Ministerio del Interior | Dirección de Investigaciones de la Policía Nacional

**UNIDAD DE CIBERCRIMEN**
Carlos Quijano 1316 (2° piso) – Montevideo – Uruguay
dipn-cibercrimen@minterior.gub.uy

**Oficio: 134/A/25/PDRM.----------**

**Referencia**: **PNSP (2025–2035)**

Montevideo, 17 de Octubre del 2025.

**SR ASESOR DEL MINISTERIO DEL INTERIOR**
**DR EMILIANO ROJIDO**

## 1. Título del programa:

"Fortalecimiento de la respuesta nacional frente al Cibercrimen"

## 2. Problema específico al que responde

El crecimiento sostenido de los delitos informáticos en Uruguay —fraudes electrónicos, accesos indebidos, explotación sexual en entornos digitales y vulneraciones a sistemas críticos — ha generado un impacto creciente sobre la seguridad pública, la confianza institucional y la economía digital del país. Estos hechos presentan un alto nivel de complejidad técnica y transnacionalidad, lo que exige capacidades especializadas, equipamiento avanzado y mecanismos sostenibles de cooperación.

La carencia de formación específica, la falta de articulación interinstitucional y la insuficiente infraestructura tecnológica limitan la capacidad de respuesta ante un fenómeno que evoluciona constantemente y que incide directamente en la protección de los derechos ciudadanos.

## 3. Principales factores o causas del problema

- Rápida expansión de la digitalización y del acceso a tecnologías emergentes. Limitada conciencia ciudadana sobre riesgos cibernéticos y buenas prácticas de seguridad digital.
- Déficit de infraestructura tecnológica avanzada para el análisis forense, monitoreo y respuesta ante incidentes. Escasa articulación institucional entre organismos públicos, el sector financiero, telecomunicaciones y la academia.
- Alto volumen de denuncias y necesidad de asesoramiento ciudadano, principalmente en casos de fraude.
- Dificultades en la retención y captación de talentos en ciberseguridad, tanto técnicos como policiales.
- Ausencia de formaciones académicas y policiales específicas en materia de cibercrimen y evidencia digital.

## 4. Objetivo principal del programa

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.

Objetivos específicos:

- Generar condiciones para la retención y desarrollo de profesionales especializados al servicio de la Unidad.
- Impulsar acciones de prevención y sensibilización ciudadana frente a los riesgos digitales.
- Desarrollar una capacidad nacional de innovación e investigación aplicada en tecnologías de ciberseguridad y análisis digital dentro de la Unidad de Cibercrimen.
- Posicionar a la Unidad como referente técnico y operativo del ecosistema nacional de ciberseguridad.
- Unidad referente en cuestiones de capacitación, formación y protocolos especializados en la materia, a nivel policial.

- Unidad de enlace y punto focal, para cuestiones de cooperación internacional, relativas a plataformas digtales.

## 5. Población objetivo

- Ciudadanía en general, especialmente personas y empresas usuarias de servicios digitales.
- Funcionarios policiales, fiscales y operadores judiciales que intervienen en investigaciones.
- Instituciones públicas y privadas con infraestructuras críticas o sensibles.

## 6. Cobertura temporal y territorial

Duración estimada: 10 años (2025–2035)
Territorio: Cobertura nacional, con eje operativo en Montevideo y presencia técnica en todas las Jefaturas Departamentales a través de nodos regionales de cibercrimen.
Se prevé la necesidad de incorporación de laboratorios móviles, que permitan la atención descentralizada y la movilidad operativa en todo el país.

## 7. Descripción de las actividades a desarrollar

- Mejoras en la recepción de denuncias digitales: creación de canales virtuales para denuncias y consultas ciudadanas, incluyendo denuncia en línea, chatbot de asesoramiento, terminales de autogestión y puestos de toma de denuncias con capacidad de recibir evidencia digital de forma íntegra y segura.
- Ampliación y modernización del Laboratorio Forense Digital, creación de un laboratorio de innovación e investigación aplicada y despliegue de laboratorios móviles.
- 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 ciberinvestigación, 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 (Interpol, Ameripol, Europol).
- 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.

## 8. Resultados esperados

- Reducción del impacto económico y social del cibercrimen en Uruguay. Mayor capacidad de respuesta policial, técnica y judicial ante delitos informáticos.
- Creación de una red nacional de cooperación público-privada para la prevención y detección temprana de incidentes.
- Incremento en la confianza digital ciudadana y en el uso seguro de los servicios electrónicos.
- Posicionamiento de Uruguay como referente regional en investigación, persecución y prevención del cibercrimen.
- Consolidación de la Unidad de Cibercrimen como centro nacional de referencia en investigación, innovación y formación en cibercrimen.

## 9. Instituciones responsables y aliadas

- Responsable principal: Ministerio del Interior – Policía Nacional - Dirección de Investigaciones - Unidad de Cibercrimen.
- Aliadas: Fiscalía General de la Nación, Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC), Banco Central del Uruguay, sector financiero y de telecomunicaciones, organismos internacionales (OEA, BID, INTERPOL, UNODC, Europol), academia y sociedad civil.

## 10. Recursos mínimos requeridos

- Aumento de recursos humanos operativos y técnicos-profesionales.
- Aumento y modernización de la flota vehicular.
- Ampliación edilicia o reubicación para adecuar la infraestructura al crecimiento operativo y tecnológico.

Principales rubros de gasto:

- Adquisición y actualización de equipamiento tecnológico especializado (hardware, software forense y herramientas de análisis digital).
- Formación, certificación y especialización del personal técnico y operativo.
- Compensación la adquisición y retención de talentos.
- Campañas nacionales de comunicación y prevención ciudadana.
- Infraestructura física y digital para los nodos regionales de cibercrimen.
- Monto estimado: inversión distribuida en etapas (2025–2035), se omite dada la magnitud y complejidad del programa.

## Observaciones

- La ejecución del programa requiere una visión estratégica, integral y sostenida, alineada con la Estrategia Nacional de Ciberseguridad, el Comité de Ciberseguridad y Prevención de Fraudes, y los compromisos internacionales en via de ser asumido por Uruguay, Convenio de Budapest y Convenio de Naciones Unidas contra la Ciberdelincuencia.
- La consolidación de la Unidad de Cibercrimen como estructura técnica, operativa y

estratégica constituye un eje central en la modernización del sistema de seguridad pública nacional. En un escenario donde la tecnología es el nuevo campo de confrontación del delito, esta área se proyecta como una de las más sensibles y determinantes para la seguridad pública del país.