Plan Nacional
de Seguridad Pública

Encuentros por seguridad

Ronda 4 de 5

Eje estratégico: **Ciberdelitos**

Lunes 20 de octubre de 2025
Montevideo, Uruguay

Mesas temáticas

Objetivo general

Perfilar propuestas de intervención que sean relevantes, oportunas y viables.

Objetivo de hoy

Formular propuestas relevantes con recursos y responsables claros.

Agenda

9:00	Bienvenida y dinámica de trabajo
9:15	Ronda de presentación de los participantes
9:30	Análisis de propuestas
11:00	Pausa para café
11:15	Ideas emergentes
12:45	Cierre y próximos pasos

Mesas temáticas

Ronda de presentación de los participantes

Por favor, indique brevemente:

¿qué institución representa, cuál es su nombre y posición?

Propuestas recibidas

Propuesta 1

Creación de la especialización en Cibercrimen, Forensia Digital y Marco Jurídico

Universidad de la República

Objetivo

Implementación de un plan de formación profesional formal de dos semestres lectivos en cibercrimen y forense digital con un claro manejo del marco jurídico nacional e internacional.

Población

- Profesionales de las áreas de Derecho, Tecnologías de la Información, (Ciber)Seguridad, Ciencias Forenses, y afines.
- Funcionarios judiciales, policiales y militares especializados en delitos informáticos.
- Técnicos en ciberseguridad y protección de datos.

Acciones

Crear una especialización para formar expertos que puedan actuar eficazmente en investigaciones judiciales y en la protección de datos en el contexto uruguayo, promoviendo la justicia y la seguridad digital conforme a la normativa vigente.

Instituciones responsables

- UdelaR
- Docentes especializados
- Poder Judicial
- Policía Nacional
- Ejército Nacional
- AGESIC

Cobertura

Todo el territorio

(Modalidad semipresencial/en línea con encuentros presenciales)

Propuesta 2

“La información es prevención”

Defensoría Criminal – Poder Judicial

Objetivo

Reducir el ciberdelito y los fraudes informáticos.

Lograr que los casos que se registren sean procesados por el sistema de forma eficiente.

Acciones

- Dictar talleres educativos, mesas de trabajo donde se trasladen dificultades y compartirlas entre los distintos operadores del sistemas procesal penal con la finalidad de intercambiar información y transmitir necesidades desde los distintos roles.
- Procesar de forma efectiva el trabajo, posibilidad de participar en mesas de discusión que puedan incidir en tratamientos normativos del tema.

Población

- Infancias
- Padres de infancias
- Adultos mayores
- Ministerio del Interior
- Operadores jurídicos
- Instituciones vinculadas

Instituciones responsables

- Anep
- Poder Judicial
- Fiscalía
- Ministerio del Interior
- Instituciones vinculadas

Cobertura

Todo el territorio

Duración continua

Propuesta 3

“Uso de Inteligencia artificial para la detección de patrones comunes en las denuncias de Estafas”

Fiscalía General de la Nación

Objetivo

Generar una herramienta de IA que pueda identificar automáticamente denuncias con “modus operandi” similares.
La herramienta deberá además, leer extensos documentos, analizar audios y videos, entre otra información propia de las denuncias.

Población

La herramienta sería utilizada por la Fiscalía General de la Nación - principalmente el Departamento de Depuración, Priorización y Asignación de la Fiscalía (DPA) y las unidades de Políticas Públicas e Informática de Fiscalía- pero su uso impactaría en toda la población.

Acciones

1.Desarrollar la herramienta
2.Capacitar abogados y fiscales para su uso
3.Coordinar acciones entre la policía y la Fiscalía a fin de asignar las denuncias en un tiempo breve y tomar las medidas más urgentes de manera inmediata.
4.Campañas preventivas en medios de comunicación para concientizar a la población sobre modalidades de engaño

Instituciones responsables

- Fiscalía
- Ministerio del Interior
- Agesic
- Empresa desarrolladora de la herramienta

Cobertura

Todo el territorio

Propuesta 4

“Escudo digital social: seguridad financiera, identidad y justicia para la población vulnerable”

Colectivo Ni Todo Está Perdido (NITEP)

Objetivo

Garantizar el ejercicio pleno de los derechos humanos a la identidad digital y la protección social para la población vulnerable, mediante la erradicación del analfabetismo digital en esta población, la digitalización segura de las prestaciones sociales (BPS/MIDES) y la articulación de un sistema estatal de prevención y justicia

Instituciones responsables

- Ministerio del Interior
- Ministerio de Desarrollo Social
- Ministerio de Educación y Cultura
- Banco de Previsión Social
- Banco Central del Uruguay
- Fiscalía General de la Nación
- Poder Judicial
- Instituto del Niño y Adolescente del Uruguay (INAU)
- AGESIC
- DNIC

Población

- Personas en situación de calle o en dispositivos MIDES
- Niños, Niñas y Adolescentes en Centros INAU que son beneficiarios de la TUS, AFAM-PE u otros subsidios del BPS

Cobertura

48 meses de duración en todo el territorio

Acciones

- **Talleres intensivos de alfabetización digital crítica y ciber-higiene financiera** en centros sociales, dictados por el MEC, con énfasis en el uso seguro de identidades y la prevención de fraudes de subsidios
- **Implementación de puntos-ID sociales** para el trámite de CI exprés/exonerado y la **asistencia técnica** para validar el **usuario gub.uy**
- Planificación estratégica a 48 meses para la transición de la Tarjeta Uruguay Social (TUS) y las prestaciones de AFAM-PE a una **cuenta social digital segura**
- **Diseño de un protocolo de denuncia** simplificado que articule la denuncia desde los centros MIDES/INAU, el patrocinio gratuito de la Defensoría Pública (DINADEF), y la coordinación con Fiscalía y BPS **para la recuperación inmediata de fondos defraudados**

Propuesta 5

“Fortalecimiento de la respuesta nacional frente al Cibercrimen”

Dirección de Investigaciones de la Policía Nacional - Unidad de Cibercrimen

Objetivo

Fortalecer de manera integral la capacidad del Estado uruguayo, a través de la Unidad de Cibercrimen, para prevenir, investigar y responder eficazmente al cibercrimen, garantizando la protección de los derechos fundamentales y la confianza digital de la sociedad

Instituciones responsables

- Ministerio del Interior (Policía Nacional - Dirección de Investigaciones - Unidad de Cibercrimen)
- Fiscalía
- AGESIC
- Banco Central del Uruguay
- Sector financiero
- Sector de telecomunicaciones
- Organismos internacionales (OEA, BID, INTERPOL, UNODC, Europol)
- Sector académico
- Sociedad Civil

Población

- Ciudadanía en general
- Funcionarios policiales, fiscales y operadores judiciales
- Instituciones públicas y privadas con infraestructuras críticas o sensibles

Cobertura

Duración estimada: 10 años

Todo el territorio

Propuesta 5

“Fortalecimiento de la respuesta nacional frente al Cibercrimen”

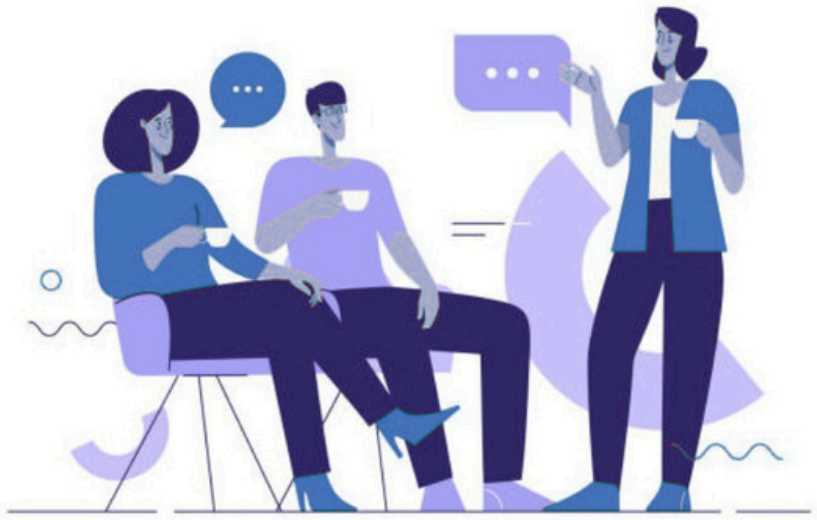
Dirección de Investigaciones de la Policía Nacional - Unidad de Cibercrimen

Acciones

- Crear **canales virtuales para denuncias** y consultas ciudadanas con capacidad de **recibir evidencia** digital de forma íntegra y segura.
- Ampliación y modernización del **Laboratorio Forense Digital**
- **Capacitación** continua y certificación internacional del **personal policial, técnico y forense**.
- Desarrollo de un **sistema integrado de prevención y respuesta al fraude electrónico**, en cooperación con bancos y el sistema financiero.
- **Campañas nacionales de concientización ciudadana** en cibercrimen y protección de datos personales.
- Elaboración y actualización de **protocolos operativos de ciber-investigación**, coordinación interinstitucional y gestión de incidentes.
- Fomento de **carreras y especializaciones en cibercrimen y evidencia digital**, dentro de la Dirección Nacional de Educación Policial.
- Implementación de **mecanismos de compensación y estímulo profesional** para la captación, retención de expertos y talentos en la temática.
- Fortalecimiento de los canales de **cooperación internacional** y adhesión activa a convenios de cooperación y agencias internacionales
- Integración de **herramientas de inteligencia artificial, análisis blockchain y OSINT** en las investigaciones digitales.
- Creación de un **área jurídica asesora** especializada en temas de **cibercrimen y tecnologías emergentes**.
- Creación de un área de **apoyo psicológico**, orientado a la contención del personal expuesto al material de **explotación sexual de niñas niños y adolescentes**, cómo también al abordaje primario de las víctimas del delito.

Mesas temáticas

Pausa para café



Ideas emergentes para desarrollar

Ideas emergentes sobre

marco legal y sancionatorio

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.

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.

Para cada idea se propone definir

Objetivo | Acciones | Instituciones responsables | Población | Cobertura

Ideas emergentes sobre

fortalecimiento institucional y capacidades especializadas

3 Crear una **fiscalía especializada en ciberdelitos** con competencias técnicas y procesales que permitan actuar con mayor eficacia y celeridad

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

5 Aumentar la **capacitación de jueces, fiscales y policías** en valoración de evidencia técnica y peritajes digitales y f**ormar al personal policial** para que pueda identificar direcciones IP y origen de mensajes al recibir denuncias

Para cada idea se propone definir

Objetivo | Acciones | Instituciones responsables | Población | Cobertura

Ideas emergentes sobre

coordinación operativa e interinstitucional

6

Establecer **convenios interinstitucionales** entre AGESIC, MIDES, bancos y empresas de telecomunicaciones para **implementar protocolos de bloqueo y respuesta rápida ante fraudes digitales**, incluyendo sistemas de alerta en aplicaciones estatales (ej. Verifica.uy) y **fortalecer los mecanismos de control financiero digital** mediante trazabilidad de tarjetas prepagas, cuentas digitales y programas de asistencia (ej. Tarjeta Uruguay Social), incorporando controles antifraude para proteger especialmente a los sectores más vulnerables.

Para cada idea se propone definir

- Objetivo
- Acciones
- Instituciones responsables
- Población
- Cobertura

Ideas emergentes sobre

prevención social y cultura de ciberseguridad

7

Desarrollar una **estrategia nacional de educación digital y cultura de ciberseguridad** que incluya formación desde edades tempranas (Plan Ceibal), capacitación en enseñanza formal (docentes, bancarios, adultos mayores), alfabetización digital en grupos vulnerables mediante agentes comunitarios y campañas nacionales masivas de sensibilización sobre estafas y fraudes, coordinadas desde Presidencia y difundidas en formatos digitales accesibles (TikTok, Instagram, videos cortos) con apoyo de organizaciones sociales.

Para cada idea se propone definir

- Objetivo
- Acciones
- Instituciones responsables
- Población
- Cobertura

Ideas emergentes sobre

cooperación, soberanía y protección

8 Elaborar un **catálogo nacional de infraestructuras críticas** (energía, agua, comunicaciones, pagos sociales) y establecer **medidas de protección y respuesta** ante ataques cibernéticos.

9 Fortalecer la **cooperación internacional formal** (Convención de Budapest) **e informal** (canales directos entre policías y fiscalías) para acelerar la persecución penal y el congelamiento de activos.

10 Definir límites claros para el **ciberpatrullaje y la ciberinteligencia**, garantizando control judicial y evitando abusos y **fortalecer la coordinación y el intercambio de información** entre instituciones mediante protocolos de interoperabilidad y alerta temprana.

Para cada idea se propone definir

Objetivo · Acciones · Instituciones responsables · Población · Cobertura

Próximos pasos

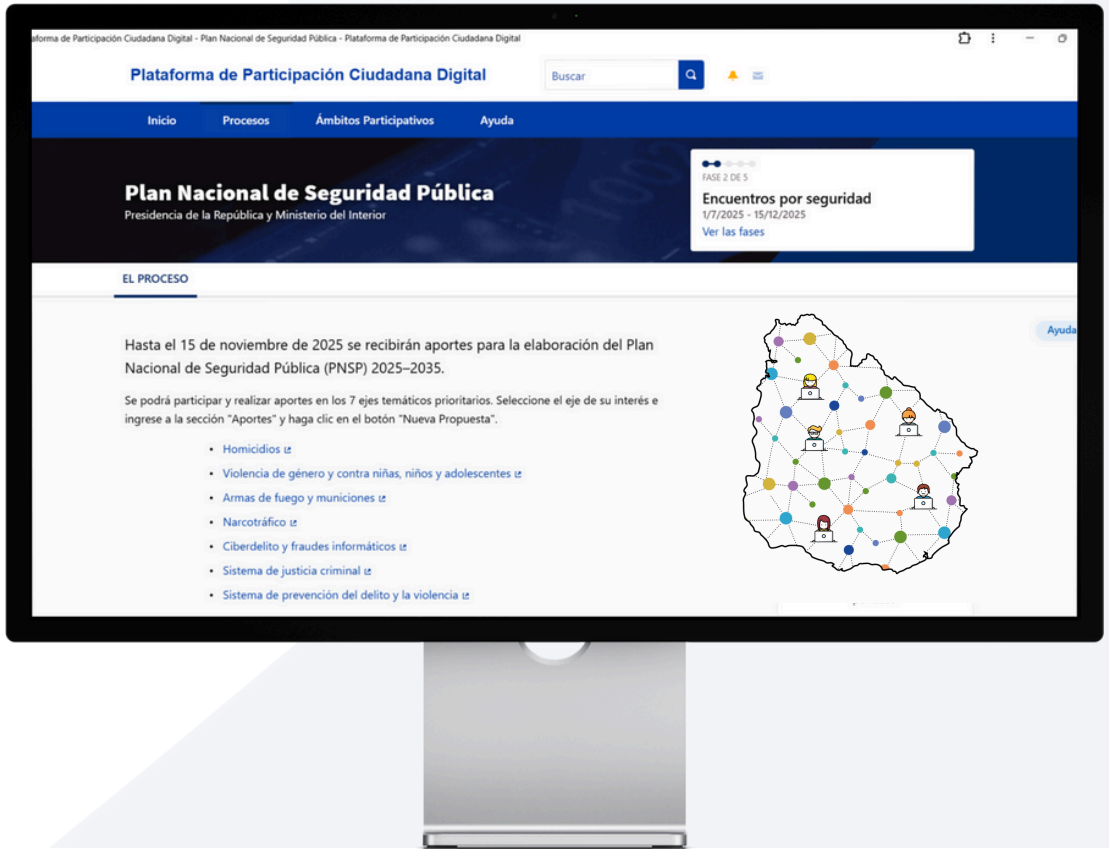
22 - 26 de setiembre 29, 30, 1 y 3 de octubre	**Ronda 3** - Encuentros por Seguridad
7 de octubre	Eventos por Seguridad: Homicidios
13 - 17 de octubre 20, 21, 22 y 24 de octubre	**Ronda 4** - Encuentros por Seguridad
3 - 7 de noviembre 10, 11, 12, 14 de noviembre	**Ronda 5** - Encuentros por Seguridad
18 de noviembre	Eventos por Seguridad: Trata y explotación

Novedades

Plataforma de Participación Ciudadana

Todas las personas podrán participar y **realizar aportes** en los siete ejes temáticos prioritarios.

Disponible **hasta el 15 de noviembre**.



Novedades

YouTube

Contacto

secretaria.pnsp@minterior.gub.uy

gub.uy/plan-nacional-de-seguridad-publica

pnsp.uy pnsp.uy pnsp_uy pnsp-uy

Presidencia
Uruguay

Ministerio
del Interior

Plan Nacional
de Seguridad Pública