Ficha Programática
PNSP (2025–2035)

Esta ficha sirve para describir una propuesta de programa. No es necesario tener formación técnica para completarla. En algunos ítems encontrará ejemplos o sugerencias para orientarse. En caso de dudas, consulte a los miembros de la Secretaría Técnica.

Información básica

Fecha de llenado: 10/11/2025
Nombre de la persona proponente: Ken Eddi Chang Breindembach
Institución / organización (si aplica): Colectivo Ni Todo Esta Perdido (NITEP)
Correo electrónico o contacto de referencia: katherineuruguaymontevideo@gmail.com

1. Título del programa

Programa: Generación Segura: Sembrando un Futuro Digital

2. Problema específico al que responde

Aumento del Ciberdelito (Eje 5 del PNSP 2025-2035) que incrementa la vulnerabilidad de la población en situación de calle, adultos mayores, NNA y receptores de subsidios, facilitando indirectamente la comisión de delitos asociados al Narcotráfico (Eje 4) y el lavado de activos (Ley 17.835). Existe una brecha en la respuesta institucional para la prevención, la trazabilidad financiera del crimen organizado y la reparación integral de las víctimas, afectando la Justicia Social y la Convivencia.

3. Principales factores o causas del problema

1. Baja Alfabetización Digital Crítica: Insuficiente conocimiento en ciber-higiene, manejo de la identidad digital (Usuario gub.uy) y detección de fraudes (incluyendo esquemas de lavado de activos/Narcotráfico) en poblaciones vulnerables.
2. Fragilidad en el Acceso a la Justicia Terapéutica y Restaurativa: Alto coste del patrocinio legal especializado y falta de protocolos unificados para la atención psicosocial de víctimas de ciberdelito.
3. Vulnerabilidad Estructural en la Seguridad Social: Riesgo de fraude y suplantación de identidad en el cobro de transferencias sociales (TUS, AFAM-PE, subsidios BPS) que pueden ser explotadas por el crimen organizado.
4. Fragmentación Institucional: Desarticulación entre las agencias de Seguridad, Justicia y Desarrollo Social para el combate coordinado del Crimen Organizado y el Narcotráfico en el ámbito digital (Decreto 95/025)

4. Objetivo principal del programa

Reparar y beneficiar el Tejido Social, Institucional, de Convivencia y Humano promoviendo la Justicia Preventiva y Territorial (con la alfabetización digital masiva), la Justicia Social y Restaurativa (garantizando el acceso a la Defensa Pública Digital y la asistencia psicosocial), y fortaleciendo la seguridad pública al reducir las oportunidades de fraude y lavado de activos del Narcotráfico mediante la seguridad financiera estructural (Cuenta Social Digital Segura), cumpliendo con los lineamientos del PNSP 2025-2035.

5. Población objetivo

Población Vulnerable: Individuos en situación de calle, extrema vulnerabilidad, NNA, adultos mayores, y perceptores de transferencias sociales (TUS, AFAM-PE, subsidios BPS).
Víctimas de Ciberdelito: Especialmente aquellas con bajos ingresos o violencia de género asociada (Ley 19.580).
Funcionarios Públicos y Actores Clave: Personal del MI, FGN, Poder Judicial (DINADEF), MIDES, MEC y BPS, que requieren capacitación especializada y certificación en forensia digital y atención a la víctima

6. Cobertura temporal y territorial

Duración estimada de la intervención: 60 meses (5 años), garantizando la continuidad como Política de Estado.
Fase 1 (18 meses - Piloto y Capacitación): Desarrollo de contenidos, capacitación masiva (Act. 7) y certificación a 30% de funcionarios; implementación piloto de los Puntos-ID y las Células de Asistencia Rápida (CARR) en 5 Intendencias priorizadas por el PNSP.
Fase 2 (24 meses - Expansión e Implementación Estructural): Expansión de la cobertura territorial de Módulos de Prevención Digital (Act. 1, 2) ; implementación total de la Cuenta Social Digital Segura ; especialización de la Defensa Pública Digital (DINADEF).
Fase 3 (18 meses - Consolidación y Continuidad): Evaluación Intermedia de Gobierno (Mes 42) para ajuste de objetivos y reajuste de la gobernanza; homologación y ratificación de protocolos internacionales; sistematización de buenas prácticas para la continuidad institucional más allá del período de gobierno (Política de Estado).
Territorio: Nacional, con focalización en las zonas de mayor índice de vulnerabilidad social y afectación por ciberdelito/narcotráfico

7. Descripción de las actividades a desarrollar

Prevención Digital y Acceso Comunitario
1. Módulos de Prevención Digital y Ciber-Higiene Financiera, dictados en Espacios Comunitarios: Uso de la red de Centros MEC e Infocentros (Red USI) como Puntos de Contacto y Capacitación Gratuitos.
MEC (Centros MEC), MIDES, Intendencias Departamentales, AGESIC.
Aprovechamiento de Infraestructura Existente: Uso de la red física de Centros MEC/Intendencias para reducir el coste de infraestructura y maximizar el alcance territorial.

Educación a Distancia y Población Vulnerable
2. Programas de Estudio Digital a Distancia (MBD) para Población Vulnerable: Uso de la plataforma CECAP del MEC o Aula Virtual y la red de Infocentros (Red USI) para capacitar a la población en situación de calle y extrema vulnerabilidad.
MEC (CECAP/Aula Virtual), MIDES, Red USI/AGESIC, ONGs.
Costo Mínimo por Canal Existente: Uso de plataformas de enseñanza a distancia (*e-learning*) y puntos de acceso gratuitos (Infocentros), minimizando el coste de docentes presenciales.

Identidad Digital
3. Implementación de Puntos-ID Sociales: Trámite de CI *exprés/exonerado* y asistencia técnica para validar el Usuario gub.uy a Nivel Intermedio.
MIDES, DNIC, AGESIC.
Sinergia con Eje 1 y 2: Utilización de los mismos Puntos de Contacto (Centros MEC/Infocentros) para el soporte técnico de identidad.

Seguridad Financiera Estructural

4. Planificación Estratégica para la Cuenta Social Digital Segura: Transición de la TUS y AFAM-PE a una Cuenta Social Digital Segura. Requisito: Autenticación fuerte con Usuario gub.uy Nivel Intermedio.

MIDES, BPS, BCU.

Fondos BID/Préstamo: Financiación del desarrollo tecnológico mediante convenios con organismos de desarrollo (ej. BID) para el *software* de la Cuenta Segura.

Atención a la Víctima / Primera Respuesta (CARR)

5. Establecimiento de Células de Asistencia Rápida y Psicosocial (CARR): Puntos Focales de Atención a la Víctima en Centros MEC/Infocentros para contención, asistencia psicológica inicial y derivación efectiva de denuncias.MIDES, MEC/Centros MEC, FGN, MI (Unidad Cibercrimen).

Capacitación Transversal Gratuita: El costo se cubre capacitando al personal social existente (MIDES/MEC) en atención a la víctima y primeros auxilios psicológicos a través de Cooperación Técnica No Retributiva (UNODC/OEA).

Defensa Ciudadana / Acceso a la Justicia (DINADEF)

6. Fortalecimiento de la Defensa Pública Digital (DINADEF): Protocolo de Especialización en Ciberdelitos dentro de DINADEF, garantizando la representación legal gratuita y especializada a víctimas vulnerables (ingresos menores a 5 BPC).Poder Judicial (DINADEF), COMJIB, EUROsociAL+ (UE).

Servicio Existente Especializado (Costo 0): El costo de la especialización y certificación de los Defensores Públicos es cubierto por Cooperación Internacional (COMJIB, UE), garantizando el Acceso a la Justicia sin costo fiscal adicional.

Perfeccionamiento de Protocolos y Capacitación Técnica Certificada

7. Capacitación Técnica Periódica y Certificada: Capacitación obligatoria a funcionarios de FGN, MI, Poder Judicial, MIDES y BPS en forensia digital, atención a la víctima y Ley de Ciberdelitos (20.327), con certificación internacional (OEA, UNODC, UE).MI, FGN, Poder Judicial, MIDES, BPS, OEA, UNODC, EUROsociAL+ (UE).

Cooperación Técnica No Retributiva: Asistencia técnica gratuita periódica de organismos internacionales cubre el costo de la formación y la certificación del personal a Costo 0.

Fortalecimiento Judicial y Cooperación Internacional

8. Protocolos de Adhesión y Homologación de Evidencia Digital: Homologación interna de protocolos judiciales y técnicos alineados con el Convenio de Budapest, la Convención de Viena (ONU) y el Convenio COMJIB.MRREE, Poder Legislativo, FGN, MI, Poder Judicial, AUCI.

Sinergia Intergubernamental: La capacitación certificada y la homologación de protocolos judiciales (Actividad 7) crean la base operativa para la ratificación de los acuerdos internacionales.

8. Resultados esperados

1. Incremento del nivel de Alfabetización Digital Crítica en la población vulnerable en al menos un 40%.
2. Implementación y operación total de la Cuenta Social Digital Segura dentro de los 48 meses, alcanzando al 100% de los perceptores de TUS, AFAM-PE y subsidios BPS.

3. Reducción en un 25% de los casos de fraude y suplantación de identidad en el cobro de transferencias sociales, dificultando el flujo de dinero ilícito del Narcotráfico (Eje 4).
4. Incremento en la tasa de denuncias formales de ciberdelito en un 20% , reflejo de la mejora en el acceso a la justicia y la confianza en la respuesta institucional (CARR).
5. Homologación de protocolos de evidencia digital y el inicio del proceso de adhesión a convenios internacionales (Budapest, COMJIB).
6. Establecimiento de un equipo de Defensores Públicos especializados en ciberdelito, garantizando la representación legal gratuita a víctimas vulnerables

9. Instituciones responsables y aliadas

Responsables de Gobernanza y Ejecución: Ministerio del Interior (MI) , Ministerio de Desarrollo Social (MIDES).

Aliadas Estratégicas Clave (Prevención y Educación): Ministerio de Educación y Cultura (MEC) , Intendencias Departamentales, Instituto del Niño y Adolescente del Uruguay (INAU), ONGs.

Aliadas de Identidad y Tecnología: AGESIC (Red USI / Infocentros Comunitarios), Dirección Nacional de Identificación Civil (DNIC).

Aliadas Estratégicas y Financieras (Seguridad Social): Banco de Previsión Social (BPS) , Banco Central del Uruguay (BCU).

Aliadas de Persecución y Justicia (DD. HH. y Acceso a la Justicia): Fiscalía General de la Nación (FGN) , Poder Judicial (Dirección Nacional de Defensa Pública - DINADEF).

Aliadas de Cooperación Internacional (Costo Cero): AUCI, MRREE, Poder Legislativo, OEA, UNODC, EUROsociAL+ (UE), COMJIB.

10. Recursos mínimos requeridos

Principales rubros de gasto (Maximización de Costo Cero/Bajo):
1. Cooperación Técnica No Retributiva: Cobertura de la capacitación y certificación obligatoria del personal (Actividades 5, 7) por organismos internacionales (OEA, UNODC, UE). *Costo 0.*
2. Infraestructura y Personal Existente: Uso de la red física de Centros MEC/Intendencias , plataformas CECAP/Aula Virtual , y reasignación de personal social (MIDES/MEC) para los CARR y Módulos de Prevención. *Costo Mínimo.*
3. Financiamiento No Retributivo para Desarrollo Tecnológico: Fondos de organismos multilaterales (ej. BID) para el desarrollo e implementación del software de la Cuenta Social Digital Segura (Actividad 4). *Costo Bajo/Financiación Externa.*
Monto total estimado: Mínimo (Cubierto por recursos reasignados y cooperación no retributiva, evitando un costo fiscal adicional)

Observaciones

1. Viabilidad y Fortaleza del Modelo de Costo Cero
El modelo de financiamiento es altamente viable porque se basa en la optimización interna y el apalancamiento de marcos de cooperación ya vigentes (Marco UE-Mercosur, Estrategia BID 2021-2025).

- Costo Fiscal Mínimo: La estrategia de Maximización de Recursos Existentes (MEC, MIDES, AGESIC) convierte los rubros de infraestructura y personal en Costo Cero a nivel de

nueva inversión, al depender de la reasignación de partidas presupuestales ya aprobadas, lo que minimiza la fricción política y la dependencia de leyes presupuestales adicionales.

- Alineación Estratégica: El programa se alinea directamente con áreas de prioridad no reembolsable de los organismos multilaterales:
    - BID: Prioridad en la Transformación Digital y el Fortalecimiento de Servicios Gubernamentales (referencia a precedentes como el Préstamo 5783/OC-UR).
    - Unión Europea (EUROsociAL+): Prioridad en el Estado de Derecho, Cohesión Social, Género y Ciberdelito, garantizando una alta probabilidad de conseguir los fondos de capacitación y especialización de la Justicia.

2. Acciones Críticas y Riesgos Pendientes (TBD)

El éxito inmediato del programa radica en la gestión urgente de los instrumentos aún por formalizar:

- Foco Crítico: La Cuenta Social Digital Segura (Act. 4):
    - Esta es la innovación central del programa y requiere la negociación de un Acuerdo de Cooperación Técnica No Reembolsable (ATN) con el BID. Es fundamental que la gestión priorice esta solicitud, haciendo referencia a los proyectos digitales exitosos anteriores (ej. UR-L1152, UR-L1193) para asegurar un número de convenio específico y evitar que el componente de desarrollo tecnológico quede sin financiamiento externo.
- Formalización de la Capacitación:
    - Los acuerdos de formación con OEA (CICTE), UNODC y COMJIB deben ser formalizados a través de Memorandos de Entendimiento (MDEs) o Acuerdos de Implementación Específicos con las instituciones ejecutoras nacionales (MI, FGN, PJ). La dependencia de un marco amplio (Ley N° 17.053) debe traducirse en convenios de ejecución con plazos claros.

3. Sostenibilidad a Largo Plazo y Legado Institucional

El modelo asegura que los resultados permanentes no generen deuda ni costos recurrentes significativos:

- Capital Humano Duradero: Al financiar la certificación en Forensia Digital y Atención a la Víctima (Act. 5, 7) con CTNR, el programa genera una capacidad instalada (personal especializado en FGN, MI, DINADEF) cuyo costo posterior es el de la planilla interna ya existente, no el del desarrollo del *know-how*.
- Blindaje Normativo: La estructura de costo cero se refuerza al cumplir directamente con leyes y normativas nacionales clave, lo que obliga a las instituciones ejecutoras a darle continuidad:
    - La especialización de DINADEF (Act. 6) atiende directamente el mandato de la Ley N° 19.580 (Violencia basada en Género).
    - La Cuenta Social Digital Segura (Act. 4) es la principal acción preventiva contra el fraude y el lavado, alineándose con la Ley N° 17.835 y el PNSP (Ejes 4 y 5).