FAMILYPROTECT-IA

PROTECCIÓN DIGITAL INTELIGENTE · PRIVACIDAD POR DISEÑO · IA RESPONSABLE

DOSSIER PROFESIONAL

CONSULTA PÚBLICA Y PARTICIPACIÓN MULTIACTOR

SOBRE NIÑAS, NIÑOS, ADOLESCENTES, ENTORNOS DIGITALES E INTELIGENCIA ARTIFICIAL

Aporte de FamilyProtect-IA a la construcción de políticas públicas que protejan derechos, garanticen privacidad y promuevan entornos digitales seguros, inclusivos y éticos.

ORIGEN DEL PROYECTO:

CASO REAL ANONIMIZADO

Una historia real que impulsó una solución diferente: proteger sin espiar, acompañar sin invadir y fortalecer la seguridad sin vulnerar derechos.

SEGURIDAD EN PROFUNDIDAD | **PRIVACIDAD POR DISEÑO** | **IA RESPONSABLE Y ÉTICA** | **GOBERNANZA MULTIACTOR** | **ALINEADO A DERECHOS HUMANOS**

PRESENTADO POR

ATHENARA S.A.S

DESARROLLO TECNOLÓGICO · INNOVACIÓN · SEGURIDAD · CONFIANZA

VERSIÓN 1.0

JUNIO 2026

IMPULSADO JUNTO A:

PARLAMENTO DEL URUGUAY · agesic DESARROLLANDO EL URUGUAY DIGITAL · Ceibal · unicef para cada infancia · PNUD

SOBERANÍA TECNOLÓGICA · INNOVACIÓN CON PROPÓSITO · CONFIANZA QUE TRASCIENDE

www.familyprotect-ia.uy

ATHENARA S.A.S

DOCUMENTO PARA CONSULTA PÚBLICA

FamilyProtect-IA

SISTEMA SOBERANO · INTELIGENCIA ARTIFICIAL RESPONSABLE

DOSSIER PROFESIONAL

Consulta Pública y Participación Multiactor Niñas, Niños, Adolescentes, Entornos Digitales e Inteligencia Artificial

Protección digital por capas · privacidad por diseño · resiliencia frente a la evasión

CASO REAL ANONIMIZADO · APRENDIZAJE PARA POLÍTICA PÚBLICA
El origen de una solución diferente.

- SEGURIDAD
- PRIVACIDAD
- AUTONOMÍA PROGRESIVA
- GOBERNANZA
- IA RESPONSABLE

FamilyProtect-IA

REPÚBLICA ORIENTAL DEL URUGUAY
Aportes de FamilyProtect-IA · Versión 1.0
18 de agosto de 2026

familyprotect-ia.uy

Origen y respaldo del proyecto

Por qué existe FamilyProtect-IA

FamilyProtect-IA nació de un caso real y muy particular. Una persona de 12 años con una habilidad digital fuera de lo común lograba burlar, una tras otra, todas las medidas de control parental que su madre —desesperada— intentaba aplicar. Herramientas comerciales, filtros, límites de aplicaciones: nada alcanzaba. La persona conocía el dispositivo mejor que quien intentaba protegerlo y encontraba siempre una ruta alternativa.

Lo que ninguna solución del mercado pudo resolver, este proyecto sí lo resolvió. Ese punto de partida define toda la filosofía del producto: un sistema de protección infantil debe diseñarse asumiendo que la persona protegida puede ser técnicamente competente, curiosa y persistente. La seguridad no puede depender de que la persona usuaria no sepa evadirla.

> **No existe un producto infalible —y sería deshonesto prometerlo—. Lo que sí es posible, y es nuestro objetivo, es ir un paso adelante del pensamiento del ciberdelincuente.**

Quién está detrás

El proyecto se sostiene sobre una trayectoria de más de dos décadas en ámbitos donde la seguridad no admite errores:

Ámbito	Rol y aporte al producto
Jefatura de Policía de Montevideo — 10 años	Oficina Centralizadora de Información Táctica, ESMAGE y Dirección de Seguridad. Análisis de amenazas reales, inteligencia táctica y anticipación al modus operandi delictivo.
Abitab Central — 16 años	Tecnología, en cargos de liderazgo. Sistemas críticos, alta disponibilidad y protección de infraestructura sensible a escala nacional.
Arnaldo Castro — actualidad	Auditoría Interna de la Nación, Ministerio de Economía y Finanzas. Control, cumplimiento y rigor en entornos de máxima exigencia.
Formación en Inteligencia Artificial	Certificaciones en Inteligencia Artificial de IBM y de la Universidad de Palermo.

Esa combinación —inteligencia policial para pensar como el adversario, tecnología crítica para construir con solidez, auditoría del Estado para no tolerar fallos y formación específica en inteligencia artificial— es la que hizo posible un producto robusto: no infalible, pero diseñado para adelantarse al ciberdelincuente en lugar de reaccionar tarde.

> FamilyProtect-IA es un producto de Athenara S.A.S., sociedad recientemente constituida por un único socio. El proyecto se desarrolla, hoy, con recursos propios.

Contacto y perfiles verificables

Autor y responsable — José Duarte Marchesano: Perfil de LinkedIn

FamilyProtect-IA · Seguridad infantil en medios digitales: Perfil de LinkedIn

Índice

1. Propósito y encuadre

FamilyProtect-IA se presenta a la Consulta Pública y Participación Multiactor con una pregunta concreta: ¿cómo puede una familia proteger a una persona menor de edad frente a riesgos digitales reales cuando los controles comerciales habituales pueden ser evadidos, sin convertir la protección en vigilancia permanente?

La propuesta no plantea que la tecnología sustituya a la familia, a la escuela, a los profesionales de la salud o al Estado. Plantea lo contrario: la tecnología debe funcionar como una capa de apoyo que reduzca riesgos previsibles, preserve la privacidad y favorezca el desarrollo de autonomía digital.

La consulta nacional transita su fase de intercambio multiactor, prevista del 23 de junio al 10 de setiembre de 2026, para generar información pública de calidad, apoyar la deliberación parlamentaria, fortalecer la coordinación institucional y orientar posibles acciones públicas.

1.1. Precisión metodológica

El caso relatado proviene de la experiencia de la familia promotora y se utiliza como caso de aprendizaje. No se presenta como estudio epidemiológico ni como prueba de causalidad. Su valor es mostrar un patrón de fallo de los controles y abrir preguntas de diseño, no adjudicar responsabilidades. El proyecto tampoco utiliza el diagnóstico de salud mental de una persona menor de edad como explicación de su conducta.

2. Resumen ejecutivo

El caso que origina FamilyProtect-IA expone una brecha que merece estar en la agenda pública: instalar controles parentales gratuitos, limitar aplicaciones y configurar filtros no garantiza por sí mismo un entorno digital seguro. Una persona de 12 años con elevada capacidad para comprender y utilizar tecnología encontró caminos para sortear controles convencionales y acceder a contenidos no adecuados para su edad.

El origen del proyecto está en el pedido de ayuda de una madre desesperada ante una situación que combinaba exposición a riesgos digitales, dificultades de supervisión y una necesidad urgente de acompañamiento. Lo relevante para la política pública es el aprendizaje: el dispositivo puede convertirse, involuntariamente, en una herramienta de distracción, acceso o continuidad de actividad, sin resolver por sí mismo la necesidad de protección, contención y acompañamiento.

La respuesta de FamilyProtect-IA es una arquitectura de defensa en profundidad, con un principio central: proteger no equivale a espiar. La propuesta se alinea con el enfoque de derechos que Uruguay ya aplica a la niñez y a la protección de datos (Ley N.º 17.823 y Ley N.º 18.331).

> **PROPUESTA CENTRAL EN UNA FRASE**
>
> *Pasar del «control parental basado en una lista de bloqueos» a un modelo de protección digital adaptativa, verificable, proporcional y centrada en derechos, capaz de resistir evasiones sin convertir el dispositivo de una persona menor de edad en un instrumento de vigilancia.*

3. Por qué este caso importa para Uruguay

La consulta pública impulsada por el Parlamento, Agesic, el Consejo Nacional Consultivo Honorario de los Derechos del Niño y Adolescente, Ceibal, UNICEF y PNUD busca identificar riesgos, oportunidades, habilidades y responsabilidades frente a redes sociales, plataformas, videojuegos, sistemas algorítmicos e inteligencia artificial.

FamilyProtect-IA aporta una dimensión que suele quedar entre dos extremos: la discusión abstracta sobre regulación de plataformas y la recomendación familiar de «hablar con los hijos». Entre ambos existe una capa tecnológica de protección del dispositivo que puede ser determinante cuando la persona menor de edad posee capacidades suficientes para evadir controles simples.

Problema observado	Límite del enfoque tradicional	Necesidad que revela
Evasión de filtros	Bloquear una URL o app puede no alcanzar	Defensa en profundidad y verificación de integridad
Múltiples rutas de acceso	Cambios de navegador, DNS, cuentas o apps	Control coordinado de dispositivo, red, identidad y apps
Exposición accidental a situaciones adultas	El filtro web no controla el entorno familiar	Acompañamiento emocional y educación, además de tecnología
Persona con alta capacidad técnica	La evasión supera a la configuración parental	Modelo adaptativo y proporcional
Supervisión limitada por horarios laborales	No siempre hay un adulto disponible	Automatización segura, alertas de bajo ruido y escalamiento
Riesgo de vigilancia excesiva	Registrar todo crea nuevos riesgos de privacidad	Minimización, procesamiento local y transparencia

4. El caso real, anonimizado

> **DECLARACIÓN DE ANONIMIZACIÓN**
>
> Este dossier no identifica sexo, nacionalidad, residencia, nombre, institución, familiares, diagnóstico clínico ni ningún atributo sensible de la persona de 12 años. La información se limita a lo necesario para explicar el problema y las decisiones de diseño. Ningún dato del caso debe usarse para reidentificar a la persona.

4.1. Qué reveló

El punto técnico relevante es que el atacante y el usuario protegido eran la misma persona, que conocía el dispositivo, sus configuraciones y las rutas alternativas de acceso. Una situación familiar compleja puede interactuar con el entorno digital: el dispositivo puede convertirse en mecanismo de distracción, acceso, evasión o exposición, y la tecnología por sí sola no resuelve las dimensiones emocionales, educativas ni familiares.

4.2. Qué falló en el enfoque tradicional

- Suponer que un único filtro representa todo el riesgo.
- Depender de controles que la propia persona protegida puede modificar o desinstalar.
- La ausencia de defensa frente a cambios de DNS, navegador, VPN/proxy, cuentas o ajustes.
- La falta de un modelo de riesgo contextual y gradual; confundir supervisar con registrar.

- La falta de mecanismos de recuperación y evidencia mínima cuando un control es alterado.

> **El aprendizaje: la seguridad debe construirse como un sistema adversarial. No basta con que funcione en condiciones normales; debe seguir protegiendo cuando la persona usuaria intenta encontrar una salida. Y robustecer el control no puede significar capturar todo lo que hace: se minimiza lo observado, se procesa localmente cuando es viable y se envía al adulto solo lo necesario para actuar.**

5. Lecciones de los controles tradicionales

5.1. De lista de bloqueo a arquitectura de protección

Los controles simples operan como listas: apps permitidas, páginas bloqueadas, horarios, límites de pantalla. Son útiles, pero no constituyen una arquitectura de seguridad. La respuesta profesional es defensa en profundidad: cada capa asume que otra puede fallar.

5.2. No confiar en un único indicador

No debe inferirse riesgo porque alguien abrió una app o visitó una categoría. El sistema correlaciona señales técnicas y contextuales, y mantiene un umbral alto antes de generar alertas.

5.3. Control reversible y explicable

Cuando una política se activa, la familia debe saber qué regla la produjo, qué se bloqueó, por cuánto tiempo y cómo revisarla. La persona menor de edad recibe una explicación adecuada a su edad. Las excepciones quedan auditadas. El objeto técnico es el entorno digital y sus condiciones de seguridad, no la personalidad de la persona: por diseño, no se construyen perfiles psicológicos.

6. Protección sin espionaje

FamilyProtect-IA es una plataforma de gestión y protección digital de dispositivos, con arquitectura local-first / offline-first, orientada a familias, centros educativos e instituciones. Reduce la exposición a riesgos previsibles mediante controles técnicos, educación y acompañamiento.

Sí hace	No debe hacer
Detectar que una política de seguridad fue alterada	Leer mensajes privados por defecto
Bloquear categorías de riesgo configuradas	Crear un historial exhaustivo de navegación
Detectar instalación de apps no autorizadas	Grabar el micrófono de forma permanente
Detectar señales de evasión del agente	Activar la cámara para vigilancia
Informar una alerta de seguridad de alto nivel	Construir un perfil psicológico
Procesar localmente una señal de riesgo	Enviar contenido bruto a la nube sin necesidad

7. La suite: Parental, Mobility y SCI — seguridad de toda una generación

FamilyProtect-IA no es un producto aislado: es una suite pensada para acompañar a una persona a lo largo de su vida digital y a las instituciones que la rodean. Estas son sus capacidades —qué hacen, no cómo lo hacen—, con un principio transversal: proteger sin espiar.

> **Todo lo que sigue ya está implementado en un MVP funcional, disponible para demostración en vivo. Por resguardo de la propiedad intelectual, este documento describe QUÉ hace cada módulo, no los detalles internos de CÓMO lo logra.**

FamilyProtect Parental — el escudo de la familia

- Vinculación segura entre el equipo del tutor y el de la persona menor, incluso sin router.
- Control de aplicaciones: ver, permitir, bloquear, aprobar instalaciones nuevas y desinstalar a distancia; con apps esenciales del sistema siempre protegidas.
- Ubicación en tiempo real y zonas seguras (geocercas) con aviso de entrada y salida.
- Tiempo de uso: horarios por aplicación, límite diario y hora de descanso.
- Modo perdido / antirrobo: bloqueo remoto, hacer sonar el equipo, foto de emergencia y borrado seguro, con doble confirmación.
- Botón de emergencia y contactos de auxilio en la pantalla de bloqueo; avisos que llegan aunque el teléfono esté en silencio.
- Resistencia a la evasión: la protección sobrevive al reinicio y se auto-repara.

FamilyProtect Mobility — moverse con seguridad

- Transporte en tiempo real: paradas cercanas, buses en el mapa y próxima parada, para que la familia sepa por dónde va.
- Planificador de viajes con estimación de llegada calculada por una inteligencia artificial propia y soberana.
- Estimaciones honestas: se indica la confianza del dato y su fuente; nunca se inventan horarios.

SCI — instituciones, comunicación única y prevención

- Canal ÚNICO de comunicación entre la institución y las familias: se termina la dispersión de WhatsApp, correos y aplicaciones sueltas. Un solo lugar, tanto para comunicados como para todo lo demás.
- Detección proporcional de señales de riesgo grave, con revisión humana obligatoria y sin castigos automáticos.
- Prevención de la captación de menores por bandas criminales: detección de señales de un léxico de reclutamiento (lenguaje carcelario y marginal usado para captar), tratado como señal para revisión humana —nunca como juicio sobre la persona—, con finalidad definida y salvaguardas.
- Riesgo de llamadas: analiza solo metadatos (quién, cuántas veces, a qué hora, cuánto dura), nunca el contenido, y muestra un semáforo explicable. Todo lo sensible se procesa en el propio equipo y solo viaja el resultado, cifrado.

> **Parental, Mobility y SCI comparten una misma convicción: la seguridad de una persona menor de edad —y, sumadas, la de toda una generación— no puede depender de la suerte ni construirse a costa de su intimidad.**

8. Arquitectura y defensa por capas

La protección se organiza en capas independientes; cada una asume que otra puede fallar. Se describe la función de cada capa y su criterio de privacidad, sin exponer detalles de implementación.

Capa	Función	Privacidad
1. Identidad	Determinar quién administra y qué equipo se protege	Datos de identidad mínimos
2. Integridad	Detectar manipulación del agente	Telemetría técnica limitada
3. Dispositivo	Aplicar las políticas del equipo	Sin contenido personal por defecto
4. Aplicaciones	Controlar instalación y ejecución	Solo los metadatos necesarios
5. Red	Reducir el acceso a dominios y categorías de riesgo	Registros minimizados
6. Contexto	Aplicar horarios y reglas de entorno	No requiere leer contenido
7. Riesgo	Correlacionar señales técnicas	Preferencia por el procesamiento local
8. Respuesta	Actuar de forma proporcional	Explicación y revisión
9. Auditoría	Demostrar qué ocurrió	Retención limitada
10. Recuperación	Volver a un estado confiable	Preserva la continuidad

8.1. Límites explícitos (honestidad)

Ningún sistema de control parental puede garantizar que una persona menor de edad jamás verá contenido nocivo. Otro dispositivo, un equipo de terceros, una cuenta ajena o una plataforma no administrable pueden quedar fuera de control. La promesa correcta es reducción de riesgo, no seguridad absoluta.

9. Inteligencia artificial responsable y altamente auditable

La IA aporta valor cuando ayuda a priorizar señales, clasificar categorías de riesgo o detectar anomalías técnicas. En el caso de personas menores de edad, debe estar subordinada a los derechos, a la explicabilidad y a la supervisión humana. Nuestra IA es propia y soberana; no depende de terceros.

> **Usamos inteligencia artificial responsable y ALTAMENTE AUDITABLE. Cada función registra métricas de precisión, tasas de falsos positivos y negativos, análisis de sesgo, versiones y pruebas adversariales. Todo puede medirse, revisarse y explicarse.**

Usos aceptables

- Clasificación local de categorías de contenido cuando el sistema lo permita de forma segura.

- Detección de anomalías técnicas y patrones de evasión; priorización de alertas para evitar la fatiga parental.
- Explicaciones comprensibles sobre por qué se activó una política.

Usos prohibidos o desaconsejados

- Inferir diagnósticos psicológicos o psiquiátricos; asignar una puntuación de «peligrosidad».
- Analizar conversaciones privadas como práctica rutinaria; tomar decisiones disciplinarias automáticas.
- Usar datos de riesgo infantil para publicidad o perfilado comercial.

10. Privacidad, derechos y autonomía progresiva

El Código de la Niñez y la Adolescencia reconoce a niñas, niños y adolescentes como titulares de derechos, entre ellos el derecho a la privacidad. La Ley N.º 18.331 establece la protección de datos personales como derecho humano e incorpora la responsabilidad proactiva, la privacidad desde el diseño y por defecto, y la evaluación de impacto. La Observación General N.º 25 del Comité de los Derechos del Niño extiende esos derechos al entorno digital.

> **Principio de mínima intrusión: el nivel de observación debe ser el mínimo necesario para una finalidad concreta. Un indicador técnico de manipulación no requiere conocer una conversación; un bloqueo de categoría no requiere almacenar cada página; una alerta de riesgo no requiere conservar el contenido que la provocó.**

A medida que aumentan la edad y la madurez, las políticas se flexibilizan: la protección evoluciona desde controles más estrictos hacia herramientas de acompañamiento, educación y autocuidado (autonomía progresiva).

11. Gobernanza y salvaguardas

Cualquier despliegue institucional debería contar con un comité independiente de salvaguardas — derechos de infancia, protección de datos, ciberseguridad, educación, participación adolescente y tecnología— y con evaluaciones obligatorias:

- Evaluación de impacto en protección de datos y en derechos de la niñez y adolescencia.
- Evaluación de ciberseguridad y auditoría de los modelos de IA.
- Pruebas de evasión y abuso; pruebas de accesibilidad; evaluación de falsos positivos y negativos.

12. Modelo de adopción y sostenibilidad

FamilyProtect-IA llega a las familias por dos caminos complementarios, que se potencian entre sí:

Vía de adopción	Cómo funciona	Beneficio
Centros de estudio (institucional)	La institución adopta la suite para entornos administrados y para el canal único de comunicación con las familias.	Entorno escolar más seguro y ordenado; una sola vía de comunicación.
Familias (directo)	Cada familia contrata la protección para el equipo de su hija o hijo.	Protección inmediata, sin depender de la institución.

Vía de adopción	Cómo funciona	Beneficio
Familias a través de su centro	Las familias vinculadas a un centro adherido acceden con un descuento.	Menor costo para la familia y mayor cobertura para la comunidad.

> **Cuando un centro de estudios adhiere, sus familias acceden con un descuento. La seguridad deja de ser un privilegio individual y pasa a ser un beneficio de toda la comunidad educativa —el camino más directo hacia la seguridad de toda una generación—.**

12.1. Sobre la gratuidad y la sostenibilidad

Es importante decirlo con honestidad: un producto de esta naturaleza, ofrecido de forma totalmente gratuita, es hoy una utopía. Alimentar la inteligencia artificial, mantener la infraestructura soberana y sostener el desarrollo tiene costos reales, que actualmente asume el proyecto con recursos propios. Un modelo enteramente gratuito solo sería viable si el Estado —y otros actores— se integraran como socios para impulsar el proyecto antes de su eventual exportación. Mientras tanto, el modelo de adopción descrito busca que la protección sea accesible sin comprometer su continuidad.

13. Propuestas para la consulta pública

Propuesta	Contenido
1. Estándar nacional de protección digital infantil	Un baseline técnico y de derechos con capacidades mínimas para dispositivos administrados en ámbitos familiares, educativos e institucionales.
2. Seguridad por defecto	Configuraciones seguras desde la primera activación, con recuperación robusta y controles resistentes a la evasión.
3. Protección por capas	Que la política no se limite a filtros de contenido: integrar dispositivo, apps, identidad, red, integridad y educación.
4. Privacidad por defecto	Prohibir, como regla general, la vigilancia de contenido privado. Priorizar señales técnicas y procesamiento local.
5. Gobernanza de IA infantil	Exigir documentación, auditoría, explicabilidad y supervisión humana.
6. Prohibición del perfilado psicológico	No usar diagnósticos ni puntuaciones de «peligrosidad» para restricciones automáticas.
7. Certificación independiente	Un esquema que mida resistencia a la evasión, privacidad, seguridad y usabilidad.
8. Interoperabilidad y soberanía	Evitar la dependencia de un único proveedor; permitir soluciones abiertas y auditables.

14. Hoja de ruta, indicadores y conclusiones

Etapa	Período	Entregables
0. Consulta y co-diseño	2026	Mapa de riesgos; participación infantil/adolescente; requisitos de derechos.

Etapa	Período	Entregables
1. MVP y prototipo controlado	2026–2027	Agente Android/Windows; motor de políticas; auditoría; pruebas de evasión.
2. Piloto educativo/familiar	2027–2028	Pilotos independientes; evaluación de eficacia y privacidad; métricas públicas.
3. Interoperabilidad	2028–2029	APIs, estándares e integración con ecosistemas educativos.
4. Escalamiento	2029–2030	Certificación, despliegues voluntarios y evaluación externa.

Ninguna fase debería avanzar por entusiasmo tecnológico, sino si la evidencia demuestra que la solución protege mejor que las alternativas, genera menos intrusión y puede ser auditada. Las metas de un piloto son propuestas de diseño, no resultados demostrados.

Conclusión y llamado a la acción

> **La oportunidad para Uruguay es un tercer camino: seguridad robusta sin vigilancia total.**
>
> Se puede lograr, pero solo si la seguridad, la privacidad y los derechos se diseñan juntos desde el primer requisito. FamilyProtect-IA propone aportar a ese proceso con un modelo técnico —y un MVP funcional— que puede ser sometido a prueba, auditoría, crítica y mejora.

Anexo A · Matriz riesgo → respuesta

Riesgo	Respuesta técnica	Respuesta humana	Dato mínimo
Evasión de controles	Integridad, políticas resistentes, detección de manipulación	Conversación y revisión de la configuración	Evento técnico
Acceso a contenido nocivo	Filtrado multicapa, DNS seguro, clasificación	Educación y acompañamiento	Categoría / resultado
Instalación no autorizada	Gestión de aplicaciones	Revisión de necesidad	Identificador de la app
Uso excesivo	Horarios, pausas y modos de descanso	Rutinas familiares	Tiempo agregado
Captación por bandas criminales	Señal de léxico de reclutamiento	Revisión humana y protocolo	Señal, no contenido
Manipulación del sistema	Estado de integridad	Recuperación guiada	Estado de seguridad
Riesgo alto	Escalamiento proporcional	Intervención humana	Alerta resumida

Anexo B · Principios no negociables

- 1. El interés superior de la persona menor de edad orienta toda la solución.
- 2. La privacidad no es un obstáculo a la seguridad: es parte de la seguridad.
- 3. Ningún diagnóstico clínico se usará como puntuación de riesgo.
- 4. La IA no sustituirá el juicio humano en decisiones de alto impacto.
- 5. El sistema debe poder explicar por qué se activó una política.
- 6. El procesamiento local se prefiere cuando es viable y seguro.
- 7. La recolección de datos debe ser mínima y con retención limitada.
- 8. Toda capacidad de vigilancia debe tener finalidad, necesidad, proporcionalidad y base jurídica.
- 9. El sistema asume intentos de evasión sin tratar a la persona como un adversario.
- 10. La solución fortalece la relación familiar; no la sustituye.
- 11. Toda afirmación de eficacia debe estar respaldada por pruebas reproducibles.
- 12. La plataforma reconoce sus límites técnicos y no promete seguridad absoluta.
- 13. Debe existir auditoría independiente y mecanismos de reparación.

Anexo C · Fuentes oficiales

- Consulta Pública y Participación Multiactor — Plataforma de Participación Ciudadana Digital, Uruguay (23 de junio al 10 de setiembre de 2026).
- Agesic — Noticia oficial de lanzamiento (25 de junio de 2026).
- PNUD Uruguay — Lanzamiento de la consulta pública (24 de junio de 2026).
- Convención sobre los Derechos del Niño — Observación General N.º 25 (2021).
- Ley N.º 17.823 — Código de la Niñez y la Adolescencia (Uruguay).

- Ley N.º 18.331 — Protección de Datos Personales (Uruguay).
- UNICEF Uruguay — Informe Kids Online Uruguay 2022.

Anexo D · Auditabilidad, transparencia y soberanía

FamilyProtect-IA asume un compromiso explícito con la auditabilidad. Cualquier juez competente, acompañado por un profesional idóneo que entienda la materia, puede auditar en todo momento nuestros algoritmos y nuestras decisiones automatizadas. No hay cajas negras impuestas: hay lógica explicable, registros y métricas.

> **NUESTRA PREMISA**
>
> Transparencia y honestidad en lo que el sistema hace y en lo que no hace.
>
> Soberanía sobre nuestros datos y sobre nuestros equipos tecnológicos.
>
> **Que seamos nosotros —las familias— quienes tomemos las decisiones sobre nuestra generación de hijos e hijas.**

> *Nota de integridad. Este dossier integra la visión estratégica de FamilyProtect-IA con información pública oficial. Las referencias al caso real son deliberadamente anonimizadas. No constituye dictamen jurídico, diagnóstico clínico, certificación de seguridad ni evaluación científica de eficacia.*