RESUMEN EJECUTIVO - Anexo II

Premio de Privacidad y Protección de Datos en Iberoamérica – AEPD

Título:

Privacy AI Studio: gobernanza y privacidad por diseño para el uso seguro de inteligencia artificial generativa en Iberoamérica

Autor/es o Entidad/es responsables:

Entidad responsable del diseño:
Laboratorio de Innovación e Inteligencia Artificial (IALAB)
Facultad de Derecho – Universidad de Buenos Aires

Entidad desarrolladora tecnológica:
Puzzle AI Agents

Descripción general de la candidatura

Privacy AI Studio es una plataforma tecnológica diseñada por el Laboratorio de Innovación e Inteligencia Artificial (IALAB) de la Facultad de Derecho de la Universidad de Buenos Aires, y desarrollada con Puzzle AI Agents, que permite a organizaciones públicas y privadas utilizar inteligencia artificial generativa para procesar documentos, audios y videos que contienen datos personales y sensibles, protegiendo los datos de identificación personal contenidos en ellos.

La plataforma fue diseñada como un software de “privacy-by-design” que integra tres capacidades críticas: (i) anonimización lingüística robusta ejecutada localmente mediante motores de procesamiento de lenguaje natural no generativos combinados con reglas configurables por proyecto; (ii) transcripción local de audios y videos con inteligencia artificial, asistida por mapas de calor de confiabilidad y validación humana obligatoria; y (iii) conectores controlados a modelos de lenguaje (LLMs) que solo permiten el procesamiento de texto previamente anonimizado, curado y validado por una persona humana.

Cada operación queda registrada mediante identificadores únicos, hash, logs de usuario, timestamp, parámetros aplicados y resultados, lo que permite auditoría completa, reconstrucción forense y rendición de cuentas institucional. La arquitectura implementa un esquema de gobernanza embebida por roles (administradores, operadores y auditores), que colabora a prevenir el uso indebido de datos personales y previene la exposición de información sensible a plataformas externas de IA.

Adecuación de la candidatura al objeto del premio

La candidatura se encuadra plenamente en el objeto del Premio de Privacidad y Protección de Datos en Iberoamérica al constituir una herramienta práctica, con arquitectura técnica y gobernanza institucional, orientada a fortalecer la protección de datos y la cultura de privacidad en contextos reales de uso de inteligencia artificial.

Privacy AI Studio responde a uno de los principales riesgos contemporáneos en Iberoamérica: el fenómeno del *Shadow AI*, es decir, el uso no autorizado y no gobernado de plataformas de IA generativa por parte de equipos que procesan documentos, audios o bases de datos con información personal sin contar con garantías legales, técnicas ni éticas. La plataforma ofrece una alternativa institucional que permite innovar con IA sin exponer derechos fundamentales ni generar incumplimientos normativos.

El diseño se alinea con los marcos regulatorios de protección de datos (como la Ley 25.326 de Argentina y principios del RGPD) y con los estándares internacionales de la Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial (2021), incorporando por diseño principios de privacidad, proporcionalidad, supervisión humana significativa, gobernanza y rendición de cuentas.

Contribución a la difusión de la protección de datos entre los ciudadanos

Privacy AI Studio contribuye de forma directa y verificable a la difusión y efectividad de la protección de datos en Iberoamérica en dos dimensiones complementarias.

En el plano operativo, la plataforma reduce hasta un 80 % el tiempo destinado a tareas de anonimización manual y permite que equipos de trabajo puedan utilizar IA generativa sin exponer datos personales, al habilitar el acceso a modelos únicamente sobre texto previamente anonimizado, curado y validado. Esto habilita una adopción segura y masiva de IA en organizaciones que antes se veían obligadas a prohibirla o a usarla informalmente, con alto riesgo de fuga de información.

En el plano institucional y cultural, la plataforma materializa el principio de privacidad por diseño y por defecto, trasladando la protección de datos desde el plano de las políticas declarativas al de las reglas técnicas ejecutables. De este modo, promueve una cultura organizacional en la que la protección de los derechos de las personas no depende del comportamiento individual, sino de una arquitectura que previene errores, registra cada acción y habilita la auditoría continua.