Presidencia Uruguay

Ministerio del Interior

Plan Nacional de Seguridad Pública (2025 - 2035)

MESA INTERSECTORIAL: CIBERDELITOS Y FRAUDES INFORMÁTICOS

Relatoría

10 de noviembre de 2025

1. Introducción

La presente relatoría sistematiza los principales aportes de la Mesa Temática sobre ciberdelitos y fraudes informáticos realizada en el marco del quinto Encuentro por Seguridad del Plan Nacional de Seguridad Pública (PNSP), llevada a cabo el 10 de noviembre 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 temática sobre ciberdelitos y fraudes informáticos.
Fecha: Lunes, 10 de noviembre de 2025.
Hora: 9:00 a 13:00
Lugar: Sala 2B, Edificio Anexo de Torre Ejecutiva (Liniers 1280, Montevideo)
Número de asistentes: 20
Moderación: Emiliano Rojido, coordinador del PNSP
Asistencia técnica: Guzmán Pérez y Lucía Pintos
Presentación: Disponible aquí

Instituciones participantes

- Agencia para el Gobierno Electrónico y la Sociedad de la Información y del Conocimiento (AGESIC)
- Asociación Uruguaya de Empresas Aseguradoras (AUDEA)
- Centro de Almaceneros Minoristas, Baristas, Autoservicistas y Afines del Uruguay (CAMBADU)
- Instituto Nacional de las Mujeres (Inmujeres)
- Intendencia de Maldonado (IDM)
- Fiscalía General de la Nación (FGN)
- Oficina de Planeamiento y Presupuesto (OPP)
- Universidad de la República (Udelar)
- Unidad de Ciberdefensa del Ejército – Ministerio de Defensa Nacional (MDN)
- Unidad de Cibercrimen – Ministerio del Interior (MI)
- Poder Judicial
- Ministerio de Economía y Finanzas (MEF)
- Poder Legislativo

Consejo Internacional de Observación y Cooperación [1]

- Banco de Desarrollo de América Latina y el Caribe (CAF)
- Organización de los Estados Americanos (OEA)
- Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC)

[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".

3. Desarrollo del Encuentro

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

El moderador dio inicio al encuentro agradeciendo la participación en las instancias anteriores y las propuestas formales presentadas. Explicó que el objetivo de esta reunión era profundizar en dichas propuestas, clasificándolas según su **impacto (bajo/alto)** y su **costo (bajo/alto)**, con el fin de **priorizar aquellas de alto impacto y bajo costo**, así como **analizar, de acuerdo con los recursos disponibles, las propuestas de alto costo y alto impacto**. Finalmente, explicó que **las propuestas de alto costo y bajo impacto serán descartadas.**

3.2 Ronda de presentación

Cada participante se identificó indicando institución, nombre y cargo.

3.3 Análisis de Propuestas

Propuesta 1: Especialización en Cibercrimen, Forensia Digital y Marco Jurídico - UdelaR.

Aportes específicos:

- **UdelaR:**
  - Clasificó el costo de la propuesta como razonable. Enfatizó que, al ser una introducción en cibercrimen y forensia digital, la capacitación debe enfocarse en una introducción razonable sin invertir demasiado en equipos avanzados de alto costo.
  - Postuló la necesidad de que la formación sea permanente y esté alimentada por la actividad de investigación para generar una masa crítica nacional y consolidar el conocimiento en el país .
  - Estimó un impacto muy alto del programa, al ser una expertise de gran amplitud que serviría para impartir justicia, como también para defender la infraestructura crítica y soberanía digital del país.

- **AGESIC:**
  - Consideró que es una propuesta de alto impacto al derramar conocimiento a todo el sistema estatal, donde actualmente existe un déficit.
  - Mencionó que AGESIC podría colaborar, ya que esto se alinea con el fortalecimiento de capacidades nacionales, e incluso ofreció poner a disposición contactos internacionales de la agencia que cuentan con herramientas de forensia digital.

- **Unidad de Cibercrimen:**
  - Clasificó la propuesta como de muy alto impacto. Coincidió en que los costos se centran en los recursos humanos (docentes) más que en infraestructura o software.

- Recomendó que la capacitación se enfoque en la metodología de trabajo y no en herramientas o productos de marca específicos y de alto costo.

- **FGN:**
  - Calificó a la propuesta como necesaria y de alto impacto.
  - Consideró que la primera etapa de transmisión de conocimientos no requeriría altos costos.
  - Propuso que la formación sea dirigida a funcionarios de todo el sistema de justicia, incluyendo FGN, y no solo el Poder Judicial como está planteado.

- **Unidad de Ciberdefensa del Ejército:**
  - Reconoció que la propuesta requiere una inversión en equipos y licencias, pero su alto impacto y urgencia justifican una planificación a largo plazo.
  - Consideró que existen equipos y personal capacitado en el MI que podrían aportar a la especialización.
- **NITEP:**
  - Sugirió utilizar el préstamo BID de transformación digital o explorar préstamos de la CAF o convenios con la Unión Europea y el Mercosur para financiar los costos de implementación de la especialización.

Propuesta 2: "La Información es Prevención" - Defensoría Criminal.
Aportes específicos:

- **AGESIC:**
  - Consideró ambiciosa la propuesta por su amplio público objetivo, pero muy positiva y con potencial de bajo costo si las infraestructuras existentes y convenios con la Administración Nacional de Educación Pública (ANEP) y con el Centro de Estudios Judiciales del Uruguay son utilizados.
  - Sugirió acotarla a la prevención de estafas en adultos mayores y los peligros de la tecnología en infancias y padres.

- **UdelaR:**
  - Resaltó a AGESIC como potencial aliado, por su experiencia en campañas de concientización y sus herramientas.
  - Cuestionó el segundo objetivo de "lograr que los casos sean procesados por el sistema de forma eficiente". Propuso complementar la sensibilización con la creación de una base de datos centralizada con taxonomía y clasificación de los accidentes y delitos.

- **Inmujeres:**
  - Mencionó que Inmujeres y ANEP tienen una campaña de prevención de ciberdelitos y fraudes dentro de la campaña de "noviazgos libres de violencia" que incluye ciudadanía digital, y podría ser una herramienta útil para implementar esta propuesta dado su amplio alcance en la población adolescente.

- **Poder Legislativo:**
  - Consideró a la propuesta como amplia, debiendo ser delimitada las responsabilidades y los objetivos para su correcta aplicación.
  - Concordó en la necesidad de involucrar a AGESIC y a la Oficina Nacional del Servicio Civil.

Propuesta 3: "Uso de Inteligencia artificial para la detección de patrones comunes en las denuncias de Estafas" – Fiscalía General de la Nación.

Aportes específicos:

- **FGN:**
  - Consideró que tiene alto impacto ya que el logro de condenas en delitos de estafa ayuda a disminuir la impunidad y desincentivar el delito, a la vez que aumenta la confianza para denunciar.
  - Mencionó que la FGN está explorando la posibilidad de llegar a un acuerdo con el Ministerio Público de Chile, que cuenta con su propia herramienta "HeredIA" desarrollada por la Universidad de Chile, lo que podría reducir significativamente el costo de aplicación.
  - Sugirió comenzar la aplicación de la IA con el delito de estafa debido a su menor criticidad en la aplicación de patrones, para luego extenderla a otras conductas delictivas.

- **NITEP:**
  - Sugirió aprovechar el préstamo BID de transformación digital ya vigente.
  - Recomendó excluir a las empresas desarrolladoras e incluir a la UdelaR para que desarrollen la IA como líneas de investigación, utilizando el concepto de educación para mantener el préstamo como no retributivo .

- **Unidad de Cibercrimen:**
  - Destacó que el uso de canales virtuales para realizar la denuncia podría facilitar la inmediatez para reaccionar ante ciberdelitos, por ejemplo bloquear cuentas.
  - Advirtió que, aunque soluciones sencillas, como WhatsApp, son atractivas no cumplen con la institucionalidad ni la regulación de la prueba necesaria.

Propuesta 4: “Prueba electrónica en el CPP. Incorporación de un capítulo específico para el tratamiento de sus particularidades”.

Aportes Específicos:

- **Unidad de Cibercrimen:**
  - Calificó la propuesta como una de las propuestas más prioritarias y críticas, siendo un cimiento para el cibercrimen.
  - Sostuvo que Uruguay está atrasado en materia legislativa y que el principal problema es la falta de priorización política.
  - Consideró que, si no hay un marco jurídico claro, tanto el investigador como la investigación quedan expuestos.
- **Poder Legislativo:**
  - Consideró que es necesario y urgente la regulación de la prueba digital, ya que la falta de un capítulo específico dificulta casos complejos, como los allanamientos digitales.
  - Subrayó que es vital la capacitación previa de todos los operadores jurídicos para hablar "el mismo idioma" y poder aplicar la ley una vez que exista.
  - Cree que la dificultad no es presentar la ley, sino armar el proyecto de ley por los conocimientos que esto requiere.
  - Calificó el costo de implementación como bajo, al ya tener recursos como magistrados y expertos en ley, siendo necesario solamente una consultoría con expertos en el tema.

- **FGN:**
  - Consideró la propuesta como fundamental y vital.
  - Señaló que la normativa actual del Código del Proceso Penal no contiene un capítulo de evidencia digital.
  - Mencionó que es necesario armar un equipo que complemente la visión jurídica con el conocimiento técnico informático, ya que el tema excede la formación de los abogados.
  - Opinó que es necesaria una campaña de sensibilización para los políticos para elevar la prioridad del tema.

- **Unidad de Ciberdefensa del Ejército:**
  - Afirmó que la propuesta tiene bajo costo y alto impacto, siendo una medida urgente.
  - Postuló que es indispensable para el técnico forense y la iniciativa de la especialización, pues sin el capítulo normativo de prueba digital la solidez de la investigación queda en riesgo.

- **NITEP:**
  - Sugirió que Uruguay se adhiera a los convenios de Budapest y la Convención de la Ciberdelincuencia, ya que estos ofrecen asesoría técnica no retributiva para el desarrollo de protocolos y podría disminuir los costos de la implementación de la propuesta.

- **Inmujeres:**
  - Mostró un gran interés en la regulación de la prueba digital al muchas mujeres ser víctimas de agresiones en línea.

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 Análisis de propuestas (11:15 – 12:45)

Propuesta 5: “ESCUDO DIGITAL SOCIAL: Seguridad Financiera, Identidad y Justicia para la Población Vulnerable” - Colectivo Ni Todo Está Perdido.

- **NITEP:**
  - Afirmó que casi la totalidad de la propuesta puede ser financiada por préstamos del BID ya existentes, como el BID 5354 (apoyo a laboratorios forenses) y el BID 4687 (estrategias de gobierno digital), quedando "prácticamente a costo cero".
  - La adhesión a los convenios de Budapest también provee asesoría técnica no retributiva para protocolos operativos.

- **Unidad de Cibercrimen:**
  - Consideró que cada actividad de la propuesta debería ser una propuesta aislada, por su generalidad y profundidad.
  - Consideró que si bien los bancos y entidades financieras tienen un registro de los ciberdelitos y estafas, la cultura es de bloqueo de las amenazas y no de reportar los delitos cibernéticos al Ministerio del Interior.
  - Reafirmó en la necesidad de innovar y mejorar los canales de denuncia digitales para agilizar la reacción ante ciberdelitos y estafas.

3.6. Espacio de reflexión y retroalimentación.

El moderador invitó a los participantes a describir su participación en los Encuentros por Seguridad y sus expectativas sobre los siguientes pasos.

3.7 Cierre y Próximos pasos (12:45 - 13:00)

El moderador agradeció la participación y el compromiso de los sectores presentes, destacando que los aportes recabados serán sistematizados y analizados como insumos para la redacción del Plan Nacional de Seguridad Pública (PNSP).

El moderador informó que el 15 de noviembre se cerrará la plataforma de participación ciudadana y, con ello, la posibilidad de enviar fichas programáticas. Además, extendió una invitación al evento sobre seguridad sobre trata y explotación sexual, que se realizará en Paysandú el 18 de noviembre. Por último, invitó a los participantes a participar del evento de agradecimiento que se celebrará el 8 de diciembre en la Torre Ejecutiva donde se presentará el documento síntesis de los Encuentros por Seguridad.

4. Anexos

4.1 Lista de participantes

Instituciones Participantes

Institución	Nombre del Representante
Agencia para el Gobierno Electrónico y la Sociedad de la Información y del Conocimiento (AGESIC)	Maria Eugenia Corti
Asociación Uruguaya de Empresas Aseguradoras (AUDEA)	Facundo Dariz
Cámara Empresarial de la Distribución de Automotores y sus Componentes (CAMBADU)	Daniel Fernández
Instituto Nacional de las Mujeres (Instituto de las Mujeres)	Paola Campos
Intendencia de Maldonado (IDM)	Cecilia Villaverde
Fiscalía General de la Nación (FGN)	Patricia Marquisá
Oficina de Planeamiento y Presupuesto (OPP)	Gimena García
Oficina de Planeamiento y Presupuesto (OPP)	Federico Ott
Universidad de la República (Udelar)	Gustavo Betarte
Unidad de Ciberdefensa del Ejército — Ministerio de Defensa Nacional (MDN)	Javier Bussi
Unidad de Cibercrimen — Ministerio del Interior (MI)	Saul Scanziani

Poder Judicial	María Sol Bellomo Peraza
Ministerio de Economía y Finanzas	Marcelo Pereira
Poder Legislativo	Dario Madeiro

CONSEJO INTERNACIONAL DE OBSERVACIÓN Y COOPERACIÓN

Institución	**Nombre del Representante**
Banco de Desarrollo de América Latina y el Caribe (CAF)	Daniel Castro
Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC)	Carla Cohen
Organización de los Estados Americanos (OEA)	Nathalie Castello

ORGANIZACIÓN DEL ENCUENTRO

Institución	**Nombre del Representante**
Ministerio del Interior	Emiliano Rojido
	Lucía Pintos
	Guzmán Pérez

4.2 Registro Fotográfico

Presidencia
Uruguay

Ministerio
del Interior