Presidencia Uruguay

Ministerio del Interior

Plan Nacional de Seguridad Pública (2025 - 2035)

MESA INTERSECTORIAL: CIBERDELITO Y FRAUDES INFORMÁTICOS

Relatoría

20 de octubre de 2025

1. Introducción

La presente relatoría sistematiza los principales aportes de la primera mesa intersectorial sobre ciberdelito y fraudes informáticos, en el marco de los Encuentros por Seguridad del Plan Nacional de Seguridad Pública (PNSP), realizada el 20 de octubre de 2025 en Montevideo.
El documento se elaboró a partir de la transcripción del encuentro, con apoyo de herramientas de inteligencia artificial, y fue revisado por la Secretaría Técnica del PNSP. Antes de su publicación, el documento fue validado por los participantes, quienes dispusieron de 48 horas para formular observaciones.

2. Características del evento

Título: Mesa intersectorial sobre ciberdelito y fraudes informáticos
Fecha: Lunes 20 de octubre de 2025
Hora: 9:00 a 13:00
Lugar: Sala 2B, Edificio Anexo de Torre Ejecutiva (Liniers 1280, Montevideo)
Número de asistentes: 25
Moderación: Emiliano Rojido, coordinador del PNSP
Asistencia técnica: Lucía Pintos, Guzmán Pérez y Sofía Lopes Aphesteguy

Instituciones participantes

- Asociación de Despachantes de Aduana (ADAU)
- Asociación de Bancarios del Uruguay (AEBU)
- Defensoría Criminal
- Ejército Nacional
- Fiscalía General de la Nación (FGN)
- Intendencia de Maldonado (IDM)
- Ministerio de Economía y Finanzas (MEF)
- Ni Todo Está Perdido (NITEP)
- Oficina de Planeamiento y Presupuesto (OPP)
- Poder Judicial
- Poder Legislativo
- Policía Nacional
- Secretaría Nacional de Drogas (SND)
- Secretaría Nacional Contra el Lavado de Activos y el Financiamiento al Terrorismo (SENACLAFT)
- Universidad de la República (UDELAR)

Consejo Internacional de Observación y Cooperación [1]

- Banco de Desarrollo de América Latina y el Caribe (CAF)
- Organización de los Estados Americanos (OEA)
- Programa de las Naciones Unidas para el Desarrollo (PNUD)

3. Desarrollo del Encuentro

3.1 Bienvenida y dinámica de trabajo (9:00 - 9:15)

El moderador dio inicio al encuentro con un agradecimiento por la participación en las instancias anteriores y por las propuestas formales presentadas. Realizó una breve recapitulación de los encuentros previos, destacando el valor del intercambio sobre ciberdelitos y fraudes informáticos, que permitió identificar ideas relevantes para el eje correspondiente del PNSP. Explicó que el objetivo de esta reunión era profundizar en dichas propuestas e ideas, y presentó el cronograma de trabajo previsto.

3.2 Ronda de presentación (9:15 - 9:30)

Cada participante se identificó, indicando institución representada, nombre y cargo.

3.3 Análisis de propuestas (9:30 - 11:00)

3.3.1 Propuesta 1 – Especialización en Cibercrimen, Forensia Digital y Marco Jurídico (disponible aquí)

- **FGN**
  - Consideró positiva y necesaria la propuesta dado que la temática avanza muy rápido y los técnicos en derecho tienen dificultades con el contenido, el lenguaje y el conocimiento sobre qué se puede hacer y cómo solicitarlo, ya que el lenguaje técnico les resulta 'absolutamente ajeno
  - Sugirió que la formación tenga una "vocación de permanencia" debido a la naturaleza constante de los avances en el tema.
  - Aclaró que el concepto de "sistema de Justicia" en la propuesta debe incluir a la Fiscalía, la Policía (para investigaciones), la Defensa, y los Jueces, al ser necesario que todos compartan el mismo lenguaje.

- **Policía Nacional**
  - Destacó que, actualmente, las capacitaciones suelen ser continuas y provienen del exterior. Por lo tanto, consideró que tener una formación adaptada al contexto nacional es un punto "clave y favorable" para la policía y evita depender de contrataciones en otros países.

[1] Las agencias internacionales podrán participar de todos los Encuentros en calidad de observadoras, con un rol no deliberativo, velando por el cumplimiento de las "Reglas del diálogo".

- Enfatizó que el respaldo formal de un diploma o especialización brinda una garantía cuando los expertos presentan informes/pruebas en el contexto judicial.

- **UDELAR**
  - Señaló que la formación debe tener la "vocación lo más abierta posible" para apuntar a perfiles heterogéneos (derecho, tecnología, forense, funcionarios policiales y judiciales). Reconoció que ya existen programas de formación interna en la Policía, el Ejército y el Poder Judicial.
  - Aclaró que la propuesta inicial era solo un punto de partida para la discusión, basada en lo que se ofrece en otros países, y que está abierta a recibir insumos de todos los participantes.

- **Poder Judicial**
  - Sugirió ampliar el alcance para que no solo involucre al Poder Judicial, sino también a otros actores del sistema. Además, propuso incorporar los esfuerzos del Centro de Estudios Judiciales para unificar el plan docente.
  - Propuso la necesidad de crear una suerte de actualización permanente además del diplomado, dado que la tecnología y las modalidades delictivas avanzan constantemente y el diploma sólo se realiza una vez.

- **Junta Nacional de Drogas**
  - Sugirió aprovechar el conocimiento y las capacitaciones internacionales de la Agencia de Ciberdelitos de la UNODC.

- **SENACLAFT**
  - Consideró la propuesta atractiva, con un gran alcance que daría validación extra a los peritos en los procesos judiciales.

- **ADAU**
  - Elogió que la propuesta conecta el cibercrimen, la ponencia digital (recolección de pruebas), la ciberseguridad y la Protección de Datos.
  - Subrayó que las investigaciones a menudo requieren acceso a bases de datos, resaltando la importancia de capacitar al personal en el manejo de estas.

3.3.2 Propuesta 2 Defensoría Criminal – La información es prevención (disponible aquí)

- **Defensoría Pública**
  - Señaló que el planteamiento aborda dos aspectos fundamentales: la Preparación de los actores para enfrentar mejor el ciberdelito cuando sucede el ataque y trabajar en la prevención con niños y adultos mayores.
  - Sugirió que las campañas preventivas sean más efectivas y se enfoquen en mostrar los procedimientos y los modus operandi de los delincuentes, y no solo en la casuística o "cuento del tío".
  - Incentivó a que los informes (ej. de Policía Científica) sean claros y fáciles de comprender para las personas que no son expertas en el tema (como fiscales, defensores, víctimas y diputados), haciendo que el trabajo fluya mejor en las primeras etapas de procesamiento.

- **Poder Judicial**
  - Sugirió agregar al MIDES (Ministerio de Desarrollo Social), específicamente al Instituto de las Personas Mayores, ya que los adultos mayores son frecuentemente víctimas de estos fraudes y estafas.
  - Señaló como complementaria la propuesta a la formación en cibercrimen, apuntando a públicos distintos.
  - Apoyó el punto de poder incidir en tratamientos normativos del tema, manifestando que le gusta que el sistema de Justicia y la Academia sean escuchados en el Parlamento.

- **Poder Legislativo**
  - Sugirió agregar a INAU como actor aliado y responsable, dado a que el programa trabajaría con las infancias.
  - Propuso incluir al BCU como un organismo de contralor en el proceso deliberativo.

- **UDELAR**
  - Basándose en la necesidad de un procesamiento efectivo, sugirió que sería beneficioso establecer una base de datos o repositorio centralizado donde se registren y cataloguen los casos que ocurren en el país, permitiendo introducir una taxonomía y categorizar los fraudes.
  - Consideró que teniendo información catalogada y centralizada sería una gran ayuda para las campañas de prevención, introducir explicaciones menos técnicas y, sobre todo, obtener un repositorio que sirva de referencia para entender los patrones que se repiten.

3.3.3 Propuesta 3: Fiscalía General de la Nación – Uso de Inteligencia artificial para la detección de patrones comunes en las denuncias de Estafas (disponible aquí).

- **FGN**
  - Enfatizó que, aunque la fiscalía ya trabaja con IA, no hay posibilidades de alcanzar todas las denuncias ni analizar el universo de estafas que se produce a nivel país.
  - Consideró que la herramienta propuesta puede ayudar a ver patrones, analizar dónde se produce, aproximarse a lo que pasa, siendo necesario priorizar o imputar para desincentivar, lo que también aumenta el interés en la denuncia.

- **UDELAR**
  - Consideró la idea como "muy buena" y señaló que hay un equipo "muy fuerte" de procesamiento de lenguaje natural en el Instituto de Computación de la Facultad de Ingeniería de la UdelaR.
  - Mencionó que estos investigadores ya trabajan en análisis de lenguaje natural, utilizando técnicas de aprendizaje automático y aprendizaje profundo, e incluso han trabajado con la base jurídica nacional para tipificar, generalizar y relacionar casos.
  - Sugirió que este proyecto representa una oportunidad interesantísima para el país y que podría generar interés desde la Academia.

- **Ejército Nacional**
  - Consideró que además de aumentar la velocidad de procesamiento de casos, esta propuesta serviría para aumentar la precisión, definir una taxonomía e identificar patrones normales y anormales sin necesidad de mayor conocimiento técnico.

- **Policía Nacional**
  - Sugirió que, en lugar de centrarse solo en las denuncias formales, la Fiscalía podría explorar la información que manejan las entidades financieras y bancos, al la mayoría de los intentos de fraude son bloqueados por los bancos y nunca llegan a ser denuncias.
  - Señaló que hay iniciativas similares en otros países (como el "Sistema Tentáculos" en Brasil) que detectan patrones en los flujos de intentos de fraude, no en las denuncias. El desafío para implementar esto es alinear a todas las entidades financieras y agencias para que compartan información.

3.3.4 Propuesta 4 Ni todo Está Perdido – Escudo Digital Social (disponible aquí).

- **Poder Legislativo**
  - Planteó que personas vulnerables son usadas como titulares de empresas ficticias, lo que les impide acceder a prestaciones del BPS. Esto ilustra un fraude no digital que se debe controlar, y que el BCU debería ser un actor mucho más preponderante y participativo.

- **FGN**
  - Citó el caso de la estafa de las garrafas gestionada por MIDES, donde esta población fue atacada digitalmente a través de una app. Esto demostró que, aunque MIDES y ANCAP trabajaron en la modificación de la aplicación, el Estado debe "perseguir esta situación" para que los delincuentes no sigan atacando a este mismo núcleo poblacional vulnerable.

- **UDELAR**
  - Si bien compartió la iniciativa de alfabetización, advirtió que esta solo tiene sentido si se asume que las transacciones se realizarán en medios digitales.
  - Señaló que las organizaciones en el país a menudo utilizan aplicaciones y sitios web que no son concebidos con seguridad, siendo tecnologías vulnerables.
  - Enfatizó que, si el Estado va a manejar activos críticos, como el propuesto, las herramientas que utilice deben ser seguras y no debe depender únicamente de las capacidades de alfabetización del usuario, sino que la tecnología debe ser inherentemente lo más segura posible.

- **AEBU**
  - Postuló que el BCU debería intervenir más y obligar a las instituciones a evaluar el riesgo de TI de los clientes, y que los controles sobre las tercerizaciones de servicios que manejan información deben ser más estrictos, especialmente ante recientes modificaciones normativas que reducen las exigencias del BCU.

3.4 Pausa para café (11:00 – 11:15)

Espacio breve de descanso que permitió a los participantes recuperar energía y mantener intercambios informales.

3.5 Ideas emergentes para desarrollar (11:15 – 12:45)

3.5.1 Idea Emergente 1: Reformar la normativa penal y financiera digital para incorporar los ciberdelitos, tipificar el crimen bancario y ajustar las penas tanto en los delitos telemáticos de alto monto vinculados al lavado de activos como en las estafas digitales, atendiendo a su impacto creciente sobre personas vulnerables.

- **Defensoría Pública**
  - Expresó que las penas deben ir de mínimos a máximos, marcando un rango amplio para que el fiscal y el juez puedan ajustarlo a la situación concreta.
  - Enfatizó que subir el rango mínimo podría resultar en situaciones donde la pena aplicada no es proporcional al delito.
  - Mencionó que hay que tener cuidado con legislar sobre nuevos delitos, ya que muchas situaciones que se hacen ahora a través de plataformas electrónicas ya estaban reguladas, y la regulación paralela puede generar contradicciones.

- **FGN**
  - Enfatizó que la inflación penal no es la solución y que la mayoría de las situaciones delictivas no son de grandes daños económicos, sino menores, a cuentagotas, por lo que los mínimos deben cuidarse.
  - Invitó a repensar medidas alternativas para que se ajusten al delito cometido. Por ejemplo, si estafó a personas de la tercera edad, que vayan a realizar tareas de ayuda a residenciales.

- **Poder Judicial**
  - Estuvo a favor del ajuste de penas, pero para todos los delitos, buscando una dosimetría penal acorde. Consideró que las grandes mega estafas con lavado de activos podrían ser el camino para ajustar penas, diferenciándolas de las estafas de menor valor.
  - Propone ver en protocolos, con la academia, parlamento y la cadena de justicia para protocolizar los marcos legales de prueba digital.

- **SENACLAFT**
  - Informó que el proyecto de ley modificativo (con media sanción del Senado) incluye ahora los ciberdelitos como delito precedente de lavado de activos. Este proyecto modifica el numeral 34 (que antes preveía el fraude informático con un umbral alto) por un concepto más abarcativo de ciberdelitos y baja el umbral a 100.000 unidades indexadas (alrededor de 1.000 dólares). También incluye el fraude a entidades del sistema financiero.

3.5.2 Idea Emergente 2: Regular la prueba digital mediante una ley específica que garantice derechos, defina estándares y protocolos claros para su obtención, preservación y valoración, evitando dispersión y demoras.

- **Poder Judicial**
  - Abogó por la necesidad de un capítulo específico de prueba digital similar a otras legislaciones extranjeras, que cubra la obtención, preservación y valoración.
  - Señaló que el país está "súper atrasado" y que esta regulación facilitaría a que la Fiscalía se "juegue" a ir a juicio, pues la ausencia de capacidad específica dificulta resolver la valoración de la prueba, especialmente la adulteración.

3.5.3 Idea Emergente 3: Crear una fiscalía especializada en ciberdelitos con competencias técnicas y procesales que permitan actuar con mayor eficacia y celeridad.

- **FGN**
  - Argumentó que una Fiscalía especializada en cibercrimen es "absolutamente insuficiente" para abordar la criminalidad en este ámbito.
  - Mencionó que el cibercrimen no solo abarca estafas, sino también temas de violencia sexual y otras violencias, siendo el cibercrimen un medio y no un tipo de crimen.
  - Reafirmó que pensar en un solo acto especializado es "exactamente insuficiente", dado que abarca "un montón de figuras delictivas".

3.5.4 Idea Emergente 4: Crear laboratorios de forense digital como capacidad estratégica nacional para la investigación y prevención de ataques y desarrollar programas nacionales de formación en análisis forense digital, integrando a la academia, la policía, el sistema judicial y la defensa.

- **Policía Nacional**
  - Apoya que el laboratorio de forense digital abarque diferentes perspectivas: investigación (la Policía ya tiene laboratorios enfocados en la persecución y contribución técnica), capacitación y prevención.
  - Enfatizó que la gobernanza es la palabra clave, ya que muchas cuestiones se solapan o pisan entre instituciones, por lo que es necesario un capítulo que defina las responsabilidades de cada uno.

- **UDELAR**
  - Indicó que la universidad es convocada con frecuencia para hacer peritajes a jueces, etc., pero que no tienen capacidades específicas definidas para prestar estos servicios, aunque sí hacen investigación en esas líneas.
  - Afirmó que, si se quiere montar un laboratorio con esa escala, se necesita un marco formal preciso que actualmente no existe. Sugirió que la gobernanza para laboratorios, infraestructura y activos críticos debería recaer en una agencia especializada (como la Agencia Nacional de Ciberseguridad de Chile).
  - Argumentó que Uruguay debería centralizar este tipo de servicios, ya que no tiene las capacidades ni los recursos para tener diferentes laboratorios de forense digital.

3.5.5 Idea Emergente 5: Elaborar un catálogo nacional de infraestructuras críticas y establecer medidas de protección:

- **UDELAR**
  - Señaló que AGESIC no cubre todas las infraestructuras críticas y no podría armar el catálogo de activos críticos.
  - Destacó que el sistema de trazabilidad es un activo ultracrítico al que nunca se le dio la importancia debida y cuya infraestructura se maneja sin la seguridad adecuada.
  - Indicó que la creación del catálogo es una decisión política que requiere relevar con 4 o 5 interlocutores clave de alto nivel.
  - Sostuvo que, al ser activos digitales, sus sistemas deben estar definidos y diseñados para ser lo más seguros posible.
  - Advirtió que la gestión de esto debe ser continua y dinámica, y que debe haber una visión general central, ya que habrá activos críticos que no son del Estado.

- **Policía Nacional**
  - Enfatizó que el inventario de activos críticos debe estar bajo siete llaves porque, una vez escrito, se convierte en un punto de vulnerabilidad o un "atractivo" para el crimen.
  - Mencionó que, si bien hay varios inventarios separados, no hay uno consolidado.

3.5.6 Idea Emergente 6: fortalecer la Cooperación Internacional formal e informal para acelerar la persecución penal y el congelamiento de activos.

- **FGN**
  - Explicó que la "informalidad" es necesaria para la celeridad en ciberdelitos y que está relacionada con la comunicación rápida entre fiscales de distintos países (ej. a través de la Red de Ministerios Públicos de Latinoamérica).

- **SENACLAFT**
  - Señaló que se suele hablar de "cooperación informal" por oposición a "cooperación formal", términos que equivaldrían a "cooperación administrativa" y "cooperación jurídica" respectivamente.
  - En el punto específico de congelamiento de activos o búsqueda de activos, se mencionó que la SENACLAFT opera con la Red de Recuperación de Activos de Gafilat (RRAG), forma de cooperación informal sin validez probatoria, lo cual sirve para activar el mecanismo de cooperación jurídica formal.

3.5.7 Idea Emergente 7: Desarrollar una estrategia nacional de educación digital y cultura de ciberseguridad que incluya formación desde edades tempranas (usando Plan Ceibal), capacitación a docentes y alfabetización digital en grupos vulnerables (mediante agentes comunitarios y campañas masivas).

- **FGN**
  - Cree oportuno la utilización de la infraestructura de Plan ceibal y Plan Ibirapita, al nuclear Niños, educadores, familias y jubilados.

- **ADAU**
  - Señaló que las empresas ya utilizan simulacros de phishing con sus empleados, lo que podría ser una opción para medir la vulnerabilidad.

- **UDELAR**
  - Mencionó que AGESIC tiene una plataforma que utilizan para educar a las personas mayores y que Plan Ceibal podría proporcionar la plataforma completa para la estrategia de ciberseguridad, ya que tienen el equipamiento.
  - Destacó que el problema principal es armar una campaña que sea adecuada.

También fueron discutidas otras ideas emergentes, entre ellas: establecer convenios interinstitucionales para protocolos de bloqueo y respuesta rápida ante fraudes (AGESIC, MIDES, bancos, telecomunicaciones); fortalecer controles antifraude en instrumentos financieros digitales que protegen a sectores vulnerables (tarjetas prepagas, Tarjeta Uruguay Social); capacitar a operadores de justicia y policía en evidencia técnica y rastreo digital; definir límites claros para ciberpatrullaje con control judicial; y fortalecer la coordinación interinstitucional mediante protocolos de interoperabilidad y alerta temprana

3.6 Cierre y próximos pasos (12:45 - 13:00)

El moderador agradeció la participación y el compromiso de los actores presentes, destacando que los aportes recabados serán sistematizados. A su vez indicó que en la semana del 3 de noviembre y del 10 de noviembre se realizará el quinto, y último, Encuentro por Seguridad.

4. Anexos

4.1 Lista de participantes

Participantes

Nombre del Representante	Institución
Leonardo López	Asociación de Despachantes de Aduana
Emanuel Da Silva	
Manuel García	Asociación de Bancarios del Uruguay
Patricia Marquisá	Fiscalía General de la Nación
Cecilia Villaverde	Intendencia de Maldonado
Marcelo Pereira	Ministerio de Economía y Finanzas
Ken Chang	Ni Todo Está Perdido
Juan Manuel Regules	Oficina de Planeamiento y Presupuesto
Federico Ott	
Juan Pablo Novella	Poder Judicial
María Sol Bellomo	

Jenyfer Saavedra	Defensoría Criminal
Mario Madeiro	Poder Legislativo
Andrea Rizzo	Secretaría Nacional de Drogas
Madelón Couso	Secretaría Nacional Contra el Lavado de Activos y el Financiamiento al Terrorismo
Javier Bussi	Ejército Nacional
Saul Scanziani	Policía Nacional
Gustavo Betarte	Universidad de la República

Consejo Internacional de Observación y Cooperación

Institución	**Nombre del Representante**
Banco de Desarrollo de América Latina y el Caribe (CAF)	Daniel Castro
Organización de los Estados Americanos (OEA)	Sebastián Gómez
Programa de las Naciones Unidas para el Desarrollo (PNUD)	Mariela Solari

Organización

Institución	**Nombre del Representante**
Ministerio del Interior	Emiliano Rojido
Ministerio del Interior	Guzmán Pérez
Ministerio del Interior	Lucia Pintos
Ministerio del Interior	Sofía Lopes Aphesteguy

4.2 Registro fotográfico

Presidencia
Uruguay

Ministerio
del Interior