes nos representan con su conocimiento en a especialidad ante el Primer Congreso Internacional de Cibercrimen como fenómeno delictivo de una nueva era digital, tipologías, modalidades, nuevas figuras y estructuras delictivas, cibercriminalidad y seguridad ciudadana como coyuntura de carácter nacional e internacional que ataña la seguridad ciudadana; ya que sin la presencia no sería posible el presente simposio, que representa un gran paso en el avance de la lucha contra la criminalidad organizada a través del uso de las tecnologías información y comunicaciones, que viene azotando nuestro país, de manera tal que todos los operadores de justicia y la sociedad en su conjunto debemos estar alertas y afrontar desde nuestras posiciones una lucha frontal contra esta criminalidad, con la búsqueda de soluciones y mecanismos normativos como operadores de justicia.

“PALABRAS INAUGURALES DEL PRIMER CONGRESO INTERNACIONAL DE CIBERCRIMEN”

Dr. VICTOR ROBERTO PRADO SALDARRIAGA

Juez Supremo de Justicia de la Republica del Perú
Presidente del Grupo de Alto Nivel para la
Aplicación de la Pena Justa y Contra la
cibercriminalidad Organizada



Dirige sus saludos a la Dra. Miluska Giovanna Cano López quien es Presidenta de la Corte Superior de Justicia de Lima, al señor Dr. Bonifacio Meneses Gonzales Presidente de la Comisión del Congreso Internacional de Cibercrimen, así como a los señores y señoras Presidentes (as) de las distintas Cortes Superiores, a los colegas de las distintas instancias que se han dado espacio para poder acompañar y seguir de cerca la presentación de los señores expositores extranjeros, a quienes se agradece la gentileza de asistir al Perú para regalarnos sus conocimientos, experiencias, aporte en el análisis, desarrollo y herramientas que debemos implementar desde los sistemas de justicia para hacer frente a esta nueva tipología de criminalidad organizada que se desarrolla en el ciberespacio a lo largo de estas tres jornadas; que marcará de alguna manera la posibilidad de entender la gramática experiencia de la virtualización, de los contactos sociales, relaciones económicas y claro esta la nueva modalidad de modus operandi de la criminalidad organizada, que como criminalidad vinculada a la creación de mercado de espacios para la producción, distribución, circulación, comercialización de bienes y servicios ilegales necesitaba tener una salida que fue encontrada en el ciberespacio, que fue generando una dinámica social muy diferente a la que nos estamos adaptando todos y dentro de ese proceso hemos conocido la presencia múltiple de tipológicas que van desde lo que podríamos llamar delitos comunes hasta las expresiones tan graves que comprometen infraestructura crítica, seguridad de los estados y que se han potenciado con el apoyo de la inteligencia artificial; por lo que es de señalar que en el presente congreso tendremos la oportunidad de mirar de cerca lo que ya en el devenir de algunos años se ha convertido en alguna realidad patente para muchos países y que genera unos de los desafíos mas trascendentes y urgentes para los países latinoamericanos y específicamente para el nuestro, donde si

“La Justicia es la reina de las virtudes republicanas y con ella se sostiene la igualdad y la libertad”

bien hemos contado con esfuerzos en la presente década, no han alcanzado los estándares que nos aproximen a la realidad actual del problema en el Perú; en ese mismo orden, es de esencial importancia verificar si se logró la eficacia de las distintas unidades del sistema penal de control, con una necesidad urgente de transformar nuestra actividad en estas distintas unidades con la inter operatividad que permita justamente cubrir el panorama de la ciberdelincuencia que hoy preocupa a todos; como es el hecho de avanzar a menor intensidad en el espacio de la justicia penal, en el ámbito concreto de la actividad jurisdiccional; y, es por ello que le complace mucho que la Corte Superior de Justicia haya tenido la presente iniciativa, agradeciendo a las Naciones Unidas ya que permitió que el Perú participe directamente en lo que fue y hoy es la convención de la Ciberdelincuencia donde Perú tuvo un aporte como es el de incluir de manera expresa los activos virtuales, por todas esas razones es grato dar por inaugurado el presente Congreso Internacional de Cibercrimen, Inteligencia Artificial y Nuevas Figuras Delictivas.

“RENIEC: PRESERVACIÓN Y PROTECCIÓN DE DATOS ANTE EL CIBERCRIMEN”

Dra. CARMEN MILAGROS VELARDE KOECHLIN

Jefa Nacional del Registro Nacional de Identificación y Estado Civil de Perú - RENIEC

¿Está preparado el Estado para luchar contra el cibercrimen? Para ello debemos analizar la vulnerabilidad de las instituciones peruanas, focalizadas en la medida de implementación y desafíos frente a una adecuada normatividad y falta de preparación efectiva para proteger los datos personales; es así que, de la evaluación y análisis profundo del Registro Nacional de Identificación y Estado Civil, se ha confirmado que de enero a noviembre de 2025 hemos sido blanco de 94.6 millones de ataques informáticos que se ha podido llegar a repeler y bloquear, lo que representa cuatro veces más que los 20 millones registrados en el año 2024; por consiguiente, el Jefe de la oficina de tecnología de la información ya ha previsto que para las elecciones muy probablemente seremos víctimas de hacker con la finalidad de querer hacer caer los sistemas de nuestra institución, para la obtención del registro único de identidad de personas naturales de la cual están inscritos todos los peruanos mayores y menores de edad, que cuentan con Documento Nacional de Identidad, ello con el objetivo de que algunos partidos políticos puedan realizar su marketing y enviar publicidad o en el caso de los cibercriminales usurpar identidades para cometer fraudes, por estas consideraciones es de sugerir la implementación del delito de “receptación digital”, para castigar a quienes compran registro de datos obtenidas ilegalmente; en esa misma línea, también se debe de genera una mayor protección respecto al acceso legal que a través de las normas se generan convenios con terceros como es el caso de notarias, bancos, empresas de telecomunicaciones y entidades del estado, entre otras, para evitar exposiciones del registro de datos internos a terceros por la obtención de tu huella digital o libre acceso; así también, es de dar conocer que el Perú a través de la Secretaría de Gobierno y Transformación Digital generó la creación de normas para implementar la plataforma de interoperatividad del Estado para un mejor servicio, sin tomar en cuenta el principio de protección de datos personales; entonces, lo que sucede es que tenemos normas que nos exigen un acceso legal sin la debida protección de las mismas, es en ese sentido que RENIEC para cuidar los datos personales se encuentra eliminando y reduciendo los convenios de servicios en línea, es el caso que antes contábamos con al menos 6500 convenios, de los cuales ahora se tiene 2918 convenios por ley, toda vez que muchos no tienen por qué tener servicio en línea por ser indebidamente utilizados motivo por el cual se cortó el acceso a más de 32000 usuarios que han utilizado mal el servicio, en consecuencia estamos tratando de lograr que ya no haya más convenios, debiendo masificarse el DNI electrónico para que la identificación se lleve a cabo por intermedio del chip que también contiene la huella digital registrada.



Es de informar que la RENIEC se encuentra enviando cartas a las instituciones públicas y privadas remitiendo la información de determinadas personas que se encuentran sustrayendo datos de terceros para luego venderlas a través del Telegram, y así se les pueda apertura procedimientos administrativos, del mismo modo solicita que medidas y medios de seguridad se encuentran utilizando para que este tipo de sucesos no vuelva a ocurrir; es en ese mismo sentido que para evitar ese tipo de sucesos es que se creó la plataforma IDPERÚ (plataforma de identidad digital), la cual te permite que con las facciones de tu rostro o tu DNI electrónico pueda reconocer e identificar quien fue la persona que realizo la consulta y garantizar la identidad de todos los peruanos, actualmente 23 entidades públicas vienen utilizando el IDPERÚ, existen 5 millones de consultas, 50 servicios integrados en acceso de certificados digitales (naturales y jurídicos), 3.4 millones de soles invertidos en licencias para prueba de vida. Además, la RENIEC cuenta con el nuevo certificado C4, que lo que se pretende es eliminarlo progresivamente, este certificado anteriormente contenía 13 tipo de datos, lo cuales han sido reducidos a 6, generando la restricción a los usuarios ya que para poder acceder a ellos tienen que requerirlos utilizando sus datos personales o uno mismo.

La RENIEC a través del ABIS a creado una vigilancia activa con optimización del Firewall de aplicaciones web (WAF), implementando centro de operaciones de seguridad, con una red de vigilancia que verifica un control biométrico inmediato, con más de 900 ventanillas con captura en vivo con optimización de los procesos de captura de datos e imágenes para reducir el riesgo de suplantación, centros de cómputo para el DNI electrónico, tablets de identificación con nuevos filtros y software para seguridad de la información, logrando así bloquear más de 416 mil casos de identidad irregular entre el 2020 y 2024; finalmente, ya se tiene el DNI 3.0 que es el más seguro en todo Sudamérica que contiene foto protegida por dispositivo holográfico con permutación de colores, chip electrónico con datos biográficos y biométricos, interfaz dual para identificación digital, 64 llaves de seguridad, imágenes de costa - sierra - selva en offset y grabado láser, tinta ópticamente variable, imagen láser múltiple de foto miniatura, diseño de seguridad UV invisible para lograr una mayor seguridad ante la vulneración de datos personales.

“EL PACCTO (EUROPA LATINOAMERICA PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO). DELITOS ASISTIDOS MEDIANTE INTELIGENCIA ARTIFICIAL: HACIA UN MARCO REGIONAL SOBRE IA Y JUSTICIA PENAL PARA AMERICA LATINA”

Dr. CRISTOS VELASCO SAN MARTIN

Abogado y Doctor en Derecho, especialista en ciberdelincuencia, ciberseguridad, inteligencia artificial y protección de datos, asesor del sistema de justicia en 18 países y profesor de la Universidad Duale Hochschule Baden-Württemberg (Alemania).

El Perú según las estadísticas de ciberdelitos, sigue apareciendo como uno de los cuatro países más atacados a nivel mundial incrementándose cada vez su actuar delictivo, generándose una mayor repercusión cuando es utilizada la inteligencia artificial a través del crimen organizado, lo que conlleva que el costo de ciberdelitos a nivel mundial alcanzara los USD \$ 13,82 billones de dólares para el año 2028. Respecto a la inteligencia artificial y delitos cometidos a través de sistemas, el año pasado en Costa Rica se realizó el reporte de inteligencia artificial y crimen organizado en el que se identificó muchas tendencias de delitos con uso de sistemas de inteligencia artificial en Europa y Latinoamérica, generándose la recomendación de que se tenía que fortalecer el marco jurídico relacionados con delitos informáticos (los códigos penales tanto sustantivos como procedimentales de los países de Latinoamérica debiendo ser utilizados para incluir delitos o circunstancias agravantes relacionadas al uso malicioso de la IA, como la generación y difusión de deepfakes, la manipulación algorítmica y el fraude automatizado); así como el fomento de la colaboración pública y privada para establecer alianzas entre las empresas tecnológicas y proveedoras de servicios digitales con el sector público para desarrollar soluciones tecnológicas que puedan identificar y bloquear contenidos maliciosos, debiéndose compartir la información sobre amenazas emergentes; asimismo, se propició el fortalecimiento y creación de unidades especializadas dentro de las fuerzas del orden dedicadas exclusivamente al cibercrimen y al uso indebido de la IA como una propuesta más rápida y efectiva; de esa manera es propicio generar estrategias nacionales sobre la IA y sub-estrategias para autoridades de seguridad, justicia y el poder judicial que contengan objetivos y metas específicas que sean medibles en la implementación y el uso de sistemas de la IA por parte de las autoridades de justicia y el poder judicial, en ese mismo contexto implementar programas de formación para desarrollar los conocimientos y habilidades necesarias para aprovechar la IA para generar un enfoque unificado de la adopción de la IA.

El reporte del Pacto 2.0 como instrumentalización de la inteligencia artificial ante la



delincuencia en el mundo, a identificado que el crimen organizado utiliza el manejo de “drones automatizados” que son empleados para el transporte de la droga y direccionar ataques a gran escala, de ejemplo tenemos que el cartel de Jalisco Nueva Generación que cuenta con elementos especializados en manejo de drones para el transporte de la droga y para dirigir ataques a otros grupos; es así que, en el año 2025 se reportó un ataque con un dron contra la fiscalía de Baja California en Tijuana, atribuido al CJNG; como otro ejemplo tenemos que el Comando Vermelho ha empleado drones para responder a operativos policiales con ataques violentos usando explosivos y armamento pesado donde murieron más de 150 persona en noviembre de 2025; otra de las herramientas imprescindibles para los ciberdelincuentes es el “malware polimórfico” es el tipo de software malicioso que cambia su código y apariencia digital que dificulta la detección y bloqueo por parte de los antivirus tradicionales toda vez que se encuentra en constante mutación y técnicas de ofuscación de código para alterar su estructura, tal es el caso que las estadísticas recientes demuestran que el 41% de las familias ransomware en 2025 incluyeron módulos de IA adaptativos y la mutación de código dio lugar a un promedio de 21 variantes por familia de malware identificados, a su vez la IA generativa puede automatizar ataques, identificar vulnerabilidades de seguridad e inclusive gestionar el pago de rescate de la información comprendida y cifra en ataques de ransomware, es en ese sentido que, conforme al estudio de MIT Sloan 2025 muestra que el 80% de los ataques recientes de ransomware examinados utilizaron IA desde ingeniería social basada en deepfakes hasta phishing generados por IA y cifrados automáticos de contraseñas a mayor escala y con gran sofisticación; otro de los mecanismos es por medio de los ataques de generación de servicio distribuido (DDoS), delitos financieros, estafas y fraudes financieros (criptofraude), herramientas delito como servicio (CasS) esta última cuenta con disponibilidad de red abierta siendo utilizada para generar correos electrónicos phishing, generar malware a tiempo real, implementar ransomware y para eludir los sistemas de detección tradicional; asimismo, este se encuentra alojado en servidores propios y es accesible a través de GitHub, Youtube y Discord, encontrándose disponible por USD \$ 200 (versión de bot de Telegram) o USD \$ 300 (versión de aplicación web), este servicio proporciona la orientación sobre la orientación de armas nucleares; antes tales tendencias delictivas el Paccto con otros expertos en consulta con los países que forman parte del proyecto se dedicaron a elaborar una Ley Regional sobre Inteligencia Artificial Aplicada a Justicia y Seguridad que ofrece un análisis exhaustivo de los principales delitos cometidos con herramientas de IA, casos actuales y ejemplo de tipologías de delitos; así como, el reporte, mapeo y perfilamiento de las redes criminales más amenazadoras de América Latina y el Caribe en EL PACCTO, así también brinda antecedentes y justificación sobre amenazas emergentes en la UE, un marcos legales que permita a los países integrar un marco normativo y jurídico según sus necesidades específicas, como una ley especial independiente o generar futuras reformas a la legislación penal sustantiva o procesal a nivel nacional para contrarrestar el uso de sistemas de IA con fines delictivos y maliciosos por parte de grupos delictivos organizados que operan y atacan a víctimas ubicadas en los países ALC.

“LA COMPLEJIDAD PARA INVESTIGAR LOS CIBERDELITOS – EL DECIDIDO APORTE DE LA FISCALIA PARA SU INVESTIGACIÓN”

Dra. DANIELA SILVIA DUPUY

Fiscal coordinadora de la Unidad Especializada en Delitos y Contravenciones Informáticas del Ministerio Público de la Ciudad de Buenos Aires (UFEDyCI), Doctora en Derecho Penal y Procesal, Directora de Postgrado Iberoamericano en Cibercrimen y Evidencia Digital.

La dinámica del Cibercrimen y su constante evolución, ha propiciado que delincuentes que hace poco actuaban de manera aislada, sin coordinación, con alcance local, en la actualidad formen parte de organizaciones transnacionales complejas de cibercrimen, que conlleva a la fiscalía en la que trabaja a contar con apoyo institucional y trabajo conjunto con la policía especializada para gestionar la cantidad de casos que ingresan a la Republica de Argentina con autores diseminados en diferentes países y víctimas en otros y evidencia digital alojada en extraña jurisdicción donde se encuentran empresas de comunicantes y apps internacionales a quienes se les pide constantemente información para llevar adelante las investigaciones, de ejemplo tenemos Microsoft, Twitter, Tik Tok, Meta, etc; pero la mayoría de esas empresas cuentan con distintas sucursales que tienen alojados todos los datos que requiere la fiscalía para realizar las investigaciones y aquí es donde viene el reto que comprende la territorialidad y soberanía nacional, por lo que se requiere a las empresas a través de tratados de cooperación internacional entre estados tengan mayor accesibilidad, a fin de evitar un plazo muy prolongado para la obtención de la evidencia y no tarde tanto tiempo para llegar al Juez y así impedir que la prueba de haya perdido teniendo el inconveniente que el tiempo corre en nuestra contra, por lo tanto la cooperación internacional a través de redes 24/7 donde cada uno de los países cuente con un focal point a quien se le pueda solicitar la información, intercambiar experiencias y profundizar los mecanismos cooperativos en el sector público y privado, para identificar algunas conductas, de ejemplo tenemos la explotación de menores donde su actuar delictivo se da por intermedio de video llamadas, distribución o comercialización de imágenes y videos de bebés, niños y niñas de muy corta edad, como adolescentes siendo abusados por adultos, encontrando muy fácilmente su obtención en las redes sociales o redes internacionales de explotación sexual infantil, es así que a diferencia de Argentina, en Estados Unidos existe una Ley General que contiene penas y multas la exigencia a todas las empresas que cuenten con apps y su manejo sea por intermedio de redes sociales cumplan con reportar a la ONG “National Center for Missing & Exploited Children”, la detecte por intermedio de sus bots o inteligencia artificial al usuario que subió, compartió o publicó algún video o foto de menores de edad siendo abusados sexualmente por adultos; ahora bien, en Argentina, la fiscalía especializada al



realizar la investigación y verificar que el autor no se encuentra en la ciudad de Buenos Aires se reparte inmediatamente por medio del sistema VPN a todas las provincias donde se tiene ubicado a todos los sospechosos que se contactaron para cometer este delito y así sea mucho más factible la investigación; pero aun así, se cuenta a nivel de Latinoamérica con una cantidad aproximada de 124 mil reportes de abuso y explotación sexual infantil; y, para contrarrestar tan alta suma de reportes de abusos sexuales como de otro tipo de delitos cometidos a través de sistemas informáticos las fuerzas de seguridad para actuar con prevención policial cuentan con el software de predicción criminal llamado crime prediction tech, que permite a las autoridades pronostiquen un crimen bajo la obtención de una cantidad de datos y variables que en base a algoritmos de aprendizaje automatizados elaboran predicciones en tiempo real mostrando un mapa de delitos para organizar las políticas de prevención; como otros tipos de prevención sería importante el ciberpatrullaje, agente encubierto digital, tecnovigilancia de personas y lugares, espionaje de dispositivos electrónicos, activación de cámara y microfono, la obtencion de software judicial a distancia que permitiría a las autoridades competentes acceder a datos informáticos almacenados en la computadora del imputado a distancia y buscar la información necesaria para combatir el cibercrimen.

“INTELIGENCIA ARTIFICIAL – DETECCIÓN Y CONTROL DE AMENAZAS EMERGENTES”

Ing. MARIO YUNIS ARROYO

Ingeniero de sistemas, especialista en transformación digital con estudios en Harvard Business School (transformación digital en empresas) y Universidad de Stanford (Machine Learning), miembro blue hacker de Pacific Hackers Association (Silicon valley – California). Ponente de ciberseguridad en BASC.

Dentro del contexto global, se sabe que la inteligencia artificial es completamente transversal, atacando todo el ecosistema de las personas, pues contamos con dispositivos, conexiones, puertas abiertas que no se encuentran totalmente protegidas, por un contexto global de fuerzas tecnológicas, que están creando nuevas experiencias y generan disrupción en los modelos de negocios, haciéndonos las preguntas ¿A qué nos estamos enfrentando en el día a día? ¿Qué es lo que está sucediendo? entonces tenemos análisis exhaustivo sobre cómo la inteligencia artificial (IA) ha transformado el panorama de amenazas digitales que enfrentan las instituciones públicas, el sector privado y, de manera particular, los sistemas de justicia. Su exposición partió de una premisa fundamental: la IA ya no es únicamente una herramienta de innovación, sino también un mecanismo que amplifica de manera significativa la capacidad operativa de actores malintencionados. “La inteligencia artificial no solo aumenta la velocidad de los ataques; redefine la forma misma en que entendemos el riesgo”, señaló el expositor al inicio de su intervención. A lo largo de su ponencia, Yunis explicó cómo técnicas delictivas que antes requerían altos niveles de especialización hoy están al alcance de ciberdelincuentes con poco conocimiento técnico, gracias a modelos de IA capaces de generar phishing casi perfecto, voces sintéticas que imitan con precisión a funcionarios o superiores jerárquicos, y videos deepfake utilizados para manipular decisiones operativas críticas. De igual modo, se describieron esquemas de vishing automatizado —capaces de lanzar miles de llamadas simultáneas con audio generado por IA— y ataques DDoS potenciados por botnets inteligentes que permiten alcanzar volúmenes de tráfico sin precedentes. La ponencia profundizó también en casos emblemáticos de grupos delictivos como LAPSUS\$, Scattered Spider y ShinyHunters, cuyas operaciones combinan ingeniería social avanzada, compra de accesos internos, explotación de APIs mal configuradas y técnicas de extorsión digital sin necesidad de cifrado. Al respecto, el expositor advirtió que “los grupos criminales ya no dependen únicamente de vulnerabilidades tecnológicas; dependen de vulnerabilidades humanas y organizacionales”. Este enfoque fue especialmente relevante para el público del ámbito judicial, pues demuestra cómo el delito informático evoluciona más rápido que los marcos



tradicionales de persecución penal. Uno de los aportes más importantes de la presentación fue el análisis del scraping automatizado, un riesgo aún poco visibilizado en las instituciones del Estado. Se explicó que esta técnica permite extraer grandes volúmenes de información sensible desde cuentas que poseen permisos legítimos, sin necesidad de vulnerar servidores ni generar huellas evidentes de intrusión. Este tipo de ataque es particularmente crítico para plataformas judiciales, administrativas y de gestión ciudadana, ya que puede comprometer datos personales, información reservada o documentación procesal. “La amenaza más peligrosa no es la que derriba puertas digitales, sino la que entra por una puerta legítima sin ser detectada”, enfatizó Yunis. En su análisis institucional, la ponencia subrayó que la ciberseguridad dejó de ser un asunto circunscrito al área de tecnologías de la información para convertirse en una responsabilidad estratégica que afecta directamente la continuidad operativa, la reputación institucional y la confianza ciudadana en los sistemas de administración de justicia. La inteligencia artificial, al incrementar tanto la probabilidad como el impacto de los riesgos, obliga a revisar los modelos de auditoría interna, fortalecer los controles operacionales y replantear la estructura de gobernanza digital. El expositor advirtió que “muchas organizaciones siguen evaluando riesgos como si el entorno no hubiese cambiado, mientras que los atacantes operan en un escenario completamente transformado”. El cierre de la ponencia se centró en tres pilares esenciales para enfrentar las amenazas emergentes en el contexto actual: 1. Actualización rigurosa de las matrices de riesgo institucional Yunis resaltó que las matrices de riesgo tradicionales no contemplan las capacidades actuales de la IA ni los nuevos vectores de ataque. Señaló la necesidad de incluir amenazas como deepfakes en procesos de validación, phishing automatizado, scraping inteligente, manipulación de sistemas de autenticación, suplantación de funcionarios y automatización en masa de llamadas fraudulentas. La actualización no debe ser meramente documental, sino asociada a controles reales, verificables y en constante revisión. 2. Fortalecimiento de la comunicación interna El expositor indicó que la falla más frecuente no está en los sistemas, sino en la falta de comunicación entre las áreas operativas, administrativas, tecnológicas y directivas. “Una institución puede tener controles robustos, pero si la información no fluye de manera clara, oportuna y estructurada, esos controles no se ejecutarán adecuadamente”. Subrayó que la comunicación interna es un componente indispensable del ecosistema de ciberseguridad, especialmente en procesos sensibles como autorizaciones, manejo de evidencia digital, atención a incidentes y preservación de cadena de custodia. 3. Necesidad de un Poder Judicial capacitado en delitos informáticos y custodia digital Finalmente, Yunis remarcó la urgencia de que el Poder Judicial, como garante final de la protección de derechos y de la sanción del delito, cuente con capacidades fortalecidas para enfrentar estas nuevas formas de criminalidad. Señaló que se requiere formación especializada en IA, técnicas modernas de investigación digital, análisis forense avanzado, tratamiento de evidencia tecnológica y cadena de custodia digital acorde a estándares internacionales. Asimismo, destacó que la evolución del delito demanda jueces, fiscales, peritos y operadores del sistema jurídico capaces de comprender la complejidad técnica detrás de estas amenazas, pues “la justicia no solo debe ser oportuna y objetiva, sino también tecnológicamente competente”.

“MODALIDAD DEL CIBERCRIMEN: ATAQUES CONTRA DATOS Y SISTEMAS INFORMÁTICOS”

Dr. RICARDO ELIAS PUELLES

Abogado por la Pontificia Universidad Católica del Perú, maestro en Razonamiento Probatorio de la Universidad de Girona (España) y la Universitat Degli Stuti di Genova (Italia), cuenta con estudios de especialización en Derecho Penal, Derecho Procesal Penal, Litigación Oral cursados en Perú, Argentina, España y Alemania, Docente para la American Bar Association – Rule Of Law Initiative, es Presidente del Instituto Peruano de Razonamiento Probatorio y del Observatorio Peruano de Cibercriminalidad, miembro de la Sociedad de Derecho Empresas Digitales y corresponsal de la red Net Against Cyberfraud.

El objeto de los delitos contra la seguridad informática es la reflexión entorno a los delitos que existen hoy en día, que tienen que ver con el acceso ilícito, atentados contra datos, ataques contra sistemas informáticos, intersección de datos y abuso de mecanismos y dispositivos informáticos, para ello es importante tomar algunos datos o hitos importantes de la lucha de 25 años contra ciberdelincuencia en el Perú, contando como base el Convenio de Budapest en el año 2001, la creación de la División de investigación de Delitos de Alta Tecnología en el año 2005, la implementación de la Ley 30096 de Delitos Informáticos en el año 2013, la Ley 30171 que modifico de la Ley de Delitos Informáticos en el año 2014, la adhesión al Convenio de Budapest en el año 2019, la creación de la Unidad Fiscal Especializada en Ciberdelincuencia en el año 2021, la adhesión a la Convención de las Naciones Unidas contra la Ciberdelincuencia, en el año 2024, la creación de la Ley 32314 que incorpora la Inteligencia Artificial como agravante al Código Penal y a la Ley de Delitos Informáticos, que se encuentra en constante cambio y evolución, lo que nos lleva a crear métodos alternativos de investigación que no dependan necesariamente de pericias informáticas, si no también de algunas otras formas o métodos metodológicos de prueba en base a búsqueda de fuentes abiertas, convenios con empresas en el sector privado para fortalecer las investigaciones, porque si no la delincuencia va seguir aumentando y no vamos a tener un correcto procesamiento conforme al desarrollo de nuevas figuras y estructuras delictivas tradicionales y modernas y evitar así que la mayoría de denuncias se archiven por distintas limitaciones; toda vez que el objeto no es tener un numero amplio de denuncias, lo importante es obtener resultados en base a la formalización, la acusación y una eventual sentencia.

Ahora bien, respecto a las modalidades de cibercrimen, tenemos que dirigirnos a la



convención de las Naciones Unidas contra la ciberdelincuencia que es el primer tratado de organización en el ciberespacio, así como el convenio de Budapest y de este último, nuestra Ley de Delitos Informáticos ha hecho suyo algunos actuare delitos que son ataques contra confidencialidad, integridad, disponibilidad de datos y sistemas informáticos, como es el de acceso ilícito previstos en el artículo 2°, atentados contra datos informáticos previsto en el artículo 3°, atentado contra los sistemas informáticos previsto en el artículo 4°, existiendo problemas con los delitos de intersección de datos previsto en el artículo 7°, creándose un capítulo especial llamados delitos contra la inmovilidad y el secreto de las comunicaciones lo cual es inadecuado; empero, lo que debería de darse es seguir el modelo de Budapest y reubicarse en el capítulo de delitos contra la seguridad informática o contra la confidencialidad, integridad y disponibilidad (trinomio CIA); en esa misma perspectiva, se tiene el artículo 10° que prevé el delito de abuso contra mecanismos y dispositivos informáticos, debiendo cubrir el espacio previo para sancionar aquellas conductas previas y no esperar a que se cometan los ataques ilícitos contra los datos o contra los sistemas informáticos para estar un paso adelante conforme así ya lo prevé el convenio de Budapest y la convención de las Naciones Unidas y no como lo tiene previsto nuestra Ley de Delitos Informáticos que cuenta con una clausula general que cubre no solamente los delitos que ya hemos visto si no cualquier otro delito previsto en el Ley de Delitos Informáticos como son fraude informáticos, grooming, prestamos extorsivos, siendo un problema sistemático que deberíamos solucionarlo en una eventual norma legislativa, que preserven el bien jurídico protegido como la integridad y disponibilidad, en base a los verbos rectores que es de dañar, borrar, deteriorar, alterar, suprimir, introducir, generar inaccesibilidad datos y sistemas informático. En esa misma perspectiva, da a conocer que cuando hablamos de delitos contra la seguridad informática, se debe de tomar como reflexión, la necesidad de fortalecer nuestras unidades especializadas no solamente la policía y la fiscalía, si no también el Poder Judicial, la necesidad que los legisladores analicen y edifiquen con capacidad y conocimiento las solicitudes presentadas por el Ministerio Publico así como la identificación del tipo penal y la proporcionalidad de las medidas como las penas, así como la adhesión a convenio y tratados que no limite la competencia del legislador en base a su territorialidad para alcanzar así los fines del derecho y su protección a la sociedad.

“INTELIGENCIA ARTIFICIAL - RETOS DE LA DELINCUENCIA ORGANIZADA - DELITOS DEL AMOR”

Dra. ROSA MARIA TOME GARCÍA

Magistrada de la Audiencia Nacional de España,
ex Coordinadora General Plenipotenciaria de la
Agencia Española de Cooperación Internacional.



Es de comentar que la mezcla de amor y sociedad que podría ser tan bonita, se ha convertido, desde hace unos años en uno de los nuevos escenarios más crudos de la violencia, sobre todo contra las mujeres, aunque también contra hombres, no tratándose de una violencia psicológica para apoderarse de nosotros dejándonos indefensos en nuestros momentos más vulnerables abordando una alarmante y cada vez más común las llamadas Estafas del Amor o Estafas Romance, un tipo de cibercrimen que explota la necesidad humana de afecto y compañía, transformando el deseo de amar en una forma de violencia psicológica y económica; este fraude es un terreno de engaño y maltrato donde se baja la guardia, aprovechando la soledad y vulnerabilidad de las personas, aunque la violencia no es física, es calmada y silenciosa, apoderándose de las víctimas, dejándolas sin dinero, autoestima ni amor propio, con daños psicológicos y morales muy difíciles de superar. El término despectivo de los estafadores para referirse a sus víctimas es **“Pig Butchering”** (engorde de cerdos), aunque la INTERPOL desaconseja su uso por estigmatizar a las víctimas; asimismo, el fraude se nutre de dos elementos principales que convergen en la sociedad moderna que versa entre Soledad y la Tecnología que converge como uno de los males más relevantes del siglo XXI, siendo las mujeres de 50 años unos de los grupos masa afectados, en España, el porcentaje de mujeres de 65 años o más que viven solas se acerca al 30%. esta situación de aislamiento convierte a las personas en blancos vulnerables, deseosas de cariño y atención, siendo las redes y las aplicaciones de citas (Dating Apps como Tinder, OkCupid, Meetic) se han convertido en un aliado para romper el encierro de la soledad, incluso para el sector senior; sin embargo, para los seniors, estas aplicaciones son un territorio nuevo, lo que los hace menos cautelosos y más susceptibles al engaño, en el que el género destaca como un factor: mientras los hombres suelen buscar encuentros casuales, las mujeres (especialmente las maduras) buscan relaciones estables basadas en el amor, este "sentimentalismo" las hace actuar más con el corazón que con la razón, siendo objetivos perfectos para los estafadores. El perfil del estafador y mecánica de engaño individual (Suelen ser personas solitarias con rasgos psicopáticos: egocéntricos, narcisistas, amorales y con poca o nula empatía. Tienen una alta inteligencia social y capacidad de manipulación) y catfish (Es el método más utilizado por las organizaciones criminales. Consiste en crear perfiles falsos (imágenes y vidas inventadas), a veces usando imágenes de famosos (el "Falso Brad Pitt" o "Keanu Reeves") o creadas con Deepfake/IA. El perfil estándar es el de un hombre de éxito: militares americanos, médicos, o empresarios con

alto poder adquisitivo, familiar y romántico); así como las estafas llevadas a cabo por organizaciones criminales transnacionales que utilizan los aplicativos yahho boys y Sakawa Boys, estos grupos están entrenados en tecnología y manipulación psicológica, haciéndose pasar por hombres blancos y atacando a sociedades occidentales, justificando sus acciones como una "recuperación de la riqueza" arrebatada durante el régimen colonial; lo que nos conlleva a realizar un estudio de las consecuencias y a la lucha legal ante la presente actividad delictiva; en el que las víctimas enfrentan un doble daño que es la pérdida económica y el daño psicológico, ya que la estafa del amor explota el vínculo emocional produciendo una profunda vergüenza de ser juzgados y ridiculizados, lo que dificulta la imposición de denuncias, por el miedo de la crítica social sobre la víctima; y, ello deriva a una complejidad de la prueba penal endeble y voluntaria, obteniendo solo pantallazos o mensajes de la víctima y la dificultad de rastrear el destino del dinero, como también el probar que el acto de disposición patrimonial no fue una entrega voluntaria o regalo, ya que no hay intimidación ni violencia; adicionalmente, es de precisar que otro tipo de delitos que se cometen se dan cuando los estafadores implican a sus víctimas en fraudes de lavado de dinero pidiéndoles que abran cuentas bancarias para transferir fondos ilícitos. Las identidades de las víctimas también son utilizadas para cometer otros delitos, lo que puede llevar a que la víctima sea encausada como autora o cómplice. La tendencia emergente es considerar estas estafas como una nueva forma de violencia contra las mujeres. México ha presentado una iniciativa para incluir la Estafa Romance en su Ley de Acceso de las Mujeres a una Vida Libre de Violencia, buscando cerrar los vacíos legales. En España, asociaciones como ANCEME abogan por que se reconozca el fraude como violencia digital y que se le otorgue la misma protección que a las víctimas de otros delitos.

“LA IMPORTANCIA DE LA PROTECCIÓN DE DATOS PERSONALES PARA LA PREVENCIÓN DE DELITOS CIBERNÉTICOS”

Dr. CARLOS TOMÁS ALVEAR PEÑA

Doctor en Jurisprudencia por la Universidad del Azuay y Magister en Derecho Digital por la Universidad Internacional de Ecuador, mediador y secretario arbitral de las Cámaras de la Producción en Azuay. Ex Director General del Consejo de la Judicatura del Ecuador y Ex Director Nacional de la Escuela de la Función Judicial, actualmente Director Ejecutivo del Instituto Iberoamericano de Justicia y Experto en Cibercrimen.

la protección de datos personales es sin duda uno de los pilares fundamentales de la seguridad digital contemporánea, en un entorno donde las amenazas cibernéticas crecen día a día, la adecuada gestión y resguardo de la información personal constituye una estrategia esencial para prevenir delitos informáticos y mitigar riesgos asociados al uso de nuevas tecnologías, especialmente la inteligencia artificial; que conlleva a mitigar el riesgo con estrategias y asociación de nuevas tecnológicas; gestionar datos con fines estratégicos para el resguardo de información personal, para generar la prevención de delitos.



La importancia de la protección de datos personales es vital para garantizar derechos fundamentales como la privacidad, la autodeterminación informativa y la seguridad jurídica, los datos personales se han transformado en el activo mas valioso del entorno digital y al mismo tiempo, en el más vulnerable ante amenazas bajo múltiples conductas ilícitas como robo o filtro de datos sensibles (phishing), suplantación de identidad, extorción digital mediante ransomware, fraude financiero electrónico, ataques de ingeniería social que explotan vulnerabilidades humanas, data breach, identity theft, malware, siendo las causas más frecuentes de filtración de datos los errores humanos, fallas de seguridad, ataques externos e internos maliciosos que se develan en vulnerabilidades ocultas, de ciberdelitos masivos, vulnerabilidades no corregidas e infraestructuras obsoletas; y como tal, tenemos el caso Equifax, que es un caso de ciberdelito masivo, ocurrido en el año 2017, que fue una de las mayores filtraciones de datos de la historia, afectando a mas de 140 millones de personas, siendo que su vulnerabilidad no corregida fue la que permitió que ciberdelincuentes accedan a datos financieros, números de seguridad social y otra información totalmente sensible; y el ataque ransomware a la ciudad de Atlanta en el año 2018 que fue un ataque que

paralizo servidores; en esa misma perspectiva, el uso de la inteligencia artificial haya incrementado más riesgos tanto en la satisfacción de los ataques como en la capacidad defensiva; sin embargo, también abre nuevas áreas de exposición como el Deepfakes (para incidir en proceso electorales, judiciales o extorción), automatización de ataques masivos, modelos de IA que pueden ser atacados para extraer información sensible; entonces, nos hacemos la pregunta ¿Cómo mitigar los riesgos de la IA? para ello debemos implementar tecnología para detectar y contrarrestar los deepfakes para proteger los proceso electorales y prevenir la extorción; así como desarrollar sistemas de defensa para contrarrestar los ataques masivos automatizados, asegurando la seguridad de la red, debiendo de fortalecer los modelos de IA para prevenir la extracción de información sensible a través de ataques; y, como estrategias de prevención se debe de implementar las políticas robustas de seguridad digital, capacitación continua sobre ingeniería social, actualización de sistemas y parches de seguridad, implementación de cifrado y métodos avanzados de autenticación, políticas claras de tratamiento de datos personales que mejoren el manejo de datos personales con la finalidad de generar una cultura de protección de datos con una sociedad digital segura con responsabilidad y uso de la información que involucre la educación, cumplimiento normativo, auditorias constantes con interacción responsable con las tecnologías emergentes, para una adecuada gestión de riesgo que permita afrontar desafíos de la era digital con mayor resiliencia y seguridad para prevenir delitos ciberneticos.



SEGUNDO DIA

“DE LA CURIOSIDAD TECNOLÓGICA A LA RESPONSABILIDAD PENAL – MENORES E INTELIGENCIA ARTIFICIAL EN EL CIBERCRIMEN”

Dr. ANTONI BOSCH PUJOL

Licenciado en Ciencias Físicas por la Universidad de Barcelona, Master en Auditoría Informática del CENEI, Diplomado en Alta Dirección de Empresas ESADE y en Managing Information Technology del Center For Information Systems Research - MIT Sloan School, cursos de Doctorado en la Universidad Autónoma de Barcelona, Auditor Certificado en Sistemas de Información (CISA), Director Certificado en Seguridad de la Información (CISM), Certified in the Governace of Enterprise It (CGEIT), experto certificado en protección de datos (ECPD), Leal Auditor 27001 Director de los cursos de Experto Certificado en Protección de Datos (ECPD) con la Pacífico Business School en Perú y Asobancaria en Colombia, Compliance Officer con CENTRUM (Pontificia Universidad Católica del Perú), Director del Curso de Experto Internacional en Protección de Datos e Inteligencia Artificial (IAITG).

La evolución de las tecnologías y humanidad es cambiante, tanto es así que en los años 80 el solo hecho de que una persona hablara de uno podría significar algo bueno o malo, pero en la actualidad eso cambio, ya que ahora buscamos que todo el mundo hable de nosotros subiendo toda nuestra información a las redes sociales, conllevándonos a que todo se vuelva inmanejable ya que ni nosotros mismos podemos manejar ni mantener nuestra privacidad, lo que nos lleva a saber de manera tan sencilla y factible el saber a tiempo real lo que están haciendo nuestro hijos, familiares, amigos o personas ajenas a nuestro entorno con la sola consulta de las redes sociales; ahora bien, el panorama digital en el Perú se estructura en el que el 78% de la conectividad está determinado a menores de edad entre los 12 a 17 años con acceso diario a internet de 6.2 horas diarias como promedio de tiempo con el uso de dispositivos móviles en un 89%, motivados a la exploración, por presión social, la gamificación, el reconocimiento y beneficio económico; este último puede direccionar en algunos casos a una conducta criminal bajo una experimentación inocente (prueba herramientas de la IA por curiosidad, sin dirección delictiva inicial), lo que direcciona al descubrimiento de capacidades donde se identifican potenciales para crear contenidos falsos convincente y dañinos, para orientar



al uso indebido del menor para generar una transgresión como broma, venganza o prueba entre pares y conduce a conductas sistemáticas de escala criminal (extorción, fraude, difusión masiva de contenido falso); al llegar ese punto, nos damos cuenta que nos encontramos en una línea difusa donde la experimentación se convierte en delito y hace inferir al menor que no existe conciencia de ilegalidad frente a las consecuencias reales en la tipicidad objetiva de ciertos delitos, sin tomar en cuenta el riesgo emergente de los afectados como conducta típica de actuar delictivo sistemático; es así que, ante esta brecha o línea difusa se debe tomar en cuenta las señales de alerta, con el uso excesivo de dispositivos en horarios inusuales, ocultamiento de pantalla, múltiples cuentas, ingresos inexplicables, transacciones digitales no supervisadas, solicitudes de criptomonedas, ansiedad al separarse del dispositivo, cambios bruscos de humor, aislamiento social físico, conocimiento tecnológico desproporcionado para su edad, lenguaje técnico específico de hacking, conflicto con compañeros vinculados a contenido digital, denuncias de otros padres, uso de aplicaciones de mensajería cifrada, resistencia a compartir contraseña con sus padres. De otra parte, la generación del engaño entre el menor y la inteligencia artificial hace que se genere una percepción falta de anonimato, ya que muchos de ellos creen que la tecnología los hace invisibles, lo cual es totalmente falso ya que toda actividad digital deja huellas con la ayuda de direcciones IP, metadatos, patrones de comportamiento e información de dispositivos, trazas digitales, metodologías específicas por evidencia generada por la IA; y, al obtener la información digital, ello generaría la denuncia con orden inmediata de prevención de evidencia digital antes de que se elimine, para el análisis forense digital, para identificarlo bajo el rastreo el IP, cuentas de usuarios, patrones de comportamiento digital, direccionados a la recopilación de pruebas de su historial de navegación, logs del sistema, metadatos, capturas de pantalla certificadas, para emitir un informe pericial que explique en lenguaje comprensible como se cometió el delito y el rol de la IA con la respectiva integridad de los datos, autenticidad técnica, intencionalidad demostrable para la proporcionalidad del peritaje. Como prevención y recomendaciones es brindar una formación continua en círculos escolares sobre ciudadanía digital, ética, tecnología y consecuencias legales, generar programas de alfabetización digital para padres, campañas de concientización para la regulación de acceso a herramientas de IA, sugerir charlas preventivas por personal policial en centros educativos donde se toquen temas respecto a las repercusiones de este tipo de hechos delictivos; de igual forma, generar responsabilidad corporativa en diseño de herramientas seguras y colaboración con las autoridades por parte del sector privado y por último la capacitación continua al Poder Judicial en tecnología emergente para especializar a los jueces en cibercrimen juveniles.

“EL AGENTE ENCUBIERTO ONLINE EN LA INVESTIGACION DEL CIBER CRIMEN”

Dra. LAURA VIVIANA MAYER LUX

Catedrática de Derecho Penal en la Pontificia Universidad Católica de Valparaíso – Chile, Doctora en Derecho por la Universidad de Bonn – Alemania, Presidenta del Instituto de Ciencias penales de Chile.

Dr. JAIME VERA VEGA

Abogado de la Pontificia Universidad Católica de Valparaíso – Chile, Magister en Derecho Penal por la Universidad Pompeu Fabra y de Barcelona – España, Doctor en Derecho por la Pontificia Universidad Católica de Valparaíso, reconocido por su labor como docente e investigador en el ámbito penal.

El agente encubierto constituye una institución usualmente establecidas en los sistemas jurídicos penales iberoamericanos, se encuentra prevista por ejemplo en España, Argentina, México, Perú, Chile, entre otros, desde el punto de vista general un agente encubierto corresponde a un funcionario policial que simula su identidad oficial y se infiltran en organizaciones criminales o meras agrupaciones con propósitos delictivos con el objetivo de identificar a los participantes, reunir información y recoger antecedentes necesarios para la investigación; su consagración cuenta además con fundamentos de carácter internacional ya que la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional del año 2000 lo consagra en su Artículo 20.1. Una característica que destaca en esta figura es su naturaleza híbrida, pues presenta una dimensión procesal y otra sustantiva que regulan y contemplan el tratamiento jurídico penal, el funcionario policial que actúa como tal ya que en esa calidad podría incluso llegar a ejecutar comportamientos tipificados como delitos, bajo esa perspectiva es tradicional la previsión de normas eximentes o excluyentes de responsabilidad que suelen interpretarse como causales de justificación o excusas legales absolutorias respecto del agente que incurra en los hechos típicos señalados; esta figura tiene como objeto de análisis ante nuevas figuras delictivas a través de sistemas informáticos “al agente encubierto online o agente encubierto en línea – también conocido como agente cibernético” que ya se caracteriza justamente por su actuar en el internet, para obtener información sobre comportamiento delictivos de delitos intangibles cometidos actualmente en la red como el ciberterrorismo, el narcotráfico, trata de personas, pedofilia, entre diversas formas de criminalidad, es por ello que el ordenamiento jurídico debe de responder mediante nuevas técnicas de investigación que posibiliten el esclarecimiento de los hechos y bajo ese contexto surge el agente encubierto online, con medidas intrusivas de alto impacto que limita derechos fundamentales en la medida que la actuación del agente encubierto sea



de modo virtual o real, restringe derechos de suma importancia para los investigados o terceros, situándose entre las técnicas más lesivas que prevé la Ley valiéndose del engaño para presentarse como un copartícipe; es así que, para la intervención del agente encubierto solo debe utilizarse si cumple las condiciones de la exigencia en merito (*fumus boni iuris*) bajo la exigencia de indicios más o menos claros que haga plausible la exigencia del hecho delictivo y la participación de los responsables, no es un estándar de condena pero si con requerimiento de base fáctica, ello con idoneidad, necesidad y ponderación. La justificación táctica del agente encubierto online está basada en la inmaterialidad del delito haciendo la distinción en la exigencia del uso de mecanismos tecnológicos, ya que no se trata solo de delincuentes individuales sino también de organizaciones criminales dedicadas a la perpetración de cibercrimes, en la que el agente con naturaleza intimista hace vínculos de confianza operando bajo códigos secretos con estructura hermética que hace posible la infiltración del agente pero con alto riesgo de peligrosidad; empero, el agente encubierto es una respuesta necesaria y poderosa a la complejidad de la cibercriminalidad pero con supervisión judicial con clave a la legitimidad que valida la operación y la protección de los derechos fundamentales dependan de una estricta supervisión judicial y el cumplimiento riguroso de los principios de necesidad y proporcionalidad; por último, con una claridad conceptual imperativa en la que se diferencia nitidamente el agente encubierto del ciberpatrullaje, del inadmisibles agente provocador y de otras técnicas como el registro remoto que es vital para prevenir abusos, garantizar la validez probatoria y proteger la integridad del sistema de justicia.

“LA CONCAUSALIDAD, CORRESPONSABILIDAD O AUTOPUESTA EN PELIGRO EN LOS CIBERDELITOS”

Dr. DINO CARLOS CARO CORIA

Presidente de la Asociación Internacional de Compliance, Doctor en Derecho por la Universidad de Salamanca – España, Estancia de Investigación Postdoctoral en Max Planck Institut Fur Ausländisches und Internationales Strafrecht de Freiburg im Breisgau – Alemania, Profesor de Derecho Penal en la Pontificia Universidad Católica del Perú, Universidad de Lima, Profesor de Compliance y Buenas Prácticas Corporativas de la Universidad del Pacífico, Gerente General del Centro de Estudios de Derecho Penal Económico y de la Empresa, Socio fundador y Gerente General de Caro & Asociados.

La expansión de la criminalidad informática ha obligado al Derecho Penal repensar categorías clásicas de imputación objetiva, en conceptos de concausalidad, principio de corresponsabilidad y autopuesta en peligro, desarrollados originalmente para delitos de resultado en contexto físico que hoy deben dialogar con un ecosistema digital caracterizado por la mediación tecnológica, la automatización, la asincronía y la participación activa o imprudente de la propia víctima, es en este aspecto que la Ley N° 30096, Ley de Delitos Informáticos, proporciona un marco normativo idóneo para analizar estas categorías, pues tipifica conductas donde el resultado lesivo suele producirse mediante interacciones complejas entre el autor, sistemas informáticos y como usuario la víctima, haciéndonos la pregunta central ¿hasta qué punto la conducta de la víctima – negligente, descuidada o incluso temeraria incide en la imputación penal del autor en los ciberdelitos? entonces, lo que hacemos es entender primero que la concausalidad se presenta cuando varias conductas contribuyen de manera relevante a la producción del resultado sin que una anule completamente la eficacia causal de la otra; es decir, en la imputación objetiva el problema no es causal en sentido naturalístico si no normativo, para entender que riesgos son jurídicamente relevantes y atribuibles al autor con actividad estructural (el atacante diseña un malware, el sistema representa vulnerabilidades y el usuario ejecuta la acción final con el simple hecho de hacer click, realizar una descarga o generar una validación); lo que nos lleva al principio de correspondencia de riesgo que exige que el resultado sea una realización del riesgo jurídicamente desaprobado creado por el autor y no de un riesgo distinto, autónomo o ajeno, en entornos digitales este principio es crucial para evitar imputaciones expansivas o, por el contrario, absoluciones indebidas en la conducta de la víctima; no obstante la autopuesta en peligro de la víctima



excluye la imputación cuando la víctima conoce el riesgo, lo asume deliberadamente y el resultado es consecuencia directa de esa asunción autónoma, en cibercrimes, esta figura debe de aplicarse con extrema cautela porque existe asimetría técnica entre el autor y la víctima, aparte que el conocimiento de riesgo suele ser aparente – no real y el engaño digital simula un contexto de confianza. La integridad de datos y sistemas respecto a la concausalidad estructural se encuentran establecidos en el ámbito normativo en el artículo 3° atentado contra la integridad de datos informáticos, artículo 4° atentado contra la integridad de sistemas informáticos en el que ambos delitos parten de escenarios de causalidad compleja; no obstante, la concausalidad como regla general el resultado suele provenir de la interacción entre vulnerabilidades preexistentes del sistema y la conducta dolosa del agente y solo el riesgo jurídicamente desaprobado introducido por el autor es imputable penalmente, por lo que la vulnerabilidad del sistema no es una causa excluyente de responsabilidad en ese sentido es de aclarar la ley no protege sistemas perfectos si no su integridad funcional en el que el riesgo penalmente relevante es el creado por el atacante; por lo que es de concluir que la dogmática penal aplicable a los cibercrimes debe resistir una tentación peligrosa como el de culpar a la víctima por no ser experta en tecnología, por lo que el derecho penal no protege al usuario ideal sino al usuario real.

“CIBERCRIMEN Y LA ACCION DE EXTINCION DE DOMINIO DEL DERECHO DE DOMINIO – VISION COLOMBIA Y PERÚ”

Dr. DAVID GUTIERREZ CASTAÑO

Juez del Tribunal Superior de Medellín de la Sala Especializada de Extinción de Dominio, Abogado Asesor y Consultor de Extinción de Dominio, Director de la Maestría en Derecho Penal de la Universidad de Medellín.

Los elementos que definen y estructuran la acción de extinción del derecho de dominio y cibercriminalidad se dan bajo el nexo causal de una actividad ilícita y el bien que va tomar origen o destino, siendo este un instrumento jurídico fundamental diseñado para debilitar las estructuras financieras de las organizaciones criminales, despojando a los delincuentes de los bienes adquiridos a través de distintas actividades ilícitas y con el crecimiento exponencial del cibercrimen en el siglo XXI, es esencial analizar cómo se establece el nexo causal entre la nueva modalidad de criminalidad con las que se generó provecho y la aplicación de la extensión de dominio y como tales tenemos fraudes informáticos, estafas a traves del phishing, ransomware, entre otras, que del dinero obtenido a través del engaño o rescate pagado por criptomonedas, billeteras digitales o plataformas peer-to-peer para mover u ocultar ganancias a través del blanqueo son el producto del delito que el bien a exigir es el activo digital, por lo tanto la trazabilidad de activos digitales se da bajo la determinación de la naturaleza jurídica del activo digital definiendo el objeto de la extinción, por esta razón nadie debe ni puede beneficiarse de un patrimonio ilegal, por lo que la Extinción de Dominio actúa como un mecanismo eficaz no solo para recuperar los activos obtenidos mediante delitos informáticos, sino también para desmantelar la infraestructura tecnológica y financiera que permite que el cibercrimen organizado prospere, obteniendo como desafío actual el adaptarse a la velocidad y complejidad del entorno digital para garantizar la trazabilidad de los activos y la efectividad de la justicia; bajo ese mismo contexto la Extensión de Dominio debería o en el mejor de los casos debe de recaer no solo sobre las ganancias, sino también sobre los bienes que fueron utilizados como instrumento o medio para facilitar la comisión del delito, esto incluye servidores, equipos informáticos de alta gama, software especializado, o las cuentas bancarias usadas exclusivamente para recepcionar pagos ilícitos, golpeando así la capacidad operativa de los ciberdelincuentes. De otro lado también debemos tener presentes que la jurisdicción y trasnacionalidad genera que los ataques cibernéticos y la dispersión de los activos a menudo crucen fronteras en la que debería exigir una compleja cooperación judicial en base a tratados y convenios que conlleve a una cooperación entre las autoridades para rastrear los fondos de las víctimas



y así poder exigir los bienes como activo final; entonces, el delito informático abre las puertas a otras capacidades de generar dinero, bienes o garantías de origen ilícito vinculadas a la criminalidad organizada por lo que urge replantear la teoría del delito porque no podemos seguir estudiando el cibercrimen con la teoría clásica que tiene más de ciento treinta años y que fue concebida para un mundo analógico, donde la conducta y la causalidad eran los elementos centrales, elementos que hoy son abstractos en los cibercrímenes, y ello exige una nueva teoría del delito para el universo de la cibercriminalidad; además del reto del espacio, porque se vuelve difuso saber dónde se comete el delito para determinar jurisdicción.

“MINISTERIO PÚBLICO EN EL PERÚ ANTE LA CIBERDELINCUENCIA”

Dra. AURORA REMEDIOS FÁTIMA CASTILLO FUERMAN

Fiscal Superior Titular de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, Jefa de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con Competencia Nacional; y, coordinadora Nacional de las Fiscalías Especializadas en Ciberdelincuencia, Ex Presidenta de la Junta de Fiscales Superiores de Lima Centro, Magister en Derecho Empresarial por la Universidad de Lima.

El incesante y vertiginoso desarrollo de la tecnología de la información y comunicaciones nos tiene en el mundo cada vez más conectados digitalmente con acceso generalizado a la tecnología de la información y las comunicaciones contando con proveedores de servicios privados a nivel global, permitiéndonos que la información fluya con mayor facilidad en distintas partes del mundo, donde las fronteras han dejado de ser barreras para el flujo en el ciberespacio, que dicho sea de paso dinamiza el desarrollo económico y social como la comisión de nuevos delitos nacionales y transnacionales con su uso, tras el anonimato de los autores y partícipes de estos; que conlleva a genera la tipología de lucha contra la ciberdelincuencia en diversos países de la Asociación Iberoamericana del Ministerio Público (AIAMP), generando la creación de Unidades de Investigación Centralizadas Nacionales Especializadas, Unidades de Coordinación Nacional con Descentralización de la Investigación en Puntos Focales, Unidades Nacionales de Coordinación (centradas específicamente en la capacitación y el apoyo a distancia) Dispersión de la Investigación, Unidades Nacionales de Apoyo Técnico con Dispersión de la Investigación, Inexistencia de especialización; en ese mismo orden, el Perú a través del RFN 1503-2020-MP-FN de fecha 30 de diciembre de 2020, se crea la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, que dio inicio a sus funciones el 15 de febrero de 2021, que cuenta con una red de fiscales en ciberdelincuencia nivel nacional quienes constituyen puntos de contacto de la Unidad Fiscal especializada en los distintos distritos fiscales del país; asimismo, es de señalar que se ha implementado la plataforma “Unidad de Ciberdelincuencia – UCIBER”, que permite a los fiscales a nivel nacional registrar solicitudes de acompañamiento técnico en la realización de la investigación; en ese mismo orden, se ha inaugurado el laboratorio de ciberdelincuencia del Ministerio Público, implementado con equipamiento donado por la Oficina de las



Naciones Unidas contra la Droga y el Delito – UNODC y la contribución del Gobierno de Noruega; además, la Unidad Fiscal Especializada en Ciberdelincuencia promueve la articulación entre el Ministerio Público y la Policía Nacional del Perú para la coordinación funcional y dirección efectiva de la investigación fiscal en los delitos informáticos, como coordinaciones a nivel interno con las presidencias de las juntas de fiscales superiores del país, escuela del ministerio público, oficina de peritaje, unidad de cooperación judicial y extradiciones, entre otras áreas fiscales y administrativas, así como la coordinación con organismos estatales y privados a fines de la ciberdelincuencia como la Secretaria de Gobierno Digital de la PCM, con los representantes de proveedores de servicios internacionales y nacionales, entidades financieras, bancarias entre otras, también coordina y promueve la capacitación especializada con la escuela del Ministerio Público, del mismo modo contamos con una guía práctica para el abordaje integral del ciberdelito; de esa misma forma, mediante Resolución de la Fiscalía de la Nación N° 341-2025-MP-FN del 05 de febrero de 2025 resuelve aprobar 05 instructivos (1. Generación y obtención del Valor HASH de documentos y archivos digitales; 2. Exportar correo electrónico para su análisis como evidencia digital; 3. Exportar chat de WhatsApp para su análisis como evidencia digital; 4. Identificar información del registrante de un documento de internet e información de una IP pública; 5. Identificar la URL original de una página web desde una URL corta).

“DEL CIBERESPACIO AL TRIBUNAL: INVESTIGACION Y PERSECUCION DEL CIBERCRIMEN”

Ins. LUIS CARLOS CABALLERO CABALLERO

Inspector Jefe de la Policía Nacional de España y Jefe de la Sección Operativa del Consejo General del Poder Judicial Tribunal Supremo y Audiencia Nacional.

Dentro de la Policía Nacional española, la Comisaría Especial del Consejo General del Poder Judicial, del Tribunal Supremo y de la Audiencia Nacional presta protección y seguridad a los diferentes órganos judiciales mencionados, incluida la protección personal de diferentes magistrados, jueces y fiscales que los forman; asimismo, en la Audiencia Nacional, existe un Juez Central de Instrucción que es especialista en ciberdelincuencia, lo que facilita enormemente la investigación de estos delitos, al contar con la formación necesaria para entender la idiosincrasia de este tipo de delitos tan específicos, y a veces, complicados de entender; cuando se habla de “seguridad”, hay que tener claro que el factor más débil dentro de la seguridad es el factor humano. Por mucha tecnología de última generación que se utilice para proteger a las personas o a los bienes, si detrás no hay una persona o personas que puedan intervenir, no serviría para nada; además, también hay que tener claro que detrás de todos los delitos que se comenten a través de internet siempre está el factor humano. Siempre habrá un hacker (activistas, profesionales), un estafador (phishing, vishing), grupos organizados (ciberterroristas) o outsiders/insiders (espías, empleados descontentos), por eso no debemos tener temor o reparo en afrontar las investigaciones para identificarlos y detenerlos; por lo que este tipo de delincuentes utilizan básicamente dos tipo de vectores de ataque para cometer sus delitos; por una parte, realizan un reconocimiento técnico de la infraestructura del objetivo que pretenden atacar. Este reconocimiento consiste en identificar y analizar toda la estructura expuesta a internet de una empresa/organización, lo que les permite descubrir, entre otras cosas: dominios – subdominios – direcciones IPs - servidores – puertos abiertos; buscando la vulnerabilidad que pueda tener la empresa para poder acceder a lo que les interesa, normalmente información o datos con los que cometer sus delitos; por otro lado, usan métodos de inteligencia de fuentes abiertas, también llamado OSINT, que no es más que una recopilación de datos y análisis de la información pública que se puede encontrar en internet, como en las redes sociales, sitios web corporativos, foros, publicaciones, registros públicos, etc, es decir, información que se puede obtener de cualquier fuente que este abierta a internet, y que después de obtenerla la analizan y explotan según les convenga. Hacen un estudio de todos los trabajadores, sus puestos de trabajo y su información personal. Esto les permite identificar roles y recursos a los que tienen acceso. También



se estudian empresas asociadas, proveedores o colaboradores; es en ese sentido que vez que sabemos cómo actúan los ciberdelincuentes, la investigación de los delitos que cometen no difiere mucho del resto, aunque sí hay que tener en cuenta unas ciertas consideraciones; es cierto también que nos enfrentamos a hechos delictivos novedosos, como el phishing, el smishing, whatsapping, hacking, cracking, pharming, skimming, carding, "man in the middle" (mitm), sexting no consentido, etc, que en principio hasta nos puede generar dudas, llegando incluso a pensar que la presunta víctima pueda estar engañando. Por ejemplo, esta situación ocurrió en España la primera vez que se dio una denuncia por una estafa conocida como Man in the middle, y que al denunciar parecía imposible que hubiera ocurrido como se contaba, pensando incluso que pudiera tratarse de una estafa de la propia empresa. No fue hasta que los investigadores detectaron el modus operandi delictivo cuando se dio certeza a la denuncia; en consecuencia, el procedimiento de investigación debe tener al menos:

- 1.- Comprobar la veracidad del hecho
- 2.- Averiguar IP desde donde se cometieron los hechos objetos de investigación. Si se trata de una IP dinámica consultar con la empresa suministradora para saber a quién estaba asignada en ese momento.
- 3.- Usuario de la IP investigada.
- 4.- En el caso del uso de celulares, hacer la misma operativa con el número del celular.
- 5.- Número de tarjeta (débito o crédito) utilizada.
- 6.- Número de cuenta (IBAN si se conoce) de autor y/o víctima, y cantidad defraudada.
- 7.- Datos conocidos del posible autor (Nick, casos de anuncios, alquileres, venta o subastas).
- 8.- Comercio dónde se utilizó la tarjeta (física o virtualmente) o página web utilizada para el fraude.
- 9.- Mail que utilice el autor.
- 10.- Consultar con las bases de datos policiales. Analizar la información obtenida.
11. Existen herramientas en internet gratuitas y públicas donde se pueden hacer consultas.
- 12.- También es muy relevante incluir en la investigación un informe patrimonial del autor o autores. Se aplicará una metodología y un protocolo determinado, con una estructura sencilla y con un relato cronológico adecuado.
- 13.- Garantizar la cadena de custodia de todas las pruebas digitales obtenidas; empero en este tipo de investigaciones nos encontramos en diferentes dificultades como la competencia judicial, identidades falsas, multas y ubicación de servidores en el extranjero. Durante la investigación también se pueden utilizar informáticos, donde el Juez inspector podrá utilizar a la policial judicial a actuar en comunicaciones de canales cerrados intercambiando o enviando por sí mismo archivos ilícitos por razón de su contenido. Desde el inicio de la investigación se debe realizar un análisis de inteligencia adecuado y exhaustivo, para ser más eficientes, debido a que muchos de los delitos cibernéticos, como el phishing, smishing, etc, tienen multitud de víctimas. Así se gestionan de manera adecuada los recursos, muchas veces limitados, afectando positivamente en las investigaciones. Tanto para las investigaciones como para su judicialización es muy importante dar relevancia a la formación de todos los actores, desde los investigadores hasta los fiscales y magistrados, no necesariamente dando un conocimiento exhaustivo, pero sí que puedan conocer las técnicas y procedimientos que utilizan los ciberdelincuentes. En cuanto a la persecución de estos delitos, en España se están creando grupos especializados, tanto de cibercrimen como de todo lo relacionado con las criptomonedas. También se están centralizando investigaciones con un mismo origen delictivo, y, por supuesto, se está potenciando la colaboración policial internacional, al ser el cibercrimen un hecho globalizado, a través de Interpol y Europol.



TERCER DIA

“CRIMINALIDAD ORGANIZADA, ECONOMÍAS ILEGALES Y LAVADOS DE ACTIVOS EN EL PERÚ: IMPACTO EN LA CIFRA NEGRA”

Dr. VÍCTOR ROBERTO PRADO SILDARRIAGA

Juez Supremo Titular de la Corte Suprema de la República, actualmente Presidente de la Sala Penal Transitoria, Presidente del Grupo de Alto Nivel para la Aplicación de la Pena Justa y contra Cibercriminalidad Organizada, Abogado de la Universidad Mayor de San Marcos y Doctor en Derecho por la Universidad de Valencia – España, ha realizado estudios de especialización en Derecho Penal y Política Criminal en el Max Planck Institut für Strafrecht de Freiburg im Breisgau en Alemania y en las Universidades de Alcalá de Henares y Alicante en España, también ha realizado cursos internacionales sobre Políticas de Control y Prevención del Trafico Ilícito de Drogas, Lavado de Dinero y Crimen Organizado en varios países Europeos y América.

Hace 37 años la convención de Viena dio origen a la criminalización internacional del lavado de activos con el propósito de interdictar el rendimiento económico, así como reducir las capacidades de reinversión y crecimiento de la criminalidad organizada como plano internacional, que en aquel entonces se encontraban representadas por el Trafico Ilícito de Drogas; es así que, transcurrido el tiempo desde aquel entonces, podemos constatar que la criminalidad organizada no solo se ha diversificado y crecido adquiriendo la condición de amenaza híbrida global sino que además su modelo económico ha logrado producir la implacable de tres a cinco billones de dólares por año; es en ese sentido que el informe de Europol de 2025 reporta que la criminalidad organizada contemporánea se ha transformado y potenciado su modus operandi a través del ciberespacio con el empleo de criptomonedas e inteligencia artificial para la ejecución y ocultamiento del delito, lo que lleva a una nueva ruta respecto a las ganancias de origen criminal conocidas como el lavado de activo virtual – criptolavado, estructurados bajo la siguiente ruta: La colocación (los fondos ilegales se introducen en el sistema de criptomonedas a través de diversos medios como comprarlos en un intercambio, minarlos o recibirlos como pagos por actividades ilícitas); Estratificación (serie de transacciones distintas a ocultar la propiedad de los fondos, como convertirlos en diferentes criptomonedas, transferirlos a múltiples cuentas o utilizar servicios de mezcla que agrupan múltiples transacciones para ocultar el origen de los fondos); Integración (los fondos lavados se devuelven al sistema financiero legítimo como fondos aparentemente legales, ya sea vendiendo las criptomonedas por moneda fiduciaria o usándola para comprar bienes o servicios); de modo que, los ciberdelincuentes implicados en



ciberataques y servicios relacionados, así como los que comercian y administran mercados en la web oscura, realizan sus transacciones financieras casi exclusivamente en criptomonedas, es por esta razón que hacen un amplio uso de técnicas de ofuscación para anonimizar sus actividades financieras antes de cobrar los beneficios ilícitos; por consiguiente, el PACCTO 2.0 en un informe de 2024 destacó que la aplicación de criptomonedas en las operaciones de lavado de las ganancias ilegales con herramientas de inteligencia artificial es un *modus operandi* más eficaz y seguro, que permite a las organizaciones criminales ocultar el origen ilícito de sus ingresos mediante transacciones automatizadas y complejas redes financieras que evaden los controles tradicionales ellas realizadas mediante algoritmos de la IA. Cabe destacar que recientemente Argentina (2023), Brasil (2022) Chile (2022) y Colombia han formalizado reformas en su legislación nacional sobre delitos de lavado de activos para comprender expresamente los activos virtuales; en esa misma línea, bajo los nuevos estándares internacionales a iniciativa de la delegación peruana la convención de las Naciones Unidas incluyó expresamente el término “Activo Virtual” entre las definiciones contenidas en el artículo 2 sobre bienes; de modo tal que, los activos virtuales ahora son un tipo especial de bienes según la convención de las Naciones Unidas contra la Ciberdelincuencia, considerando que ello evitaría problemas hermenéuticos futuros que afecten la criminalización interna de las operaciones de lavado con activos virtuales, así como los procedimientos de cooperación judicial internacional entre los estados por ese delito; firmando el Convenio de Hanoi el 25 de octubre de 2025. En el Perú se estimó que las principales economías ilegales entre los años 2023 y 2024 produjeran más de 12 millones de dólares por año y en el 2025 bordearan los 20 millones de dólares, teniendo como flujo el capital de economías ilegales hacia el lavado de activos virtuales; por cuanto, las habilidades que favorecen las operaciones de lavado de activos virtuales en el Perú y su cifra negra se desarrollan en los sectores económicos y población económicamente activa con alta tasa de informalidad, entornos sociales con sensibles carencias de conectividad para la identificación y supervisión de proveedores de servicios de activos virtuales formales, informales y criminales, contando con instrumentos normativos de regulación, prevención aun básicos e insuficientes, sobre todo con ausencia de una unidad jurisdiccional especializada en competencia para delitos de lavado de activos virtuales; frente a ello como estrategia y alternativas institucionales desde el Poder Judicial para disminuir la cifra negra, se debe elaborar un acuerdo plenario sobre tipologías de lavado de activos virtuales asociados a la criminalidad organizada, generar la organización y constitución de la unidad jurisdiccional especializada para procesamientos de delitos en cibercriminalidad organizada y con empleo en inteligencia artificial, así como el de presentar un proyecto de Ley para adaptar la criminalización de delitos de lavados de activo y los nuevos estándares internacionales, fomentar el desarrollo de un programa que consolide en base a una tabla única de delitos la interoperatividad entre UIF, PNP, MP, PJ, IMPE y produzca estadísticas homogéneas sobre frecuencias y tipologías de lavado de activos virtuales.

“CONVENIO DE NACIONES UNIDAS CONTRA LA CIBERDELINCUENCIA”

Dra. MARIA DE LOURDES GUTIERREZ ORTIZ MONASTERIO

Abogada Especialista de Derecho Penal, Criminología, Derechos Humanos y Cibercrimen, Coordinadora Regional del Programa Global de Cibercrimen de la UNODC para Centroamérica y el Caribe, con sede en Panamá.

La convención de las Naciones Unidas contra la ciberdelincuencia, es el nuevo mecanismo internacional que servirá para fortalecer la cooperación internacional en la lucha contra los delitos cometidos mediante las Tecnologías de la Información y las Comunicaciones y para el intercambio de pruebas electrónicas de delitos graves; asimismo, es el primer tratado mundial para hacer frente al uso indebido de la tecnología con fines delictivos y el primer tratado de justicia penal en más de 20 años que ha proporcionado un marco global para prevenir y combatir la ciberdelincuencia, reforzar la cooperación internacional y permitir a investigadores y fiscales transmitir pruebas a través de las fronteras. Las tecnologías de la información y las comunicaciones están transformando nuestra vida en innovación, difusión de conocimientos y conectividad entre las personas, pero esa promesa de revolución digital conlleva de la mano muchos riesgos, como la ciberdelincuencia que es una de las amenazas de más rápido crecimiento en nuestro mundo actual, en la que los delincuentes se aprovechan de su rapidez y anonimato para perpetrar ataques a través de las fronteras, mediante todo tipo de actividades como ransomware, phishing, suplantación de identidad, el robo de datos, estafas, grooming, sextorsión, y difusión de material de abuso sexual infantil, que son direccionados a que dichas conductas sean regladas para regular las conductas individuales y organizadas bajo medidas procesales para la prevención y adquisición de pruebas electrónicas de investigación de cualquier tipo de delito penal direccionado a cooperaciones internacionales y medidas procesales internacionales para cooperación de pruebas en materia de pruebas electrónicas como conservación, revelación recolección, acceso e interceptación de datos 24/7, extradición y otros, bajo políticas de coordinación y mejoras prácticas; en ese mismo orden, es de señalar que la tecnología también contribuye a exacerbar otros delitos como el tráfico ilícito de drogas, el contrabando de armas, lavado de dinero, utilizando la dark web y criptomonedas para buscar el cifrado, el anonimato de las conexiones IP que dificulta en gran medida las investigaciones; de otro lado, también existen tendencias a futuro y amenazas emergentes con distintas modalidades digitales que conforme al violentómetro digital contamos con la IA generativa (deepfakes sexuales, CSAM sintética o voice – cloning & chat-bots), cripto-economía (sextorsión y revenge porn “pay-offs”, estafas románticas o lavado de ganancias), IoT Ubicuo (stalkerware doméstico, Etiquetas de rastreo



“Airtags/GPS” o filtración de datos fisiológicos) Anonimato Cifrado (canales cifrados “Tor, I2P, Telegrama, E2E” o encubrimiento de grupos “Incel” y misógenos), Realidad virtual aumentada y metaverso (Acoso y agresión sexual en VR, ciber-exposición 360° o estafas NFT/skins dirigidas a jugadores jóvenes); lo que demuestra que las consecuencias son reales y pueden ser devastadoras, erosionadas a través de la confianza que ponen en peligro la vida y medios de subsistencia, aumentando los riesgos para la paz y la seguridad de las naciones, motivo por el cual resulta de vital importancia que se conozca que el crimen se está cometiendo utilizando las TICs y el ciberespacio y como podemos organizarnos para combatirlo bajo los siguientes retos: Creación de comisiones nacionales sobre ciberdelitos y ciberseguridad – Gobernanza digital, cadenas de custodia digital – Valores Hash, costumbres – confianza – autorización previa del Juez – autorización posterior – temor a cambiar la forma de investigar, agente encubierto digital – patrullaje cibernético, ley de protección de datos – revelación – acceso a datos de usuario sin necesidad de una orden judicial, rompimiento de contraseña – fuerza bruta – huella – reconocimiento facial, auditorías forenses, identificación de víctimas – clientes – productores, regulaciones para expedientes electrónicos, regulaciones de criptomonedas – su decomiso – almacenaje – brokers – casas cambio, exchangers, entre otras.

“RAZONAMIENTO PROBATORIO EN LAS CONDUCTAS DE CIBERCRIMINALIDAD”

Dr. LUIS JORGE GAMBOA OLEO

Doctor en Derecho, Maestro en Derecho Penal, Especialista en Cibercrimen, Ex Magistrado Presidente del Superior Tribunal de Justicia de Morelos – Cuernavaca, Profesor Universitario de la Universidad de Medellín, Universidad de Morelos y capacitador en materia penal en Centro América y Sudamérica.

El razonamiento probatorio es el proceso por el cual jueces evalúan la evidencia presentada por la fiscalía y abogados en un juicio para construir y justificar una conclusión, se diferencia de un enfoque puramente normativo al sentarse en los hechos y la forma de probarlos, asegurando que las decisiones judiciales estén motivadas y basadas en la evidencia, lo que aporta racionalidad y objetividad al proceso y aunque la certeza absoluta es inalcanzable, el razonamiento probatorio busca la verdad relativa y aproximativa, donde lo decidido o resuelto se acerque a lo mas posible de lo que realmente sucedió; ahora bien, en la irrefrenable digitalización de la sociedad actual, el ámbito jurídico no se queda atrás, la evidencia electrónica comúnmente referida



como prueba digital, puede ser determinante cuando se presente documentación electrónica (correos electrónicos, archivos de Word, Excel o PDF, hojas de cálculo y demás documentos similares), registro de comunicaciones (historial de chats, llamadas VoIP, mensajes en aplicaciones de mensajería, entre otros), contenido multimedia (fotografías, grabaciones de audios y videos), datos almacenados (comprende la información en discos duros, unidades USB y otros dispositivos de almacenamiento), registro de navegación web (almacenan historiales de navegación, cookies y otros datos asociados a la actividad online), metadatos (datos que describen otros datos, como fechas de creación o modificación de archivos), registro de transacciones, datos de geolocalización, registro de redes sociales, registro de acceso y seguridad, datos en la nube, datos de aplicaciones específicas; no obstante es de precisar que la evidencia electrónica y la evidencia digital son términos que si bien es cierto se encuentran relacionados estos no son sinónimos, toda vez que la evidencia digital se refiere a cualquier información almacenada o transmitida en formato digital, por el contrario que la evidencia electrónica se enfoca en el hardware o dispositivo electrónico que contiene dicha información, mientras que la evidencia electrónica son los medios físicos donde se encuentra, para conceptualizarlo, de ejemplo tenemos que un correo electrónico que contiene información relevante sobre un caso sería la evidencia digital, sin embargo la computadora desde la cual se envió el correo sería la evidencia electrónica; es así que, a diferencia de otro tipo de pruebas como puede ser la documentación de papel, las evidencias electrónicas son pruebas físicas aunque de carácter intangible, ya que generalmente son rastros almacenados en equipos

informáticos, lo que demuestra que un ordenador registra los datos o logs de todas las actividades que realiza y estas resultan ser fundamentales en las investigaciones informáticas siempre que se pueda comprobar que estas han sido manipuladas para dichos fines ilícitos. El razonamiento probatorio en la cibercriminalidad implica también la aplicación de principios lógicos para valorar la prueba digital como datos de sistemas, comunicaciones, etc; para producir hechos probados a partir de ellas, superando los desafíos de la autenticidad la integridad y la cadena de custodia a partir de los indicios digitales; asimismo, es fundamental que los jueces respeten el principio de contradicción, garantizando el acceso a toda la prueba, ya que esta no puede ser ocultada a ninguna de las partes. La pirámide de valoración de la prueba prioriza la libertad probatoria y la licitud como base, la cibercriminalidad exige un razonamiento probatorio con un análisis riguroso y la apertura mental de los jueces, reconociendo la existencia de evidencia digital, aunque no esté regulada en los códigos. Los principales desafíos son: entender la existencia de la prueba electrónica, usarla para la reconstrucción de la verdad, y garantizar su integridad y autenticidad mediante técnicas forenses como el hash y la preservación de metadatos. El ciberespacio introduce la volatilidad y fragilidad de la evidencia digital, que puede ser programada para desaparecer, haciendo crucial la cadena de custodia. Un reto fundamental es el anonimato y la atribución, es decir, vincular la creación de contenido digital a una persona específica. La competencia técnica de jueces y abogados debe mejorar, junto con la cooperación por la transnacionalidad del delito, buscando homologar leyes entre países. En esencia, el derecho procesal debe adaptarse a la era digital basándose en la lógica y la ciencia forense, para garantizar un juicio justo y respetando el trabajo de todos los actores del proceso. Que en México tienen una etapa intermedia en que la Fiscalía se descubre probatoriamente y permite a la defensa conocer los registros, conforme al Código Nacional de Procedimientos Penales de México implica que, si la Fiscalía tiene fotos a color o un plano, estas mismas fotos a color o plano deben ser entregadas a la defensa pudiendo ser excluidos si no fueron entregados en los mismos términos. En cuanto a la prueba por indicios éstas se asemejan a las pesquisas y es indiciaria porque no se tiene claro qué se está investigando, por ello siempre tiene que haber una conexión entre lo que se está investigando, el acto que se está proponiendo y cómo se está desahogando, para tener certeza; a los operadores de justicia no se les exige valorar ni prevalorar las pruebas, sino mantener la lógica entre la investigación, la solicitud de pruebas y lo obtenido; y la cadena de custodia digital es un tema crucial que requiere legislación, regulación y preparación técnica urgente. Esto es indispensable para el correcto manejo y validez de la prueba electrónica y digital en los procesos judiciales modernos.

“CIBERCRIMINALIDAD: CIBER ATAQUES, ANALISIS Y CONSECUENCIAS PUNITIVAS”

Dr. DANIEL IVAN TAIPE DOMINGUEZ

Coronel de la Fuerza Aérea del Perú, Ingeniero de Sistemas, Licenciado en Administración, Magister en Informática, Magister en Administración y Doctrina, certificaciones internacionales en Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), Certified Security Analyst (ECSA), Certified Eccouncil Instructor (CEI), Diplomado en Ciberseguridad en el Centro de Altos Estudios Nacionales (CAEN), actualmente Docente en el Diplomado y en la Maestría de Ciberseguridad, Diplomado en Seguridad Informática y Técnicas de Anti Hacking por la Institución StackOverflow en Madrid – España, Diplomado en Cibersecurity Executive Training en la Universidad de Jerusalén – Israel, Curso Ejecutivo, Desarrollo de Políticas Cibernéticas en Washington – EEUU.

Hace 35 años ya existían personas que pensaban que el uso del internet era un peligro ya que el solo hecho de conectarnos a través de un modem ya generaba un riesgo, que fue previsto por hackers mucho antes de que se popularizara su uso, lo cual evidencia una enorme ventaja de tiempo en temas de seguridad, entonces imaginémonos el tiempo que nos pueden llevar de adelanto estos hackers en temas de ciberseguridad, pero para contextualizar lo precedente debemos de saber que el cibercrimen son delitos que utilizan sistemas y redes informáticas para robar información extorsionar o interrumpir operaciones digitales, teniendo como objetivos principales datos personales, financieros, de propiedad intelectual, secretos comerciales, generar la interrupción de negocios para exigir rescates, a través de ingeniería social, manipulación psicológica, phishing, suplantación de identidad, malware, ransomware y software maliciosos, entre otros, que según el foro económico mundial precisa que el 71% de los expertos a advertido que las defensas tradicionales son insuficientes para las nuevas ciberamenazas, teniendo como sectores mas afectados el de Salud y las Instituciones gubernamentales en Latinoamérica, esta tendencia se evidencio en ataques devastadores que comprometieron datos sensibles y la operatividad de servicios críticos en toda la región; entonces, la vulnerabilidad de estos sectores subraya la necesidad urgente de fortalecer las ciberdefensas y proteger la infraestructura critica garantizando la continuidad de los servicios para mantener la confianza de los ciudadanos en las instituciones, de ejemplo tenemos el ataque a un hospital infantil en Perú, que sufrió un cifrado de 30GB de datos por ransomware, mientras que en Argentina se filtraron 665,000.00 imágenes médicas, demostrando una grave amenaza; aunado a ello, es de poner en conocimiento que en el año 2024, el ransomware afecto a mas de 100 países y paralizó hospitales lo que evidencia



la creciente sofisticación y el impacto masivo de los ataques, que conforme a su evolución y nuevas tendencias en el 2025 se incluyó la IA Generativa, gestión colaborativa de riesgos, optimización tecnológica y enfoque en la resiliencia cibernética, lo que nos conlleva a recomendar las siguientes medidas de resguardo y recomendaciones como la autenticación multifactor (utiliza múltiples capas de seguridad para verificar la identidad del usuario y proteger las cuentas), capacitación continua (educar sobre la ciberamenazas y las mejores prácticas para fortalecer la primera línea de defensa), iniciativa gubernamental (Perú impulsa el programa virtual gratuito de ciberseguridad y ciberdefensa 2025), prevención proactiva (activar estrategias para mitigar riesgos y combatir el cibercrimen el Perú y el mundo); bajo esa misma línea, es de útil importancia conocer cual es la forma de trabajo del hacker, que cuenta con un proceso metódico y similar al de un ladrón, mismo que se desarrolla en las siguientes fases: el reconocimiento (recolección pasiva de información sobre la víctima), el escaneo (uso de herramientas para identificar vulnerabilidades como puertos abiertos o falta de parches), la explotación o ataque (creación del vector de ataque más eficiente), el mantenimiento (dejar accesos abiertos para un futuro ingreso) y el borrado de huellas, eliminando o alterando el log del sistema, que funciona como la "cicatriz" de toda actividad forense. Se demostró la facilidad con que se pueden obtener herramientas, incluso gratuitas o de bajo costo (como keyloggers que capturan usuarios y contraseñas), para escanear redes, romper passwords wireless o extraer metadatos de sitios web públicos, subrayando que la tecnología para el ataque es fácilmente accesible para cualquiera que sepa dónde buscar.

“LOS DELITOS INFORMATICOS – OPTICA DE LA JUSTICIA ECUATORIANA FRENTE AL PLURIOFENSIVO CIBERDELITO”

Dr. JULIO AGUAYO URGILES

Juez Provincial de la Corte del Guayas, con amplia trayectoria en el Sistema de Justicia Ecuatoriano, Ex Director Nacional del Consejo de la Judicatura, Presidente de la Corte Provincial, Juez Penal y Agente Fiscal, Magister en Ciencias Internacionales y Diplomacia, Autor de 17 Obras Jurídicas, Conferencista Nacional e Internacional, Docente Universitario.

La seguridad ha sido una preocupación constante a lo largo de la historia, esencial para la estabilidad y el desarrollo de las sociedades, sin embargo en el siglo XXI la naturaleza de las amenazas ha evolucionado rápidamente debido a los avances tecnológicos y los cambios globales; es así que, con la digitalización en todos los aspectos de la vida moderna, la ciberseguridad ha emergido como un desafío crucial ya que los ciberataques con cada vez más frecuentes y sofisticados, abordando desde el ransomware hasta avanzados esquemas de phishing paralizando estructuras críticas, robar datos personales como empresariales que causan enormes pérdidas económicas, pero para mitigar estos riesgos, es necesario desarrollar sistemas de ciberdefensas robustos, capacitar a profesionales en ciberseguridad y concienciar al público sobre las amenazas; por cuanto ya tenemos claro que el internet y las cosas han revolucionado la forma en que interactuamos con la tecnología conectando miles de millones de dispositivos a la red, sin embargo esta conectividad también aumenta la vulnerabilidad de los ataques, de ejemplo tenemos los dispositivos IoT inseguros que pueden servir como puertas de entrada para comprender sistemas más grandes, afectando la seguridad personal y pública, motivo por el cual la implementación de estándares de seguridad y el diseño seguro desde el inicio son fundamentales para protegernos de estas amenazas. De otro lado, tenemos a las redes criminales transnacionales aprovechan la globalización y la tecnología para expandir sus actividades ilícitas, como el tráfico de drogas, armas y personas. Estas actividades no solo socavan la seguridad de las naciones, sino que también afectan la estabilidad económica y social de las ciudades en crecimiento y modernas que enfrentan desafíos significativos en términos de seguridad con el crimen organizado que conlleva a la violencia es así que la tecnología de vigilancia puede ayudar a gestionar otros problemas pero a su vez plantea preocupaciones sobre la privacidad y desinformación que representa una amenaza crítica ya que estas pueden paralizar sociedades y socavar la confianza de las instituciones, entonces para combatir el problema que se desarrollan ante procesos democráticos por la falta de desinformación e información falsa que se distribuye en las redes sociales, se requiere una educación mediática con regulación en plataformas digitales y desarrollo de tecnologías para detectar y mitigar la desinformación; de otro lado, también se ha sumado



la inteligencia artificial y la automatización que se encuentran transformando sistemas de seguridad que presentan oportunidades como riesgos, es así que, las decisiones autónomas en contexto crítico pueden tener consecuencias imprevistas y es crucial establecer marcos éticos para el desarrollo y uso de esta tecnología con parámetros de preparación para tecnologías emergentes, como la computación cuántica para proteger la información en el futuro; otro de las evoluciones es la biotecnología que conforme a sus avances ofrece prometedoras soluciones en campos como la medicina y la agricultura pero también presentan riesgos de seguridad biológica, con la posibilidad de crear organismos genéticamente modificados o patógenos sintéticos que plantea preocupación sobre el bioterrorismo y los accidentes de laboratorio motivo por el cual es crucial establecer regulaciones estrictas y promover la cooperación internacional para supervisar la investigación de biotecnología asegurando que esta se realice de manera ética y segura; sin embargo esta no es la única preocupación de los avances de la ciencia y la tecnología sobre la seguridad tierra si no también en el espacio que a medida que las naciones y empresas privadas explotan y utilizan esta última, surge el cuidado respecto a la congestión de satélites, riesgo de colisión y la militarización del espacio que son temas que requieren una gobernanza global efectiva, para establecer normas y acuerdos internacionales para el uso pacífico y sostenible del espacio que es esencial para prevenir conflictos y garantizar el acceso equitativo a los recursos espaciales. Ahora bien, es de precisar que los desafíos de seguridad en el siglo XXI son complejos y multifacéticos, que requiere un enfoque integral que convine tecnología, política y participación ciudadana, contar con una cooperación global con innovación continua para desarrollar estrategias efectivas y garantizar un futuro seguro, ya que al abordar estos desafíos con creatividad y colaboración podemos construir un mundo más seguro y equitativo para todos, acompañados de herramientas tecnológicas para combatir la delincuencia como la inteligencia artificial - análisis de datos (Big Data), vigilancia y monitoreo inteligente, análisis forense digital, robots de seguridad y drones, entre otras técnicas disruptivas para combatir las y superarlas, con una legislación actualizada, tecnología avanzada, cooperación internacional y concientización de la población.

“ALTERNATIVAS DE PREVENCIÓN DEL CIBERCRIMEN: PRIVACIDAD, IA, OPEN BANKING”

Dr. MAURICIO GARRO GUILLÉN

Master en Empresas Internacionales y Comercio Exterior por la Universidad de Barcelona y Master en Derecho de la empresa por la Universidad Pompeu Fabra - España, Excoordinador General del ILANUD y Ex Director General de Preservación de Datos en Costa Rica, con experiencia en Derecho Empresarial, Comercio Internacional y Protección de Datos.

La identidad digital en esencia es una colección de atributos y credenciales recopiladas de forma automatizada que describen de manera única a una persona dentro de un sistema digital o entorno de red, siendo el equivalente de la persona física en el mundo digital, también se constituye por todo el andamiaje de expresiones que terceros hacen de nosotros en el ciberespacio y es el conjunto de información que dejamos al navegar en el ciberespacio; de otro lado, tenemos los datos sensibles en el que se prohíbe el tratamiento de datos personales que rebelan el origen racial o étnico, las opciones políticas, las convenciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de forma unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física; así como, los datos biométricos resultantes de un tratamiento técnico específico relativos a las características físicas, fisiológicas o comportamiento de una persona física que permitan o confirmen la identificación única de una persona, dentro de estas características tenemos: las conductuales (responden a acciones, comportamientos y respuestas de los individuos en su entorno); las fisiológicas (replican al funcionamiento del organismo humano); y, las físicas (refiere a las huellas dactilares, rasgos físicos patrón del iris, geometría de las manos y estructura de las venas); empero, ello debe de estar debidamente relacionado a la responsabilidad proactiva de tratamiento de datos que se direcciona a la seguridad de la información, transparencia sobre la documentación, análisis y evaluación buenas prácticas, bajo sus principios rectores como el de licitud, transparencia y lealtad que justifique el legítimo tratamiento; además de que el interesado ha de tener total claridad de que datos suyos están siendo recopilados y en que medidas serán utilizados generando la accesibilidad de un lenguaje claro y sencillo, con el objeto de que el interesado pueda conocer exactamente los fines con los que se realizará el tratamiento, igualmente se prohíbe que el tratamiento que no se ajuste específicamente a las finalidades autorizadas, con la limitación del plazo de conservación, seguridad, integridad, disponibilidad, confidencialidad de los datos personales, responsabilidad proactiva y exactitud que obliga a mantener los datos tratados actualizados, suprimir o modificar los



mismos en el momento que los mismos recaigan en exactitud; asimismo, el reglamento de (UE) 2024/1183 reforma la identidad digital, en el que cada usuario podrá utilizar servicios en línea, compartir documentos digitales como una licencia de conducir móvil o una receta electrónica, abrir cuentas bancarias o realizar pagos con total control de datos personales; además, el programa Europa Digital, desarrolla cuatro componentes piloto de estudio en más de 360 empresas y entidades públicas de 26 países de la Unión, con un costo de UD\$ 46 millones, que para el 2026 todos los países de la Unión Europea deberán operar al menos con un monedero digital; entre otras regulaciones tenemos el Reglamento UE 910/2014 eIDAS Identificación Electrónica y Servicios de Confianza, Reglamento (UE) 2022/2065 Servicios Digitales, Segunda Directiva de Servicios de Pago (PSD2) 2015.

Ahora bien, cuando nos referimos a neuroderechos estos se pueden definir como los principios éticos, legales, sociales o naturales de libertad o titularidad relacionados con el dominio cerebral y mental de una persona; es decir las reglas normativas fundamentales para la protección y preservación del cerebro y la mente humana, que cuenta con principios interamericanos en materia de neurociencia, neurotecnologías y derechos humanos (OEA 2023), como es el de identidad, autonomía, privacidad de la actividad neuronal (fomenta preservar y garantizar el control de cada persona sobre su propia identidad individual; así como, asegurar la autodeterminación y la libertad de pensamiento de las personas), protección de los derechos humanos desde el diseño de neurotecnología (busca la protección integral del respecto de los derechos humanos a partir del diseño de las neurotecnologías, métodos de investigación como la implementación, comercialización y uso del mismo), datos neurales como datos personales sensibles (la persona responsable del uso y tratamiento de los datos neuronales su obligación es adoptar medidas de seguridad y privacidad bajo sus límites de aplicación y técnicas y evitar que esos datos por su descodificación sean compartidos a terceros), consentimiento informado, no discriminación y acceso equitativo a las neurotecnologías e integridad neurocognitiva, supervisión y fiscalización de las neurotecnologías, acceso a la tutela efectiva y acceso a remedios asociados al desarrollo y uso de las neurotecnologías que establece un marco a fin de proteger los neuroderechos dentro de su libre albedrío, privacidad, acceso e identidad personal, psíquica, moral de las personas.

“SOCIEDAD DE LA INFORMACION, CIBERDELINCUENCIA Y ORGANISMOS INTERNACIONALES”

Dr. JUAN CARLOS CARRETERO

Doctor en Derecho y Especialista en Cibercriminalidad por la OEA y la Universidad de León, Vicedecano de la Facultad de Derecho y posgrado de la Universidad de Concepción Uruguay, asesor del Ministro de Relaciones exteriores de Argentina, Autor de Diversos Artículos sobre Cibercrimen y Derechos Internacionales.

La sociedad de la información surge a finales del siglo XX para describir un modelo social en el cual la producción, circulación y uso de la información se convierten en los principales motores del desarrollo económico, político y cultural. Castells (2010) sostiene que esta transformación no es meramente tecnológica, sino estructural: redefine las relaciones de poder, las formas de interacción social y los procesos productivos; siendo que, la UNESCO (2005) amplía esta perspectiva al señalar que la sociedad de la información implica no solo acceso a tecnologías, sino también la capacidad de utilizarlas para generar conocimiento; en este sentido, la información se convierte en un recurso estratégico comparable a los recursos naturales tradicionales, pero con una particularidad: su capacidad de reproducirse y circular sin límites físicos, contando con tres pilares que sostienen este paradigma que son: La Comunicación (comprende la expansión de internet y las redes digitales ha generado un ecosistema de hiperconectividad global. La comunicación deja de ser lineal y se vuelve interactiva, descentralizada y multidireccional); Innovación tecnológica (comprende tecnologías como la inteligencia artificial, la computación cuántica y el internet de las cosas impulsan nuevas dinámicas económicas y sociales “European Commission, 2021”); y Datos (comprende la economía contemporánea se estructura en torno al procesamiento masivo de datos “big data”, lo que plantea desafíos éticos y regulatorios vinculados a la privacidad, la vigilancia y la seguridad “OCDE, 2019”) en el que la digitalización no solo transforma la vida cotidiana, sino también las instituciones, los mercados y los sistemas jurídicos.



La cibercriminalidad como fenómeno global emerge como una consecuencia directa de la expansión digital. Goodman (2015) describe este fenómeno como un “nuevo territorio criminal” caracterizado por su bajo costo operativo, su alta rentabilidad y su capacidad de afectar simultáneamente a millones de personas; misma que cuenta con tres características estructurales que la definen como: Anonimato (la arquitectura técnica de internet permite ocultar identidades mediante redes privadas virtuales, cifrado y técnicas de suplantación. Esto dificulta la atribución de responsabilidades y desafía los modelos tradicionales de investigación penal); Economía del Delito (Los cibercrimenes requieren poca

infraestructura, pueden automatizarse y escalar globalmente. Desde fraudes financieros hasta ataques de ransomware, la economía criminal digital se ha profesionalizado, generando mercados ilícitos altamente organizados “Goodman, 2015”); Internacionalidad (la transnacionalidad es el rasgo más problemático. Los ataques pueden originarse en un país, ejecutarse desde servidores ubicados en otro y afectar a víctimas en múltiples jurisdicciones. La ONU (2021) destaca que esta fragmentación dificulta la cooperación judicial y exige marcos normativos armonizados; por lo tanto, la ciberdelincuencia no puede abordarse desde una perspectiva exclusivamente nacional: requiere coordinación internacional, estándares comunes y mecanismos ágiles de cooperación). En esa misma línea contamos con las respuestas institucionales de los organismos internacionales y marcos normativos como la ONU que ha desarrollado instrumentos orientados para fortalecer la cooperación internacional en materia de ciberdelincuencia, y el convenio sobre Ciberdelincuencia que se abrió a la firma el 25 de octubre de 2025 como principal marco de referencia global para la tipificación de delitos informáticos y la cooperación transfronteriza; además de la UNODC que promueve programas de asistencia técnica para fortalecer capacidades estatales de investigación digital, preservación de evidencia electrónica y cooperación digital; asimismo, contamos con la Organización de los Estados Americanos (OEA) en el ámbito regional, la OEA ha sido un actor clave que a través del Comité Interamericano contra el Terrorismo (CICTE), impulsa programas de ciberseguridad, capacitación técnica y fortalecimiento institucional, en esa misma perspectiva la Reunión de Ministros de Justicia de Iberoamérica (REMJA) ha promovido lineamientos para la armonización legislativa y la cooperación penal en delitos informáticos (OEA, 2019). Y como proceso de integración regional se ha generado marcos relevantes como el Convenio de Budapest, Mercosur, Ley de Inteligencia Artificial de la Unión Europea, que reflejan una tendencia global hacia la construcción de un ecosistema normativo que permita enfrentar amenazas digitales desde una perspectiva coordinada y multilateral, pero que distan de normar sobre la responsabilidad por los daños ocasionados, sobre todo en materia de Inteligencia Artificial, lo que nos hace concluir que la sociedad de la información constituye un nuevo paradigma estructural que redefine la economía, la política y la vida social. Sin embargo, su consolidación depende de la capacidad de los Estados y organismos internacionales para enfrentar la ciberdelincuencia mediante marcos normativos coherentes, cooperación transnacional y políticas públicas orientadas a la seguridad digital. La capacitación y el conocimiento de los tratados internacionales por parte de los operadores del derecho son fundamentales a la hora de resolver los problemas vinculados con la ciberdelincuencia. La articulación entre tecnología, derecho y gobernanza global será determinante para garantizar un entorno digital seguro, inclusivo y respetuoso de los derechos fundamentales.

“PALABRAS DE CLAUSURA DEL PRIMER CONGRESO INTERNACIONAL DE CIBERCRIMEN”

Dr. WALTER ELEODORO MARTÍNEZ LAURA
Ministro de Justicia y Derechos Humanos



Que, por dirección y en representación del Presidente Constitucional de la Republica del Perú José Enrique Jerí Oré; y, con la finalidad de velar por el orden y seguridad de la Republica así como el adecuado, correcto, valioso y eficaz aporte de la Corte Superior de Justicia de Lima, que como pretensión al bienestar de la ciudadanía frente al eje e impulso de prevención para combatir la criminalidad y su evolución a través de las tecnologías de la información y sus comunicaciones así como el de capacitar a Magistrados y servidores jurisdiccionales del sistema de justicia, es que la presente actividad académica para una visión clara y actualizada sobre la amenazas digitales que enfrenta al estado Peruano, doy por clausurado el Primer Congreso Internacional de Cibercrimen como fenómeno delictivo de una nueva era digital – tipologías, modalidades, nuevas figuras delictivas, estructuras delictivas – cibercriminalidad y seguridad ciudadana como coyuntura de carácter nacional e internacional que a contado con la participación de grandes expositores de distintos países como Alemania, México, Panamá, Argentina, Ecuador, Costa Rica, España, Colombia, Chile; así como, excelentes juristas y panelistas representantes de nuestra Republica de Perú.



**PROGRAMA DEL CONGRESO
INTERNACIONAL DE
CIBERCRIMEN**



Congreso internacional de cibercrimen
“Nuevas figuras Delictivas – Procesamiento en Flagrancia”
Del 26 al 28 de noviembre

DÍA 1 miércoles 26 de noviembre

CIRECRIMINALIDAD COMO FENOMENO DELICTIVO DE UNA NUEVA ERA DIGITAL

DÍA 2 jueves 27 de noviembre

TIPOLOGICAS, MODALIDADES Y ESTRUCTURAS DELICTIVAS

DÍA 3 viernes 28 de noviembre

CIBERCRIMINALIDAD Y SEGURIDAD CIUDADANA

DÍA UNO

08:00 – 08:15 a.m.

Registro de participante

08:15 – 08:30 am

Palabras de bienvenida y presentación

Dra. Miluska Giovanna Cano López
Presidenta de la Corte Superior de Justicia de Lima


08:30 – 09:00 a.m.

Palabras inaugurales

Dra. Janet Ofelia Lourdes Tello Giraldi
Presidenta de la Corte Suprema de la Republica

09:00 – 09:45 a.m.

Ponencia

Dra. Carmen Milagros Velarde Koechlin 
 Preservación de datos, ciberseguridad y protección desde RENIEC
 contra el cibercrimen

Panelistas

Dr. Segismundo León Velasco
 Dr. Roger Pari Taboada

10:00 – 10:45 a.m.

Ponencia

Dr. Cristos Velasco San Martin  
 El pacto (Europa Latinoamérica Programa de Asistencia contra el
 crimen Transnacional Organizado – Delitos Asistidos mediante
 inteligencia artificial hacia el marco regional sobre la IA y Justicia
 penal para América Latina).



Panelistas

Dra. María de los Ángeles Álvarez Camacho
Dr. Juan Carlos Aranda Giraldo

11:00 – 11:10 am Coffee Break

11:15 – 12:00 p.m.

Ponencia

Dra. Daniela Silva Dupuy 

La complejidad para investigar los ciberdelitos – el decidido aporte de la fiscalía para su investigación.

Panelistas

Dra. Luz Edith Córdova Padilla
Dr. Orlando Carbajal Rivas

12:15 – 13:00 p.m.

Ponencia

Dr. Mario Yunis Arroyo 

Retos y urgencias de la justicia especializada en ciber crimen

Panelistas

Dr. Víctor Joe Manuel Enríquez Sumerinde
Dra. Yessica Bahamondes Hernández

13:00 – 14:00 p.m. Receso

14:00 – 14:45 p.m.

Ponencia

Dr. Ricardo Elías Puelles 

Modalidad de ciber crimen: ataques contra datos y sistemas Informáticos.

Panelistas

Dra. Loreta Monzon Valencia
Dra. Sonia Mercedes Bazalar Manrique

15:00 – 15:45 p.m.

Ponencia

Dra. Rosa María Tome García 

Inteligencia Artificial retos de la delincuencia organizada.
Delitos del amor

Panelistas

Cnel. Jorge Eduardo Maguiño Porras
Dr. Carlos Alfredo Escobar Antezana



16:00 – 16:45 p.m.

Ponencia

Dr. Carlos Tomas Alvear Peña 

La importancia de la protección de datos para la prevención de delitos cibernéticos

Panelistas

Dra. María Arango Yamashiro

Dr. Manuel Chuyo Zavaleta

DÍA DOS

08:30 – 09:00 a.m.

Registro de participante

09:00 – 09:45 a.m.

Ponencia Presencial

Dr. Antoni Bosch Pujol. 

De la curiosidad tecnológica a la responsabilidad penal: Menores e inteligencia artificial en el ciber crimen.


Panelistas

Dr. Carlos Gómez Arguedas

Dr. Rene Santos Zelada Flores

10:00 – 10:45 a.m.

Ponencia

Dra. Laura Viviana Mayer Lux – Dr. Jaime Vera Vega 

El agente encubierto online en la investigación del ciber crimen

Panelistas

Dra. Miluska Giovanna Cano López

Dra. Lisdey Bueno Flores

11:00 – 11:10 a.m.

Coffe break

11:15 – 12:00 p.m.

Ponencia

Dr. Dino Carlos Caro Coria 

La concausalidad, correspondencia o autopuesta en peligro en los Ciber delitos.

Panelistas

Dr. Robinson Ezequiel Lozada Rivera

Dr. Nicolas Iscarra Pongo

12:15 – 13:00 p.m.

Ponencia

Dr. David Gutiérrez Castaño 

Ciber crimen y extinción de dominio, una realidad global en Colombia.




Panelistas

Dr. Cesar William Bravo Llaque
Dra. María Esther Felices Mendoza

13:00 – 14:00 p.m. **Receso**

14:00 – 14:45 p.m. Ponencia

Dra. Aurora Remedios Fátima Castillo Fuerman 
Ministerio Público en el Perú ante la Ciberdelincuencia

Panelistas

Dr. Cesar Augusto Vásquez Arana
Dr. Luz Victoria Sánchez Espinoza


15:00 – 15:45 p.m. Ponencia

Luis Carlos Caballero Caballero 
Del ciberespacio al Tribunal: Investigación y Persecución del cibercrimen.

Panelistas

Dr. Víctor Revoredo Farfán
Dr. Marco Antonio Hanco Paredes

16:00 – 16:45 p.m. Ponencia

Dr. William Fernando Quiroz Salazar 
La necesidad de implementar la justicia especializada en el cibercrimen

Panelistas

Dra. Emperatriz Elizabeth Pérez Castillo
Dr. Richard Rodríguez Alvan

DÍA TRES

08:30 – 09:00 a.m. Registro

09:00 – 09:45 a.m. Ponencia

Dr. Víctor Prado Saldarriaga 
Criminalidad Organizada y Lavado de Activos Virtuales en el Perú: El Impacto de la Cifra Negra.

Panelistas



Dr. Ricardo Guillermo Vinatea Medina
Dr. Jorge Luis Díaz Cabello

10:00 – 10:45 a.m.

Ponencia

Dra. María de Lourdes Gutiérrez Ortiz Monasterio 
La convención de las Naciones para la lucha contra la ciberdelincuencia

Panelistas

Dra. Tatiana Lizbeth Molina Nanfuñay
Dr. Galileo Galilei Mendoza Calderón

11:00 – 11:10 a.m.

Intervalo (pausa/café)

11:15 – 12:00 p.m.

Ponencia


Dr. Luis Jorge Gamboa Olea 
Razonamiento Probatorio en las conductas de cibercriminalidad

Panelistas

Dr. Jonathan Portillo Vela
Dra. Emperatriz Elizabeth Pérez Castillo

12:15 – 13:00 p.m.

Ponencia

Dr. Daniel Ivan Taipe Dominguez 
Ciber criminalidad: Ciber ataques, análisis y consecuencias punitivas

Panelistas

Dra. Glenda Zegarra Bravo
Dr. Jhonny Hans Contreras Cuzcano

13:00 – 14:00 p.m.

Receso

14:15 – 15:00 p.m.

Ponencia

Dr. Julio Aguayo Urgiles 
Los Delitos informáticos - óptica de la justicia Ecuatoriana frente al pluriofensivo ciber delito.

Panelistas

Dr. Iván Alberto Quispe Aucua
Dr. Francisco Álvarez Dávila

15:15 – 16:00 p.m.

Ponencia

Dr. Mauricio Garro Guillen 
Prevención del delito en Costa Rica, necesidad de homologar criterios



en América Latina.

Panelistas

Dr. Raúl Vidal Coronado

Dr. Máximo Belisario Torres Cruz

16:00 – 16:45 p.m.

Ponencia

Dr. Juan Carlos Carretero 

Sociedad de la información y organizaciones internacionales: ciberdelitos y lavado de activos

Panelistas

Dra. Carmen Liliana Arlet Rojjasi Pella

Dr. Ángel Ubaldo Gonzales Farfan

17:00 p.m.

Palabras de clausura

Presidente Constitucional de la República del Perú 

Dr. José Enrique Jeri Oré



**FOTOS DEL CONGRESO
INTERNACIONAL DE
CIBERCRIMEN**























“La Justicia es la reina de las virtudes republicanas y con ella se sostiene la igualdad y la libertad”



**CAPACITACIONES PREVIAS AL
CONGRESO INTERNACIONAL DE
CIBERCRIMEN**

CSJLIMA

CORTE SUPERIOR DE JUSTICIA DE LIMA
Servir es nuestra misión, la justicia con rostro humano nuestro objetivo

Boletín Informativo

11/07/2025



CON ÉXITO CORTE DE LIMA REALIZÓ CONFERENCIA INTERNACIONAL SOBRE CIBERCRIMEN

El juez coordinador de las salas penales del subsistema de corrupción de funcionarios de la Corte Superior de Justicia de Lima, Dr. Bonifacio Meneses, con el apoyo del Área de Capacitación, organizaron la conferencia internacional "Ciberamenazas 2025: retos y urgencia de una justicia especializada en el ciberespacio"; evento académico que contó con la presencia de los especialistas Mario Lara Orellana, docente chileno y jefe del Departamento de desarrollo institucional del Poder Judicial de Chile; y con el Ing. Mario Yunis Arroyo, consultor experto en ciberseguridad.



Asistieron a la conferencia jueces y servidores de la especialidad penal, quienes participaron con preguntas sobre tan importante tema.

Al finalizar el evento fueron distinguidos los invitados con un reconocimiento por parte de la Corte de Lima.





CAPACITACIÓN SOBRE CIBERAMENAZAS 2025: RETOS Y URGENCIAS DE UNA JUSTICIA ESPECIALIZADA EN EL CIBERESPACIO EN LA CORTE SUPERIOR DE JUSTICIA DE LIMA

La Corte Superior de Justicia de Lima realizó una importante capacitación dirigida al Poder Judicial, Ministerio Público, Policía Nacional del Perú y público en general, con el objetivo de informar y actualizar sobre los ciberdelitos en el Perú, abordando la realidad actual y las técnicas especiales de investigación.

El evento, titulado "Ciberamenazas 2025: retos y urgencias de una justicia especializada en el ciberespacio", contó con la participación del General de la Policía Nacional del Perú, José Antonio Zavala Chumbiauca, quien expuso sobre la situación actual de los ciberdelitos en el país. Además, la Dra. María del Carmen Arango Yamashiro, Fiscal Adjunto Superior Provisional de la Fiscalía Superior de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, presentó las técnicas especiales de investigación utilizadas para combatir este tipo de delitos.

Esta capacitación reafirma el compromiso de las instituciones involucradas en fortalecer la justicia especializada en materia de ciberdelincuencia, ante los retos y urgencias que plantea el ciberespacio en la actualidad.



CSJLIMA

CORTE SUPERIOR DE JUSTICIA DE LIMA
*Servir es nuestra misión, la justicia con
 rostro humano nuestro objetivo*

Boletín Informativo

27/08/2025

CIBERAMENAZAS 2025: RETOS Y URGENCIA DE UNA JUSTICIA ESPECIALIZADA EN EL CIBERESPACIO



Con el objetivo de fortalecer las capacidades del sistema de justicia frente a los desafíos del cibercrimen, la Corte Superior de Justicia de Lima llevó a cabo el evento académico "Ciberamenazas 2025: Retos y urgencia de una justicia especializada en el ciberespacio", el cual se realizó este martes a partir de las 4:00 p.m. en la sede Carlos Zavala Loayza.

La presidenta de la Corte de Lima, Dra. Miluska Cano López, dio las palabras de bienvenida y destacó la relevancia de contar con operadores de justicia capacitados frente a la evolución de los delitos informáticos y la necesidad de contar con una justicia especializada en el ciberespacio.

Seguidamente, el Dr. Bonifacio Meneses, juez superior de la Séptima Sala Penal de Apelaciones, asumió el rol de moderador del evento, explicando las pautas metodológicas y el desarrollo de las conferencias.

La primera ponencia estuvo a cargo del reconocido jurista Dr.

Dino Carlos Caro Coria, quien expuso el tema "Análisis dogmático jurídico de los cibercrimes", brindando una visión profunda sobre los fundamentos legales y desafíos jurídicos que presentan los delitos cometidos en el entorno digital.

Posteriormente, el Dr. Ricardo Elías Puelles desarrolló la segunda conferencia titulada "Ataques contra datos y sistemas informáticos", abordando los riesgos más frecuentes y las tipologías de ataques que afectan a instituciones públicas y privadas.

El evento culminó con una ronda de preguntas, promoviendo un espacio de reflexión e intercambio académico, seguido de la entrega de diplomas a los expositores, a cargo de la Dra. Miluska Cano López.

Con esta actividad, la Corte de Lima reafirma su compromiso con la actualización permanente de magistrados y operadores de justicia ante las nuevas amenazas del entorno digital.



CSJLIMA

CORTE SUPERIOR DE JUSTICIA DE LIMA
Servir es nuestra misión, la justicia con rostro humano nuestro objetivo

Boletín Informativo

11/09/2025

CONTINÚA CON ÉXITO CAPACITACIÓN SOBRE CIBERAMENAZAS Y JUSTICIA ESPECIALIZADA EN EL CIBERESPACIO

Continuando con la capacitación sobre ciberamenazas en la Corte de Lima, el Dr. William Fernando Quiroz Salazar, juez superior titular del Distrito Judicial de Lima Norte, desarrolló el tema: "Acreditación procesal de la evidencia digital obtenida por la Fiscalía y vía cooperación internacional en el juzgamiento oral", abordando los retos probatorios y los mecanismos de colaboración transnacional.

Posteriormente, el Dr. Bonifacio Meneses Gonzáles, juez superior del Sistema Anticorrupción de la CSJLIMA disertó sobre: "Víctimodogmática en el cibercrimen - La víctima culpable", en la que se analizó el rol de la víctima en los delitos informáticos desde una perspectiva crítica y dogmática.

Al finalizar el evento académico el juez superior Segismundo León hizo entrega de reconocimiento a los expositores.





SALUDOS DE LOS PATROCINADORES

El congreso Internacional de Ciber Crimen, inteligencia artificial y nuevas figuras delictivas, ha sembrado el empeño y compromiso de todas las instituciones vinculadas al quehacer de la lucha contra este fenómeno criminal, mi saludo a la Corte Superior de Justicia de Lima, en la persona de Miluska Cano López, su presidenta.
Bucarest, 30 de noviembre de 2025.

Catalina Stroe
Consejo de Europa y Coordinadora del Proyecto Glacy e

Auguro éxitos en los resultados y desde ya apoyamos cualquier nueva iniciativa que comprometa al Instituto Iberoamericano de Justicia, este congreso Internacional de Ciber Crimen, inteligencia artificial y nuevas figuras delictivas, ha despertado el interés de todas las fuerzas vivas de Iberoamérica en resolver y plantear nuevas formas de combate contra la ciber criminalidad.

Quito, 1 de diciembre del 2025.

Dr. PhD. Gustavo Jalkh Roben
Presidente IIBJ

Nuestra casa de estudios la Pontificia Universidad de Salamanca, situada entre las mejores universidades españolas por su formación, por rendimiento académico e inserción laboral. La UPSA asciende al TOP 3 de las universidades españolas enseñanza y Aprendizaje en el ranking CYD. quinto lugar en el ranking de universidades españolas mejor valoradas por sus alumnos, de ahí haber patrocinado el congreso Internacional de Ciber Crimen, inteligencia artificial y nuevas figuras delictivas, organizado por la Corte Superior de Justicia de Lima, a quien extiendo mis parabienes.

Cáceres, 29 de noviembre del 2025.

Manuel Lázaro Pulido
Profesor Principal.

La Universidad Austral es una institución educativa de excelencia, reconocida por su enfoque interdisciplinario en docencia, investigación e innovación. Con sedes en Pilar, Buenos Aires y Rosario, integra un ecosistema único que incluye el IAE Business School, el Hospital Universitario Austral y el Parque Empresarial Austral. Inspirada en valores humanos y cristianos, fomenta la formación integral de profesionales comprometidos con la responsabilidad social y el impacto positivo en la sociedad. Ahora desde el observatorio de ciber crimen tenemos mayor presencia en un carácter frontal contra la ciber criminalidad, de ahí mi saludo a la Dra. Cano López, por haber llevado a cabo uno de los mejores congresos sobre la materia.

Buenos Aires, 02 de diciembre de 2025

Daniela Silvia Dupuy.

La concepción del derecho plasmado en la capacitación, en la investigación y difusión del paradigma central del desarrollo de hombres y mujeres de derecho, es el pilar fundamental de la Universidad de San Martín de Porres, por ello apoyar a nuestro dilecto alumno y docente Bonifacio Meneses Gonzales, en la realización del Primer congreso Internacional

de Ciber Crimen, inteligencia artificial y nuevas figuras delictivas, resulta la expresión del clamor en el concepto central de erigirse esta casa de estudios en el compromiso académico de su desarrollo, expreso además el saludo a la Sra. Presidenta Miluska Cano López, distinguida ex alumna de este claustro educativo, en el afán de forjar en la Corte Superior de Justicia de Lima, el mismo espíritu.

La Molina, 03 de diciembre de 2025.

José Antonio Chang Escobedo
Rector UPSMP

Me queda solo saludar desde este hermoso lugar, capital académica de Colombia, la realización del Primer congreso Internacional de Ciber Crimen, inteligencia artificial y nuevas figuras delictivas, llevado a cabo en la noble ciudad de los Reyes, Lima Perú, habiendo sido debidamente representados por nuestro Director Académico de Pos grado David Gutiérrez Castaño, nuestro docente Bonifacio Meneses Gonzales y magister de esta casa de estudios Jean Paul Meneses Ochoa, todos integrantes de esta digna familia, espero tenerlos aquí luego del compromiso efectuado a la Dra. Miluska Cano López, de hacer las pasantías e intercambios educativos a los señores Jueces y personal administrativo como Jurisdiccional de la Corte Superior de Justicia de Lima – Perú.

Villa de Nuestra Señora de la Candelaria de Medellín, 03 de diciembre de 2025.

Néstor Posada Arboleda
Rector de la Universidad de Medellín.

Después de muchos años en el Perú, veo con grata sorpresa y emotivo desenlace, un Congreso de tal magnitud, mas de mil quinientas personas enlazadas o presenciales que deben sentir ya la preocupación de la evolución del crimen informático, llama más la atención que lo haya hecho un Poder del Estado, donde se puede ver la preocupación latente de este extremo del derecho que debe ser mejor estudiado como es el ciber crimen, inteligencia artificial y todo lo que corresponda como nuevas figuras delictivas, saludo por tanto a la Dra. Cano López por esta iniciativa y que vengan los siguientes congresos sobre la materia.

Antoni Bosch Pujol
Director General del Instituto of Audit & IT-Governance, responsable del área de IT-Governance, Risk, Compliance y Protección de Datos

La Academia Peruana de Ciber Seguridad y Derecho Penal Informático, se ha vestido de gala al apoyar este Primer Congreso de ciber criminalidad organizado por la Corte Superior de Justicia de Lima, donde 24 expositores y 48 panelistas, colocaron el dedo en la llaga, donde duele mas el avance del ciber crimen y salimos airosos con el resultado de entendimiento y envergadura de sus conclusiones, sentimos que estos proyectos son los que la ciudadanía jurídica del país lo requiere, saludos y éxitos en la gestión Dra. Miluska Cano López, presidenta de la Corte Superior de Justicia de Lima.

Miraflores, 03 de diciembre de 2025.

Jean Paul Meneses Ochoa
Presidente

la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) lidera los esfuerzos, coordinando la nueva Convención de las Naciones Unidas contra la Ciberdelincuencia (adoptada en 2024, abierta a firma en 2025), un tratado clave que busca

establecer un marco legal global para investigar y procesar delitos en línea, fortaleciendo la cooperación internacional y la capacidad de los Estados para combatir amenazas como el fraude, el abuso infantil y la difusión no consentida de imágenes íntimas. La lucha contra el ciber crimen es el primer propósito que realizar en la próxima década y el fortalecimiento de su integridad es el puntual esfuerzo cada día, por ello agradecemos el compromiso de la Corte Superior de Justicia de Lima, al haber invitado a la Dra. María de Lourdes Gutiérrez Ortiz Monasterio, coordinadora para Centro América y el Caribe en el Primer Congreso de Ciber Crimen, inteligencia artificial y nuevas figuras delictivas, llevado a cabo en Lima Perú, entre el 26 y 28 de noviembre del año en curso.

El Cairo, 06 de diciembre del 2025

Ghada Fathi Waly

Directora General de UNODC