Maestría en

Protección de

Trabajo de investigación previo a la obtención del título de

Magíster en Protección de Datos

AUTORES:

Arellano Lara Leonardo Oliver

González Tapia Jhony Onofre

Guamán Gavilanes Edgar Francisco

Hallo Manosalvas Marcelo Nicolás

Jiménez Jiménez Gilson Alexander

Román López Iván Rafael

TUTORES:

Profesor PBL1: Humberto Ortiz Rodríguez

Profesor PBL2: Camila Valdez González

Profesor PBL3: Jacqueline Guerrero Carrera

"Privacidad desde el diseño y por defecto: aplicación al uso de biometría en el escenario de una entidad educativa"

Quito, junio 2026

Certificación de autoría

Nosotros, **Arellano Lara Leonardo Oliver; González Tapia Jhony Onofre; Guamán Gavilanes Edgar Francisco; Hallo Manosalvas Marcelo Nicolás; Jiménez Jiménez Gilson Alexander; Román López Iván Rafael,** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Leonardo Oliver Arellano Lara
Time Stamping Security Data

Firma del graduando

Arellano Lara Leonardo Oliver

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JHONY ONOFRE GONZALEZ TAPIA

Firma del graduando

González Tapia Jhony Onofre

EDGAR FRANCISCO GUAMAN GAVILANES
Firmado digitalmente por EDGAR FRANCISCO GUAMAN GAVILANES
Fecha: 2026.07.05 22:18:27 -05'00'

Firma del graduando

Guamán Gavilanes Edgar Francisco

MARCELO NICOLÁS HALLO MANOSALVAS
Firmado digitalmente por MARCELO NICOLÁS HALLO MANOSALVAS
Fecha: 2026.07.05 19:16:21 -05'00'

Firma del graduando

Hallo Manosalvas Marcelo Nicolás

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
GILSON ALEXANDER JIMENEZ JIMENEZ

Firma del graduando

Jiménez Jiménez Gilson Alexander

Ivan Rafael Roman Lopez
Firmado digitalmente por Ivan Rafael Roman Lopez
Fecha: 2026.07.05 20:41:49 -06'00'

Firma del graduando

Román López Iván Rafael

Autorización de Derechos de Propiedad Intelectual

Nosotros, **Arellano Lara Leonardo Oliver; González Tapia Jhony Onofre; Guamán Gavilanes Edgar Francisco; Hallo Manosalvas Marcelo Nicolás; Jiménez Jiménez Gilson Alexander; Román López Iván Rafael**, en calidad de autores del trabajo de investigación titulado "***Privacidad desde el diseño y por defecto: aplicación del uso de biometría en el escenario de una entidad de*** **educativa"**, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes del Código Orgánico de la Economía Social del Conocimiento, la Creatividad y la Innovación.

D. M. Quito, junio 2026.

Leonardo Oliver Arellano Lara
Time Stamping Security Data

Firma del graduando

Arellano Lara Leonardo Oliver

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JHONY ONOFRE GONZALEZ TAPIA

Firma del graduando

González Tapia Jhony Onofre

EDGAR FRANCISCO GUAMAN GAVILANES
Firmado digitalmente por EDGAR FRANCISCO GUAMAN GAVILANES
Fecha: 2026.07.05 22:19:00 -05'00'

Firma del graduando

Guamán Gavilanes Edgar Francisco

MARCELO NICOLÁS HALLO MANOSALVAS
Firmado digitalmente por MARCELO NICOLÁS HALLO MANOSALVAS
Fecha: 2026.07.05 19:16:44 -05'00'

Firma del graduando

Hallo Manosalvas Marcelo Nicolás

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
GILSON ALEXANDER JIMENEZ JIMENEZ

Firma del graduando

Jiménez Jiménez Gilson Alexander

Ivan Rafael Roman Lopez
Firmado digitalmente por Ivan Rafael Roman Lopez
Fecha: 2026.07.05 20:41:25 -06'00'

Firma del graduando

Román López Iván Rafael

Aprobación de dirección y coordinación del programa

Nosotros, **Nombre del Director/a de la Maestría en Protección de Datos y Jacqueline Guerrero Carrera, Coordinadora UIDE,** declaramos que los graduandos: **Arellano Lara Leonardo Oliver; González Tapia Jhony Onofre; Guamán Gavilanes Edgar Francisco; Hallo Manosalvas Marcelo Nicolás; Jiménez Jiménez Gilson Alexander; Román López Iván Rafael,** son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ELSA JACQUELINE GUERRERO CARRERA

_____

Director/a de la
Maestría en Protección de Datos

Jacqueline Guerrero

Coordinadora de la

Maestría en Protección de Datos

DEDICATORIA

Leonardo A.

A V., mi verso más hermoso y mi historia favorita, con quien tejo, hilo a hilo, la trama de cada sueño. Y a mi hijo, la página más luminosa que la vida ha escrito en mí.

Jhony G.

E T y A G., raíz firme de cuanto soy y ejemplo de cuanto aspiro a ser, por enseñarme con su vida el valor del esfuerzo, la honestidad y la perseverancia; a mis hermanos, compañeros de historia, cómplices de recuerdos y apoyo constante en cada etapa de mi camino; y a mi familia, por ser el refugio donde nacieron mis sueños y la fuerza que me impulsó a perseguirlos.

Edgar G.

A mi familia, raíz firme de cada paso y por ser el refugio constante en cada desafío. A quienes, respaldado mis sueños, mis desvelos y mis metas, convirtiéndose en el puntal y soporte silencioso detrás de cada logro.

Gilson J.

A mis padres, por ser mi pilar fundamental, mi refugio cuando la vida se pone cuesta arriba, y por su eterno amor incondicional y perseverancia conmigo, y por ser el brillo de mis ojos.

Marcelo H.

A mis padres, por su amor incondicional y su esfuerzo silencioso, por enseñarme con el ejemplo el valor de la perseverancia y por creer en mí aun cuando el camino parecía incierto. Cada página de este trabajo lleva la huella de su entrega.

Iván R.

A mi familia, por ser mi apoyo constante y principal motivación para salir adelante.

AGRADECIMIENTOS

Leonardo A.

A mi hijo, por el amor que me da sentido y por la complicidad con la que acompaña cada esfuerzo, incluso los que aún no comprende: este trabajo también es suyo. A mi padre, ejemplo de integridad, trabajo y palabra cumplida; gracias por enseñarme a sostener el rumbo cuando el camino se hace cuesta. A mi madre, fortaleza incansable y raíz de cuanto soy; gracias por enseñarme que el amor también es coraje.

A V., amor mío y refugio, por elegirme cada día y dejarse elegir, por hacer que todo lo bueno de este camino tenga el calor de tu nombre.

Jhony G.

A mis padres, por ser el origen de cada uno de mis logros. Gracias por enseñarme, con su ejemplo, que el esfuerzo, la honestidad y la perseverancia son el camino para alcanzar los sueños. Su apoyo incondicional, sus consejos y su confianza en mí fueron la fuerza que me sostuvo en los momentos de incertidumbre y el impulso que me permitió llegar hasta aquí. A mis hermanos, por acompañarme con cariño, paciencia y comprensión durante este proceso. Gracias por celebrar mis avances, por alentarme en las dificultades y por recordarme siempre que ningún desafío es imposible cuando se enfrenta con determinación.

Edgar G.

A mis padres, por enseñarme con su ejemplo el valor del esfuerzo, la disciplina y la perseverancia. Todo logro encuentra su origen en las oportunidades, principios y enseñanzas que me han brindado a lo largo de la vida.

Gilson J.

A mi familia, por todos y cada uno de sus consejos que han marcado mi forma de pensar, y así poder formarme y ser el proyecto de ser humano que quiero ser. Agradezco a Dios por permitirme gozar de esta etapa y poder terminarla. Por último, agradezco a mi enamorada E. C., por ser mi amada compañera y ser mi primer rayo de sol en mis días de oscuridad.

Marcelo H.

Expreso mi más profundo y sincero agradecimiento a MM y CV, quienes han sido mis mentores a lo largo de este camino. Su guía constante, al compartir conocimiento y experiencia han sido pilares fundamentales en el desarrollo de este trabajo y en mi formación académica y profesional.

Gracias por confiar en mí, por exigirme siempre lo mejor y por acompañarme en cada etapa de este proceso. Su orientación no solo dio forma a estas páginas, sino que dejó en mí una enseñanza que perdurará mucho más allá de ellas.

Iván R.

A Dios por darme fortaleza y sabiduría para alcanzar mis metas. A mis padres, por todo su apoyo y amor incondicional. A mi esposa, por creer en mí y darme ánimo para superar las adversidades.

Finalmente, agradezco a mis profesores y compañeros por compartir sus conocimientos y guiarme en este proceso.

RESUMEN

El presente trabajo analiza la viabilidad jurídica del tratamiento de datos biométricos faciales de estudiantes menores de edad mediante un sistema de reconocimiento facial con inteligencia artificial, provisto por BioTrust S. A. como encargado, para el control de asistencia en la Unidad Educativa Particular Andes del Sur, responsable del tratamiento.

El estudio se enmarca en el régimen ecuatoriano de protección de datos personales, integrado por la Constitución de la República, la Ley Orgánica de Protección de Datos Personales (LOPDP), Reglamento General (RGLOPDP) y la normativa secundaria de la Superintendencia de Protección de Datos Personales (SPDP).

El objetivo general consiste en determinar si dicho tratamiento puede sostenerse jurídica y operativamente antes de cualquier despliegue; la metodología articula tres instrumentos: una evaluación normativa del caso, una ponderación de derechos conforme al test de proporcionalidad y una evaluación de impacto a la protección de datos sustentada en un análisis de riesgos.

La ponderación demuestra que la medida, aun siendo idónea, no supera los exámenes de necesidad ni de proporcionalidad en sentido estricto, pues existen alternativas equivalentes menos intrusivas y la afectación grave de derechos reforzados de los menores no se compensa con un beneficio ordinario de eficiencia.

La evaluación de impacto confirma que, aun aplicando la totalidad de los controles propuestos, el riesgo residual permanece inaceptable y de naturaleza estructural, concentrado en las dimensiones de privacidad y gobernanza. Se concluye que el proyecto no es jurídicamente viable en su configuración actual (No Go) y que solo podría reabrirse mediante una reconfiguración integral que acredite necesidad estricta, alternativa no biométrica operativa, consentimiento libre y salvaguardas reforzadas.

Palabras clave: protección de datos personales, biometría facial, interés superior del niño, ponderación de derechos, evaluación de impacto.

ABSTRACT

This study analyzes the legal feasibility of processing the facial biometric data of minor students through an artificial intelligence–based facial recognition system provided by BioTrust S.A., acting as the data processor, for attendance monitoring purposes at Unidad Educativa Particular Andes del Sur, acting as the data controller.

The analysis is framed within the Ecuadorian personal data protection regime, which comprises the Constitution of the Republic, the Organic Law on Personal Data Protection (LOPDP), the General Regulation to the LOPDP (RGLOPDP), and the secondary regulations issued by the Superintendence for Personal Data Protection (SPDP).

The general objective is to determine whether such processing can be legally and operationally justified prior to any implementation. The methodology combines three instruments: a normative assessment of the case, a balancing of rights based on the proportionality test, and a data protection impact assessment supported by a risk analysis.

The balancing exercise demonstrates that, although the measure is suitable for achieving its intended purpose, it does not satisfy the requirements of necessity or proportionality in the strict sense, since there are equally effective but less intrusive alternatives, and the significant impact on the enhanced rights of minors is not outweighed by an ordinary efficiency benefit.

The impact assessment confirms that, even with the full implementation of the proposed safeguards, the residual risk remains unacceptable and structural in nature, particularly in the areas of privacy and governance. The study concludes that the project is not legally viable in its current configuration (No Go) and could only be reconsidered through a comprehensive redesign demonstrating strict necessity, the absence of a feasible non-biometric alternative, freely given consent, and strengthened safeguards.

Keywords: personal data protection, facial biometrics, best interests of the child, balancing of rights, data protection impact assessment.

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

CAPITULO I

1. INTRODUCCION

El reconocimiento facial con inteligencia artificial se ha incorporado con rapidez a entornos cotidianos, incluido el ámbito escolar, donde se ofrece como solución para el control de asistencia; el presente trabajo examina, desde el derecho ecuatoriano de protección de datos personales, un caso concreto: la evaluación, por parte de la Unidad Educativa Particular Andes del Sur, de un sistema biométrico facial provisto por BioTrust S. A. para registrar la asistencia diaria de estudiantes menores de edad. La institución actúa como responsable del tratamiento y el proveedor como encargado, sobre una arquitectura en nube híbrida con identificación uno a muchos.

El problema central no es de novedad tecnológica, sino de licitud: determinar si el tratamiento de datos biométricos sensibles de niñas, niños y adolescentes puede sostenerse bajo el marco constitucional vigente, la Ley Orgánica de Protección de Datos Personales (LOPDP), Reglamento General (RGLOPDP) y la normativa secundaria de la Superintendencia de Protección de Datos Personales (SPDP); la concurrencia de datos sensibles, titulares en especial vulnerabilidad, decisiones automatizadas y escala masiva sitúa el caso en el régimen más exigente del ordenamiento.

El objetivo general del trabajo es determinar la viabilidad jurídica del tratamiento antes de cualquier despliegue, contrastando finalidad, necesidad y proporcionalidad, valorando alternativas menos intrusivas y exigiendo una evaluación de impacto previa.

La tesis sostenida, coherente a lo largo de los entregables del Proyecto Integrador, es de no viabilidad (No Go) del proyecto en su configuración actual.

Para fundamentarla, el documento articula tres instrumentos complementarios: una evaluación normativa del caso, un análisis de riesgos y de gobernanza; y, en el Capítulo IV, una ponderación de derechos conforme al test de proporcionalidad, una evaluación de impacto a la protección de datos y el dictamen final de viabilidad con recomendaciones.

El Capítulo I delimita el marco metodológico y conceptual; el Capítulo V recoge las conclusiones; y los anexos consolidan las matrices e instrumentos operativos que sustentan el análisis.

2. MARCO METODOLÓGICO

2.1 Presentación y planteamiento del problema

La Unidad Educativa Particular evalúa la implementación de un sistema biométrico de reconocimiento facial con inteligencia artificial, provisto por BioTrust S.A., para el control de asistencia diaria de estudiantes menores de edad; el responsable del tratamiento es la institución educativa; el encargado, en los términos de los artículos 34 y 35 de la Ley Orgánica de Protección de Datos Personales (en adelante, LOPDP) (Ley Orgánica de Protección de Datos Personales, 2021), es BioTrust S.A.

La arquitectura propuesta opera en nube híbrida con identificación uno a muchos, motor de inteligencia artificial con detección de vida, soporte remoto del proveedor y posible intervención de subencargados para respaldo, monitoreo y mantenimiento del modelo, el flujo del tratamiento no se reduce a una captura puntual: comprende habilitación del servicio, obtención del consentimiento del representante legal, enrolamiento biométrico, generación de plantilla facial, captura diaria, verificación automatizada uno a muchos, registro de asistencia con efecto disciplinario, almacenamiento centralizado, respaldos, atención de derechos, gestión de incidentes y eventual eliminación.

Por su configuración, biometría facial sobre niñas, niños y adolescentes, modalidad uno a muchos, decisiones automatizadas con efectos sobre derechos del titular, intervención de inteligencia artificial y dependencia operativa de un encargado tecnológico, el caso configura un tratamiento de alto impacto sujeto al estándar reforzado del ordenamiento ecuatoriano; la Ley Orgánica de Protección de Datos Personales clasifica el dato biométrico como sensible, y los datos de menores como categoría especial; esta doble acumulación normativa impone al responsable la carga probatoria más exigente del sistema (Oficio N.º SPDP-IRD-2025-0262-O, 2025); a esto, se suma la regulación específica para sistemas de inteligencia artificial contenida en la Resolución N.º SPDP-SPD-2026-0009-R, expedida el 12 de febrero de 2026, cuyo artículo 1 alcanza a quienes desarrollen, entrenen, implementen, desplieguen o provean sistemas de inteligencia artificial que traten datos de titulares ecuatorianos, con independencia de la ubicación del sistema (Resolución N.º SPDP-SPD-2026-0009-R, 2026).

El problema no es de novedad tecnológica, es, fundamentalmente, un problema de demostrabilidad jurídica, entonces la pregunta institucional pertinente no consiste en si la biometría funciona o si automatiza el proceso de asistencia; la pregunta consiste en si el responsable puede sostener jurídicamente esa decisión con evidencia trazable, controles suficientes y gobernanza madura, ese es el examen que esta investigación se propone realizar sobre el caso concreto, articulando tres planos de análisis que reproducen el ciclo de cumplimiento previsto por la propia normativa: la fijación del estándar normativo aplicable, la identificación y valoración de riesgos derivados de las brechas frente a ese estándar; y, el diseño de la respuesta operativa frente a incidentes y vulneraciones cuando los controles preventivos no logren neutralizar el riesgo residual.

2.1.1 Antecedentes.

El régimen ecuatoriano de protección de datos personales atravesó una fase de consolidación intensa entre 2021 y 2026, la Ley Orgánica de Protección de Datos Personales se publicó en el Quinto Suplemento del Registro Oficial número 459, de 26 de mayo de 2021 (Ley Orgánica de Protección de Datos Personales, 2021); el Reglamento General fue expedido mediante Decreto Ejecutivo número 904 y publicado en el Tercer Suplemento del Registro Oficial número 435, de 13 de noviembre de 2023 (Reglamento General a la LOPDP, 2023); posteriormente, la Superintendencia de Protección de Datos Personales densificó este marco con un cuerpo de resoluciones que conviene retener por su relevancia directa para el caso: la Guía de Gestión de Riesgos y Evaluación de Impacto, aprobada por la Resolución N.º SPDP-SPD-2025-0003-R (Resolución N.º SPDP-SPD-2025-0003-R, 2025) y actualizada en su Versión 2 durante 2026 (Guía de gestión de riesgos y evaluación de impacto, versión 2 [SPDP], 2026); el Reglamento del Delegado de Protección de Datos Personales, contenido en la Resolución N.º SPDP-SPD-2025-0028-R, cuyo artículo 10 amplía expresamente los supuestos de designación obligatoria al sector educativo (Resolución N.º SPDP-SPD-2025-0028-R, 2025); y, de manera central para el caso, la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial, contenida en la Resolución N.º SPDP-SPD-2026-0009-R (Resolución N.º SPDP-SPD-2026-0009-R, 2026).

La Resolución N.º SPDP-SPD-2026-0009-R, expedida el 12 de febrero de 2026, constituye la pieza regulatoria de mayor incidencia sobre el caso; su artículo 4, inciso segundo, garantiza al titular, en todo momento, el derecho a no ser objeto de decisiones basadas única o parcialmente en valoraciones automatizadas, junto con los derechos de información y oposición, su artículo 5 impone, con carácter obligatorio para responsables y encargados, deberes específicos de transparencia reforzada sobre el

carácter automatizado del tratamiento, gestión de riesgos y evaluación de impacto previas, medidas de seguridad proporcionales al estado de la técnica, inclusión del tratamiento en el Registro de Actividades de Tratamiento y auditoría del funcionamiento del sistema en función del nivel de riesgo, el artículo 6 exige evaluación de impacto previa al desarrollo del sistema siempre que haya tratamiento de datos personales. Su artículo 7, numeral 1, obliga a registrar en el Registro de Actividades de Tratamiento las decisiones automatizadas que generen impactos jurídicos o que afecten derechos y libertades del titular, el artículo 8 sujeta el incumplimiento al régimen sancionatorio de la Ley Orgánica de Protección de Datos Personales; y, su artículo 10 reconoce a la autoridad de control la potestad expresa de auditar sistemas de inteligencia artificial y adoptar medidas correctivas o cautelares (Resolución N.º SPDP-SPD-2026-0009-R, 2026).

Junto a la normativa positiva se ha consolidado una doctrina administrativa sancionatoria que fija parámetros interpretativos exigibles, los casos FAN ID, vinculado a LIGAPRO (Resolución N.º RES-SPDP-ICS-2025-0005, 2025), y FANFEF, vinculado a la Federación Ecuatoriana de Fútbol (Resolución N.º RES-SPDP-ICS-2025-0006, 2025), constituyen los pronunciamientos más significativos en materia de tratamiento biométrico, en FAN ID, la autoridad determinó infracción por no aplicar de correctamente los principios de protección de datos desde el diseño y por defecto, particularmente en la determinación de finalidades legítimas y delimitadas y en la minimización del tratamiento biométrico, en FANFEF, la autoridad calificó como conceptualmente defectuosa una evaluación de impacto que concluía en riesgo residual cero, por carecer de la metodología funcionalmente idónea que la normativa exige; ambos pronunciamientos resultan directamente aplicables al caso: la lógica argumental que la autoridad utilizó para sancionar a LIGAPRO y a la Federación Ecuatoriana de Fútbol es la misma que aplicaría, con mayor rigor por tratarse

de menores, a un colegio que desplegara biometría facial sin evaluación de impacto previa y sin arquitectura de minimización demostrable.

A la dimensión jurídica se suma la dimensión técnica internacional, la norma ISO/IEC 24745 sobre protección de plantillas biométricas (International Organization for Standardization [ISO], 2022a) y la norma ISO/IEC 42001 sobre sistemas de gestión de inteligencia artificial (ISO, 2023b) fijan controles específicos que la institución debe demostrar haber considerado; los marcos del NIST, Privacy Framework (National Institute of Standards and Technology [NIST], 2020) y AI Risk Management Framework (NIST, 2023), ofrecen estructuras de gestión de riesgos algorítmicos.

Son el reconocimiento facial aplicado a menores, la literatura especializada ha documentado tasas de error desiguales según fototipo, edad y desarrollo morfológico (Grother et al., 2019; Jain et al., 2016), lo que vuelve crítica la auditoría de sesgos del motor algorítmico cuando los titulares son niñas, niños y adolescentes en crecimiento.

Se ha documentado exhaustivamente este horizonte, fijando el estándar mínimo acumulativo aplicable, articulando los bloques constitucional, legal, reglamentario y secundario; identificando veintiséis riesgos concretos del tratamiento, distribuidos en cuatro dimensiones: privacidad, seguridad de la información, discriminación y sesgos algorítmicos, y gobernanza, valorados sobre una matriz bidimensional probabilidad por impacto (5x5) alineada con la norma ISO/IEC 27005 (ISO, 2022b) y con la Guía de la SPDP, y arrojó un riesgo residual de un crítico, seis altos, once medios y ocho bajos, aun aplicando la totalidad de los controles propuestos; además, se diseñó el Plan de Respuesta ante Incidentes de Seguridad relacionados con datos biométricos procesados por sistemas de inteligencia artificial, con tipología de incidentes T1 a T10, criterios objetivos de severidad, árbol de decisión sobre notificación,

siete fases operativas y anexos modelo (acta de incidente, notificación al representante legal, oficio a la SPDP y bitácora forense). Esta investigación toma como base ese cuerpo documental y lo eleva a la condición de tesis académica.

2.1.2. Delimitación del problema.

La delimitación del problema se construye sobre cinco ejes que precisan el alcance de la investigación, en cuanto al objeto, el estudio analiza la viabilidad jurídica del sistema biométrico de reconocimiento facial con inteligencia artificial provisto por BioTrust S.A. para el control de asistencia diaria de estudiantes menores de edad en la Unidad Educativa Particular, considerando la arquitectura uno a muchos sobre nube híbrida y la operación continua del tratamiento durante el período lectivo; dejando fuera del objeto los usos biométricos en contextos no educativos, los tratamientos no biométricos de información estudiantil y las aplicaciones que el mismo proveedor pueda ofrecer en otros sectores.

En cuanto al sujeto, el análisis se concentra en la Unidad Educativa Particular como responsable y en BioTrust S.A. como encargado especializado del cual depende la operación técnica del sistema, la perspectiva del estudiante menor se asume desde la titularidad reforzada que el ordenamiento le reconoce y desde el principio del interés superior del niño, la perspectiva del representante legal se analiza en cuanto presta consentimiento sustitutivo, sin que ello agote la cuestión sobre la validez material del mismo conforme al artículo 20 del Reglamento General a la Ley Orgánica de Protección de Datos Personales (en adelante, RGLOPDP) (2023).

En cuanto al espacio, la investigación se circunscribe al ordenamiento ecuatoriano, las referencias comparadas al Reglamento (UE) 2016/679, a las directrices del Comité Europeo de Protección de Datos sobre tratamiento biométrico (European Data Protection Board [EDPB], 2020) y a estándares técnicos

internacionales: ISO/IEC 27001, 27002, 27005, 27035, 27701, 24745 y 42001, junto con NIST Privacy Framework y NIST AI Risk Management Framework, operan como apoyo doctrinal y técnico sin desplazar al derecho ecuatoriano vigente.

En cuanto al tiempo, el corpus normativo considerado abarca la Constitución de la República del Ecuador (2008), la Ley Orgánica de Protección de Datos Personales (2021), el Reglamento General (2023) y la totalidad de la normativa secundaria expedida por la Superintendencia hasta el cierre de la presente investigación, con énfasis en las resoluciones SPDP-SPD-2025-0003-R sobre gestión de riesgos y su Versión 2 de 2026, SPDP-SPD-2025-0028-R sobre delegado de protección de datos, SPDP-SPD-2026-0005-R sobre tratamientos a gran escala y SPDP-SPD-2026-0009-R sobre sistemas de inteligencia artificial; las resoluciones sancionatorias FAN ID y FANFEF, dictadas en 2025, integran la doctrina administrativa que la investigación invoca.

En cuanto al enfoque, el trabajo se construye desde una perspectiva jurídico-dogmática complementada con análisis técnico-organizacional; se trata de un estudio de caso instrumental que utiliza el expediente Unidad Educativa-BioTrust como vehículo para iluminar problemas regulatorios más amplios sobre biometría, inteligencia artificial, neuroderechos; y, protección reforzada de menores, la orientación metodológica general es deductiva: parte del marco constitucional, desciende a la regulación secundaria y a la doctrina administrativa, y culmina en la aplicación al caso; la orientación específica articula tres líneas que reproducen el ciclo norma-riesgo-respuesta documentada en los tres entregables previos: análisis jurídico del estándar normativo aplicable, identificación y valoración de riesgos con metodología bidimensional probabilidad por impacto, y diseño operativo de respuesta ante incidentes y vulneraciones.

Los límites probatorios deben enunciarse con claridad, el expediente disponible no acredita de forma cerrada la ubicación completa de la infraestructura del proveedor, el mapa exhaustivo de subencargados ni la eliminación verificable de la totalidad de copias y respaldos; tampoco constan, en la documentación de trabajo, la identificación nominal definitiva del Delegado de Protección de Datos y del Comité Interno, los canales formales de reporte habilitados ni el contrato vigente con BioTrust S.A. con cláusulas de encargo, transferencia y subencargo, las conclusiones sobre transferencias internacionales, supresión integral y control pleno de terceros se formulan, por tanto, con la cautela que el principio de responsabilidad probatoria exige.

2.2. Justificación

La pertinencia de esta investigación se sostiene en cuatro dimensiones articuladas: doctrinal, metodológica, práctica y ética. Se desarrollan en ese orden, sin pretender agotar cada una, sino mostrando por qué su confluencia justifica el esfuerzo académico.

En el plano doctrinal, el trabajo se ubica en una zona de frontera del derecho ecuatoriano de protección de datos: la convergencia entre biometría, inteligencia artificial, neuroderechos, decisiones automatizadas y protección reforzada de niñas, niños y adolescentes; la doctrina nacional ha tratado estos elementos de manera fragmentaria y hay desarrollos sobre datos sensibles, sobre consentimiento, sobre delegado de protección de datos y sobre evaluación de impacto, pero pocas obras los integran como sistema.

El caso analizado, ofrece la oportunidad de hacerlo, porque exige que la respuesta jurídica articule simultáneamente los principios del artículo 10 de la LOPDP, la doble acumulación de los artículos 25 y 26 sobre categorías especiales y datos sensibles, la protección reforzada de menores de los artículos 21 de la

ley y 19 y 20 del Reglamento, los deberes del artículo 37 sobre seguridad apropiada al estado de la técnica, el principio de privacidad desde el diseño del artículo 39, los deberes específicos sobre inteligencia artificial de la Norma General SPDP-SPD-2026-0009-R, y la incorporación progresiva de los neuroderechos en el debate regulatorio comparado.

En el plano metodológico, la investigación articula una cadena de trazabilidad funcional entre estándar normativo, identificación de riesgos y respuesta operativa, que reproduce la lógica que la propia Superintendencia utiliza en sus pronunciamientos sancionatorios, esta cadena se materializa en tres productos complementarios: Primero, un análisis jurídico que fija el estándar exigible al tratamiento. Segundo, una matriz integral de riesgos con veintiséis riesgos nominados, distribuidos en cuatro dimensiones, privacidad, seguridad de la información, discriminación y sesgos, gobernanza, valorados mediante metodología bidimensional probabilidad por impacto sobre escala 5x5, con clasificación de controles según naturaleza preventiva, detectiva, correctiva o disuasoria y cálculo de riesgo residual conforme a la Guía de la SPDP en su Versión 2 (Guía de gestión de riesgos y evaluación de impacto, versión 2 [SPDP], 2026). Tercero, una arquitectura de respuesta operativa que incluye plan ante incidentes con tipología T1 a T10, criterios objetivos de severidad, árbol de decisión sobre notificación a la autoridad y al titular, siete fases secuenciales, matriz RACI específica de incidentes y anexos modelo. La trazabilidad entre estos tres productos es lo que permite que la investigación resista escrutinio académico y, eventualmente, escrutinio administrativo.

La investigación también clarifica una distinción metodológica que la práctica institucional suele confundir: el análisis de riesgos en protección de datos personales no es un análisis de seguridad de la información; aunque comparten lenguaje y herramientas, su objeto tutelar es distinto, la gestión de

riesgos en LOPDP centra el análisis en los derechos y libertades del titular; la gestión de riesgos en seguridad de la información lo centra en los activos de la organización. Esta diferencia condiciona los criterios de severidad y la decisión sobre notificación de vulneraciones, la distinción entre evento, alerta, incidente y vulneración, desarrollada a partir de la ISO/IEC 27035 (ISO, 2023a) y aplicada al caso, tampoco es semántica: produce consecuencias jurídicas concretas sobre los deberes de notificación a la autoridad y al titular.

En el plano práctico, la investigación tiene utilidad inmediata para tres tipos de actores: las instituciones educativas ecuatorianas que evalúen desplegar tecnologías biométricas dispondrán de un modelo de análisis aplicable, con preguntas verificables y criterios de decisión explícitos, los profesionales del derecho que asesoren a responsables y encargados encontrarán un mapa de obligaciones articulado con la doctrina administrativa más reciente, los delegados de protección de datos del sector educativo, cuya designación obligatoria precisó la Resolución N.º SPDP-SPD-2025-0028-R en su artículo 10, contarán con una referencia técnico-jurídica para construir sus propios análisis de riesgos, sus evaluaciones de impacto y sus pronunciamientos internos.

Las autoridades de control encontrarán, también, un caso documentado de aplicación práctica de la Resolución SPDP-SPD-2026-0009-R, recientemente expedida y aún de jurisprudencia administrativa incipiente.

En el plano ético, el trabajo se sostiene en una convicción que conviene declarar sin rodeos: la innovación tecnológica en entornos educativos no puede construirse a costa del interés superior del niño, cuando una institución decide tratar biometría de menores mediante sistemas algorítmicos, no opera en un mercado neutral de servicios; opera sobre derechos fundamentales de personas cuya autonomía

jurídica aún se está formando, y cuya identidad biométrica los acompañará durante toda la vida. La tutela de esa autonomía exige preguntas que la práctica institucional muchas veces evita: ¿se eligió la biometría porque es estrictamente necesaria, o porque resulta cómoda? ¿Existe alternativa equivalente menos intrusiva? ¿Se garantizó la voluntariedad material del consentimiento, más allá de la firma del representante en el contrato de matrícula? ¿Se previó el riesgo de estigmatización por errores algorítmicos sobre menores en pleno crecimiento morfológico? ¿Se protegió la dimensión emergente de los neuroderechos cuando el sistema pueda producir inferencias sobre estados emocionales o conductuales? Estas preguntas articulan la justificación última del estudio.

2.3. Problemas jurídicos

La complejidad del caso impide reducir el problema jurídico a una pregunta única. El análisis se organiza, en consecuencia, sobre tres problemas jurídicos generales, alineados con los capítulos de la memoria y los análisis realizados del caso, que fijan el eje de viabilidad, conveniencia y aceptabilidad del riesgo; y, a partir de ellos, sobre cinco preguntas conductoras que precisan dimensiones específicas del expediente Unidad Educativa-BioTrust y orientan el desarrollo de los capítulos posteriores.

2.3.1. Problemas jurídicos generales.

¿Es jurídicamente viable la implementación de un sistema de biometría en la organización educativa, conforme a la normativa de protección de datos personales y a los principios de licitud, necesidad, proporcionalidad y minimización?

¿Resulta recomendable el uso de biometría en la organización educativa desde una perspectiva de protección de datos y derechos fundamentales, considerando los riesgos inherentes, la irreversibilidad del dato biométrico y la existencia de alternativas menos intrusivas?

¿Permite la Evaluación de Impacto en la Protección de Datos justificar que el riesgo residual del uso de biometría es aceptable y controlable, o corresponde recomendar su no implementación o su uso condicionado?

2.3.2. Preguntas conductoras del análisis.

¿Puede la Unidad Educativa Particular sostener jurídicamente, bajo el marco constitucional vigente, Ley Orgánica de Protección de Datos Personales, Reglamento General; el tratamiento de datos biométricos faciales de estudiantes menores de edad mediante un sistema con identificación uno a muchos y motor de inteligencia artificial, para fines de control de asistencia escolar, cuando existen alternativas no biométricas equivalentes como tarjetas RFID, ¿códigos QR o procedimiento manual?

¿Constituye el consentimiento del representante legal, obtenido en el contexto de matrícula escolar, una base de licitud suficiente para el tratamiento biométrico de menores, considerando la asimetría estructural entre institución y familia, la falta acreditada de alternativa equivalente al día uno del despliegue y la cláusula de invalidez por menoscabo del interés superior del niño contenida en el artículo 20 del Reglamento General a la LOPDP?

¿Qué efectos jurídicos produce, sobre la viabilidad del tratamiento, la aplicación concurrente de la Resolución N.º SPDP-SPD-2026-0009-R sobre sistemas de inteligencia artificial, particularmente sus artículos: 4, 5, 6, 7 y 10, a un proceso de decisión automatizada con efecto disciplinario, ejecutado sobre menores, sin evaluación de impacto previa favorable, ¿sin auditoría documentada de sesgos algorítmicos del motor de BioTrust S.A. y sin supervisión humana significativa institucionalizada?

¿Permite la matriz integral de riesgos del caso, evaluada con metodología bidimensional probabilidad por impacto y aplicando la totalidad de los controles propuestos, sostener materialmente

que el riesgo residual del despliegue es aceptable, cuando subsisten un riesgo residual crítico y seis riesgos altos, distribuidos en las dimensiones de privacidad, seguridad de la información, discriminación-sesgos y gobernanza institucional?

¿Qué consecuencias regulatorias, en términos de medidas correctivas y régimen sancionatorio del Título IX de la LOPDP, se derivarían de un despliegue que no acredite necesidad estricta, proporcionalidad sustantiva, privacidad desde el diseño, evaluación de impacto previa favorable, contrato de encargo robusto con BioTrust S.A. con prohibición expresa de uso secundario, no entrenamiento de modelos y obligaciones de notificación de incidentes en plazo cierto?

2.4. Objetivos

2.4.1. Objetivo general.

Determinar la viabilidad jurídica del tratamiento de datos biométricos faciales de estudiantes menores de edad mediante el sistema provisto por BioTrust S.A. para el control de asistencia en la Unidad Educativa Particular, articulando estándar normativo, identificación de riesgos y respuesta operativa conforme al ciclo de cumplimiento previsto por la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la normativa secundaria de la Superintendencia de Protección de Datos Personales, con énfasis en la Resolución N.º SPDP-SPD-2026-0009-R sobre sistemas de inteligencia artificial, para formular una conclusión fundamentada sobre la viabilidad, la inviabilidad o la viabilidad condicionada del proyecto y elaborar recomendaciones operativas conforme al principio de privacidad desde el diseño y por defecto.

2.4.2. Objetivos específicos.

Para alcanzar el objetivo general, la investigación se desarrolla a través de seis líneas específicas de trabajo, articuladas entre sí y trazables hacia los productos finales del estudio:

1. Analizar el marco normativo aplicable al tratamiento biométrico de menores en el Ecuador, identificando las bases de licitud admisibles conforme al artículo 26 de la Ley Orgánica de Protección de Datos Personales, las exigencias reforzadas del artículo 21 de la ley y de los artículos 19 y 20 del Reglamento General, y los desarrollos contenidos en la normativa secundaria de la Superintendencia de Protección de Datos Personales, con énfasis en la Norma General sobre sistemas de inteligencia artificial.

2. Examinar las implicaciones jurídicas del uso de inteligencia artificial en el sistema biométrico, en particular las exigencias derivadas de la Resolución N.º SPDP-SPD-2026-0009-R sobre transparencia reforzada, evaluación de impacto previa al desarrollo, supervisión humana significativa, gestión documentada de sesgos algorítmicos, inclusión de las decisiones automatizadas en el Registro de Actividades de Tratamiento y auditoría del sistema en función del nivel de riesgo.

3. Construir una matriz integral de riesgos del tratamiento mediante metodología bidimensional probabilidad por impacto sobre escala 5x5, alineada con la norma ISO/IEC 27005 y con la Guía de Gestión de Riesgos y Evaluación de Impacto de la Superintendencia en su Versión 2, identificando riesgos en cuatro dimensiones -privacidad, seguridad de la información, discriminación y sesgos algorítmicos, gobernanza institucional-, clasificando controles según su naturaleza preventiva, detectiva, correctiva o disuasoria, y calculando el riesgo residual posterior a la implementación de los controles propuestos.

4. Diferenciar metodológicamente, sobre la base de la ISO/IEC 27035 y la doctrina administrativa de la Superintendencia, las categorías de evento, alerta, incidente y vulneración aplicadas al tratamiento

biométrico, precisando las consecuencias jurídicas concretas que cada categoría produce sobre los deberes de notificación a la autoridad de control y a los titulares afectados conforme a los artículos 43 y 46 de la LOPDP y 24 a 28 del Reglamento General.

5. Diseñar la arquitectura de respuesta operativa ante incidentes y vulneraciones de seguridad relacionados con datos biométricos procesados por sistemas de inteligencia artificial, incluyendo tipología de incidentes, criterios objetivos de severidad, árbol de decisión sobre notificación, fases secuenciales de detección, contención, calificación, notificación, remediación y aprendizaje organizacional, matriz de roles y responsabilidades específica de incidentes y modelos anexos de acta de incidente, oficio a la Superintendencia, comunicación al representante legal y bitácora forense de evidencia.

6. Identificar y ponderar los impactos del tratamiento sobre los derechos fundamentales involucrados: privacidad, protección de datos personales, no discriminación, autodeterminación informativa, libertad cognitiva y la dimensión emergente de los neuroderechos cuando concurran inferencias sobre estados emocionales o conductuales, integrando la perspectiva del interés superior del niño y la doctrina administrativa de la Superintendencia derivada de los casos FAN ID y FANFEF, para formular recomendaciones operativas aplicables al expediente concreto y proyectables a tratamientos análogos en el sector educativo ecuatoriano.

3. Fundamentos Teóricos

3.1. Privacidad y protección de datos personales: una visión global, regional y local

Quien estudia hoy la protección de datos personales se enfrenta a una paradoja útil: privacidad y protección de datos suelen usarse como sinónimos; y, sin embargo, son posiciones jurídicas distintas; la privacidad, en su tradición liberal, protege la esfera de reserva del sujeto frente a la mirada ajena; opera

por sustracción; y, la protección de datos, en cambio, atribuye al titular un haz de facultades activas sobre la información que lo identifica o lo hace identificable: decidir sobre su recolección, su uso, su circulación, su conservación y su eventual reutilización.

La doctrina alemana fijó esta segunda dimensión bajo el nombre de autodeterminación informativa y la jurisprudencia constitucional comparada la ha consolidado como derecho autónomo (Pérez Luño, 2014).

Esta diferenciación es importante ya que mueve el eje del análisis, cuando el dato circula sin control, no se afecta solamente la intimidad: se afectan, en cascada, la igualdad, la libertad económica, el debido proceso administrativo, el acceso a servicios públicos y en última instancia, la dignidad humana; de ahí que autores como Mayer-Schönberger y Cukier (2013) sostengan que la protección de datos opera como un derecho puente, indispensable para sostener el ejercicio de otros derechos en entornos masivamente automatizados; el paradigma del secreto, propio de los códigos civiles decimonónicos, ha sido sustituido por un paradigma de gobernanza del dato, donde lo decisivo ya no es impedir el acceso, sino regular el ciclo entero del tratamiento.

En el plano global, el Reglamento (UE) 2016/679, conocido como Reglamento General de Protección de Datos (en adelante, RGPD), consolidó este giro y se convirtió en estándar de referencia para los ordenamientos convergentes y su influencia es clara en América Latina, aunque con matices: la región avanza a velocidades distintas y conserva, según Remolina Angarita (2020), una tensión estructural entre digitalización acelerada y madurez institucional desigual. Ecuador, Brasil, Chile, Argentina, Colombia, México, Perú y Uruguay configuran un mosaico regulatorio donde conviven autoridades de control consolidadas y otras en proceso de implementación.

La protección reforzada de grupos vulnerables como: pueblos indígenas, niñas, niños y adolescentes, personas con discapacidad, trabajadores informales, constituye, en este contexto, uno de los rasgos diferenciales de la regulación latinoamericana, combinando amplias brechas de alfabetización digital con expansión rápida de tecnologías de vigilancia, lo que vuelve indispensable que el régimen de protección de datos cumpla, además de su función reguladora, una función correctiva de asimetrías.

En Ecuador, el marco se articula sobre tres niveles: la Constitución de la República del Ecuador (2008) reconoce el derecho a la protección de datos personales en el artículo 66, numeral 19, y consagra la acción de hábeas data en el artículo 92 como garantía jurisdiccional específica; la Ley Orgánica de Protección de Datos Personales (2021) desarrolla este derecho con un marco material que incluye principios, bases de licitud, derechos del titular, deberes del responsable y del encargado, régimen sancionatorio y autoridad de control independiente; y, el Reglamento General a la Ley Orgánica de Protección de Datos Personales (2023) precisa las reglas operativas: consentimiento, tratamiento de menores, transferencias, evaluación de impacto, registro de actividades, vulneraciones de seguridad y protección desde el diseño.

A este marco se suma, con creciente densidad, la normativa secundaria expedida por la Superintendencia de Protección de Datos Personales (en adelante, SPDP); solo entre 2024 y 2026, la autoridad de control ha emitido resoluciones sobre delegados de protección de datos (Resoluciones N.º SPDP-SPD-2025-0004-R y N.º SPDP-SPD-2025-0028-R, 2025), gestión de riesgos y evaluación de impacto (Resolución N.º SPDP-SPD-2025-0003-R, 2025), cláusulas contractuales obligatorias (Resolución N.º SPDP-SPD-2025-0006-R, 2025), seudonimización y anonimización (Resolución N.º SPDP-SPD-2025-0030-R, 2025), interés legítimo (Resolución N.º SPDP-SPD-2025-0041-R, 2025), transferencias internacionales

(Resolución N.º SPDP-SPD-2026-0004-R, 2026), tratamientos a gran escala (Resolución N.º SPDP-SPD-2026-0005-R, 2026) y sistemas de inteligencia artificial (Resolución N.º SPDP-SPD-2026-0009-R, 2026), entre otras; lo relevante de este corpus es que no se limita a desarrollar la ley, la complementa con criterios técnicos exigibles, lo que eleva el estándar de cumplimiento más allá del mero acatamiento formal.

Es fundamental, precisar que el modelo ecuatoriano no opera bajo lógica de prohibición-autorización binaria; opera, más bien, bajo una lógica de legalidad material: cada tratamiento debe poder justificarse, en cada momento, como necesario, proporcionado, transparente y seguro, sobre evidencia verificable; lo que se sanciona no es la innovación, sino la innovación que el responsable no puede sostener probatoriamente y esta diferencia, aparentemente sutil, separa el cumplimiento aparente del cumplimiento efectivo.

3.2. Desafíos de la privacidad y protección de datos personales en el Ecuador

Si se mira el estado actual del régimen ecuatoriano sin retórica, la conclusión es incómoda: el problema ya no es la ausencia de normas, La Ley Orgánica de Protección de Datos Personales (Ley Orgánica de Protección de Datos Personales, 2021), el Reglamento General (Reglamento General a la LOPDP, 2023) y la normativa secundaria de la SPDP componen, en conjunto, un marco alineado con los estándares internacionales más exigentes; y, la distancia entre norma y práctica, es lo que explica los hallazgos sancionatorios recientes.

El primer desafío es cultural, numerosas instituciones, tanto públicas como privadas, siguen entendiendo el cumplimiento como ejercicio documental; redactar una política, publicar un aviso, recolectar firmas en formularios; sin embargo, falta la mirada sistémica que el régimen exige, la SPDP lo ha

dicho con claridad en su doctrina sancionatoria: la responsabilidad proactiva no se acredita con declaraciones, sino con evidencia técnica y documental que demuestre que las medidas adoptadas son efectivas, proporcionadas al riesgo y revisadas continuamente (Resolución N.º RES-SPDP-ICS-2025-0006, 2025); el cumplimiento de papel, el que se redacta pero no se ejecuta, no es tolerable.

El segundo desafío es la asimetría tecnológica, donde el responsable adopta decisiones jurídicas sobre arquitecturas que no controla, como: infraestructuras en la nube administradas por terceros, motores algorítmicos entrenados con datasets opacos, servicios de soporte remoto con privilegios elevados, esquemas de respaldo cuya geografía no siempre se documenta; sin una gobernanza efectiva sobre encargados y subencargados, el deber de seguridad apropiada al estado de la técnica (Ley Orgánica de Protección de Datos Personales, 2021, art. 37) se convierte en una promesa de difícil verificación; y, esta brecha, lejos de ser anecdótica, atraviesa al sector público, al sistema financiero, a la salud y como veremos en el caso BioTrust, al ámbito educativo.

El tercer desafío es la profesionalización, donde la figura del delegado de protección de datos, regulada por la SPDP mediante la Resolución N.º SPDP-SPD-2025-0028-R (Resolución N.º SPDP-SPD-2025-0028-R, 2025), exige no solo designación nominal, sino independencia funcional, recursos suficientes y posición orgánica adecuada; además, el artículo 10 de esa resolución amplía expresamente los supuestos de designación obligatoria al sector educativo (inicial, básica y bachillerato, en todas las modalidades) y a cualquier actividad que conlleve tratamiento de datos de categorías especiales de menores; siendo, la consecuencia operativa directa, un colegio que trate datos biométricos de estudiantes está obligado a contar con un delegado funcional, no con un correo electrónico que figure en una política.

El cuarto desafío atañe a los tratamientos de alta sensibilidad, como: biometría, salud, datos de menores, videovigilancia masiva, decisiones automatizadas; en estos escenarios, el cumplimiento formal es insuficiente y la autoridad de control ha sido especialmente exigente con las evaluaciones de impacto que arrojan un riesgo residual de cero, calificándolas como conceptualmente defectuosas porque, como bien razona la Resolución N.º RES-SPDP-ICS-2025-0006 (Resolución N.º RES-SPDP-ICS-2025-0006, 2025), toda operación de tratamiento implica, por su propia naturaleza, una exposición residual a amenazas técnicas, organizativas, humanas o jurídicas y sostener lo contrario equivale a renunciar al enfoque basado en riesgos.

Finalmente, un quinto desafío que merece tratamiento separado: la protección reforzada de niñas, niños y adolescentes, el artículo 21 de la LOPDP prohíbe el tratamiento de datos sensibles y de datos de menores salvo autorización expresa del titular o del representante legal; o, cuando concurra un interés público esencial evaluado conforme a estándares internacionales de derechos humanos y a criterios de legalidad, proporcionalidad y necesidad; El Reglamento, en su artículo 19, exige consentimiento del representante para menores de quince años y consentimiento expreso para datos sensibles o decisiones basadas en valoraciones automatizadas; y, sobre todo, su artículo 20 introduce una cláusula de validez material, el consentimiento será inválido si menoscaba el interés superior del niño, esta cláusula no admite lectura simbólica, aplica como control sustantivo sobre la firma del representante.

Cuando estos cinco desafíos confluyen en un mismo proyecto; y, el sistema BioTrust es, en esto, un caso paradigmático, el escenario regulatorio se vuelve denso; la pregunta deja de ser si el proyecto es técnicamente viable y pasa a ser si el responsable puede sostenerlo, en sede administrativa o judicial, con

evidencia trazable y esa es la prueba que el régimen ecuatoriano impone hoy a cualquier institución que pretenda tratar datos biométricos de menores en entornos educativos.

3.3. Evolución tecnológica y protección de datos: el papel de la IA en el tratamiento de datos personales

La discusión sobre inteligencia artificial y datos personales suele plantearse como una cuestión de novedad tecnológica y no es una forma viable de entenderla, lo que la inteligencia artificial introduce no es una técnica inédita, el aprendizaje automático tiene décadas, como un cambio de escala, opacidad e intensidad inferencial; mientras los sistemas tradicionales procesaban datos declarados por el titular, los sistemas algorítmicos contemporáneos infieren información que el titular nunca entregó, estados emocionales a partir de microexpresiones, riesgos crediticios a partir de patrones de geolocalización, probabilidades de deserción escolar a partir de huellas digitales aparentemente inofensivas; el dato observado pierde protagonismo frente al dato inferido (Wachter & Mittelstadt, 2019).

Este desplazamiento tiene consecuencias jurídicas concretas, la transparencia, entendida en clave tradicional como deber de informar lo que se hace con el dato, resulta insuficiente cuando el sistema produce inferencias que el propio responsable no anticipó; la minimización, entendida como deber de tratar solo los datos necesarios, se complica cuando el modelo necesita una gran cantidad de información para aprender patrones útiles, la proporcionalidad, entendida como adecuación medio-fin, debe reevaluarse cuando el medio es un sistema cuya lógica interna no es plenamente explicable; la seguridad, finalmente, adquiere una dimensión nueva, el vicio de datos de entrenamiento, los ataques adversariales y el robo de modelos no estaban en el horizonte regulatorio hace una década.

El ordenamiento ecuatoriano ha empezado a responder a este reto; la SPDP expidió, mediante la Resolución N.º SPDP-SPD-2026-0009-R, la Norma General para la Garantía del Derecho de Protección de

Datos Personales en el Uso de Sistemas de Inteligencia Artificial (Resolución N.º SPDP-SPD-2026-0009-R, 2026), su artículo 1 establece que la norma se aplica a responsables y encargados que desarrollen, entrenen, implementen, desplieguen o provean sistemas de inteligencia artificial que traten datos personales de titulares ecuatorianos, con independencia de la ubicación del sistema o del proveedor y la cláusula territorial es relevante, alcanza al proveedor extranjero que ofrezca servicios a una institución ecuatoriana, lo que cierra el espacio para el argumento del foro favorable.

El artículo 5 de la misma norma fija deberes específicos, donde, el responsable debe informar al titular sobre el carácter automatizado del tratamiento, realizar gestión de riesgos y evaluación de impacto previas, implementar medidas de seguridad apropiadas al estado de la técnica, incluir las decisiones automatizadas en el Registro de Actividades de Tratamiento y auditar el funcionamiento del sistema en función del nivel de riesgo; el artículo 7, por su parte, exige que las decisiones automatizadas con efectos jurídicos o impacto significativo en derechos y libertades de los titulares figuren expresamente en el registro y estos deberes no son recomendaciones, son obligaciones cuya inobservancia activa el régimen sancionatorio.

A la norma sobre inteligencia artificial se suma la Norma General sobre el Tratamiento de Datos Personales a Gran Escala (Resolución N.º SPDP-SPD-2026-0005-R, 2026); esta resolución introduce un modelo de calificación cuantitativa, el Modelo de Tratamiento de Gran Escala, en adelante MTGE, que pondera seis variables: número de titulares, volumen de datos, categorías tratadas, frecuencia, permanencia y alcance geográfico.

El umbral de calificación se fija en seis puntos, calculados sobre una expresión matemática expresamente definida en su artículo 9, la presencia simultánea de categorías especiales, frecuencia

continua o periódica y permanencia prolongada (rasgos típicos de un sistema biométrico escolar), suele acercar el tratamiento al umbral, con las consecuencias regulatorias que ello supone: medidas de seguridad reforzadas, evaluación de impacto obligatoria y mayor exigencia probatoria.

En el plano internacional, marcos como el NIST Privacy Framework (NIST, 2020) y el NIST AI Risk Management Framework (NIST, 2023) ofrecen estructuras de gobierno y categorización de riesgos algorítmicos que sirven, sin desplazar al derecho ecuatoriano, como herramientas auxiliares de trazabilidad, las familias normativas de la ISO/IEC: 27001, 27002, 27005, 27035, 27701, 23894, cumplen función equivalente, a las que se ha sumado más recientemente la ISO/IEC 42001 sobre sistemas de gestión de inteligencia artificial.

La doctrina administrativa local ha sido cuidadosa con esta articulación; la Versión 2 de la Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales, publicada en 2026 (Guía de gestión de riesgos y evaluación de impacto, versión 2 [SPDP], 2026), amplió el catálogo de estándares orientativos respecto de su Versión 1, incorporando expresamente la ISO/IEC 42001 para gobernanza algorítmica y el marco DAMA-DMBOK para gobernanza y gestión de datos; y, actualizó la declaración de aplicabilidad de privacidad a la ISO/IEC 27701:2025; la misma guía, sin embargo, mantiene una advertencia que conviene transcribir literalmente:

Hay que tomar en cuenta que conformarse a estándares de mejores prácticas es útil, pero no garantiza la conformidad a la LOPDP; se trata más bien de guías para la implementación de proyectos de seguridad de la información, de privacidad y taxonomías de controles de riesgos, no abarcan la conformidad jurídica directa con la LOPDP, no proveen el insumo de datos necesarios para la gestión de riesgos, no proveen métricas para protección de datos personales, ni tampoco proveen modelos de

riesgos de protección de datos personales adaptados a contextos específicos. (Guía de gestión de riesgos y evaluación de impacto, versión 2 [SPDP], 2026, p. 6).

La advertencia merece subrayarse; una certificación ISO no exime de la EIPD; un conjunto de controles según NIST no sustituye al juicio de proporcionalidad que la ley exige al responsable; la Versión 2 de la Guía profundiza, además, en métodos cuantitativos de calibración del riesgo, el modelo FAIR, el Valor al Riesgo en sus variantes Cy-VaR y Pd-VaR, el análisis de Monte Carlo, la predicción conformal; los presenta como herramientas para construir rationales verificables, no como sustituto del análisis jurídico y la consecuencia operativa es clara: la conformidad técnica aporta orden y trazabilidad; la conformidad jurídica exige, además, juicio sobre la licitud, la necesidad y la proporcionalidad material del tratamiento.

3.4. Biometría: aproximación conceptual y jurídica

Definir biometría no es difícil; calificarla jurídicamente sí lo es; en sentido técnico, la biometría agrupa al conjunto de métodos que permiten identificar o autenticar a una persona a partir de rasgos físicos, fisiológicos o conductuales: huella dactilar, geometría facial, iris, voz, dinámica de tecleo, marcha.

La definición legal ecuatoriana es coincidente, la LOPDP describe el dato biométrico como “dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos” (Ley Orgánica de Protección de Datos Personales, 2021, art. 4).

Lo distintivo del dato biométrico no es la sofisticación del método, sino dos atributos materiales del rasgo: la intensidad identificatoria y la permanencia relativa; el rostro, la huella o el patrón vascular acompañan al sujeto a lo largo de su vida; no se cambian con la facilidad de una contraseña ni se sustituyen con la sencillez de una credencial; cuando una contraseña se filtra, el usuario la rota; cuando

una plantilla biométrica se compromete, el daño es estructural y en muchos casos, irreversible (Jain et al., 2016).

Esta asimetría entre riesgo y capacidad de remediación es la que explica que la mayoría de los ordenamientos contemporáneos, el ecuatoriano entre ellos, hayan colocado al dato biométrico en la categoría más protegida del sistema.

La LOPDP es explícita, clasifica los datos biométricos dentro de los datos sensibles, sujetos al régimen prohibitivo general del artículo 26, con causales taxativas de excepción (Ley Orgánica de Protección de Datos Personales, 2021); cuando el tratamiento recae adicionalmente sobre niñas, niños o adolescentes, que el artículo 25 califica como categoría especial, la protección se acumula: dato sensible por la naturaleza biométrica del rasgo y categoría especial por la condición del titular; entonces, el resultado es un estándar reforzado en grado máximo, donde el responsable enfrenta la carga probatoria más exigente del sistema.

La doctrina administrativa lo ha confirmado en sede consultiva, en el Oficio N.º SPDP-IRD-2025-0262-O, la Intendencia de Resolución de Denuncias sostuvo que en todo tratamiento de datos personales especiales de naturaleza biométrica resulta obligatorio cumplir los principios de la LOPDP, contar con base de legitimación, realizar análisis de riesgos y evaluación de impacto e implementar medidas de seguridad de naturaleza tecnológica, organizativa, administrativa, jurídica y física que garanticen integridad, disponibilidad y confidencialidad, con rigor especial cuando los datos pertenezcan a menores (Oficio N.º SPDP-IRD-2025-0262-O, 2025); el criterio cierra cualquier intento de modulación discrecional, el estándar reforzado opera como mínimo material obligatorio, no como una mera aspiración.

3.4.1. Sistemas biométricos y datos biométricos.

Una distinción que la práctica suele difuminar conviene mantenerla con rigor, sistema biométrico y dato biométrico no son lo mismo; el primero, es un entorno socio-técnico complejo, compuesto por dispositivos de captura, software de procesamiento, algoritmos de comparación, plantillas, bases de datos, reglas de decisión, mecanismos de almacenamiento, interfaces de consulta, políticas de actualización y esquemas de soporte; y, el segundo, es la unidad informacional generada, derivada o procesada dentro de ese sistema.

La consecuencia jurídica es clara, el deber de protección no recae únicamente sobre el dato en abstracto, sino sobre el diseño y la operación del sistema entero, lo que conecta con el principio de protección desde el diseño y por defecto (Ley Orgánica de Protección de Datos Personales, 2021, art. 39).

Funcionalmente, los sistemas biométricos operan en dos modalidades: la autenticación uno a uno compara al titular contra una referencia previamente declarada para confirmar identidad; y, la identificación uno a muchos lo contrasta contra una galería para reconocerlo entre múltiples sujetos; la diferencia parece técnica, pero es jurídicamente decisiva, ya que la modalidad uno a muchos eleva la intensidad del tratamiento, multiplica la probabilidad de falsos positivos y negativos, requiere mantener una base de referencias permanentemente accesible y altera la lógica de la expectativa razonable de privacidad; La Organización Internacional de Normalización, en su norma ISO/IEC 24745 (ISO, 2022a) y el Comité Europeo de Protección de Datos, en sus directrices sobre videovigilancia (EDPB, 2020), coinciden en este punto: la identificación uno a muchos exige justificación reforzada.

Dentro del flujo biométrico es útil estratificar el dato, entendiendo que existen datos fuente: la imagen facial capturada, la huella original; datos transformados: la plantilla, entendida como vector

matemático del rasgo; datos derivados: el resultado de la comparación, el puntaje de similitud, los eventos de coincidencia; y, datos de soporte: logs, metadatos, respaldos, copias técnicas, esta estratificación es vital, porque las medidas jurídicas y técnicas deben aplicarse con criterios diferenciados a cada nivel, la imagen fuente debe eliminarse cuando deja de ser necesaria; la plantilla debe cifrarse y separarse de los datos de identificación; los datos derivados se someten a reglas estrictas de minimización; los datos de soporte requieren políticas coherentes de retención y supresión.

Olvidar esta estratificación lleva a un error frecuente, creer que basta con borrar la fotografía original para satisfacer el derecho de eliminación; empero, no basta, la plantilla persiste, los logs persisten, los respaldos persisten.

3.4.2. Tratamiento de datos biométricos.

El tratamiento de datos biométricos no es ilícito en sí mismo en el ordenamiento ecuatoriano, pero está sometido a un régimen reforzado por dos razones convergentes: primero, porque los datos biométricos son datos sensibles cuya regla general es la prohibición de tratamiento, sujeta a las causales del artículo 26 de la LOPDP (Ley Orgánica de Protección de Datos Personales, 2021); segundo, porque su tratamiento implica, casi por definición, un nivel elevado de identificación, persistencia e irreversibilidad práctica, lo que impone al juicio de licitud un examen sustantivo de necesidad, proporcionalidad, minimización y seguridad.

Las causales del artículo 26 deben aplicarse restrictivamente, el consentimiento explícito para fines específicos y delimitados es admisible, pero su validez depende del cumplimiento del artículo 8 de la LOPDP, que exige una manifestación de voluntad libre, específica, informada e inequívoca; la SPDP ha precisado, en su doctrina consultiva, que la libertad material del consentimiento exige más que la

ausencia de coacción explícita: requiere ausencia de desequilibrio relacional, separación efectiva del consentimiento respecto de la prestación principal y existencia de alternativa equivalente para quien decline (Oficio N.º SPDP-IRD-2025-0262-O, 2025).

Las demás causales del artículo 26, cumplimiento de obligaciones laborales con base legal expresa, intereses vitales, datos manifiestamente públicos, orden judicial, archivo en interés público, investigación o estadística, tratamiento sanitario, operan en escenarios delimitados y no funcionan como cláusulas generales habilitantes en entornos educativos.

Cuando el titular es menor de edad, el régimen se endurece, el artículo 21 de la LOPDP prohíbe el tratamiento salvo autorización expresa o interés público esencial con salvaguardas específicas; el artículo 19 del Reglamento exige consentimiento del representante para menores de quince años y consentimiento expreso si median datos sensibles o decisiones automatizadas; y, el artículo 20 del mismo Reglamento dispone una cláusula que conviene leer detenidamente:

El consentimiento obtenido para el tratamiento de datos personales de un menor de edad, no podrá, bajo ninguna circunstancia, menoscabar el interés superior de la niña, niño o adolescente, conforme a las disposiciones del Código de la Niñez y Adolescencia y demás normativa vigente. De identificarse aquello, el consentimiento obtenido será considerado inválido. (Reglamento General a la LOPDP, 2023, art. 20)

Es decir, la firma del representante no clausura la discusión, el consentimiento puede existir formalmente, sin embargo, ser inválido en sentido material si el tratamiento contraría el interés superior; esta cláusula coloca el control donde debe estar, no en la formalidad documental, sino en la sustancia del derecho.

La consecuencia operativa es contundente, en tratamientos biométricos sobre menores, el consentimiento no funciona como autorización automática, opera como base sometida a un control reforzado de libertad real, necesidad estricta, proporcionalidad sustantiva, alternativa equivalente menos intrusiva y conformidad con el interés superior; la carga de la prueba sobre estos elementos recae sobre el responsable, en virtud del principio de responsabilidad proactiva y demostrada del artículo 10, literal k, de la LOPDP, sin esa prueba, el formulario firmado no salva el tratamiento.

A esta exigencia base, se suman deberes complementarios que el régimen integra como sistema; información previa al titular o representante conforme al artículo 5 del Reglamento; necesidad estricta del medio biométrico, con análisis comparado de alternativas; proporcionalidad sustantiva conforme al artículo 10, literal f, de la LOPDP; minimización del dato y de la operación; conservación acotada con supresión verificable; seguridad apropiada al estado de la técnica conforme al artículo 37; contratos con encargados según los artículos 34 y 35 de la ley y los desarrollos de la SPDP sobre cláusulas obligatorias (Resolución N.º SPDP-SPD-2025-0006-R, 2025); designación obligatoria de delegado de protección de datos en el sector educativo (Resolución N.º SPDP-SPD-2025-0028-R, 2025, art. 10); evaluación de impacto previa conforme a los artículos 29 a 32 del Reglamento, integrada con análisis de riesgos según la Guía aprobada por la SPDP mediante la Resolución N.º SPDP-SPD-2025-0003-R (2025); Registro de Actividades de Tratamiento conforme al artículo 33 del Reglamento; gestión de incidentes y notificación de vulneraciones conforme a los artículos 24 a 28 del mismo cuerpo; y, finalmente, garantías reforzadas frente a decisiones automatizadas cuando el sistema opera mediante inteligencia artificial (Resolución N.º SPDP-SPD-2026-0009-R, 2026); estos elementos no son compartimentos aislados, funcionan como un

sistema cuya coherencia se mide en la capacidad del responsable para acreditarlos ante una eventual auditoría.

La doctrina sancionatoria reciente ha sido especialmente clara en este punto, en el caso del sistema FAN ID, la SPDP determinó que el responsable había incurrido en infracción por no aplicar de forma efectiva principios de protección de datos desde el diseño y por defecto, particularmente en la determinación de finalidades legítimas y delimitadas y minimización del tratamiento biométrico (Resolución N.º RES-SPDP-ICS-2025-0005, 2025), en el caso del aplicativo FANFEF, la autoridad observó que una EIPD que concluye en riesgo residual cero no acredita cumplimiento, sino que evidencia déficit metodológico estructural (Resolución N.º RES-SPDP-ICS-2025-0006, 2025); ambos pronunciamientos fijan parámetros que cualquier proyecto biométrico de hoy debe internalizar: la protección desde el diseño se demuestra en arquitectura, no en políticas redactadas a posteriori; el análisis de riesgos no se valida con conclusiones tranquilizadoras, sino con metodología trazable y umbrales explícitos.

3.5. Privacidad desde el diseño y por defecto

El principio de protección de datos desde el diseño y por defecto suele presentarse como buena práctica; lo cual es errado, ya que en el sistema ecuatoriano constituye un deber jurídico positivo, no una recomendación, la LOPDP lo formula con precisión al definirlo como:

El deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento, para lo cual, implementará las medidas técnicas, organizativas y de cualquier otra índole, con

miras a garantizar el cumplimiento de las obligaciones en materia de protección de datos, en los términos del reglamento. (Ley Orgánica de Protección de Datos Personales, 2021, art. 39)

No hay ambigüedad en el tiempo verbal, la medida es previa, no posterior y la ley no admite que la protección desde el diseño se construya como ejercicio de adecuación a posteriori, una vez ya elegida la arquitectura más intrusiva; exige anticipación, ponderación de riesgos y selección informada de medidas técnicas y organizativas antes del primer tratamiento.

El Reglamento desarrolla el principio en tres disposiciones complementarias: el artículo 58 obliga al responsable a aplicar medidas técnicas, jurídicas, administrativas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento es conforme a la normativa, atendiendo a su naturaleza, ámbito, finalidad y riesgos; el artículo 59 exige establecer estas medidas con carácter previo al tratamiento, considerando los riesgos de diversa probabilidad y gravedad, el estado de la técnica y el coste de aplicación; el artículo 60 cierra el sistema con la regla por defecto: solo deben tratarse los datos cuyo tratamiento sea necesario para la finalidad específica; y, deben adoptarse ajustes técnicos para que esos datos no sean accesibles a un número indefinido de personas de forma automatizada (Reglamento General a la LOPDP, 2023).

La SPDP densificó este deber mediante la Guía de Protección de Datos desde el Diseño y por Defecto, que organiza el principio en estrategias operativas: minimizar, ocultar, separar, abstraer, informar, controlar, cumplir y demostrar (Guía de protección de datos desde el diseño y por defecto [SPDP], 2025); estas estrategias se inspiran en la literatura sobre privacy design strategies (Hoepman, 2018) y se articulan con la arquitectura de cero confianza aplicada a la protección de datos, no son meras categorías

didácticas, traducen el principio en tácticas verificables, con tablas de mapeo entre riesgo, medida, responsable y evidencia; para un tribunal o un auditor, esa trazabilidad es decisiva.

Para fines del presente trabajo, conviene analizar el principio en cinco niveles articulados: primero, en el nivel conceptual, la privacidad desde el diseño y por defecto es la traducción operativa de la responsabilidad proactiva del artículo 10, literal k, de la LOPDP: el responsable no cumple porque lo declare, sino porque puede demostrarlo; segundo, en el nivel normativo, el principio dialoga con la totalidad del catálogo del artículo 10: juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización, proporcionalidad, confidencialidad, calidad, conservación, responsabilidad y con los deberes de seguridad, EIPD, registro y gobernanza de encargados; tercero, en el nivel organizacional, exige delegado de protección de datos funcional e independiente, comité de protección de datos, procesos documentados, separación de funciones y revisión continua; cuarto, en el nivel técnico se traduce en minimización efectiva, procesamiento en el borde cuando es posible, segmentación de red, cifrado robusto en tránsito y en reposo, gestión segura de llaves, supresión verificable, control de acceso por mínimo privilegio, registro de auditoría y trazabilidad de consultas; y, quinto, en el nivel decisional, finalmente, opera como criterio de validez del proyecto, si el diseño descansa sobre recolección intensa, centralización estructural, externalización no controlada y ausencia de evaluación previa, no puede sostenerse que haya sido construido conforme al principio.

La doctrina sancionatoria confirma esta lectura, en el caso FAN ID, la SPDP encontró que la falta de una arquitectura técnica, organizativa y jurídica orientada a restringir el tratamiento a lo estrictamente necesario, junto con la ampliación injustificada de finalidades hacia ámbitos comerciales y operativos, configuraba un incumplimiento sustancial del principio (Resolución N.º RES-SPDP-ICS-2025-0005, 2025); la

calificación formal de la conducta como infracción leve del responsable, conforme al numeral 2 del artículo 67 de la LOPDP, contrasta con la gravedad material del incumplimiento; y, esta paradoja merece atención, la baja calificación formal no debe inducir a error sobre el impacto real, en la práctica, la omisión del principio opera como puerta de entrada a incumplimientos más graves como: déficit de seguridad, mala minimización, EIPD defectuosa, decisiones tecnológicas incompatibles con los derechos del titular; y, la autoridad suele acompañar la sanción con medidas correctivas significativas: suspensión del tratamiento, exigencia de EIPD subsanatoria, adecuación contractual.

En contextos de alta sensibilidad donde el tratamiento biométrico de menores mediante inteligencia artificial lo es por antonomasia, la privacidad desde el diseño y por defecto funciona como criterio de validez material del proyecto, su observancia exige plantearse, antes del despliegue, preguntas que el expediente BioTrust no responde con suficiencia probatoria: ¿Puede alcanzarse el control de asistencia sin biometría? ¿Es posible un diseño descentralizado, con plantillas almacenadas localmente o procesamiento en el borde, que evite la centralización? ¿Pueden eliminarse las imágenes fuente inmediatamente tras generar la plantilla? ¿Existe un mecanismo equivalente no biométrico como: credenciales, códigos, identificadores físicos; disponible sin penalización para quienes lo elijan? ¿Está el proveedor jurídicamente impedido de reutilizar datos para entrenamiento de modelos o mejora del producto?

Cuando estas preguntas no encuentran respuesta trazable, la conclusión jurídica no es discrecional: la arquitectura no satisface el principio; y, dado que el principio opera como mandato previo, su incumplimiento no se subsana retroactivamente. Ninguna política emitida con posterioridad, ningún aviso de privacidad redactado tras la elección del proveedor, ninguna cláusula contractual incorporada

después del despliegue, convierte en compatible con el principio una arquitectura que nació desalineada con él; esto, explica por qué, en el caso analizado, la sola existencia de una política institucional bien construida no basta para sostener la viabilidad jurídica del proyecto, el principio exige incorporación temprana, no formalización tardía.

Se cierra este apartado con una observación que enlaza con los apartados siguientes: la articulación entre privacidad desde el diseño y por defecto, gestión de riesgos, evaluación de impacto, contratos con encargados, gobernanza interna y supresión verificable configura, en el sistema ecuatoriano, es el núcleo operativo de la responsabilidad proactiva y demostrada; estos elementos no son piezas independientes, son partes de un mismo sistema cuya coherencia se mide en la capacidad del responsable para acreditar, ante una eventual auditoría, que la decisión de tratar datos biométricos sensibles de menores fue tomada después de evaluar el riesgo, considerar alternativas, implementar medidas técnicas y organizativas apropiadas al estado de la técnica, asegurar gobernanza efectiva sobre encargados y subencargados, y prever mecanismos verificables de eliminación y cuando esa acreditación no existe, el tratamiento carece de fundamento material suficiente y debe rediseñarse o no ejecutarse.

Sobre esta premisa se construirá, en los capítulos siguientes, el juicio de viabilidad jurídica del sistema biométrico analizado en el caso BioTrust.

CAPITULO II

1. Evaluación normativa

1.1. Requisitos formales para el tratamiento de datos personales en el Ecuador

La evaluación normativa parte de verificar si el tratamiento satisface los requisitos formales que el ordenamiento ecuatoriano exige con carácter previo: la existencia de una base de licitud válida, el cumplimiento del deber de información, la observancia de los principios de finalidad, minimización y proporcionalidad y, tratándose de datos sensibles de menores, el estándar reforzado de los artículos 25 y 26 de la LOPDP y de los artículos 19 y 20 del RGLOPDP; en el caso BioTrust, la base alegada es el consentimiento del representante legal obtenido en el contexto de la matrícula, cuya validez material se examina críticamente en los apartados siguientes y en la ponderación del Capítulo IV.

El detalle de la contrastación requisito por requisito, esto es, la correspondencia entre obligación legal, control, evidencia y responsable, se sistematiza en la matriz normativa consolidada que consta en los anexos de este trabajo, de modo que el cuerpo del capítulo conserva el análisis argumentativo y remite a los instrumentos para el desglose operativo.

2. La necesidad de un inventario de datos

El proyecto de reconocimiento facial para control de asistencia de estudiantes menores de edad no debe aprobarse en su estado actual, este análisis jurídico y el RAT muestran que el colegio actúa como responsable del tratamiento y BioTrust como encargado, dentro de una arquitectura centralizada en nube híbrida, con identificación 1:N, intervención de terceros tecnológicos, posible transferencia internacional y control limitado del colegio sobre infraestructura crítica, respaldos y soporte. Esa configuración eleva el estándar de exigencia jurídica, técnica y organizativa desde el diseño.

La base legal alegada se concentra en el consentimiento explícito del representante legal; sin embargo, dicha base solo sería válida si el consentimiento fuera libre, específico, informado e inequívoco; y, conforme a los arts. 19 y 20 del RGLOPDP, tratándose de menores de quince años, datos sensibles y valoraciones automatizadas, además debe provenir del representante legal y no puede menoscabar el interés superior del niño; en el estado actual del caso, esa base aparece materialmente debilitada por la asimetría propia del entorno escolar, la falta de alternativa equivalente y la ausencia de necesidad estricta demostrada.

Se ha logrado describir un inventario técnico y funcional amplio del tratamiento, dado que el sistema no se reduce a una captura puntual para asistencia, sino que comprende matrícula y consentimiento, enrolamiento biométrico, generación de plantilla facial, identificación 1:N, registro automatizado de asistencia, almacenamiento centralizado, logs, respaldos, soporte remoto, atención de derechos e incidentes. Ese alcance confirma que estamos frente a un tratamiento de alto impacto y no ante una simple operación administrativa.

El RAT fortalece esa lectura porque organiza el tratamiento por actividades, finalidades, base legitimadora alegada, responsables, encargados, conservación, observaciones y riesgos. Además, en los Recursos Técnicos y Riesgos & Recomendaciones se muestra que el inventario fue aterrizado en controles técnicos, brechas de cumplimiento y criterios de evaluación de riesgo, lo cual mejora la trazabilidad del análisis y permite mostrar una representación operativa del ciclo de vida del dato.

No obstante, se evidencia brechas estructurales de cumplimiento, no existe evidencia suficiente de EIPD previa, de contrato de encargo plenamente blindado, de eliminación verificable en respaldos, de alternativa no biométrica equivalente plenamente implementado ni de validación robusta del desempeño

algorítmico en menores, esa situación es jurídicamente relevante porque, según los arts. 38 y 39 del RGLOPDP, el RAT es obligatorio en tratamientos como este; y, de conformidad con el art. 41 del mismo reglamento, la relación entre responsable y encargado debe regirse por contrato escrito.

También subsisten debilidades relevantes en seguridad y gobernanza, el RAT y la hoja de recursos técnicos reflejan avances parciales, pero aún se observan vacíos en MFA, segmentación de red, control sobre llaves, prevención de fuga de datos, anti-tampering, trazabilidad de privilegios y eliminación segura en entornos locales, nube y backups; en un tratamiento biométrico de menores, esas brechas no son accesorias: condicionan la validez práctica del modelo de cumplimiento y la capacidad de respuesta frente a incidentes, solicitudes de derechos o auditorías.

Desde la visión gerencial, el principal hallazgo no es tecnológico, sino de gobernanza y diseño de control, ya que la finalidad de asistencia escolar puede ser legítima, pero el medio escogido resulta altamente intrusivo para una población especialmente protegida, con exposición reputacional, operativa, administrativa y financiera elevada; en consecuencia, la recomendación ejecutiva sigue siendo No Go hasta que la institución pueda demostrar necesidad, proporcionalidad, voluntariedad real, alternativa equivalente, trazabilidad contractual y madurez preventiva suficiente.

En materia sancionatoria, la exposición institucional es relevante, la autoridad puede imponer medidas correctivas para corregir, revertir o eliminar conductas contrarias a la ley, incluyendo el cese del tratamiento, la eliminación de datos y la imposición de medidas técnicas, jurídicas, organizativas o administrativas; además, según considerando las infracciones que ser consideradas graves, la multa que enfrentaría sería la máxima, es decir el 1% del volumen de negocio del ejercicio económico

inmediatamente anterior, según corresponda; por ello, el riesgo no se limita a la multa: también comprende suspensión del tratamiento, adecuación obligatoria y deterioro de confianza institucional.

En síntesis, este análisis y el RAT cumplen una función valiosa de visibilización y orden documental, pero todavía no acreditan una legitimación material suficiente para sostener la viabilidad jurídica del proyecto, se ha logrado describir qué datos trata, cómo circulan, quiénes intervienen y dónde están las brechas; sin embargo, aún no demuestra que el uso de biometría facial para asistencia escolar de menores sea el medio estrictamente necesario, proporcionado y mejor controlado conforme a la LOPDP, al RGLOPDP y a la regulación secundaria aplicable; por esto, la decisión institucional correcta es mantener la no aprobación del proyecto hasta cerrar integralmente el RAT final, la EIPD, los contratos, las medidas de seguridad, la alternativa no biométrica y el esquema de conservación y supresión verificable.

3. Gobernanza de la protección de datos personales

3.1. Políticas, instrucciones de trabajo y flujogramas

3.1.1. Matriz integral de macroprocesos y procesos.

La matriz siguiente mantiene la integralidad del análisis previo, también incorpora base de definición del responsable para distinguir entre dato documentado, supuesto operativo e inferencia técnica razonable. (ANEXO 1)

3.1.2. Flujos de procesos.

Los flujos siguientes son presentados desde lo general a lo particular y mostrando la secuencia operativa y jurídica del caso, cada diagrama muestra entradas, actividades secuenciales, decisiones, puntos de tratamiento de datos, salidas y vínculos con otros procesos y las etiquetas de color azul marcan

actividades con tratamiento o manejo directo de datos; las cajas rojas representan riesgos, excepciones o ramas críticas; los diamantes corresponden a decisiones de proceso.

3.1.2.1. Flujo general.

Resume la arquitectura secuencial del caso: parte de la necesidad institucional, decisión de viabilidad, continúa con la operación escolar y soporte, derechos, incidentes y supresión.

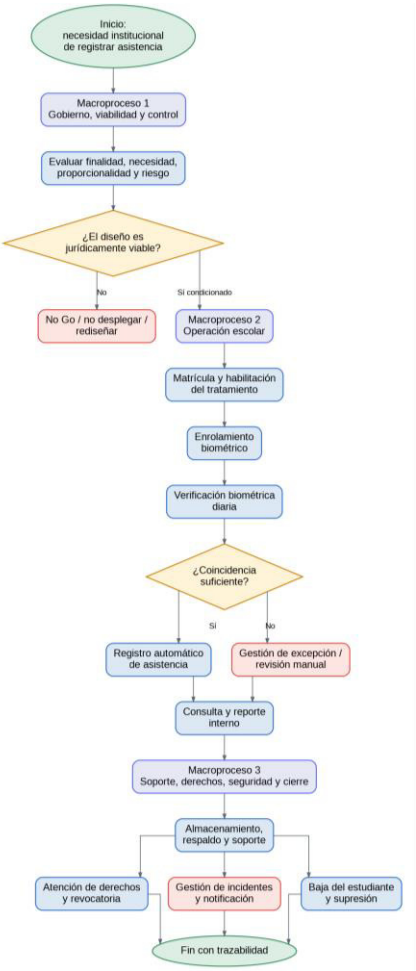

Figura 1

Flujo General

Nota*:* El flujo muestra la necesidad institucional, decisión de viabilidad, operación escolar y soporte, derechos, incidentes y supresión.

3.1.2.2. Flujo específico: evaluación de viabilidad, necesidad y proporcionalidad.

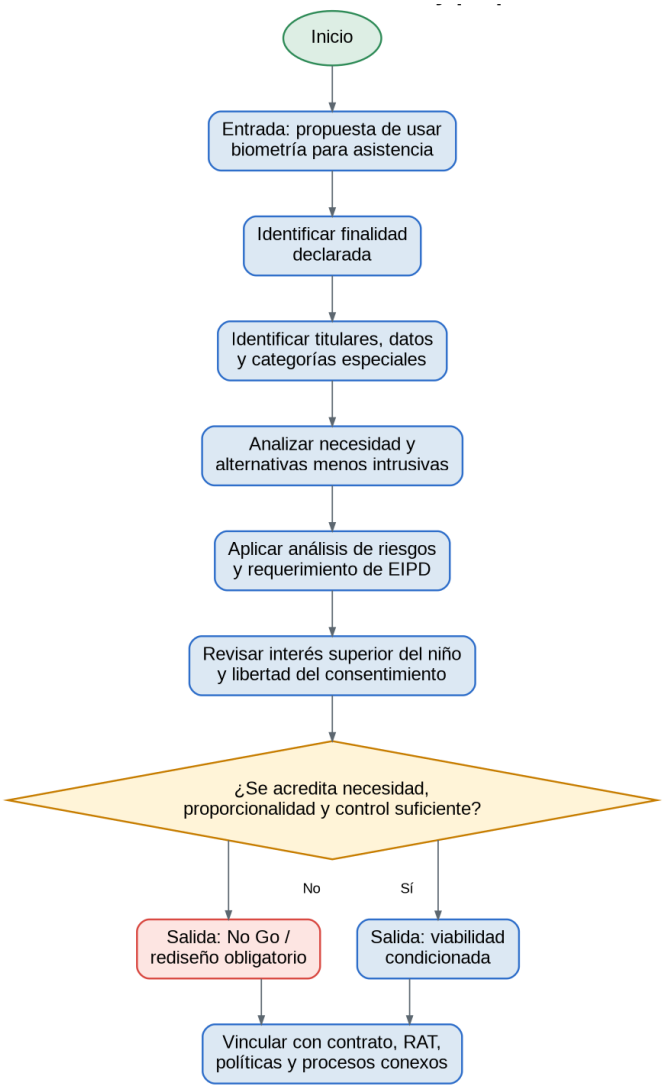

Figura 2

Evaluación de viabilidad, necesidad y proporcionalidad

Nota: Este flujo concentra la etapa estratégica del expediente, ordena la finalidad, el análisis de necesidad, el riesgo, la EIPD y la decisión NoGo o Go condicionado.

3.1.2.3. Flujo específico: gestión contractual y control de terceros.

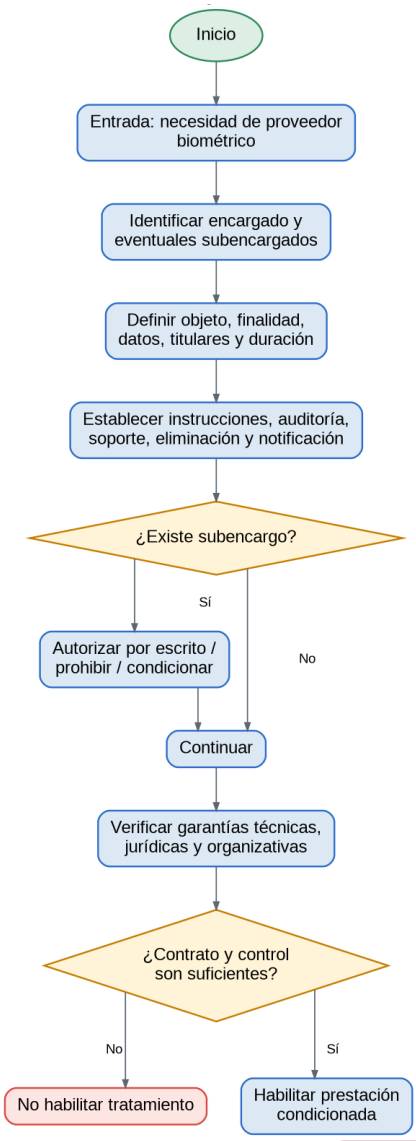

Figura 3

Gestión contractual de terceros

Nota: Control sobre BioTrust y eventuales subencargados; el proceso es crítico porque el caso describe una arquitectura híbrida con soporte y respaldo fuera del control directo del colegio.

3.1.2.4. Flujo específico: matrícula y habilitación del tratamiento biométrico.

La matrícula depende si habilita o no el tratamiento biométrico, en este flujo se separa el servicio educativo de la autorización del tratamiento y de la eventual ruta alternativa no biométrica.

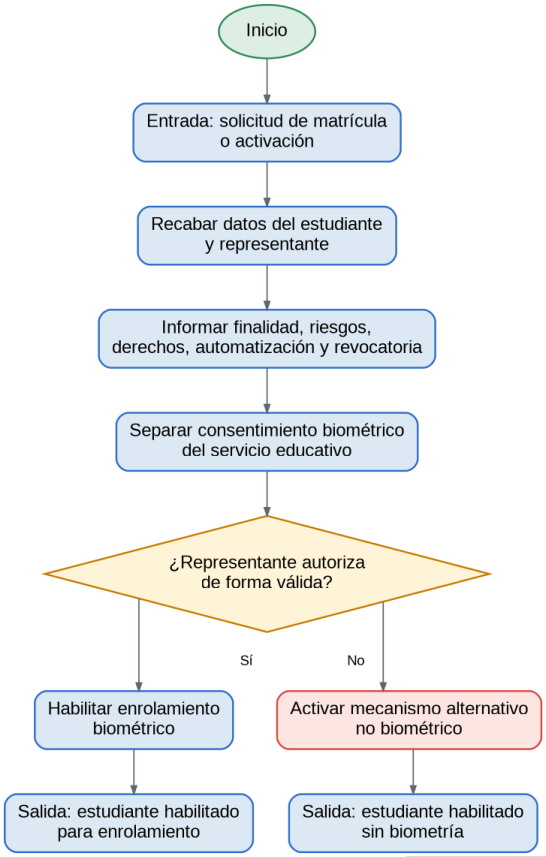

Figura 4

Matrícula y habilitación de biométricos

Nota: El flujo separa el servicio educativo de la autorización del tratamiento y de la eventual ruta alternativa no biométrica.

3.1.2.5. Flujo específico: enrolamiento biométrico del estudiante.

El enrolamiento es la captura inicial en plantilla biométrica y es un punto crítico en la existencia o no de evidencia de eliminación inmediata de imágenes crudas.

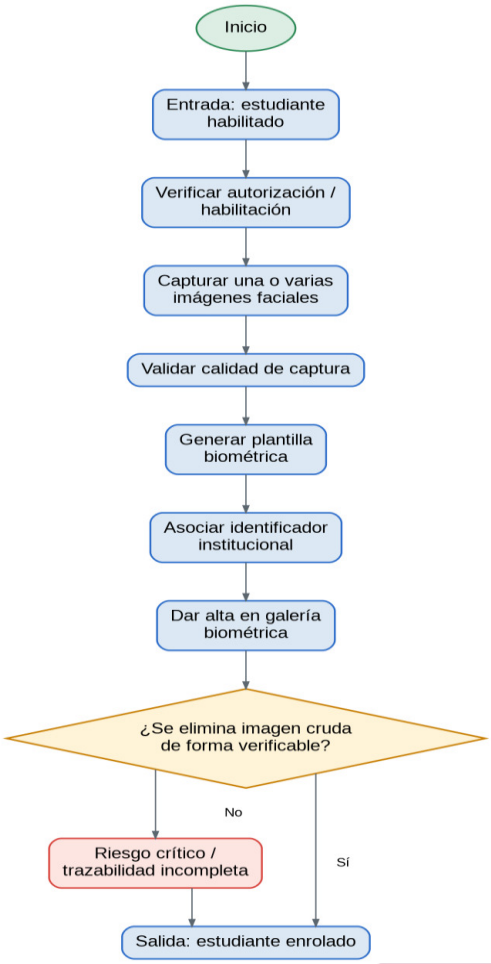

Figura 5

Enrolamiento biométrico del estudiante

Nota: Muestra el enrolamiento es la captura inicial en plantilla biométrica.

3.1.2.6. Flujo específico: verificación biométrica diaria y gestión de excepciones.

La verificación diaria es el parte primordial del funcionamiento, incorpora matching 1:N, eventos de asistencia y una rama de excepción que puede producir efectos relevantes sobre el menor.

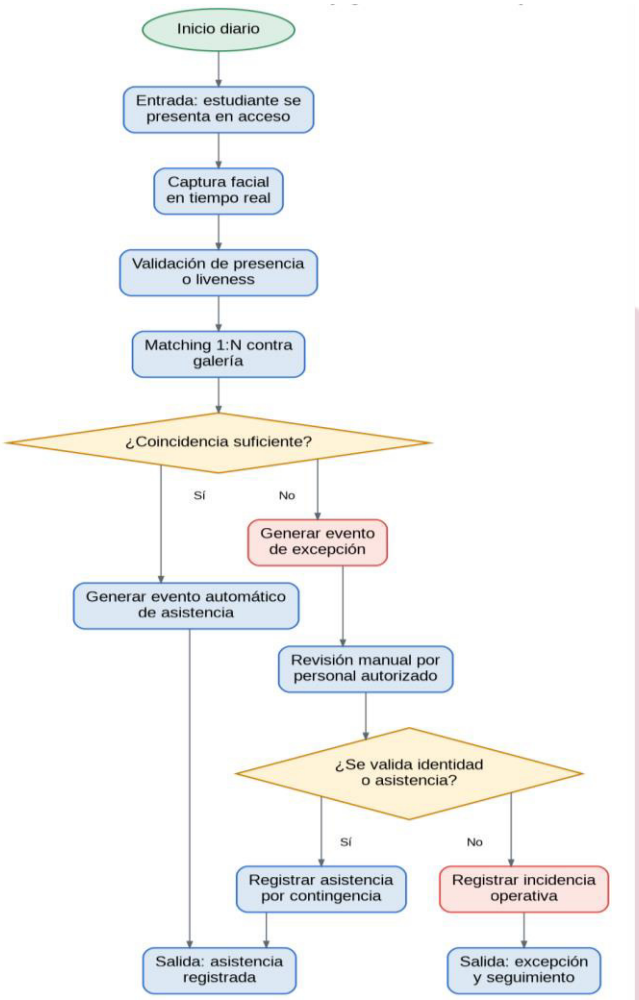

Figura 6

Verificación biométrica diaria y excepciones

Nota: Muestra la verificación diaria, eventos de asistencia y excepciones.

3.1.2.7. Flujo específico: consulta, explotación interna y reporte de asistencia.

El flujo de reporte evita expandir la finalidad, ya que el dato biométrico no termina con la captura; también se usa, consulta, exporta y conserva internamente.

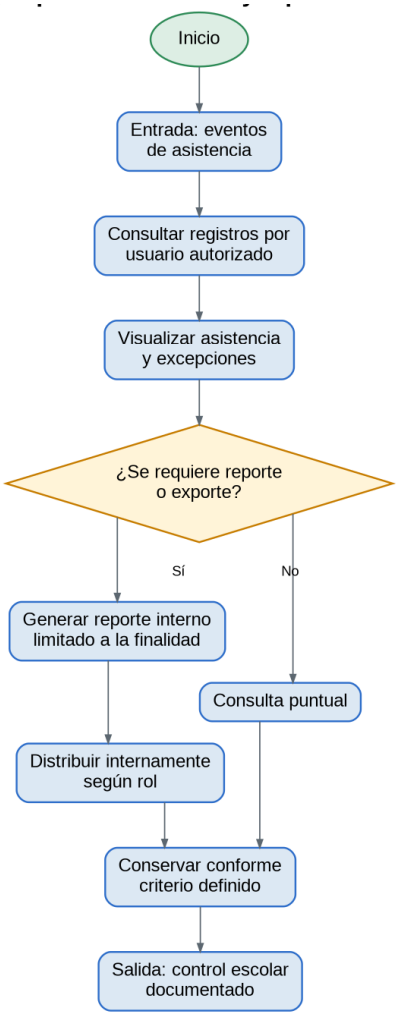

Figura 7

Consulta, exploración interna y asistencia

Nota: Muestra la generación de reportes como consulta, exportación y conserva internamente.

3.1.2.8. Flujo específico: almacenamiento, custodia, respaldo y soporte técnico

Este proceso muestra dónde y cómo persisten plantillas, eventos, logs y respaldos, la custodia efectiva depende de controles técnicos y contractuales aún no plenamente acreditados.

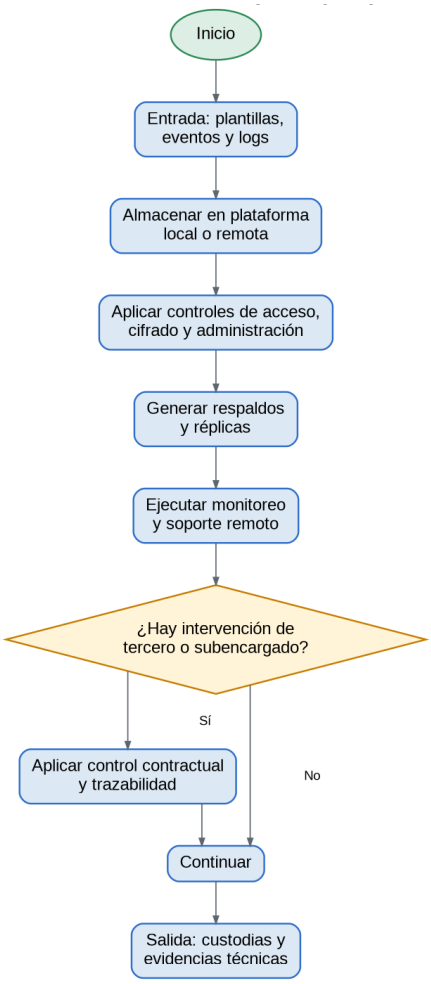

Figura 8

Almacenamiento, custodia, respaldo y soporte técnico

Nota: Muestra el proceso muestra dónde y cómo persisten plantillas, eventos, logs y respaldos.

3.1.2.9. Flujo específico: atención de derechos, revocatoria y registro de solicitudes

La atención de derechos exige localizar datos en colegio, plataforma y respaldos y en este flujo se refleja que una respuesta completa depende de cooperación efectiva entre responsable y encargado.

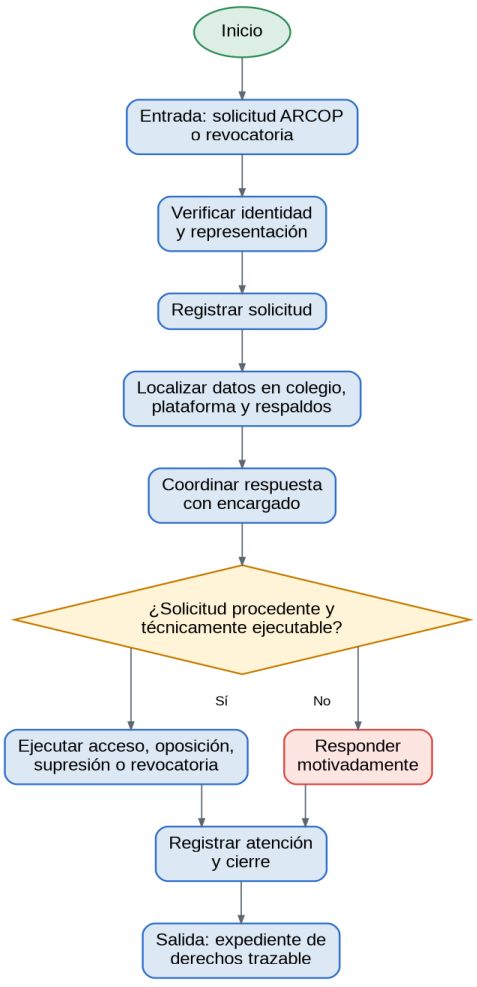

Figura 9

Atención de derechos, revocatoria y registro de solicitudes

Nota: Muestra la atención de derechos en colegio, plataforma y respaldos.

3.1.2.10. Flujo específico: baja del estudiante, supresión y cierre del ciclo de vida

El cierre del ciclo de vida no puede quedar implícito por lo que este flujo muestra la baja, supresión o bloqueo y verificación de eliminación en bases, logs y respaldos.

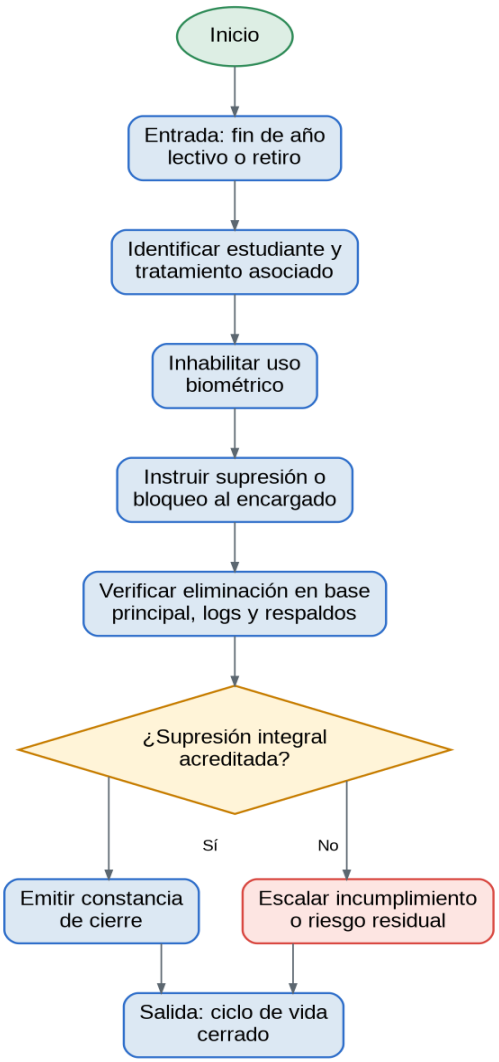

Figura 10

Baja del estudiante, supresión y cierre del ciclo de vida

Nota: Muestra la baja, supresión o bloqueo y verificación de eliminación en bases, logs y respaldos.

3.1.2.11. Flujo específico: gestión de vulneraciones, incidentes y notificación

La gestión de incidentes es transversal y de alta sensibilidad porque la biometría comprometida no puede reemplazarse como una contraseña; en este flujo se incorpora contención, notificación y remediación.

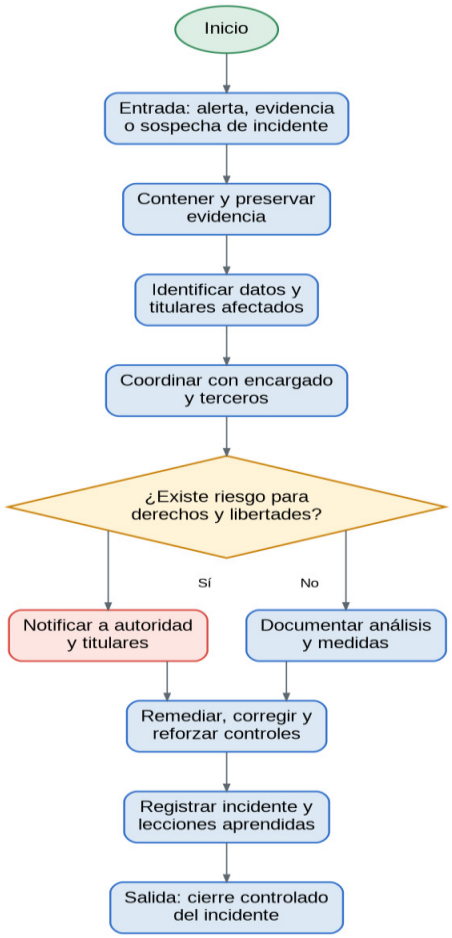

Figura 11

Gestión de vulneraciones, incidentes y notificación

Nota: Muestra gestión de incidentes e incorpora contención, notificación y remediación.

3.1.3. Arquitectura de procesos.

La arquitectura planteada no es un organigrama ni un mapa institucional genérico, más bien, es una estructura de procesos limitada al caso biométrico escolar y diseñada para ser jurídicamente apropiada, operativamente utilizable y documentalmente consistente.

El criterio rector es que el tratamiento biométrico no puede analizarse como un proceso aislado de asistencia, sino como un ecosistema de decisiones, operaciones y soportes que atraviesan el ciclo completo del dato, siendo la capa superior el macroproceso de gobierno, viabilidad y control, ya que allí se ubican la evaluación de necesidad, proporcionalidad y la gestión contractual de terceros; además, su función es previa y condicionante: sin decisión institucional sustentada, sin análisis de riesgo y sin control de encargado, el resto del flujo carece de base legítima.

La capa intermedia corresponde al macroproceso de operación escolar del registro biométrico, está compuesta por matrícula y habilitación, enrolamiento, verificación diaria y reporte interno; siendo la encargada de velar por el ciclo operativo del tratamiento desde que el estudiante ingresa al sistema hasta que el evento de asistencia es consultado o usado por el colegio.

Finalmente, la capa inferior reúne soporte, derechos, seguridad y cierre del ciclo de vida, siendo en esta capa, donde se concentra el almacenamiento y custodia, respaldo, soporte remoto, ejercicio de derechos, supresión y gestión de incidentes; esta capa es determinante para la consolidar el modelo de biometría, porque materializa la privacidad desde el diseño, la cooperación con el encargado y la capacidad real de respuesta del responsable.

La interacción entre las tres capas confirma la conclusión material planteada: el proyecto no es jurídicamente viable en su estado actual como regla general; sin embargo, la arquitectura sirve, por tanto,

como base formal para documentar la no viabilidad actual, estructurar un rediseño condicionado y convertir el caso en una plataforma seria para RAT, EIPD, contratos, procedimientos internos, matrices de riesgo y auditoría.

3.1.4. Diagrama de arquitectura de procesos.

El diagrama agrupa los diez procesos críticos en tres macroprocesos, las flechas muestran relaciones de dependencia e interacción, no una secuencia exhaustiva, por lo que debe analizarse en conjunto con la matriz integral y con los flujos específicos.

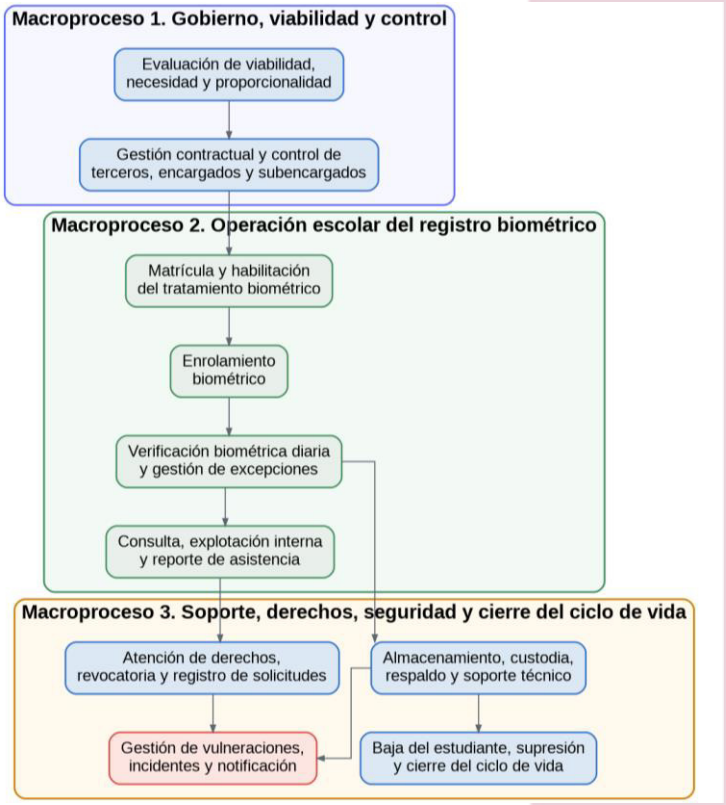

Figura 12

Diagrama de arquitectura de procesos

Nota: Abarca la arquitectura de los procesos Gobierno, Operaciones y Soporte

3.1.4.1. Síntesis de la arquitectura

Macroproceso 1. Gobierno, viabilidad y control del tratamiento biométrico: evaluación de viabilidad, necesidad y proporcionalidad; gestión contractual y control de terceros, encargados y subencargados.

Macroproceso 2. Operación escolar del registro biométrico de asistencia: matrícula y habilitación del tratamiento biométrico; enrolamiento biométrico del estudiante; verificación biométrica diaria y gestión de excepciones; consulta, explotación interna y reporte de asistencia.

Macroproceso 3. Soporte, derechos, seguridad y cierre del ciclo de vida: almacenamiento, custodia, respaldo y soporte técnico; atención de derechos, revocatoria y registro de solicitudes; baja del estudiante, supresión y cierre del ciclo de vida; gestión de vulneraciones, incidentes y notificación.

3.2. Matriz RACI

Una vez analizados los fundamentos legales, riesgos y objetivos de cada proceso en la matriz integral, se procede a la asignación de responsabilidades mediante la metodología RACI, esta matriz operativa traduce los hallazgos previos en roles claros, asegurando que cada tarea critica cuente con un responsable ejecutor (R) y una autoridad única de rendición de cuentas (A).

Definiciones:

R - Responsable:	Es quien ejecuta la tarea y hace el trabajo.
A - Aprobador / Autoridad / Dueño:	El que tiene la autoridad final y rinde cuentas.
C - Consultado:	Expertos con los que hay comunicación bidireccional antes de la tarea.
I - Informado:	Personas que deben conocer el resultado después de la tarea.

Macroprocesos y Entregables	Rectoría (Autoridad / Dueño)	DPO (Responsable Técnico)	IT / Sistemas (Consultado)	Depto. Legal (Consultado)	Inspección / DECE (Informado)	BioTrust (Proveedor)
1. INSTRUMENTOS DE GOBIERNO (DOCUMENTOS)						
Política Corporativa de Protección de Datos	A	R	C	C	I	I
Aviso de Privacidad (Interno y Externo)	A	R	I	C	C	I
Registro de Actividades de Tratamiento (RAT)	I	A	R	I	C	C
Contrato de Encargo (Anexo LOPDP con proveedor)	A	C	I	R	I	R
2. OPERACIÓN Y VIABILIDAD (PROCESOS)						
Evaluación de Impacto (EIPD) / Viabilidad	A	R	C	C	I	I
Captura de Consentimientos (Formularios)	A	C	I	C	R	I
Enrolamiento y Calidad de Huella/Rostro	A	I	R	I	I	C
3. DERECHOS Y SEGURIDAD						
Protocolo de Derechos ARCO y Revocatorias	I	A	R	C	I	I
Gestión de Incidentes y Brechas de Seguridad	A	R	C	C	I	C
Supresión y Cierre de Ciclo de Vida de Datos	I	A	R	I	C	C

Nota: La matriz asegura que ningún proceso de tratamiento de datos biométricos se realice sin el instrumento legal correspondiente (Aviso, Política o Contrato)

Tabla 1

Matriz RACI *del tratamiento biométrico*

3.3. El cumplimiento del derecho a la información: avisos de privacidad y protección de datos personales

El derecho a la información impone al responsable comunicar, de forma previa, clara y accesible, la identidad del responsable y del encargado, las finalidades, la base de licitud, los destinatarios, las eventuales transferencias, los plazos de conservación y los mecanismos de ejercicio de derechos (LOPDP, 2021, art. 12); en el caso, los avisos de privacidad y la documentación de consentimiento examinados revelan deficiencias relevantes: la información sobre la intervención de BioTrust como encargado y de eventuales subencargados, sobre la lógica del tratamiento automatizado y sobre la existencia de una alternativa no biométrica resulta insuficiente, lo que debilita la transparencia exigible cuando los titulares son menores de edad, el análisis documental de los avisos y su contraste con los requisitos legales se desarrolla con mayor detalle en los anexos.

3.4. Cláusulas contractuales entre los agentes de tratamiento de datos personales

La relación entre la Unidad Educativa Particular Andes del Sur, como responsable, y BioTrust S. A., como encargado, debe formalizarse en un contrato de encargo que delimite objeto, finalidad y duración del tratamiento, regule el subencargo, imponga garantías de seguridad y confidencialidad, prohíba el uso secundario y el entrenamiento de modelos y establezca obligaciones de auditoría, soporte, respaldo, supresión verificable y notificación de incidentes (LOPDP, 2021, arts. 47, 68 y 70; RGLOPDP, 2023, arts. 40 a 47); el expediente evidencia la ausencia de un contrato suficientemente blindado y de trazabilidad sobre los subencargados, lo que constituye una de las brechas de gobernanza que el análisis de riesgos del Capítulo III califica como críticas y el modelo de cláusulas y la matriz de control contractual se incorporan en los anexos.

CAPITULO III

1. Nivel mínimo aceptable para el tratamiento ético, responsable y estratégico de datos personales y el uso de estos en sistemas de IA

El presente capítulo integra el trabajo de gestión de riesgos desarrollado en la fase previa del Proyecto Integrador y fija el nivel mínimo aceptable de tratamiento, entendido como el conjunto de condiciones de licitud, seguridad y gobernanza por debajo de las cuales el tratamiento biométrico no puede sostenerse de forma ética, responsable ni estratégica; ese umbral no es una aspiración de buenas prácticas, sino el piso jurídico que se deriva de los principios rectores de la LOPDP y del estándar reforzado aplicable a los datos biométricos de niñas, niños y adolescentes; por ello opera, a lo largo del trabajo, como criterio de contraste de la evaluación de viabilidad que culmina en el Capítulo IV.

1.1. Habilitantes jurídicos mínimos.

El umbral exige, en primer término, una base de licitud válida y materialmente libre, una evaluación de impacto previa y favorable y un delegado de protección de datos formalmente designado y funcional; en el caso, estos habilitantes no se acreditan: el consentimiento del representante nace debilitado por la asimetría escolar y por la ausencia de alternativa no biométrica, y la evaluación de impacto, lejos de validar el tratamiento, concluye en su inviabilidad; y, la autoridad ha subrayado que una evaluación de impacto es un ejercicio sustantivo de gestión de riesgos para decidir sobre la licitud material y no un mero formulario (Resolución N.º SPDP-SPD-2025-0003-R, 2025).

1.2. Seguridad y gobernanza mínimas

En el plano técnico, el nivel mínimo comprende cifrado, autenticación multifactor, segmentación de red, custodia de llaves, control de privilegios y supresión verificable tanto en la base activa como en los

respaldos; en el plano de gobernanza, exige un contrato de encargo robusto con BioTrust, control efectivo sobre los subencargados, un registro de actividades de tratamiento actualizado y un plan de respuesta a incidentes operativo, la concurrencia de estas condiciones es la que permite afirmar que el responsable conserva el control jurídico del tratamiento pese a delegar su operación técnica en el encargado.

1.3. Salvaguarda de derechos y apetito de riesgo

Finalmente, el umbral incorpora una salvaguarda sustantiva de los derechos del titular: la existencia de una vía no biométrica equivalente y operativa que haga real la voluntariedad, tratándose de datos biométricos de menores, el apetito de riesgo admisible es mínimo, de modo que un riesgo residual asentado sobre la licitud o la gobernanza del tratamiento queda, por definición, fuera de lo tolerable.

El nivel mínimo aceptable funciona, así como un test de paso: cuando los habilitantes, los controles y las salvaguardas no se acreditan en grado operativo, la decisión correcta es no desplegar el tratamiento, conforme se sostiene en los entregables y se fundamenta en el Capítulo IV.

2. Matriz integrada de riesgos de tratamientos de datos personales biométricos, incluyendo tratamientos con uso de IA

La matriz integrada de riesgos aplica una metodología de evaluación bidimensional que cruza la probabilidad de ocurrencia de la amenaza con el impacto potencial sobre los derechos del titular, en una escala de cinco niveles para cada eje; la probabilidad se gradúa de inminente, cuando la amenaza se materializa diariamente, a improbable, cuando se materializaría una vez cada tres años, pasando por muy probable, probable y poco probable; el impacto se gradúa de crítico, daño catastrófico o irreversible, a irrelevante, sin daño relevante, el riesgo inherente resulta de la intersección de ambos ejes en una matriz de cinco por cinco, antes de considerar control alguno.

Sobre ese riesgo inherente se evalúa la existencia, eficacia y madurez de los controles, clasificados según su naturaleza en preventivos, con ponderación de 2.0, detectivos, de 1.5, correctivos, de 1.0, y disuasorios, de 0.5; el riesgo residual se obtiene dividiendo el riesgo inherente entre la ponderación del control aplicable, de modo que un control preventivo reduce con fuerza el riesgo, mientras que un control meramente correctivo lo deja prácticamente intacto y esta metodología es coherente con la guía de gestión de riesgos de la autoridad (Resolución N.º SPDP-SPD-2025-0003-R, 2025).

El ejercicio evaluó veintiséis riesgos distribuidos en cinco dimensiones: privacidad y datos personales (ocho), seguridad de la información (ocho), discriminación (tres), sesgos algorítmicos (tres) y gobernanza y cumplimiento (cuatro). En nivel inherente, el perfil arrojó ocho riesgos críticos y dieciocho altos, sin riesgos medios ni bajos, lo que evidencia una vulnerabilidad sistémica del tratamiento antes de cualquier mitigación, la distribución por dimensión, en sus perfiles inherente y residual, se sintetiza a continuación.

Dimensión	Riesgos	Perfil inherente	Perfil residual	Reducción
Privacidad y datos personales	8	3 críticos; 5 altos	1 crítico; 3 altos; 2 medios; 2 bajos	50 %
Seguridad de la información	8	1 crítico; 7 altos	4 medios; 4 bajos	100 %
Discriminación	3	3 altos	3 medios	100 %
Sesgos algorítmicos	3	1 crítico; 2 altos	2 medios; 1 bajo	100 %
Gobernanza y cumplimiento	4	3 críticos; 1 alto	3 altos; 1 bajo	25 %
Total	**26**	**8 críticos; 18 altos**	**1 crítico; 6 altos; 11 medios; 8 bajos**	**73 %**

Tabla 2

Distribución del riesgo por dimensión: perfil inherente y residual

2.1. Lectura de los resultados

Tras la aplicación de la totalidad de los controles propuestos, el riesgo se reduce un 73 % respecto del inherente; sin embargo, la reducción es marcadamente desigual, las dimensiones de seguridad de la información, discriminación y sesgos algorítmicos llevan todos sus riesgos críticos y altos a niveles medios o bajos, con reducciones del 100 %, mientras que la privacidad mitiga solo el 50 % y la gobernanza apenas el 25 %.

La mitigación más débil recae, pues, precisamente sobre las dimensiones que tutelan los derechos del titular y la rendición de cuentas del responsable.

2.2. Riesgos residuales subsistentes

El perfil residual conserva un riesgo crítico y seis altos: El crítico corresponde al consentimiento viciado del representante (P-01), que solo admite un control de naturaleza correctiva y por ello, no desciende de nivel; los altos se concentran en la desproporción del tratamiento, la ausencia de evaluación de impacto favorable y las brechas de gobernanza contractual y de control de terceros. La literatura técnica confirma, además, que el sesgo algorítmico por edad, fototipo y desarrollo morfológico del menor no es un defecto marginal del reconocimiento facial (Grother et al., 2019).

El dato decisivo es que las brechas dominantes son estructurales, no accesorias: nacen de elegir el medio biométrico para una finalidad ordinaria que admite alternativas equivalentes, de manera que un riesgo originado en la desproporción del medio no se corrige con cifrado, segmentación o auditorías, sino cambiando el medio; esta constatación cuantitativa es la que la ponderación y la evaluación de impacto del Capítulo IV traducen en un dictamen de inviabilidad.

3. Plan de respuesta a incidentes de seguridad de la información que involucren datos personales (brechas)

El plan de respuesta a incidentes establece el procedimiento operativo, jurídico y probatorio que la institución, en su calidad de responsable, ejecutará ante cualquier vulneración que afecte datos biométricos faciales de estudiantes menores o datos asociados tratados a través de la solución de BioTrust, cubre todo el ciclo de vida del tratamiento documentado en el registro de actividades y se activa ante la sospecha o la confirmación de eventos que comprometan la confidencialidad, integridad, disponibilidad o licitud del tratamiento, entre ellos el acceso no autorizado, la exfiltración de plantillas o respaldos, el uso fuera de la finalidad declarada, la transferencia no autorizada a subencargados, el mal funcionamiento del modelo de inteligencia artificial, la persistencia indebida del dato tras la baja y la manipulación física de los terminales.

Siguiendo la lógica de gestión de incidentes de la norma ISO/IEC 27035, el plan distingue tres niveles que no deben confundirse: el evento es la ocurrencia que indica una posible falla de los controles sin afectación verificada; la alerta es el evento que, tras un primer triaje técnico, presenta indicios de comprometer datos personales; y, el incidente es la alerta calificada formalmente por el delegado de protección de datos como vulneración con probable riesgo para los derechos y libertades, momento en que se activan los plazos legales y la documentación formal y sobre esa base, el plan ordena la siguiente tipología de incidentes aplicable al caso.

Código	Descripción del incidente	Dimensión afectada	Severidad presunta
T1	Acceso no autorizado a la base biométrica o a paneles administrativos.	Confidencialidad	Crítico

Código	Descripción del incidente	Dimensión afectada	Severidad presunta
T2	Filtración, exfiltración o pérdida de plantillas, imágenes, eventos o respaldos.	Confidencialidad / disponibilidad	Crítico
T3	Cifrado malicioso o destrucción (ransomware o sabotaje).	Disponibilidad / integridad	Alto a crítico
T4	Uso secundario o desviación de finalidad por BioTrust o por terceros.	Licitud / confidencialidad	Crítico
T5	Transferencia internacional no autorizada o sin garantías.	Licitud / confidencialidad	Alto a crítico
T6	Mal funcionamiento masivo del modelo de IA: sesgos, falsos negativos sistemáticos o decisiones con efecto discriminatorio.	Integridad / equidad algorítmica	Alto a crítico
T7	Suplantación o spoofing por evasión del control de vida (liveness).	Integridad / confidencialidad	Alto
T8	Persistencia indebida tras baja, revocatoria o cese de finalidad.	Licitud	Alto
T9	Manipulación física, sustracción o tampering de los terminales biométricos.	Confidencialidad / disponibilidad	Alto
T10	Indisponibilidad prolongada que afecta el acceso de estudiantes (caída sin fallback).	Disponibilidad / continuidad	Medio a alto

Tabla 3

Tipología de incidentes aplicable al caso BioTrust

3.1. Criterios de severidad y decisión de notificar

La severidad se califica de forma acumulativa según el tipo de dato afectado, el volumen de titulares, la naturaleza del compromiso, la capacidad de revertir el daño y la participación de terceros, asignándose siempre el nivel más alto aplicable; por tratarse de datos biométricos de menores y por la

irreversibilidad práctica de una plantilla facial comprometida, la mayoría de los incidentes escala a severidad crítica.

La decisión de notificar se adopta mediante un árbol de decisión que pregunta, en orden, si hubo vulneración, si es probable que esta entrañe un riesgo para los derechos y libertades, si compromete derechos fundamentales del titular y si modifica el riesgo residual del tratamiento; las respuestas afirmativas disparan, respectivamente, la notificación a la autoridad de control, la notificación a los representantes legales y la actualización del registro de actividades con eventual reevaluación de impacto.

3.2. Gobernanza y protocolo por fases

La respuesta se gestiona a través de un equipo de respuesta a incidentes liderado funcionalmente por el delegado de protección de datos y articulado con el área de tecnología, el área jurídica, BioTrust como encargado y la alta dirección, conforme a la matriz de responsabilidades de la Tabla 1. El protocolo se estructura en siete fases con plazos definidos: detección y reporte interno de forma inmediata; activación del equipo en un máximo de dos horas; contención técnica y preservación de evidencia, con cadena de custodia compatible con la norma ISO/IEC 27037 y activación del mecanismo no biométrico de respaldo, en un máximo de cuatro horas; calificación jurídica y acta de incidente en un máximo de seis horas; notificación del encargado al responsable, con un objetivo contractual de veinticuatro horas; notificación a la autoridad de control; notificación a los titulares; y, finalmente, remediación, cierre y aprendizaje organizacional, con revisión del contrato con BioTrust y decisión sobre la suspensión del tratamiento.

3.3. Deberes legales de notificación.

En sustancia, el régimen ecuatoriano impone al responsable notificar a la autoridad de protección de datos las vulneraciones de seguridad cuando sea probable que entrañen un riesgo para los derechos y libertades, con un contenido mínimo que comprende la naturaleza del incidente, los titulares afectados, las categorías y el volumen de datos comprometidos, las posibles consecuencias, las medidas adoptadas y la evaluación del riesgo (LOPDP; Reglamento General a la LOPDP).

Cuando la vulneración entrañe un riesgo para los derechos fundamentales del titular, debe comunicarse a este o a su representante legal en lenguaje claro y sencillo, salvo que proceda una excepción debidamente motivada; por ser los titulares estudiantes menores, la comunicación se dirige a los representantes legales.

El encargado, BioTrust, debe notificar sin dilación al responsable toda vulneración detectada en su entorno. El plan operacionaliza estos deberes mediante modelos de acta de incidente, de oficio de notificación a la autoridad y de comunicación a los representantes, que se incorporan en los anexos.

Dato pendiente de validación: los plazos legales precisos de notificación a la autoridad de control y a los titulares, así como la numeración exacta de los artículos de la LOPDP y de su Reglamento General que sustentan cada deber, deben confirmarse contra el texto consolidado y vigente de dichas normas, por cuanto las copias disponibles en el expediente no permitieron su verificación literal en esta fase.

CAPITULO IV

1. Ponderación de derechos: intimidad, protección de datos personales y otros derechos fundamentales

1.1. Conflicto jurídico concreto

La Unidad Educativa Particular Andes del Sur, institución privada que atiende a niñas, niños y adolescentes, enfrenta un conflicto entre el derecho a la protección de datos personales de los estudiantes menores y el interés institucional de automatizar el control de asistencia mediante reconocimiento facial con inteligencia artificial de BioTrust S. A. La identificación uno a muchos sobre población especialmente protegida y el uso de biometría para una finalidad legítima en abstracto, pero no indispensable por sí misma, convierten la cuestión en un conflicto jurídico constitucional que debe analizarse desde la perspectiva de la necesidad y la proporcionalidad (Constitución de la República del Ecuador, 2008, arts. 44, 45 y 66, num. 19; Ley Orgánica de Protección de Datos Personales, 2021, arts. 8, 25 y 26).

1.2. Derechos involucrados, titulares y vulnerabilidad

Del lado afectado concurren cuatro derechos: a) protección de datos personales y autodeterminación informativa, núcleo del conflicto por tratarse de dato sensible; b) intimidad personal y familiar; c) derecho a no ser objeto de decisiones automatizadas, pues el sistema produce una decisión con efecto disciplinario; y, de modo indirecto, d) el derecho a la educación, cuando errores del sistema generen inasistencias aparentes, retrasos o fricciones de acceso, ya que el reconocimiento facial condiciona el acceso a la jornada escolar. Transversalmente opera el interés superior del niño; el interés contrapuesto es de rango ordinario, pues se reduce a la eficiencia y organización del servicio en el registro de asistencia.

La vulnerabilidad de los titulares se incrementa por la asimetría entre familia e institución educativa, lo que debilita la libertad material del consentimiento cuando se articula con la matrícula (Reglamento General a la LOPDP, 2023, arts. 19 y 20).

1.3. Intensidad de la afectación y anuncio del juicio de razonabilidad.

La afectación al derecho a la protección de datos personales es alta, y así se sostiene conforme al análisis de riesgos del Capítulo III, por la naturaleza biométrica y sensible del dato, la continuidad y escala del tratamiento, la modalidad 1:N, la intervención de inteligencia artificial, la participación de terceros en almacenamiento, soporte y respaldo, y la irreversibilidad del daño, dado que una plantilla facial comprometida no se sustituye como una contraseña; la afectación a la intimidad también es alta, porque el cuerpo del estudiante pasa a operar como credencial permanente de control en el espacio escolar, y es media-alta respecto del derecho a no ser objeto de decisiones automatizadas. Acreditada esa intensidad, corresponde aplicar el juicio de razonabilidad en sus tres gradas sucesivas: idoneidad, necesidad y proporcionalidad en sentido estricto.

1.3.1. Idoneidad.

La medida satisface la idoneidad, dado que el reconocimiento facial efectivamente registra la presencia del estudiante y permite alcanzar el fin de control de asistencia perseguido; no obstante, la idoneidad es solo el umbral del test y no agota el análisis de proporcionalidad.

1.3.2. Necesidad

La medida fracasa en la necesidad, porque existen medios igualmente eficaces y menos restrictivos, como tarjetas RFID, códigos QR o controles manuales documentados. La doctrina administrativa ecuatoriana es explícita al respecto: el uso de datos biométricos para registro de asistencia,

no deben ser usados como primera ni única opción, sino como última elección; el solo consentimiento del titular no libera al responsable del tratamiento de llevar a cabo el test de proporcionalidad, el análisis de riesgo y la evaluación de impacto. (Oficio N.º SPDP-IRD-2025-0262-O, 2025)

Como el expediente no acredita el descarte fundado de esas alternativas, la medida no supera el examen de necesidad, pues no es el medio menos lesivo disponible para alcanzar el fin administrativo propuesto.

1.3.3. Proporcionalidad.

La proporcionalidad en sentido estricto confirma el resultado anterior: a mayor afectación de un derecho, mayor debe ser el peso del fin que la justifica (Alexy, 2008).

La afectación de los derechos del menor es grave, mientras que la satisfacción del interés contrapuesto es baja, pues la eficiencia solo añade un ahorro marginal de tiempo frente a los medios existentes; tal beneficio marginal sobre un interés ordinario no compensa un sacrificio grave de derechos reforzados.

1.4. Conclusión ponderativa

La ventaja obtenida por la institución se concentra en rapidez y trazabilidad administrativa; en cambio, la carga impuesta a los estudiantes es intensa y recae sobre derechos reforzados por la Constitución y la LOPDP, sin que el sacrificio se compense con la utilidad perseguida; en consecuencia, en el caso BioTrust, el derecho a la protección de datos personales, en conexión con la intimidad, la autodeterminación informativa y el interés superior del niño, prevalece circunstancialmente sobre la eficiencia organizacional.

La conclusión es contextual, no absoluta: no prohíbe toda biometría escolar, pero sí torna inadmisible el proyecto en su diseño actual mientras no demuestre necesidad estricta, alternativa no biométrica equivalente, voluntariedad real y salvaguardas reforzadas de diseño, riesgo y control.

El interés superior del niño, como regla de prevalencia condicionada, refuerza la conclusión (Comité de los Derechos del Niño, 2013): la restricción no es admisible mientras el tratamiento no se rediseñe para superar el test de proporcionalidad.

2. Evaluación de impacto a la privacidad y protección de datos personales

2.1. Descripción sintética del tratamiento

El tratamiento consiste en el uso de reconocimiento facial provisto por BioTrust S. A. para registrar la asistencia diaria de estudiantes menores de edad en los accesos de la Unidad Educativa Particular Andes del Sur, responsable del tratamiento, en tanto el proveedor opera como encargado, desplegado sobre arquitectura centralizada en nube híbrida, con identificación uno a muchos, motor de inteligencia artificial con detección de vida y posible intervención de subencargados; el flujo abarca consentimiento del representante, enrolamiento, generación de la plantilla facial, verificación automatizada en cada acceso, registro de asistencia con efecto disciplinario, almacenamiento, logs, respaldos, atención de derechos e incidentes y eventual supresión: un tratamiento continuo y masivo de datos sensibles sobre titulares en especial vulnerabilidad, no una simple herramienta administrativa.

2.2. Justificación de la obligatoriedad de la evaluación de impacto

La evaluación de impacto no es opcional, sino jurídicamente obligatoria, porque concurren los cuatro factores que el ordenamiento asocia al alto riesgo: la naturaleza del dato, biometría facial sensible que, al recaer sobre niñas, niños y adolescentes, acumula la categoría especial e impone el estándar más

exigente (Ley Orgánica de Protección de Datos Personales, 2021, arts. 25 y 26); la inteligencia artificial con decisiones automatizadas que producen efectos sobre el estudiante; la escala masiva, diaria y sistemática sobre todo el alumnado; y la irreversibilidad del daño, pues una plantilla facial comprometida no se revoca ni sustituye; además, el Reglamento exige realizarla antes del inicio del tratamiento, con descripción de operaciones, justificación de necesidad y proporcionalidad, evaluación de riesgos y medidas para enfrentarlos (Reglamento General a la LOPDP, 2023, arts. 29 a 32); y, la autoridad refuerza su carácter sustantivo: es gestión de riesgos para decidir sobre la licitud material, no un formulario, de modo que una evaluación con riesgo residual nulo sería metodológicamente defectuosa (Resolución N.º SPDP-SPD-2025-0003-R, 2025).

2.3. Riesgos identificados, derechos afectados y vínculo con el análisis de riesgos

Esta evaluación de impacto se apoya en el análisis de riesgos desarrollado en el Capítulo III de este trabajo, que evaluó veintiséis riesgos en cinco dimensiones: privacidad, seguridad de la información, discriminación, sesgos algorítmicos y gobernanza, mediante una metodología bidimensional que cruza probabilidad e impacto en escala de cinco niveles y pondera los controles como preventivos (2.0), detectivos (1.5), correctivos (1.0) o disuasorios (0.5).

En nivel inherente, dicho análisis arrojó ocho riesgos críticos y dieciocho altos, sin medios ni bajos, lo que evidencia una vulnerabilidad sistémica, conforme consta en el análisis de riesgos que se explica en el Capítulo III de este trabajo. Los riesgos se agrupan por categoría, vinculando cada uno con el derecho que compromete y la razón de la afectación.

2.3.1. Riesgos para la licitud, la autodeterminación informativa, la intimidad y la minimización (P-01 a P-05).

El consentimiento nace debilitado por la asimetría escolar y la falta de alternativa no biométrica; si la única vía de registro es el rostro, la negativa deja de ser opción real y el consentimiento pierde su carácter libre, comprometiendo la protección de datos, la autodeterminación informativa y el interés superior del niño; además, la identificación uno a muchos convierte el cuerpo del menor en credencial de control continuo (intimidad) y retiene más datos de los necesarios (minimización).

2.3.2. Riesgos de seguridad y control de terceros (S-01 a S-08).

Persisten vacíos en autenticación multifactor, segmentación, supresión verificable y trazabilidad contractual con BioTrust y subencargados, que comprometen la seguridad del dato, irreversible en biometría de menores.

2.3.3. Riesgos de discriminación y de decisiones automatizadas (D-01 a D-03, A-01 a A-03).

Persisten sesgos algorítmicos por edad, fototipo y desarrollo morfológico del menor (Grother et al., 2019); la tensión con la no discriminación se concreta en el falso negativo que estigmatiza o excluye del ingreso, y la del derecho a no ser objeto de decisiones automatizadas, porque el sistema califica la asistencia sin intervención humana significativa; como el reconocimiento condiciona el acceso a la jornada, un fallo repercute sobre el derecho a la educación.

2.3.4. Medidas de mitigación previstas y evaluación de su suficiencia.

Las medidas necesarias son identificables, pero la evaluación de impacto debe valorar su efectividad, suficiencia y realismo, no solo enumerarlas. En lo jurídico y organizativo: evaluación de impacto previa favorable, delegado de protección de datos funcional, consentimiento separado de la

matrícula, mecanismo no biométrico equivalente operativo desde el inicio, registro de actividades actualizado, política de biometría y contrato de encargo robusto que prohíba el uso secundario, el entrenamiento de modelos y la notificación tardía; en lo técnico: cifrado, autenticación multifactor, segmentación de red, detección de vida, control de privilegios y borrado verificable en base y respaldos.

El problema decisivo es de suficiencia: el expediente no demuestra que estas medidas existan en grado operativo, pues varias dependen de rediseño, auditoría o validación posterior; una salvaguarda proyectada no equivale a una implementada ni reduce el riesgo al momento de decidir (Resolución N.º SPDP-SPD-2025-0003-R, 2025).

2.4. Evaluación del riesgo residual

El núcleo decisional de esta evaluación exige responder tres preguntas a partir de los resultados del análisis de riesgos del Capítulo III.

¿Permanece alto el riesgo residual? Sí. Aun aplicando la totalidad de los controles propuestos, el perfil residual se reduce un 73 % respecto del inherente, pero subsisten un riesgo crítico, seis altos, once medios y ocho bajos; la reducción es marcadamente desigual: seguridad, discriminación y sesgos algorítmicos llevan todos sus riesgos críticos y altos a medio o bajo, mientras que privacidad mitiga solo el 50 % y gobernanza apenas el 25 %, según los resultados consignados en el Capítulo III, la mitigación más débil recae, pues, sobre las dimensiones que tutelan los derechos del titular y la rendición de cuentas.

¿Es jurídicamente tolerable ese riesgo residual? No en la configuración actual. El déficit no está en controles accesorios susceptibles de ajuste técnico, sino en el núcleo de licitud y gobernanza: la necesidad estricta del medio no está acreditada, la base legitimadora del consentimiento es frágil por la asimetría escolar y el control sobre encargado, subencargados, respaldos y supresión es incompleto. Un riesgo

residual asentado sobre la licitud misma del tratamiento no cabe en el apetito de riesgo admisible cuando los titulares son menores y el dato es biométrico.

¿Puede mitigarse razonablemente con ajustes incrementales? No, y esta es la conclusión más relevante. Que la mitigación más débil recaiga en privacidad y gobernanza no es accidental, sino síntoma de que las brechas dominantes son estructurales: derivan de elegir el medio biométrico para una finalidad ordinaria que admite alternativas equivalentes menos intrusivas. Un riesgo nacido de la desproporción del medio no se corrige con cifrado, segmentación o auditorías, sino cambiando el medio; el riesgo residual, aquí, no es un remanente tolerable, sino la manifestación cuantitativa de una incompatibilidad de fondo.

2.5. Conclusión de la evaluación de impacto

La evaluación concluye que el tratamiento, en su estado actual, es de riesgo inaceptable y que la decisión correcta es no desplegarlo en producción, ya que no se cumplen las condiciones reforzadas que el ordenamiento exige y la incompatibilidad es estructural, no formal.

Solo una reconfiguración integral, alternativa no biométrica operativa, consentimiento libre y separado de la matrícula, contrato de encargo robusto, controles técnicos suficientes y una nueva evaluación de impacto favorable, permitiría reabrir el análisis; mientras esas condiciones no se acrediten, la institución debe abstenerse de implementar el proyecto biométrico de BioTrust.

3. Análisis de viabilidad jurídica, decisión final y recomendaciones frente al uso de sistemas biométricos

Este apartado integra los resultados de la ponderación de derechos y de la evaluación de impacto para emitir el dictamen de viabilidad jurídica del proyecto y la conclusión es inequívoca: el sistema de reconocimiento facial propuesto por BioTrust S. A. para el control de asistencia de estudiantes menores de

edad en la Unidad Educativa Particular Andes del Sur no es jurídicamente viable en su configuración actual.

3.1. Fundamento ponderativo

La ponderación demostró que la medida, aun siendo idónea, no supera el examen de necesidad, porque existen medios igualmente eficaces y menos intrusivos cuyo descarte fundado no consta en el expediente y tampoco la proporcionalidad en sentido estricto, porque la afectación grave de derechos reforzados de los menores no se compensa con un beneficio marginal de eficiencia administrativa de rango ordinario; en consecuencia, el derecho a la protección de datos personales, en conexión con la intimidad, la autodeterminación informativa y el interés superior del niño, prevalece sobre el interés organizacional.

3.2. Fundamento de impacto y riesgo

La evaluación de impacto confirmó esa conclusión desde la gestión de riesgos: aun aplicando la totalidad de los controles propuestos, el riesgo residual permanece inaceptable, con un riesgo crítico y seis altos subsistentes, concentrados precisamente en las dimensiones de privacidad y gobernanza que tutelan los derechos del titular; la incompatibilidad es estructural, no formal, porque deriva de la elección del medio biométrico para una finalidad ordinaria que admite alternativas equivalentes, y no se corrige con ajustes técnicos incrementales.

3.3. Fundamento de principios y responsabilidad proactiva

El dictamen se sostiene, finalmente, en los principios rectores del tratamiento: licitud, minimización, finalidad, necesidad y proporcionalidad, reforzados por el interés superior del niño y por la responsabilidad proactiva; y, sobre el responsable, pesa la carga de demostrar el cumplimiento; una

salvaguarda meramente proyectada, no acreditada en grado operativo, no satisface esa carga y no habilita el despliegue.

3.4. Recomendaciones

La decisión es de no viabilidad (No Go) en el estado actual, sin que ello implique una prohibición categórica de toda biometría en el ámbito escolar, el análisis solo podría reabrirse si, de manera previa y acreditada, concurren las siguientes condiciones mínimas: (i) la implementación de una alternativa no biométrica equivalente y operativa como vía ordinaria de registro de asistencia; (ii) la reducción del alcance del tratamiento, sustituyendo la identificación uno a muchos por mecanismos menos intrusivos y verdaderamente voluntarios; (iii) un consentimiento libre, informado y separado documentalmente de la matrícula, que neutralice la asimetría escolar; (iv) un contrato de encargo robusto con BioTrust y eventuales subencargados, con garantías técnicas, de auditoría, de supresión verificable y de prohibición de uso secundario; y (v) una nueva evaluación de impacto previa y favorable que acredite la necesidad estricta del medio y un riesgo residual jurídicamente tolerable.

Mientras esas condiciones no se demuestren de forma íntegra, la institución debe abstenerse de implementar el proyecto, el dictamen es contextual: no clausura definitivamente la posibilidad de un tratamiento futuro debidamente rediseñado, pero declara inadmisible el diseño examinado, en coherencia con la prevalencia condicionada del interés superior del niño y con el estándar reforzado que el ordenamiento ecuatoriano impone al tratamiento de datos biométricos de menores.

CAPITULO V

1. Conclusiones Generales

El estudio respondió los tres problemas jurídicos generales que orientaron la investigación, en coherencia con la tesis de no viabilidad sostenida a lo largo del Proyecto Integrador.

Respecto del primer problema, relativo a la viabilidad jurídica de la implementación del sistema biométrico, se concluye que el tratamiento no es jurídicamente viable en su configuración actual, porque no supera el test de proporcionalidad: la medida es idónea, pero innecesaria, dado que existen alternativas equivalentes menos intrusivas, y desproporcionada en sentido estricto.

Respecto del segundo problema, relativo a la recomendabilidad del uso de biometría desde la perspectiva de los derechos fundamentales y de los riesgos, se concluye que no es recomendable, pues la afectación recae sobre derechos reforzados de menores y el beneficio perseguido es de rango ordinario.

Respecto del tercer problema, relativo a si la evaluación de impacto permite justificar la aceptabilidad del riesgo residual, se concluye que no: aun aplicando la totalidad de los controles propuestos, el riesgo residual permanece inaceptable y de naturaleza estructural, por lo que corresponde recomendar el no despliegue (No Go).

2. Conclusiones Específicas

Las conclusiones específicas se ordenan en torno al cumplimiento de los objetivos, la contribución del trabajo y sus limitaciones.

Análisis del cumplimiento de los objetivos de la investigación, se cumplieron los objetivos de analizar el marco normativo aplicable al tratamiento biométrico de menores, evaluar los riesgos del

tratamiento y emitir un dictamen de viabilidad fundamentado en la ponderación de derechos y en la evaluación de impacto.

Contribución a nivel académico: El trabajo articula el test de proporcionalidad y la metodología de gestión de riesgos en un caso concreto del sector educativo ecuatoriano, ofreciendo un modelo replicable de análisis de viabilidad de tratamientos biométricos que afectan a niñas, niños y adolescentes.

Contribución a nivel personal: El desarrollo del caso consolidó competencias en redacción jurídico-técnica, en la aplicación del test de proporcionalidad y en la elaboración de evaluaciones de impacto conforme al marco ecuatoriano vigente.

Limitaciones de la investigación: El análisis se circunscribe a un caso de estudio con información documental definida; la verificación de la implementación efectiva de las medidas y la identificación final de subencargados, países de alojamiento y matriz contractual completa quedan como aspectos pendientes de validación.

Bibliografía

Alexy, R. (2008). Teoría de los derechos fundamentales (2.ª ed., C. Bernal Pulido, Trad.). Centro de Estudios Políticos y Constitucionales.

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic effects (NISTIR 8280). National Institute of Standards and Technology.

Hidalgo Coloma, A., & López Ochoa, M. (2025). La protección de datos personales más allá de la ley: liderazgo institucional en la gestión de riesgos de privacidad. Ediciones Legales.

Hoepman, J. H. (2018). Privacy design strategies (The little blue book). Radboud University.

Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters, 79, 80–105. https://doi.org/10.1016/j.patrec.2015.12.013

Martínez Devia, A. (2019). La inteligencia artificial, el Big Data y la era digital: ¿una amenaza para los datos personales? Revista La Propiedad Inmaterial, 5–23.

Mayer-Schönberger, V., & Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.

Pérez Luño, A. E. (2014). Derechos humanos, Estado de Derecho y Constitución (11.ª ed.). Tecnos.

Remolina Angarita, N. (2020). Tratamiento de datos personales: aproximación internacional y comentarios a la Ley 1581 de 2012 (2.ª ed.). Legis.

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI. Columbia Business Law Review, 2019(2), 494–620.

Estándares técnicos

International Organization for Standardization. (2012). ISO/IEC 27037:2012. Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence. ISO.

International Organization for Standardization. (2022a). ISO/IEC 24745:2022. Information security, cybersecurity and privacy protection - Biometric information protection. ISO.

International Organization for Standardization. (2022b). ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection - Guidance on managing information security risks. ISO.

International Organization for Standardization. (2023a). ISO/IEC 27035-1:2023. Information technology - Information security incident management - Part 1: Principles and process. ISO.

International Organization for Standardization. (2023b). ISO/IEC 42001:2023. Information technology - Artificial intelligence - Management system. ISO.

National Institute of Standards and Technology. (2020). NIST Privacy Framework: A tool for improving privacy through enterprise risk management (Version 1.0). U.S. Department of Commerce.

National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Normativa nacional

Constitución de la República del Ecuador. Registro Oficial No. 449, 20 de octubre de 2008.

Código de la Niñez y Adolescencia. Registro Oficial No. 737, 3 de enero de 2003.

Ley Orgánica de Protección de Datos Personales. Quinto Suplemento del Registro Oficial No. 459, 26 de mayo de 2021.

Reglamento General a la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo No. 904). Tercer Suplemento del Registro Oficial No. 435, 13 de noviembre de 2023.

Resolución N.º SPDP-SPD-2025-0003-R, por la cual la Superintendencia de Protección de Datos Personales expidió la Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales. Registro Oficial: Dato pendiente de validación.

Resolución N.º SPDP-SPD-2025-0004-R, por la cual la Superintendencia de Protección de Datos Personales expidió el Reglamento del profesional Delegado de Protección de Datos Personales. Registro Oficial: Dato pendiente de validación.

Resolución N.º SPDP-SPD-2025-0006-R, por la cual la Superintendencia de Protección de Datos Personales expidió el Reglamento que establece la obligación de incorporar cláusulas de protección de datos personales en los contratos celebrados dentro del territorio de la República del Ecuador. Registro Oficial: Dato pendiente de validación.

Resolución N.º SPDP-SPD-2025-0028-R, por la cual la Superintendencia de Protección de Datos Personales expidió el Reglamento del Delegado de Protección de Datos Personales. Registro Oficial: Dato pendiente de validación.

Resolución N.º SPDP-SPD-2025-0030-R, por la cual la Superintendencia de Protección de Datos Personales expidió el Reglamento para la seudonimización, anonimización, bloqueo, suspensión y eliminación de datos personales. Registro Oficial: Dato pendiente de validación.

Resolución N.º SPDP-SPD-2025-0041-R, por la cual la Superintendencia de Protección de Datos Personales expidió la Normativa general para la aplicación del interés legítimo y su anexo. Registro Oficial:

Resolución N.º SPDP-SPD-2026-0004-R, por la cual la Superintendencia de Protección de Datos Personales expidió la Norma general de transferencias internacionales de datos personales. Registro Oficial: Dato pendiente de validación.

Resolución N.º SPDP-SPD-2026-0005-R, por la cual la Superintendencia de Protección de Datos Personales expidió la Norma general sobre el tratamiento de datos personales a gran escala. Registro Oficial: Dato pendiente de validación.

Resolución N.º SPDP-SPD-2026-0009-R, por la cual la Superintendencia de Protección de Datos Personales expidió la Norma general para la garantía del derecho a la protección de datos personales en el uso de sistemas de inteligencia artificial. Expedida el 12 de febrero de 2026; Registro Oficial: Dato pendiente de validación.

Actos administrativos y pronunciamientos de la SPDP

Guía de protección de datos personales desde el diseño y por defecto. Superintendencia de Protección de Datos Personales (2025). Resolución de aprobación y datos de publicación: Dato pendiente de validación.

Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales (versión 2). Superintendencia de Protección de Datos Personales (2026). Datos de publicación: Dato pendiente de validación.

Oficio N.º SPDP-IRD-2025-0262-O, pronunciamiento de la Superintendencia de Protección de Datos Personales sobre el tratamiento de datos biométricos y el principio de minimización (2025). Verificación pendiente: la doctrina sobre el uso de biometría para control de asistencia consta también en los Oficios N.º SPDP-IRD-2025-0031-O y N.º SPDP-IRD-2025-0065-O. Dato pendiente de validación.

Resolución N.º RES-SPDP-ICS-2025-0005, caso FAN ID (LIGAPRO). Superintendencia de Protección de Datos Personales (2025). Datos de publicación: Dato pendiente de validación.

Resolución N.º RES-SPDP-ICS-2025-0006, caso FANFEF (Federación Ecuatoriana de Fútbol). Superintendencia de Protección de Datos Personales (2025). Datos de publicación: Dato pendiente de validación.

Normativa internacional e instrumentos internacionales

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos). Diario Oficial de la Unión Europea, L 119, 4 de mayo de 2016.

Comité de los Derechos del Niño. (2013). Observación General N.º 14 sobre el derecho del niño a que su interés superior sea una consideración primordial (CRC/C/GC/14). Naciones Unidas.

European Data Protection Board. (2020). Guidelines 3/2019 on processing of personal data through video devices (Versión 2.0). https://edpb.europa.eu

ANEXOS

Matriz integral de macroprocesos y procesos

La matriz mantiene la integralidad del análisis jurídico e incorpora en gobierno del proceso: responsable definido si existe y responsable sugerido; además incorpora la base de definición del responsable para distinguir entre dato documentado, supuesto operativo e inferencia técnica razonable.

Macroproceso	Proceso	Objetivo del proceso	Actividades principales	Descripción técnica y operativa	Responsable definido si existe	Responsable sugerido	Base de definición del responsable	Relación con el caso	Datos personales tratados	Categorías de datos personales	Titulares de los datos	Riesgo o punto crítico de protección de datos	Fundamento normativo oficial ecuatoriano	Observaciones	Pendiente
Gobierno, viabilidad y control del tratamiento biométrico	Evaluación de viabilidad, necesidad y proporcionalidad	Determinar si el uso de biometría facial para asistencia escolar puede sostenerse jurídica y operativamente antes de cualquier despliegue.	Definir finalidad; contrastar necesidad; valorar alternativas menos intrusivas; aplicar análisis de riesgos; exigir EIPD; emitir decisión No Go o Go condicionado.	Proceso estratégico previo al despliegue. Ordena la lectura del caso, fija la tesis de viabilidad o inviabilidad y condiciona al resto de procesos.	Colegio como responsable del tratamiento.	Alta dirección; asesoría jurídica; TI; DPD; comité de decisión [según estructura real	Responsable definido en entregables; co-responsables sugeridos por lógica de gobierno.	Es el núcleo del caso. Sin este proceso no existe control institucional sobre la justificación del tratamiento biométrico.	Información del proyecto; categorías de datos; evidencias de riesgos; información de actores y contratos.	Documentación del tratamiento; referencias a datos biométricos y datos de menores como objeto de evaluación.	Estudiantes menores; representantes legales; colegio como responsable.	Aprobación del sistema sin demostrar necesidad, proporcionalidad, alternativa equivalente ni EIPD previa.	LOPDP arts. 4, 7, 8, 25, 26, 39, 40 y 42; RGLOPDP arts. 19, 20, 38 y 39; Resolución SPDP-SPD-2025-0003-R.	La decisión No Go actual proviene de PBL1 y se refuerza con PBL2.	acto interno que asigne formalmente comité o dueño del proceso
Gobierno, viabilidad y control del tratamiento biométrico	Gestión contractual y control de terceros, encargados y subencargados	Asegurar que BioTrust y terceros actúen solo bajo instrucciones válidas, con	Definir contrato de encargo; delimitar objeto, finalidad y	Proceso de gobierno de terceros que controla la externalización del tratamiento y evita que el proveedor	BioTrust aparece definido como encargado o tercero con intervención	Representante legal institucional; asesoría jurídica; TI; DPD.	Relación responsable-encargado documentada; dueño interno del contrato	El caso depende de un proveedor con control relevante sobre	Datos de contacto de partes; categorías de datos transferidos; logs; respaldos;	Datos identificativos de intervinientes; referencias a	Estudiantes menores; representantes; usuarios internos; contactos de	Subencargo no autorizado; uso secundario; falta de auditoría; falta de supresión verificable;	RGLOPDP arts. 40 a 47; Resolución SPDP-SPD-2025-0006-R; LOPDP arts. 47, 68 y 70.	El expediente reconoce ausencia de contrato blindado y trazabilidad	identificación final de subencargados, países de alojamiento y matriz

		garantías técnicas, jurídicas y organizativas trazables.	duración; regular subencargo; fijar auditoría, soporte, respaldo, eliminación y notificación.	amplíe finali dades o retenga control unilateral del dato.	relevante; el colegio aparece como responsable.		sugerido por lógica operativa.	infraestructura, respaldo, monitoreo y soporte.	instrucciones de tratamiento.	biometría, logs y datos de menores objeto del servicio.	proveedor y subencargados.	posible transferencia internacional.		suficiente sobre subencargados.	contractual completa
Operación escolar del registro biométrico de asistencia	Matrícula y habilitación del tratamiento biométrico	Incorporar al estudiante al servicio educativo y definir, con información adecuada, si se habilita o no el canal biométrico.	Recabar datos del estudiante y del representante; informar finalidades, riesgos y derechos; recoger consentimiento o separado; registrar negativa; habilitar alternativa no biométrica.	Proceso de entrada que no equivale a la matrícula general completa. Su función es habilitar o excluir el tratamiento biométrico dentro del vínculo educativo.	Administración institucional / BioTrust según RAT.	Secretaría académica, admisiones o unidad equivalente; asesoría jurídica; TI.	Responsable documentado de forma genérica en RAT; responsable orgánico interno inferido razonablemente.	Los supestos permiten conectar el enrolamiento con matrícula o activación del servicio escolar.	Identificación del estudiante; identificación y contacto del representante; estado de matrícula; evidencia de consentimiento o revocatoria.	Datos identificativos; contacto; datos de menores; documentación de consentimiento.	Estudiantes menores; representantes legales.	Consentimiento no libre; integración del servicio educativo con la autorización biométrica; falta de alternativa equivalente.	LOPDP arts. 7, 8, 12, 25 y 26; RGLOPDP arts. 19 y 20.	Debe separarse documentalmente la relación educativa de la aceptación biométrica.	formulario definitivo, canal alternativo no biométrico y denominación exacta del área interna
Operación escolar del registro biométrico de asistencia	Enrolamiento biométrico del estudiante	Capturar la imagen facial y generar la plantilla biométrica	Verificar habilitación; capturar imágenes; validar	Proceso de transformación del dato de entrada en dato biométrico operativo.	Administración institucional / BioTrust según RAT.	TI del colegio; personal autorizado de enrolamiento;	Responsable documentado en RAT; responsable operativo afinado por inferencia razonable.	Los supestos del caso ubican como fase distinta y previa a la	Imagen facial de enrolamiento; identificador interno; curso o nivel; estado de	Datos biométricos; datos de menores; datos	Estudiantes menores.	Conservación de imagen cruda; generación fuera del control del colegio; ausencia de validación robusta en menores.	LOPDP arts. 4, 25, 26, 39 y 40; RGLOPDP arts. 19, 20, 38 y 39.	El RAT documenta que no existe evidencia suficiente de	prueba de eliminación de imágenes crudas en todos los

		asociada al estudiante previamente habilitado.	calidad; generar plantilla; asociar identificador; alta en galería biométrica.	Constituye una fase autónoma y crítica del tratamiento.		encargado BioTrust.		operación diaria del sistema.	matrícula; metadatos de captura.	identificativos y académicos mínimos.				eliminación inmediata y verificable de imágenes crudas.	entornos técnicos
Operación escolar del registro biométrico de asistencia	Verificación biométrica diaria y gestión de excepciones	Registrar asistencia al ingreso mediante identificación biométrica y gestionar no coincidencias, validaciones manuales o fallas de ingreso.	Captura diaria; liveness; matching 1:N; decisión de coincidencia; registro automático; evento de excepción; revisión manual; contingencia.	Proceso operativo central del caso. Materializa la automatización, produce el evento de asistencia o la excepción y genera consecuencias reales para el menor.	Administración institucional / BioTrust según RAT.	Control de acceso escolar; inspectoría o personal equivalente; TI; BioTrust.	Responsable documentado de forma genérica en RAT; responsable de campo sugerido por la operativa escolar descrita en los supestos del caso	Es el corazón funcional del expediente y donde se concentran proporcionalidad, error algorítmico y riesgo de afectación de derechos.	Imagen o secuencia facial en tiempo real; plantilla biométrica; score o resultado de coincidencia; fecha, hora y punto de acceso; evento de excepción.	Datos biométricos; datos de menores; datos derivados operativos; valoraciones automatizadas.	Estudiantes menores; terceros incidentales en campo visual [si ocurre	Falsos negativos, fricción operativa, automatización con efectos relevantes, captación incidental y alta intrusión del matching 1:N.	LOPDP arts. 25, 26, 39, 40 y 42; RGLOPDP arts. 19 y 20; Resolución SPDP-SPD-2025-0003-R.	El expediente reconoce que la supervisión humana de excepciones no elimina la relevancia jurídica del proceso automatizado.	umbral de coincidencia, protocolo escrito de revisión manual y parámetro de liveness
Operación escolar del registro biométrico de asistencia	Consulta, explotación interna y reporte de asistencia	Permitir el uso interno legítimo del registro de asistencia sin expansión funcional incompatible con la finalidad declarada.	Consultar registros; visualizar asistencia y excepciones; generar reportes; distribuir internamente	Proceso posterior al evento biométrico. No trata solo visualización; también comprende exportación, circulación interna y conservación secundaria del dato.	No aparece definido de manera orgánica; se infiere a partir del flujo de eventos y del uso escolar del registro.	Coordinación académica; control escolar; secretaría; usuarios internos autorizados.	Responsable sugerido por inferencia operativa; el expediente no identifica un dueño de proceso específico.	El caso no termina en la puerta. El dato de asistencia se consulta y usa internamente, lo que exige	Identificador del estudiante; curso; estado de asistencia; fecha, hora, acceso; reportes internos.	Datos identificativos; datos de menores; datos derivados de asistencia.	Estudiantes menores.	Reutilización secundaria para disciplina, vigilancia o perfilamiento; sobreconservación; distribución excesiva.	LOPDP arts. 12, 25 y 39; RGLOPDP art. 38.	Debe limitarse a control escolar y excluir usos disciplinarios no declarados.	perfiles exactos de acceso, política de exportación y criterio formal de retención de reportes

			según rol; conservar evidencias.					limitar finalidad y accesos.							
Soporte, derechos, seguridad y cierre del ciclo de vida	Almacenamiento, custodia, respaldo y soporte técnico	Asegurar la custodia segura del ecosistema biométrico y el soporte operativo sin pérdida de control jurídico del responsable.	Almacenar plantillas y eventos; gestionar logs; ejecutar respaldos; monitorear; prestar soporte remoto; administrar accesos y cambios.	Proceso de apoyo técnico transversal a toda la operación. Controla dónde y cómo permanecen las plantillas, eventos, logs y respaldos.	BioTrust y Administración institucional aparecen en RAT como actores de custodia.	TI; seguridad de la información; DPD; proveedor BioTrust y terceros técnicos autorizados.	Responsable parcialmente documentado; capas de control institucional sugeridas por exigencia de seguridad y cumplimiento.	Los supestos enfatizan la arquitectura híbrida, plataforma multientidad, single point of failure, respaldos automatizados y control limitado del colegio.	Plantillas biométricas; eventos de asistencia; logs técnicos; logs de administración; tickets de soporte; respaldos y réplicas.	Datos biométricos; datos de menores; datos derivados y de soporte.	Estudiantes menores; usuarios internos con trazas técnicas.	Dependencia del proveedor; ausencia de control directo sobre llaves, purga de respaldos, anti-tampering y DLP integral.	LOPDP arts. 39, 40, 46 y 47; RGLOPDP arts. 40 a 47; Resolución SPDP-SPD-2025-0003-R.	El RAT evidencia controles parciales, pero no un cierre técnico completo del entorno.	evidencia contractual y técnica de cifrado, MFA, segmentación, DLP y purga de backups
Soporte, derechos, seguridad y cierre del ciclo de vida	Atención de derechos, revocatoria y registro de solicitudes	Permitir el ejercicio de derechos y la revocatoria con trazabilidad suficiente frente al colegio y al encargado.	Recibir solicitud; verificar identidad y representación; registrar; localizar datos; coordinar con encargado; responder; ejecutar y cerrar.	Proceso jurídico operativo que conecta al responsable con el encargado y exige localizar datos en plataforma, logs y respaldos para responder de forma íntegra.	No aparece orgánicamente definido; Los supestos y el RAT solo muestran su necesidad funcional.	DPD; asesoría jurídica; secretaría general; responsable de atención de derechos [según estructura real	Responsable sugerido por exigencia normativa y por la lógica del flujo de derechos del caso.	El expediente identifica expresamente que la atención integral depende de la cooperación efectiva entre colegio y BioTrust.	Datos identificativos del solicitante; prueba de representación; registros biométricos asociados; evidencia de atención.	Datos identificativos; datos de menores; datos biométricos afectados por la solicitud; registro de solicitud.	Representantes legales; estudiantes menores; adolescentes de 15 años o más [si el caso concreto llegara a involucrarlos	Respuesta parcial por falta de localización de plantillas, eventos, logs o respaldos; dependencia del proveedor.	LOPDP arts. 12 y 24; RGLOPDP arts. 15, 16, 19 y 42.	En menores de quince años, el representante legal es actor central del proceso.	procedimiento formal aprobado, canal único de recepción y registro activo de solicitudes

Soporte, derechos, seguridad y cierre del ciclo de vida	Baja del estudiante, supresión y cierre del ciclo de vida	Terminar el tratamiento biométrico y asegurar supresión, bloqueo o cierre verificable cuando el estudiante se retire o cese la finalidad.	Recibir evento de baja; inhabilitar uso biométrico; instruir supresión o bloqueo; verificar eliminación en plataforma, logs y respaldos; dejar constancia.	Proceso de cierre del tratamiento. Evita retención excesiva y permite acreditar que el dato no continúa circulando sin base.	No aparece definido con dueño orgánico expreso; depende de administración institucional y del encargado.	Secretaría académica o control escolar; TI; BioTrust; asesoría jurídica; DPD.	Responsable orgánico sugerido; participación del proveedor inferida directamente de la dependencia técnica descrita.	El expediente identifica esta fase como una de las brechas más serias por ausencia de garantías tecnológicas de destrucción integral.	Identificador del estudiante; estado de matrícula; plantilla biométrica; eventos; logs; constancias de eliminación.	Datos biométricos; datos de menores; datos derivados y de soporte.	Estudiantes menores; representantes cuando solicitan supresión o revocatoria.	Persistencia en base central o respaldos; supresión parcial; falta de certificados de destrucción; conservación desproporcionada.	LOPDP arts. 39, 47, 65 a 68; RGLOPDP arts. 38, 41 y 46.	Debe contemplar tanto retiro anticipado como cierre de período lectivo.	criterio formal de conservación, bloqueo y destrucción de réplicas y respaldos
Soporte, derechos, seguridad y cierre del ciclo de vida	Gestión de vulneraciones, incidentes y notificación	Detectar, contener, documentar y, de ser el caso, notificar vulneraciones que comprometan datos y derechos de los titulares.	Detectar incidente; contener; preservar evidencia; identificar afectados; coordinar con encargado; notificar; remediar; documentar y cerrar.	Proceso transversal crítico dada la dificultad práctica de revocar biometría comprometida y la dependencia del responsable respecto del proveedor para conocer el alcance técnico del evento.	No aparece con dueño interno nominal; sí se reconoce como necesidad expresa en los entregables.	DPD; TI; seguridad de la información; asesoría jurídica; alta dirección; encargado BioTrust.	Responsable sugerido por exigencia normativa y por la naturaleza del incidente.	PBL1 y PBL2 lo identifican como brecha crítica de gobernanza y respuesta.	Logs; evidencia forense; categorías comprometidas; datos de contacto para notificación; registro del incidente.	Datos biométricos; datos de menores; datos derivados; registros de seguridad.	Estudiantes menores; representantes; usuarios internos afectados.	No detección o notificación tardía; respuesta incompleta; imposibilidad práctica de neutralizar daño sobre biometría comprometida.	LOPDP arts. 46, 47, 65 a 68; RGLOPDP art. 24; Resolución SPDP-SPD-2025-0006-R en materia de obligaciones del encargado.	Requiere playbook, matriz de escalamiento y cooperación efectiva con el proveedor.	playbook aprobado, tiempos internos de respuesta y responsables de escalamiento