Presidencia Uruguay

Ministerio del Interior

Plan Nacional de Seguridad Pública (2025 - 2035)

MESA INTERSECTORIAL: CIBERDELITO Y FRAUDES INFORMÁTICOS

Relatoría

29 de setiembre 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 29 de setiembre 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 29 de setiembre de 2025
Hora: 9:00 a 13:00
Lugar: Sala 2B, Edificio Anexo de Torre Ejecutiva (Liniers 1280, Montevideo)
Número de asistentes: 21
Moderación: Emiliano Rojido, coordinador del PNSP
Asistencia técnica: Lucía Pintos, Guzmán Pérez y Sofía Lopes Aphesteguy

Instituciones participantes

- Centro de Altos Estudios Nacionales (CALEN)
- DATA Uruguay
- Fiscalía General de la Nación (FGN)
- Ministerio de Economía y Finanzas (MEF)
- Colectivo Ni Todo Está Perdido (NITEP)
- Poder Judicial
- Unidad de Cibercrimen – Ministerio del Interior
- Unidad de Ciberdefensa del Ejército Nacional
- 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)

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".

- Insistió en la necesidad de fomentar la cooperación entre agencias, evitando la burocracia que retrasa las investigaciones mientras los delincuentes se organizan con rapidez y con acceso a criminalidad como servicio. Defendió la interoperabilidad de plataformas y protocolos para que las instituciones puedan responder de manera coordinada y eficaz.
- Planteó que la educación ciudadana es clave para la prevención. Explicó que muchos efectivos de las Fuerzas Armadas provienen de sectores sociales vulnerables y que tanto ellos como sus familias manejan información sensible que los expone a riesgos. Por eso reclamó incorporar la cultura digital en la formación escolar y en campañas de sensibilización, promoviendo la corresponsabilidad entre ciudadanos, empresas y el Estado.
- Valoró que en estos espacios de diálogo deberían participar también representantes del sector privado —particularmente bancos— para mejorar los protocolos de intercambio de información. Reafirmó que el CALEN asume un compromiso institucional en esta agenda, tanto en la formación académica como en la promoción de la cooperación interinstitucional y en el impulso a la corresponsabilidad ciudadana.

- **DATA Uruguay:**
  - Planteó que es urgente regular la prueba digital para garantizar derechos y procedimientos claros, y sostuvo que la mera adhesión a la Convención de Budapest no alcanza si no se incorporan sus protocolos adicionales, que son los que permiten un intercambio eficaz y seguro de evidencia digital a nivel internacional. Reclamó que la cooperación transnacional sea priorizada como paso inicial para fortalecer la legislación nacional, ya que hoy la policía actúa con un marco que brinda escasa seguridad jurídica.
  - Expresó preocupación sobre cómo los jueces interpretarán en la nueva ley el concepto de “justa causa”, especialmente en relación con el acceso a sistemas, la interceptación de comunicaciones y los reportes de vulnerabilidades. Señaló que la comunidad de seguridad informática, que reporta incidentes al CERTuy de manera constante, podría retraerse si no se protege el hacking ético, y reclamó que no se penalice a quienes prueban sistemas y comunican fallas con fines de prevención.

- Cuestionó la definición de “inteligencia policial” en la Ley de Inteligencia, porque mezcla actividades de instrucción criminal con funciones de inteligencia, lo que genera un vacío en cuanto a límites y garantías. Reclamó que se defina hasta dónde puede llegar el ciberpatrullaje y en qué condiciones se requiere una autorización judicial, advirtiendo que Internet no puede considerarse automáticamente una fuente abierta.
- Defendió la necesidad de poner límites claros a las técnicas de ciberinteligencia, para evitar que se naturalicen prácticas como la creación de perfiles falsos para infiltrarse en redes sociales sin control judicial. Afirmó que no se trata de obstaculizar investigaciones, sino de proteger garantías tanto de los ciudadanos como de los propios policías, que deben contar con reglas precisas para actuar.
- Señaló que la falta de un marco normativo detallado deja a las instituciones expuestas a prácticas improvisadas, donde no está claro qué se puede hacer y qué no. Reclamó que el PNSP incluya un debate serio sobre ciberpatrullaje, fuentes abiertas y ciberinteligencia, con límites explícitos que eviten confusiones y abusos.

- **FGN:**
  - Señaló que, si bien los datos y estadísticas suelen asociarse a las estafas, el fenómeno de los ciberdelitos es mucho más amplio. No obstante, en la práctica cotidiana de la Fiscalía, lo que predomina son las denuncias de estafas, que desde 2018 pasaron del séptimo al tercer lugar entre los delitos más reportados. Advirtió que el crecimiento es sostenido y responde a que se trata de delitos con alta rentabilidad y bajo riesgo: a diferencia de una rapiña, que exige armas y contacto directo con la víctima, las estafas y otros delitos telemáticos se cometen con comodidad desde una computadora o un teléfono, reduciendo drásticamente los riesgos para el autor.
  - Explicó que existe un importante subregistro, ya que muchas víctimas no denuncian debido a la subjetividad del daño percibido (ej.: para algunas personas, perder 4.000 pesos amerita denunciar, pero para otras no). A esto se suma que la FGN debe priorizar recursos y no puede movilizar todo el aparato institucional (policía, pericias, juzgados) para montos bajos, aunque reconoció que detrás de pequeñas sumas puede haber una serie de operaciones repetidas por un mismo autor que constituyen un fenómeno de gran escala. En este sentido, destacó la necesidad de desarrollar análisis de contexto para identificar patrones, en lugar de abordar cada caso de forma aislada.

- Advirtió sobre la falta de coordinación interinstitucional y las dificultades para recuperar el dinero estafado, ya que los fondos suelen moverse con rapidez, dificultando intentos de congelamiento. Indicó que, si bien es necesario buscar la restitución de las pérdidas de las víctimas, también resulta clave dar señales de investigación y sanción, aun cuando la recuperación económica no sea posible.
- Subrayó que la persecución penal enfrenta limitaciones estructurales: faltan recursos, capacitación y especialización en temas tecnológicos dentro de la FGN y en la policía. Recalcó que los estafadores suelen tener mayor conocimiento y adaptabilidad en el uso de tecnologías que los propios operadores del sistema. La policía ha solicitado que los fiscales tengan formación más especializada, además de reforzar con fiscalías específicas tanto para estafas como para ciberdelitos, pero el presupuesto disponible es insuficiente.
- Marcó como un problema serio la falta de capacitación generalizada, no solo para fiscales, sino también para jueces y policías, lo que dificulta la comprensión de informes técnicos y afecta la tramitación de procesos abreviados, que son la vía más frecuente de resolución.
- Señaló también que el fenómeno no se limita a adultos: adolescentes y niños participan en estas maniobras, lo que genera un nuevo desafío, ya que el sistema de responsabilidad penal adolescente no está preparado para la magnitud del problema.
- En cuanto a la respuesta institucional, sostuvo que es necesario definir una política criminal clara que priorice los ciberdelitos como un área de persecución. Si se establece esa prioridad, debe garantizarse que existan equipos policiales, fiscales y judiciales preparados para trabajar en ella, y campañas sociales que promuevan la denuncia temprana. Sin esa definición estratégica, el sistema seguirá llegando tarde.
- Reconoció la tensión entre la necesidad de inmediatez en la investigación y el respeto a las garantías constitucionales. Señaló que el sistema debe buscar procedimientos más ágiles sin vulnerar derechos fundamentales, y reclamó una mayor capacidad de respuesta de la justicia para otorgar autorizaciones en plazos acordes a la dinámica criminal digital.

- **NITEP:**
  - Reclamó que la seguridad debe pensarse desde la persona y no sólo desde el delito, y que el enfoque de seguridad ciudadana debe integrar prevención, inclusión social y protección digital. Planteó que la exclusión digital incrementa la vulnerabilidad de los sectores más pobres y que es necesario articular plataformas de digitalización seguras, campañas de sensibilización y educación digital temprana para que la ciudadanía tenga capacidades mínimas de autoprotección.
  - Explicó que la pobreza y la exclusión social están directamente ligadas al ciberdelito, y que la justicia restaurativa no alcanza si no se integra inversión social orientada a reducir la vulnerabilidad previa. Reclamó que se incorpore al MIDES como socio estratégico del PNSP, en tanto su ley orgánica le otorga autonomía y recursos para la inversión social. Señaló que el ministerio administra cientos de miles de transferencias sociales, por lo que esas plataformas requieren salvaguardas digitales inmediatas, y propuso crear mecanismos conjuntos entre MIDES y el Ministerio del Interior para proteger pagos como la Tarjeta Uruguay Social frente a fraudes.
  - Cuestionó que el PNSP no contemple con suficiente peso la inversión social preventiva y advirtió que el Ministerio del Interior carece de recursos para cubrir esa dimensión, por lo que insistió en articular presupuesto y responsabilidades. Reclamó mayor convocatoria a actores sociales y privados, señalando que varias instituciones invitadas no respondieron y que resulta clave integrar a bancos y cámaras empresariales para acordar protocolos de bloqueo y reporte.
  - Propuso usar el Marco de Ciberseguridad de AGESIC como herramienta inmediata para que las organizaciones puedan medir su nivel de madurez y aplicar políticas internas, y sugirió articularlo con MIDES para alinear gobernanza técnica con prevención social. Destacó la necesidad de alfabetización digital en grupos vulnerables, como beneficiarios de programas sociales, personas en situación de calle y adultos mayores, de campañas de difusión en redes, y de formación de agentes sociales que acompañan a estos colectivos.
  - Advirtió que el uso de tarjetas prepagas y cuentas de adolescentes como “mulas digitales”, sumado a la circulación de tarjetas entre consumidores, dificulta el rastreo financiero, y planteó que deben aplicarse controles específicos a emisores de este tipo de productos. Señaló que un ataque a las plataformas de pagos podría paralizar prestaciones sociales, por lo que reclamó planes de continuidad y recuperación operativa.

- Propuso que el PNSP incorpore a MIDES como actor presupuestal y operativo en prevención, que se celebren convenios con AGESIC para aplicar estándares de seguridad en plataformas sociales, y que se comprometa al sector privado en protocolos de cooperación inmediata frente a incidentes que afecten transferencias sociales.

- **Poder Judicial:**
  - Planteó como desafío central la necesidad de revisar la dosimetría penal vinculada a los ciberdelitos y delitos conexos. Se sostuvo que delitos como la estafa, que en ocasiones alcanzan montos millonarios, deberían ser considerados en relación directa con el delito de lavado de activos. Se reclamó la actualización de la normativa de lavado para que contemple estos delitos y no se siga trabajando con herramientas desactualizadas que obligan a vincular casos individuales de manera precaria.
  - Resaltó la importancia de generar estándares y protocolos claros para la obtención y el tratamiento de la prueba digital. Hoy existe una gran dispersión sobre qué pedir, a quién y cómo hacerlo, lo que genera demoras e inconsistencias. Mencionó el trabajo en cooperación con el programa europeo PAcCTO, que busca desarrollar guías prácticas para uniformar procedimientos frente a proveedores internacionales y nacionales, facilitando la respuesta y asegurando validez en el uso de la evidencia.
  - Destacó la dificultad de valorar la evidencia digital en los procesos judiciales. Aunque algunas conductas pueden encuadrarse en figuras ya existentes, la normativa actual resulta insuficiente para los desafíos que plantea lo digital. Las definiciones son poco claras y no existen criterios uniformes. La mayoría de los casos terminan en procesos abreviados, lo que impide un análisis profundo de la calidad y validez de la prueba. Persisten prácticas como trasladar la evidencia digital al papel con certificación notarial, reproduciéndola en audiencia para darle mayor formalidad, lo que encarece y desvirtúa la prueba original. Subrayó la necesidad de capacitación especializada para jueces y fiscales en valoración de evidencia técnica y en el uso de peritajes, para evitar dudas y dependencia de criterios externos.

- Advirtió que la incorporación de nuevos tipos penales debe hacerse con cautela, evitando contradicciones con el marco normativo vigente. Ejemplificó que en algunos delitos patrimoniales el parentesco actúa como eximente, mientras que en propuestas de regulación de ciberdelitos aparece como agravante, generando incoherencias. Se sostuvo que debe existir una regulación unificada y coherente. Asimismo, señaló la necesidad de definir con claridad cuándo las ventas en línea que no se cumplen constituyen un simple incumplimiento contractual y cuándo pueden ser tratadas como estafas, ya que la acumulación de múltiples casos similares no siempre implica un artificio o engaño que encuadre en la figura penal.
- Advirtió sobre el riesgo de simplificar procesos de forma tal que se vulneren garantías fundamentales. Reconoció que la burocracia en autorizaciones judiciales puede ser frustrante frente a la inmediatez del ciberdelito, pero se sostuvo que estas demoras cumplen la función esencial de proteger los derechos de las personas, incluyendo su privacidad y el principio de inocencia. Consideró indispensable mantener al juez como tercero imparcial que autoriza medidas intrusivas, evitando excepciones que puedan debilitar el sistema de garantías.
- Reconoció que en países como Argentina o Brasil las fiscalías pueden ordenar directamente medidas como el levantamiento del secreto bancario o solicitudes a proveedores internacionales. Sin embargo, señaló que Uruguay tiene un marco constitucional distinto que exige la intervención judicial, lo que constituye una salvaguarda necesaria. No obstante, se reconoció que muchas veces la lentitud responde más a problemas de cultura institucional y de prioridades que a impedimentos normativos. Planteó que otorgar a estos delitos la misma prioridad procesal que se da a los allanamientos permitiría mejorar la celeridad, sin necesidad de modificar las reglas de fondo.

- **Unidad de Cibercrimen:**
  - Planteó que Uruguay se ha convertido en un terreno fértil para el crecimiento de los ciberdelitos, en particular las estafas, debido a la combinación de factores como penas bajas, falta de inmediatez en la cooperación internacional y obstáculos en los procedimientos internos. Subrayó que, aunque se han incorporado nuevas tipificaciones, las sanciones no cambiaron y los delincuentes primarios siguen teniendo márgenes amplios de impunidad, lo que genera una percepción de escaso riesgo.

- Advirtió sobre la falta de colaboración inmediata con otros países, lo que retrasa investigaciones durante meses o incluso años. A nivel interno, identificó serias dificultades vinculadas a los tiempos judiciales para el levantamiento del secreto bancario o para obtener información de proveedores internacionales como Meta, donde una solicitud puede demorar hasta dos meses. En este marco, señaló que en países vecinos, como Brasil o Argentina, la fiscalía puede emitir directamente estos oficios, lo que permite respuestas mucho más rápidas. Reclamó entonces que en Uruguay se considere una fiscalía especializada en ciberdelitos, con competencias técnicas y procesales que permitan actuar con mayor eficacia.
- Remarcó que la investigación de estafas está estrechamente vinculada a otros delitos y que, al no dimensionar sus conexiones, se subestima su impacto. Explicó que las cárceles se transforman en espacios de aprendizaje para estas maniobras, ya que los internos acceden a dispositivos con fines educativos que luego usan para continuar delinquiendo. Señaló también que las estafas financian fenómenos más amplios, como las narcoguerras en barrios de Montevideo, donde el dinero obtenido sostiene la compra de armas, municiones y granadas, además de sostener a internos en prisión.
- Alertó sobre la utilización de adolescentes en estas maniobras, quienes acceden a tarjetas de débito o prepagas desde los 14 años y las ofrecen a grupos criminales a cambio de pequeñas sumas, cumpliendo el rol de “mulas” sin enfrentar mayores consecuencias legales por su condición de infractores. También mencionó la dificultad de rastrear operaciones realizadas con tarjetas de consumo de bajo monto, lo que amplía la impunidad de los estafadores.
- En cuanto a la victimización, destacó que cada vez más empresas pequeñas y medianas están siendo atacadas, con pérdidas que en algunos casos comprometen casi todo su capital operativo, lo que impacta de forma directa en la economía del país. Insistió en que no se está visualizando la magnitud del problema ni los riesgos que implica la estafa como delito articulador de múltiples amenazas.
- Por otra parte, se refirió a la falencia de recursos para la persecución y la falta de una mirada integral en el análisis de los incidentes. Subrayó la brecha existente entre los más de 6.000 incidentes recibidos por CERTuy en un año y las pocas decenas que se tradujeron en denuncias policiales, lo que distorsiona las estadísticas y limita la construcción de políticas públicas efectivas.

- Reclamó una mayor inmediatez en la respuesta, ya que la burocracia actual es incompatible con la dinámica de los ciberdelitos, donde en cuestión de minutos pueden desaparecer pruebas o fondos. Propuso implementar herramientas tecnológicas y procesos automatizados que permitan, sin vulnerar las garantías existentes, agilizar bloqueos, oficios y pedidos de información. Reconoció, sin embargo, que cualquier mejora en la eficiencia debe mantener intactas las garantías procesales y constitucionales, y aclaró que el objetivo no es saltearlas, sino optimizar los mecanismos ya previstos para que funcionen en tiempos acordes a la realidad digital.

- **Unidad de Ciberdefensa del Ejército Nacional:**
  - Expresó que uno de los principales desafíos es el intercambio de información entre instituciones. Señaló que hoy no existe coordinación ni colaboración en ese sentido, lo que impide detectar si un ataque dirigido a un organismo del Estado también está afectando a otros. Recalcó que las organizaciones suelen reaccionar de manera aislada, limitándose a bloquear el ataque, sin tener una visión integral que permita dimensionar el alcance de la amenaza.
  - Advirtió que los ciberdelitos no deben ser considerados únicamente como un problema económico, sino también como un asunto de defensa nacional. La pérdida de información sensible del Estado o la posibilidad de que un ataque afecte infraestructuras críticas —como el suministro de energía, agua o comunicaciones— representa un riesgo real que ya se ha materializado en otros países, tanto por actores externos como por el crimen organizado. Recordó que, en estos casos, no solo se pone en juego la privacidad o el dinero, sino incluso la vida de personas, en particular en áreas sensibles como el Ministerio del Interior o la Fiscalía, donde una filtración de datos podría ser utilizada como mecanismo de coacción contra funcionarios.
  - Destacó además que organismos como el MIDES ya sufrieron filtraciones en el pasado, exponiendo información de personas en situación de vulnerabilidad y de sus propios funcionarios, y mencionó el caso reciente del SODRE, cuyos datos personales y de proveedores quedaron expuestos en Internet.
  - Reclamó que exista una fiscalía especializada en ciberdelitos, con formación técnica adecuada para servir de puente entre el mundo jurídico y el técnico, ya que hoy se requiere un mediador que pueda comprender ambos lenguajes y facilitar la coordinación interinstitucional.

- **UdelaR:**
  - Reclamó que Uruguay aún no cuenta con un catálogo de activos críticos, a pesar de que se intenta definirlo desde 2008, lo que impide identificar claramente cuáles son las infraestructuras críticas que deberían protegerse con prioridad. Sostuvo que esta omisión es una vulnerabilidad grave, porque sin ese catálogo no se puede diseñar un plan de defensa coherente frente a ataques que podrían afectar recursos esenciales como energía, agua o comunicaciones.
  - Planteó que "sin ciberseguridad no hay seguridad pública ni nacional" y que el país debe tomarse este tema mucho más en serio, porque si bien Uruguay fue considerado un ejemplo regional hace algunos años, hoy presenta un nivel de vulnerabilidad enorme. Afirmó que, aunque se han elaborado normas y protocolos, lo que falta es un plan de gobernanza integral que articule a todas las instituciones bajo una estrategia nacional de ciberseguridad, ciberdelito y soberanía digital.
  - Señaló que la coordinación y el intercambio de información entre agencias siguen siendo deficientes. Explicó que cuando un organismo detecta un ataque, no basta con mitigarlo de manera aislada, sino que debe informar de inmediato al resto del país para evitar que el mismo vector se replique en otras instituciones, algo que ocurre frecuentemente a nivel regional. Indicó que existen protocolos internacionales para compartir información de incidentes, pero en Uruguay no se han implementado con la gobernanza necesaria.
  - Advirtió sobre la brecha entre lo técnico-jurídico y lo técnico en ciencias de la computación y tecnologías de la información, lo que genera dificultades para que los operadores judiciales comprendan adecuadamente los aspectos tecnológicos de los ciberdelitos. Reclamó que esta brecha se reduzca mediante prácticas conjuntas, mayor entendimiento mutuo y mecanismos de traducción entre ambos mundos.
  - Señaló que el país tiene una carencia estructural en capacidades de análisis forense digital. Indicó que no existe un plan básico de formación en la materia y que, salvo iniciativas puntuales de la unidad de cibercrimen, no hay una propuesta nacional para generar técnicos capaces de recoger, preservar y analizar pruebas digitales de manera adecuada. Reclamó que se impulse la creación de programas de formación transversal que incluyan cursos de posgrado, especializaciones en ministerios y capacitación en defensa y relaciones exteriores, de modo que la capacidad forense digital se convierta en un recurso estratégico y transversal para todo el país.

- Concluyó que sin formación en análisis forense digital será muy difícil garantizar investigaciones y juicios sólidos en materia de ciberdelitos, y que este es un objetivo fundamental que debe incluirse en la estrategia nacional.

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 Pregunta disparadora 2 (11:15 – 12:45)

¿Dónde hay más oportunidades de intervenir para lograr resultados? ¿Qué iniciativas se han intentado antes y qué aprendimos de ellas?

Aportes generales

- Se consideró fundamental iniciar procesos de educación y prevención desde edades tempranas, aprovechando Plan Ceibal para enseñar sobre riesgos en redes, estafas y seguridad digital, y extender la formación también a adultos mayores, bancarios, docentes y otros profesionales, utilizando formatos atractivos como campañas en TikTok, Instagram o videos cortos.

- Se identificó la oportunidad de ampliar la formación especializada en ciberseguridad y forense digital, más allá de cursos aislados, creando programas formales y certificados que integren aspectos técnicos, jurídicos y de defensa, incluyendo la Licenciatura en Ciberseguridad que impulsa la Policía, la tecnicatura en ciberdefensa proyectada por el Ejército y los cursos gratuitos del CALEN, con la sugerencia de involucrar también a jueces y fiscales para generar un lenguaje común.

- Se remarcó que la brecha digital en poblaciones vulnerables constituye un riesgo, y se planteó actualizar mecanismos de asistencia como la Tarjeta Uruguay Social para incorporar trazabilidad y controles que reduzcan fraudes, además de generar convenios con Antel y la Red UCI para mapear brechas de acceso y seguridad digital desde un enfoque de seguridad ciudadana.

- Se señaló la necesidad de fortalecer la gobernanza y la regulación del sector privado, ampliando la capacidad normativa de AGESIC, dotando a CERTuy de roles y protocolos claros, e imponiendo sanciones a empresas que no cooperen en las investigaciones; se subrayó la importancia de tipificar el crimen bancario y de agilizar los trámites judiciales, tomando como referencia a Brasil y Argentina donde la fiscalía puede oficiar directamente a empresas o realizar incautaciones, a diferencia de Uruguay donde los trámites pueden demorar hasta dos meses.

- Se planteó la oportunidad de actualizar la política criminal en su conjunto, con fiscalías especializadas en ciberdelitos y equipos de peritos que faciliten la interpretación judicial de la prueba digital, mejorando los tiempos desde la denuncia hasta la investigación y garantizando rapidez sin vulnerar derechos.

- Se destacó la cooperación internacional, tanto formal (como el Convenio de Budapest) como informal (canales directos entre policías y fiscalías), que puede acelerar la persecución penal y el congelamiento de activos en casos de fraude transnacional.

- Se consideró que la inteligencia artificial puede aportar en la identificación de patrones y priorización de denuncias, aunque con riesgos de sesgos y manipulación, lo que exige marcos éticos y controles; también se sugirió implementar sistemas de alerta en dispositivos y aplicaciones estatales como Verifica.uy, en coordinación con bancos y empresas de telecomunicaciones.

- Se propuso desarrollar campañas nacionales masivas, unificadas desde Presidencia, para sensibilizar a la ciudadanía en la prevención de estafas y fraudes, con la colaboración de organizaciones de la sociedad civil para llegar a diferentes públicos.

- Se advirtió que las instituciones trabajan en múltiples iniciativas sin suficiente coordinación, y que una oportunidad clave es socializar avances y articular esfuerzos interinstitucionales para evitar duplicaciones y optimizar recursos.

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 13 de octubre y del 20 de octubre se realizarán mesas temáticas en el marco del Cuarto Encuentro por Seguridad.

4. Anexos

4.1 Lista de participantes

Participantes

Institución	Nombre del Representante
Centro de Altos Estudios Nacionales (CALEN)	Pedro Martín Gómez De Luca Wiler Alvez
DATA Uruguay	Patricia Díaz
Fiscalía General de la Nación (FGN)	Patricia Marquisa
Ministerio de Economía y Finanzas (MEF)	Marcelo Pereira
Colectivo Ni Todo Está Perdido (NITEP)	Ken Chang
Poder Judicial	Jennifer Saavedra Juan Pablo Novella Heilmann María Sol Bellomo Peraza
Unidad de Cibercrimen – Ministerio del Interior	Christian Alcaide Saul Scanziani
Unidad de Ciberdefensa del Ejército Nacional	Javier Bussi
Universidad de la República (UdelaR)	Gustavo Betarte

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)	Nathalie Castello
Programa de las Naciones Unidas para el Desarrollo (PNUD)	Mariela Solari
Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC)	Mariana Kiefer

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


Pregunta 10
¿Cuáles son los principales desafíos con relación a este tema?

Presidencia
Uruguay

Ministerio
del Interior