Maestría en

Protección de Datos

Trabajo de Investigación Previo a la Obtención del Título de Magíster en Protección de Datos

AUTORES:

Del Pozo Larrea Susan Fernanda

Fierro Poveda Israel Andrés

Lema Sarmiento Daniela Alejandra

Mieles Sarmiento Thalía Briggette

Peralta Villacres Cristhian Michael

Velástegui Garcés Sergio Javier

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 Entidades Públicas de Control Migratorio en Aeropuertos del Ecuador."

Quito, junio 2026

Certificación de Autoría

Nosotros, *Susan Del Pozo, Israel Fierro, Daniela Lema, Thalía Mieles, Cristhian Peralta y Sergio Velástegui* 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.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
SUSAN FERNANDA DEL POZO LARREA

Firma del graduando

Del Pozo Larrea Susan Fernanda

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ISRAEL ANDRES FIERRO POVEDA

Firma del graduando

Fierro Poveda Israel Andrés

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DANIELA ALEJANDRA LEMA SARMIENTO

Firma del graduando

Lema Sarmiento Daniela Alejandra

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
THALIA BRIGGETTE MIELES SARMIENTO

Firma del graduando

Mieles Sarmiento Thalía Briggette

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
CRISTHIAN MICHAEL PERALTA VILLACRES

Firma del graduando

Peralta Villacres Cristhian Michael

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
SERGIO JAVIER VELASTEGUI GARCES

Firma del graduando

Velástegui Garcés Sergio Javier

Autorización de Derechos de Propiedad Intelectual

Nosotros, *Susan Del Pozo, Israel Fierro, Daniela Lema, Thalía Mieles, Cristhian Peralta y Sergio Velástegui*, en calidad de autores del trabajo de in*vestigación titulado: "**Privacidad desde el Diseño y por Defecto: Aplicación al Uso de Biometría en el Escenario de Entidades Públicas de Control Migratorio en Aeropuertos del Ecuador"***, 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.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
SUSAN FERNANDA DEL POZO LARREA

Firma del graduando

Del Pozo Larrea Susan Fernanda

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
ISRAEL ANDRES FIERRO POVEDA

Firma del graduando

Fierro Poveda Israel Andrés

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DANIELA ALEJANDRA LEMA SARMIENTO

Firma del graduando

Lema Sarmiento Daniela Alejandra

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
THALIA BRIGGETTE MIELES SARMIENTO

Firma del graduando

Mieles Sarmiento Thalía Briggette

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
CRISTHIAN MICHAEL PERALTA VILLACRES

Firma del graduando

Peralta Villacres Cristhian Michael

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
SERGIO JAVIER VELASTEGUI GARCES

Firma del graduando

Velástegui Garcés Sergio Javier

Aprobación de Dirección y Coordinación del Programa

Nosotros, **Mayra Guerra y Jacqueline Guerrero Carrera, Coordinadora UIDE,** declaramos que los graduados: *Susan Del Pozo, Israel Fierro, Daniela Lema, Thalía Mieles, Cristhian Peralta y Sergio Velástegui*, 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

Mayra Guerra
Directora de la
Maestría en Protección de Datos

Jacqueline Guerrero
Coordinadora de la
Maestría en Protección de Datos

DEDICATORIA

"A mis padres, por su amor, apoyo constante y confianza en cada paso de este camino; a mis hermanas, por ser mi inspiración y la fuerza que me impulsó a alcanzar esta meta. Este logro también es de ustedes". ***Susan Fernanda Del Pozo Larrea.***

"Dedico este trabajo de titulación a mis hermanos Santiago y Leonardo Fierro Poveda quienes han sido el motor y la razón de mi esfuerzo, sacrificio y perseverancia a lo largo de este camino. Su cariño, apoyo y confianza me han impulsado a seguir adelante, incluso en los momentos más difíciles". ***Israel Andrés Fierro Poveda.***

"En primer lugar a Dios, al brindarme la oportunidad de acceder a mis estudios de cuarto nivel, una meta que tenía pendiente de cumplir hace mucho tiempo atrás, y que, por distintas circunstancias de la vida, no la había podido realizar inmediatamente. En segundo lugar, a mis padres, hermanos, familia y amigos, que creyeron fervientemente en que era posible cumplir con esta meta académica y profesional, que me abrirá paso a nuevas oportunidades a nivel personal y laboral". ***Daniela Lema.***

"Dedico este proyecto a mi esposo, por motivarme a iniciar esta maestría y acompañarme a lo largo de este camino académico con su apoyo incondicional, y aquellas personas que me inspiran día a día en mi desarrollo profesional, especialmente a quienes, desde el ámbito empresarial, promueven una cultura de respeto hacia los derechos de las personas". ***Thalía Mieles Sarmiento.***

"Dedicado a mi esposa y a mi hijo, quienes son mi principal fuente de inspiración." ***Cristhian Peralta Villacres.***

“Dedico este proyecto y este título a mis hijos y a mi esposa, quienes con su apoyo y amor me han dado la fuerza para conseguir este logro en mi vida profesional y personal”.

Sergio Velástegui.

AGRADECIMIENTOS

"A Dios, a mi familia, docentes y compañeros por ser el apoyo necesario para culminar esta meta con el éxito esperado" ***Susan Fernanda Del Pozo Larrea.***

"Quiero expresar mi más profundo agradecimiento a mis padres, Vinicio Fierro y Ximena Poveda, quienes han sido mi apoyo incondicional y el pilar fundamental en cada etapa de mi vida. Gracias por su amor, esfuerzo, sacrificio y confianza, que me han permitido superar los desafíos y alcanzar cada una de mis metas". ***Israel Andrés Fierro Poveda.***

"A Dios, a mi familia, amigos y docentes, pero por sobre todo, dedico este trabajo a mi padre Bolívar Lema, pilar fundamental en mi crecimiento personal, académico y profesional a lo largo de toda mi vida, y quién siempre anhelo estar presente al momento de la obtención de mi título de cuarto nivel, quién fue y siempre será mi apoyo incondicional, y quién me enseñó a no rendirme jamás, a esforzarme todo lo necesario para cumplir con las metas que me he propuesto y que me seguiré proponiendo a lo largo de este camino llamado vida y me enseñó de la resiliencia y fortaleza inquebrantable hasta el último día de su vida". ***Daniela Lema.***

"A Dios por ser mi guía y fortaleza, a mis docentes, compañeros y compañeras, por compartir sus conocimientos y experiencia, el intercambio de ideas y el trabajo en equipo fueron fundamentales para alcanzar esta meta y seguir mejorando cada día como profesionales de protección de datos." ***Thalía Mieles Sarmiento.***

"A Dios, a mis docentes, a mis compañeras y compañeros por compartir sus conocimientos y experiencia." ***Cristhian Peralta Villacres.***

“Agradezco a Nova Ecuador S.A. quienes también me apoyaron para la consecución de este logro. Así mismo agradezco a mis compañeros y compañeras quienes con su compromiso y dedicación también forman parte de este logro.” ***Sergio Velástegui***

RESUMEN

Esta investigación analiza la implementación de sistemas biométricos asistidos por inteligencia artificial en el control migratorio de aeropuertos ecuatorianos, bajo el marco de la Ley Orgánica de Protección de Datos Personales (LOPDP, 2021), en adelante LOPDP. El problema central radica en la naturaleza de los datos biométricos, clasificados como categorías especiales de datos sensibles por ser permanentes y únicos. El estudio examina cómo estos tratamientos masivos y sistemáticos exigen garantías reforzadas para evitar riesgos de vigilancia masiva o suplantación de identidad. Se busca equilibrar la eficiencia operativa con la tutela efectiva de la privacidad, enfrentando desafíos jurídicos y éticos significativos en la gestión de fronteras estatales.

El enfoque central se basa en los principios de privacidad desde el diseño y por defecto, aplicados al modelo de tratamiento ejecutado por la Entidad de Control Migratorio y su encargado tecnológico BioTrust. Se propone la integración de medidas técnicas y organizativas desde la fase de arquitectura de los sistemas para garantizar la minimización y limitación de la finalidad. Esto incluye el cifrado de plantillas biométricas, la retención limitada de datos y el uso de hardware seguro para proteger la información frente a accesos no autorizados. Estas salvaguardas operativas previenen el uso secundario de datos, asegurando que la modernización tecnológica no comprometa la dignidad humana.

La metodología de cumplimiento exige la ejecución de Evaluaciones de Impacto en la Protección de Datos (SPDP-SPD-2026-0012-R, 2026) y el mantenimiento de un inventario de actividades de tratamiento pormenorizado. Se establece una gobernanza institucional sólida mediante una matriz RACI que define roles y responsabilidades claras

entre el responsable público y los encargados tecnológicos privados. Un componente crítico es el Plan de Respuesta ante Incidentes, diseñado para gestionar vulnerabilidades de seguridad y fallos algorítmicos con plazos perentorios de notificación a la autoridad de control. Este marco organizativo fortalece la resiliencia institucional y asegura una gestión transparente que mitiga riesgos en el procesamiento automatizado de rasgos faciales.

Finalmente, se analiza el papel de la inteligencia artificial en la verificación migratoria, abordando específicamente los riesgos de sesgos algorítmicos y discriminación indirecta. Se enfatiza la necesidad de una supervisión humana efectiva para evitar decisiones totalmente automatizadas que afecten derechos fundamentales de los viajeros. El estudio concluye que la viabilidad jurídica de estos sistemas está condicionada al cumplimiento riguroso de la normativa y a la implementación de auditorías periódicas. Se propone un modelo de cumplimiento proactivo que proteja la autodeterminación informativa, garantizando que el uso de tecnologías avanzadas respete los estándares internacionales de seguridad y derechos digitales ciudadanos.

Palabras Clave: Biometría, Protección de Datos Personales, Evaluación de Impacto en la Protección de Datos, Control Migratorio, Inteligencia Artificial.

ABSTRACT

This investigation analyzes biometric systems assisted by artificial intelligence in Ecuadorian airports migration control, on Personal Data Protection Organic Law (LOPDP, 2021), currently. The main problem is about biometric data origin, classified like sensible data special categories, to be unique and permanent. The study exams like this massive and systematic treatments, must have effort garanties, to avoid risks of massive vigilance or identity supplantation. It researches equilibrium in the operative efficiency with the privacy effective protection, confronting juridic and ethic significant challenges in the state border management.

The central approach is based on privacy principles to the design and defect, applied to the treatment model executed by the control migratory entity and its technologic manager BioTrust. It proposes the integration of technical and organizational measures to the systems architecture phase to guarantee the finality minimization and limitation. This includes the biometric template encryption, the limited data conservation and the use of secure hardware to protect the information against denied access. These operational safeguards prevent the secondary use of data, ensuring that technological modernization doesn't compromise human dignity.

The compliance methodology demands the Data Protection Impact Assessments (DPIA) and the maintenancement of a detailed treatment activities inventory. It establishes a solid institutional governance through a RACI matrix that defines roles and clear responsibilities between the public responsible and the private technologic manager. A critical component is the Incidents Answer Plan, designed to manage secure vulnerabilities and algorithmic fails with the peremptory times to the notification of the

control authority. This organizational framework strives for institutional resilience and ensures a transparent management that mitigates risks in the automatized processment of facial features.

Finally, it analyzes the artificial intelligence role in the migratory verification, tackling specified risk algorithmic biases and indirect discrimination. It emphasizes the necessity of effective human supervision to avoid total automated decisions that affect the travelers fundamental rights. This study concludes that the juridic viability of these systems are conditioned to the rigorous compliance of the legal regulations and the periodic audits implementations. It proposes a proactive compliance model that protects the informative autodetermination, guaranteeing that the use of advanced technologies respect the secure international standards and citizens digital rights.

Keywords: Biometrics, Personal Data Protection, Data Protection Impact Assessment, Migration Control, Artificial Intelligence.

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

CAPÍTULO I

1. INTRODUCCIÓN

La implementación de un sistema de control migratorio asistido por inteligencia artificial en los aeropuertos del Ecuador representa un caso hipotético de tensión entre la eficiencia operativa de la entidad pública de control migratorio en los aeropuertos y la protección de los derechos fundamentales de los titulares de los datos personales.

El presente proyecto analiza de manera integral los desafíos jurídicos, administrativos, técnicos y organizacionales que surgen de la implementación y uso de sistemas que operan con inteligencia artificial y realizan reconocimiento facial, lectura de iris y huella dactilar para el registro de ingreso y salida de viajeros nacionales y extranjeros en aeropuertos del Ecuador.

A lo largo del presente proyecto, se analiza que los datos usados en el sistema de control migratorio no constituyen solamente datos personales, sino que se ubican dentro de la categoría especial de datos personales sensibles, lo que conlleva la aplicación de garantías reforzadas y deberes específicos para quienes realizan el tratamiento de estos.

A esta condición se suma que, la entidad pública de control migratorio asume el rol de responsable del tratamiento al definir las finalidades del control migratorio y de la seguridad nacional, mientras que BioTrust actúa como encargado del tratamiento, al ejecutar las operaciones técnicas de captura, almacenamiento y procesamiento de los datos. La distribución entre los integrantes del sistema de protección de datos, así como las garantías que deben tener la implementación del sistema de inteligencia artificial para control migratorio constituyen uno de los ejes centrales del proyecto.

Asimismo, se analizan los riesgos derivados de la utilización de inteligencia artificial en los sistemas biométricos, especialmente aquellos relacionados con la protección de los datos personales y los derechos de los titulares. En particular, se examinan los posibles sesgos algorítmicos, los errores de identificación, la discriminación indirecta hacia determinados grupos de viajeros y los desafíos de transparencia asociados al funcionamiento del sistema. La evaluación de estos riesgos permite determinar si el tratamiento de datos cumple con las garantías y principios establecidos en el ordenamiento jurídico ecuatoriano, determinando si es viable o no la implementación del sistema de IA para control migratorio.

El marco normativo que guía este análisis se encuentra encabezado por la Constitución de la República del Ecuador (CRE, 2008), que en su artículo 66 numeral 19 reconoce el derecho a la protección de datos personales y, en su artículo 92, establece la acción de hábeas data como garantía de su ejercicio, la Ley Orgánica de Protección de Datos Personales (LOPDP, 2021), en adelante LOPDP que constituye el eje central de la regulación, al definir los principios de licitud, finalidad, proporcionalidad, minimización y responsabilidad proactiva que deben observarse en el tratamiento de categorías especiales de datos, entre las que se encuentran los datos biométricos conforme al artículo 25; el Reglamento General a la LOPDP (RGLOPDP, 2023), en adelante RGLOPDP, por su parte, desarrolla las obligaciones de gobernanza, documentación y evaluación de impacto que resultan exigibles para la entidad pública de control migratorio en su calidad de responsable del tratamiento.

De igual forma, este proyecto destaca las resoluciones emitidas por la Superintendencia de Protección de Datos Personales, en adelante SPDP, que han delimitado de forma específica el alcance de las obligaciones aplicables al caso

analizado. Entre ellas la Resolución SPDP-SPD-2025-0006-R (SPDP-SPD-2025-0006-R, 2025), que establece la obligación de incorporar cláusulas de protección de datos personales en los contratos celebrados entre responsables y encargados del tratamiento; la Resolución SPDP-SPD-2026-0005-R (SPDP-SPD-2026-0005-R, 2026), que califica el tratamiento de datos biométricos en aeropuertos como un tratamiento a gran escala; y la Resolución SPDP-SPD-2026-0009-R, que fija obligaciones específicas para los sistemas de inteligencia artificial que procesan datos personales, particularmente en lo relativo a la información clara a los titulares y a la supervisión humana significativa de las decisiones automatizadas. Además, se detallan dos guías elaboradas por la propia SPDP que, sin tener el carácter vinculante de una resolución, ofrecen pautas concretas para la implementación de sistema, siendo estas: la Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales, que establece la metodología a seguir para elaborar la Evaluación de Impacto de Protección de Datos, en adelante EIPD, y la Guía de Protección de Datos Personales desde el Diseño y por Defecto (SPDP-SPD-2025-0040-R, 2025), que desarrolla en términos prácticos la aplicación de este principio previsto en el artículo 39 de la LOPDP.

A partir de este marco, el proyecto se orienta a determinar si la implementación del sistema biométrico con inteligencia artificial en el control migratorio aeroportuario resulta jurídicamente viable y, de serlo, bajo qué condiciones. Para ello, se integra el análisis normativo desarrollado en los entregables previos con una valoración de riesgos y un dictamen jurídico final, que pondera la finalidad de seguridad nacional e interés público frente a los derechos de los titulares. La hipótesis que articula el trabajo sostiene que el proyecto, si bien responde a fines legítimos y constitucionalmente admisibles, requiere de la materialización efectiva de medidas de responsabilidad proactiva, tales como la EIPD, el Registro de Actividades de Tratamiento, en adelante RAT, la

designación de un Delegado de Protección de Datos, en adelante DPD, y la aplicación del principio de privacidad desde el diseño y por defecto, para que su operación resulte plenamente compatible con las disposiciones normativas ecuatorianas e internacionales aplicables a la materia.

2. MARCO METODOLÓGICO

2.1 Presentación y Planteamiento del Problema

2.1.1 Antecedentes

Una organización integradora (“BioTrust”) provee servicios biométricos a clientes públicos y privados. BioTrust ofrece captura (cámaras/lectores), plantillas biométricas y verificación con motores de inteligencia artificial (detección de vida, antifraude, matching 1:1 y 1:N). Opera con nube híbrida y subcontratistas. Cada cliente define finalidades distintas, pero BioTrust centraliza soporte, monitoreo y actualizaciones del modelo. La presión comercial exige despliegue rápido; el área legal advierte sensibilidad del dato, necesidad de bases legales claras, medidas de seguridad y gobernanza de inteligencia artificial.

BioTrust enfrenta una decisión estratégica: continuar y ampliar el uso biométrico en entidades que ya lo usan, como en el sector público, y comenzar implementaciones nuevas, como hospitales o instituciones educativas, además de consolidar los servicios en entidades privadas, como bancos, aseguradoras o empresas de seguridad. El desafío no es solo técnico; es de protección de datos personales, gobernanza de terceros y control del riesgo, especialmente porque la biometría es difícil de “revocar”: si se

compromete una plantilla facial o una huella, la persona no puede cambiarla como una contraseña.

El primer punto de quiebre es la finalidad y proporcionalidad. En la entidad pública de control migratorio de aeropuertos, donde “la utilización es real”, la decisión se centra en si el sistema actual cumple con el marco normativo, transparencia y seguridad: no basta con “ya existe”, debe probarse que se ajusta a principios de licitud, minimización y seguridad.

A nivel operacional, BioTrust debe decidir el modelo de tratamiento: ¿centraliza plantillas biométricas para todos los clientes o permite almacenamiento local por cliente? Centralizar facilita el soporte, pero aumenta el “single point of failure” y hace más compleja la segregación. Un incidente afectaría a múltiples entidades. Una arquitectura “privacy by design” tendería a: almacenar solo plantillas (no imágenes crudas), cifrar en reposo y tránsito, utilizar hardware seguro (HSM), limitar accesos por roles, y cuando sea viable realizar matching en el dispositivo o en el dominio del cliente (especialmente para hospital y banco). También se debe definir retención: conservar datos biométricos solo el tiempo indispensable, con borrado verificable al finalizar vínculo (alta médica, egreso escolar, cierre de cuenta, baja laboral, mudanza).

En paralelo aparece la dimensión de inteligencia artificial. El motor de reconocimiento facial y detección de vida introduce riesgos de sesgo y rendimiento desigual según iluminación, edad, tonalidades de piel, dispositivos y condiciones médicas. Una decisión responsable exige evidencias: tasas de error, pruebas en condiciones reales, calibración de umbrales, monitoreo de drift y auditorías periódicas. En instituciones como un hospital el umbral debe priorizar seguridad, evitar accesos

indebidos, sin bloquear la atención clínica; en los bancos el umbral debe equilibrar antifraude con inclusión. En las instituciones educativas, incluso con buen desempeño, la pregunta vuelve a la necesidad: un sistema “preciso” puede seguir siendo desproporcionado.

2.1.2 Delimitación del Problema

El presente trabajo de investigación se limita al análisis jurídico y técnico de la aplicación de los principios de privacidad desde el diseño y privacidad por defecto en el uso de sistemas biométricos implementados en entidades públicas de control migratorio ubicadas en aeropuertos de Ecuador, durante el periodo comprendido entre la entrada en vigencia de la LOPDP publicada en el Registro Oficial Suplemento N.º 459 el 26 de mayo del 2021 a mayo del 2026. El estudio se desarrolla desde una perspectiva jurídica y doctrinal orientada a examinar la forma en que dichos principios deben materializarse en operaciones de tratamiento de datos biométricos considerados categorías especiales de datos personales.

En su dimensión normativa y temporal, la investigación se limita al análisis de la LOPDP (LOPDP, 2021), el RGLOPDP (RGLOPDP, 2023), así como a los lineamientos, resoluciones, guías y criterios técnicos emitidos por la SPDP hasta mayo del 2026. En su dimensión internacional de referencia, el análisis incorpora el Reglamento General de Protección de Datos de la Unión Europea (RGPD) - Reglamento UE 2016/679, no como marco normativo aplicable en Ecuador, sino como instrumento de interpretación analógica y como fuente doctrinaria de casos sancionatorios resueltos por autoridades de control europeas en materia de tratamiento del uso de datos biométricos para control migratorio en aeropuertos a nivel internacional, evaluación de impacto y gobernanza de

encargados; dicho soft law (resoluciones sancionatorias), si bien carecen de fuerza vinculante extraterritorial respecto del Ecuador, no constituyen jurisprudencia en sentido técnico-formal, conforman un cuerpo de doctrina para identificar criterios de cumplimiento y estándares de proporcionalidad aplicados a tratamientos biométricos funcionalmente análogos al que plantea el caso objeto de investigación, contribuyendo así a anticipar riesgos regulatorios que el ordenamiento ecuatoriano aún no ha consolidado en su aplicación práctica. De manera complementaria, como parámetros técnicos de referencia para evaluar el cumplimiento del principio de responsabilidad proactiva previsto en el artículo 10, literal k), de la LOPDP se consideran los estándares ISO/IEC 27001 referente a Sistema de gestión de seguridad de la información e ISO/IEC 27701 aplicable al Sistema de Gestión de Privacidad de la Información. Quedan fuera del marco de análisis otras legislaciones nacionales o extranjeras estudiadas desde una perspectiva comparada, así como normativa sectorial no vinculada directamente al tratamiento de datos biométricos en el contexto de control migratorio.

Desde la delimitación espacial y material, la investigación se circunscribe a entidades públicas de control migratorio que operan en aeropuertos de Ecuador, en atención a su calidad de responsables del tratamiento de conformidad al artículo 4 de la LOPDP, y a la naturaleza de estos entornos como espacios de tratamiento masivo, sistemático y continuo de datos personales sensibles.

En cuanto a la licitud del tratamiento, la investigación parte del análisis del artículo 7, numeral 4 de la LOPDP, que habilita el tratamiento de datos personales cuando este sea necesario para el cumplimiento de una misión realizada en interés público o en ejercicio de potestades públicas conferidas por una norma con rango de ley. Dicha habilitación se examina en relación con la Ley Orgánica de Movilidad Humana (LOMH,

2018), publicada en el Registro Oficial Suplemento N.º 938 del 6 de febrero de 2017, que atribuye a las autoridades migratorias funciones de identificación, verificación y registro de personas en los puntos de ingreso y salida de ciudadanos del territorio nacional.

No obstante, el objeto de estudio no se limita a la existencia de una base legal habilitante para la legitimación del tratamiento de datos biométricos, sino que se concentra en determinar cómo dicha habilitación debe articularse con el cumplimiento de los principios de finalidad, minimización, proporcionalidad, privacidad desde el diseño y privacidad por defecto, así como con la obligación de realizar evaluaciones de impacto previas al tratamiento de categorías especiales de datos, conforme a la LOPDP y la correcta aplicación de un sistema de gobernanza de protección de datos personales.

Este estudio adopta como caso jurídico de referencia el modelo de tratamiento implementado por un proveedor privado, enfocado en el procesamiento de datos biométricos tales como: rasgos faciales, iris y huellas dactilares mediante sistemas de inteligencia artificial para procesos de verificación 1:1 y 1:N, bajo esquemas de infraestructura en nube híbrida, con su participación como encargado del tratamiento de datos personales de conformidad al artículo 4 de la LOPDP y la participación de terceros subencargados.

Finalmente, esta investigación analiza las tensiones jurídicas derivadas de la aplicación de los principios de finalidad, necesidad, proporcionalidad, seguridad y responsabilidad proactiva en el tratamiento de datos biométricos, particularmente frente a la participación de múltiples actores dentro de la cadena de tratamiento y al riesgo del uso de los datos biométricos de los ciudadanos para finalidades distintas a aquellas que justifican el control migratorio. La investigación no se extiende al estudio de sistemas

biométricos utilizados por entidades privadas, controles de acceso corporativo, ni a aspectos comerciales, financieros o técnicos que no incidan directamente en el análisis jurídico del caso objeto de estudio.

Es importante señalar que el presente trabajo constituye un ejercicio académico de análisis jurídico sobre un escenario hipotético. La referencia a entidades públicas de control migratorio en aeropuertos de Ecuador cumple una función ilustrativa y metodológica, orientada a contextualizar el análisis normativo en un entorno de tratamiento masivo y sistemático de datos biométricos.

2.2. Justificación

Desde la perspectiva legal, esta investigación es de vital importancia debido al acelerado y exigente desarrollo del ecosistema regulatorio en el Ecuador. Regido por la Constitución, la LOPDP, el RGLOPDP y la normativa secundaria, la administración pública enfrenta la obligación de aplicar la responsabilidad proactiva a través de medidas técnicas y organizativas desde el diseño mismo de sus sistemas. Este deber se profundiza con la Resolución SPDP-SPD-2026-0009-R emitida por la SPDP, la cual vuelve obligatoria la ejecución de una EIPD previa para todo tratamiento automatizado de datos biométricos a gran escala y asistido por inteligencia artificial. Frente a posibles vulnerabilidades, el marco normativo determina plazos perentorios punibles para la notificación de incidentes. Por consiguiente, este estudio se consolida como un modelo técnico y preventivo esencial para salvaguardar la confidencialidad, evitando sanciones leves y graves.

El impacto social de esta investigación posee un carácter integral al referirse al tratamiento técnico de flujos migratorios de pasajeros nacionales y extranjeros, salvaguardando a colectivos vulnerables. Desde la perspectiva de la protección de datos, la tutela de la biometría es imperativa debido a su naturaleza sensible, permanente e irreversible; a diferencia de una contraseña, los rasgos y características físicas no pueden modificarse. El compromiso de estas plantillas expone al titular al riesgo de persecuciones injustas por falsos positivos algorítmicos. Por ello, este estudio se justifica socialmente como un mecanismo de defensa de los derechos humanos a la igualdad, la dignidad y el debido proceso, impidiendo de forma categórica que los aeropuertos del país se conviertan en espacios de vigilancia masiva desproporcionada.

La justificación tecnológica de esta investigación radica en analizar una arquitectura de software con niveles de amenaza inaceptables, donde la inteligencia artificial usada en control fronterizo goce de veracidad, independencia externa y aciertos algorítmicos. El mapa de riesgos devela amenazas residuales críticas en la confidencialidad de la plataforma con BioTrust y con los demás organismos que intervienen en este ejercicio de tratamiento. Frente a esto, la investigación aplica la privacidad desde el diseño para integrar controles completos, como cifrado, minimización y sistemas adecuados que mitigan las vulnerabilidades de forma previa al despliegue operativo del sistema a gran escala.

La investigación adopta como referente el caso de los Aeropuertos Españoles y Navegación Aérea (AENA) de la Agencia Española de Protección de Datos (AEPD) por excluir las arquitecturas biométricas centralizadas y obligar a una alternativa analógica. Aunque en el Ecuador en este caso, se opera bajo potestades de seguridad nacional, la naturaleza pública de la entidad no mitiga la vulnerabilidad técnica ni el riesgo residual

en el sistema gestionado con BioTrust. Finalmente, se garantiza la operatividad institucional mediante un protocolo de contingencia ante fallos de la inteligencia artificial, evitando el colapso del flujo aeroportuario sin sacrificar la tutela de los datos personales de los viajeros.

2.3. Problemas Jurídicos

¿Es jurídicamente viable la implementación de un sistema de biometría en las entidades públicas de control de migratorio de aeropuertos del Ecuador, 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 las entidades públicas de control de migratorio de aeropuertos del Ecuador, 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 EIPD justificar que el riesgo residual del uso de biometría es aceptable y controlable, o corresponde recomendar su no implementación o su uso condicionado?

2.4. Objetivos

2.4.1 Objetivo General

Determinar la viabilidad jurídica y la conveniencia del uso de sistemas de biometría en las entidades públicas de control de migratorio de aeropuertos del Ecuador, a la luz de la normativa y principios de protección de datos personales, a fin de formular una conclusión jurídica fundamentada sobre la viabilidad, no viabilidad o viabilidad

condicionada y elaborar recomendaciones conforme al principio de privacidad desde el diseño y por defecto, incluso para el supuesto de que la organización decida avanzar pese a un resultado negativo de la EIPD.

2.4.2 Objetivos Específicos

Evaluar el marco normativo aplicable al tratamiento de datos biométricos mediante sistemas de biometría, identificando las bases jurídicas que podrían legitimar su uso por parte de las entidades públicas de control de migratorio de aeropuertos del Ecuador, considerando tanto la legislación general de protección de datos como la normativa sectorial correspondiente.

Identificar la naturaleza de los datos biométricos como datos personales sensibles o de categoría especial, y determinar las implicaciones jurídicas derivadas de su tratamiento en un modelo multidentidad, especialmente en cuanto a restricciones, garantías reforzadas y deberes del responsable.

Establecer las implicaciones jurídicas del uso de inteligencia artificial en sistemas de biometría, en particular en relación con riesgos de sesgo algorítmico, errores de identificación, discriminación indirecta y transparencia del tratamiento.

Identificar y ponderar los posibles impactos del uso de biometría en los derechos fundamentales de los titulares de los datos, incluyendo el derecho a la privacidad, la protección de datos personales, la no discriminación y la autodeterminación informativa.

3. FUNDAMENTOS TEÓRICOS

3.1. Privacidad y Protección de Datos Personales: Una Visión Global, Regional y Local

El avance de la inteligencia artificial y la utilización de datos biométricos en sistemas de control de ingreso y salida de personas en aeropuertos plantea un desafío jurídico y ético de gran magnitud. La biometría, al tratarse de información sensible vinculada directamente con la identidad física y única de cada individuo, requiere un marco normativo sólido que garantice la protección de derechos fundamentales como la privacidad, la autodeterminación informativa y la protección de datos personales, siendo este último derecho, aquel que no se agota en la tutela de la intimidad ni en la capacidad del individuo de controlar su información, sino que impone obligaciones activas a quienes tratan datos, establece principios que rigen todo el ciclo de vida del tratamiento y confiere a los titulares un conjunto de derechos que pueden ser ejercidos frente a los responsables del tratamiento.

Este punto aborda el tema desde tres perspectivas: global, regional y local, con especial énfasis en la legislación ecuatoriana y su aplicación en proyectos aeroportuarios.

Visión Global: Estándares Internacionales

En el ámbito internacional, el Reglamento General de Protección de la Unión Europea de Datos (RGPD) constituye el referente más robusto en materia de protección de datos. El RGPD clasifica los datos biométricos como “categorías especiales”, cuyo tratamiento solo es permitido bajo condiciones estrictas: consentimiento explícito, interés público o seguridad nacional.

La Organización de las Naciones Unidas (ONU) y la Organización para la Cooperación y el Desarrollo Económicos (OCDE) han promovido principios universales como la transparencia, la proporcionalidad y la minimización de datos, que buscan evitar la vigilancia masiva y el uso indebido de tecnologías de reconocimiento facial.

En este contexto, los aeropuertos que implementan sistemas biométricos deben garantizar que la recopilación y almacenamiento de datos se limite a lo estrictamente necesario, evitando la creación de bases de datos que puedan ser vulneradas o utilizadas con fines distintos a la seguridad aeroportuaria.

Visión Regional: América Latina

En América Latina, la protección de datos personales ha avanzado de manera desigual. Países como Brasil con su Ley General de Protección de Datos (LGPD, 2020) y México con su Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPD, 2010), han establecido marcos normativos que reconocen la biometría como dato sensible y regulan su uso en transporte y seguridad.

La Organización de los Estados Americanos (OEA) impulsó en 2015 una Ley Modelo sobre Protección de Datos Personales (OEA, 2015), que inspiró reformas en varios países de la región. Asimismo, la Red Iberoamericana de Protección de Datos fomenta la cooperación entre autoridades nacionales para armonizar estándares.

Sin embargo, persisten retos, tales como: la falta de recursos institucionales para supervisar el cumplimiento, la escasa cultura de privacidad en la ciudadanía y la presión de intereses económicos y de seguridad que tienden a priorizar la eficiencia sobre la protección de derechos.

Visión Local: Ecuador

En Ecuador, la LOPDP constituye el marco jurídico principal. Esta ley reconoce los datos biométricos como sensibles, estableciendo que su tratamiento requiere consentimiento expreso, salvo excepciones vinculadas a la seguridad pública o al interés nacional. La normativa ecuatoriana introduce principios fundamentales:

- **Legalidad y Finalidad Específica**: Los datos biométricos solo pueden ser usados para el control de ingreso y salida en aeropuertos, no para otros fines.
- **Proporcionalidad y Minimización**: Se deben recolectar únicamente los datos estrictamente necesarios.
- **Seguridad Tecnológica**: Obligación de implementar cifrado, anonimización y protocolos de protección contra accesos no autorizados.
- **Derechos**: Los ciudadanos pueden ejercer derechos de acceso, rectificación, eliminación, oposición entre otros establecidos en la LOPDP.

La SPDP supervisa el cumplimiento de estas disposiciones, aunque enfrenta el reto de consolidar su capacidad institucional y técnica para fiscalizar proyectos de gran escala (SPDP-SPD-2026-0005-R, 2026) como los aeroportuarios.

Fundamento Jurídico y Retos

El fundamento jurídico de la protección de datos biométricos en Ecuador se basa en la CRE del 2008 (CRE, 2008), que reconoce el derecho a la protección de datos personales y a la intimidad, la LOPDP, que desarrolla este derecho y lo articula con estándares internacionales, los tratados internacionales ratificados por Ecuador, como el Pacto Internacional de Derechos Civiles y Políticos, que garantizan la privacidad, así como también, la Resolución Nro. SPDP-SPD-2026-0009-R, que establece la Norma

General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial (SPDP-SPD-2026-0009-R, 2026), expedida por la SPDP.

Entre los principales retos se incluyen: mantener el equilibrio entre seguridad y privacidad, garantizando la eficiencia en el control aeroportuario sin caer en vigilancia excesiva; posibles riesgos tecnológicos, como filtraciones de bases de datos biométricas y sesgos en algoritmos de reconocimiento facial; y, la necesidad de educar a la ciudadanía sobre sus derechos y a las instituciones sobre sus obligaciones.

La implementación de sistemas biométricos e inteligencia artificial en aeropuertos ecuatorianos debe alinearse con estándares globales, regionales y locales. Debido a esto, consideramos que la legislación ecuatoriana ofrece un marco sólido, pero su eficacia dependerá de la correcta aplicación tecnológica, la supervisión estatal y la garantía de derechos ciudadanos.

El desafío central es lograr un equilibrio entre seguridad aeroportuaria y protección de la privacidad, evitando que la eficiencia tecnológica se convierta en un riesgo para las libertades individuales.

3.2. Desafíos de la Privacidad y Protección de Datos Personales en el Ecuador

La acelerada incorporación de inteligencia artificial y tecnologías biométricas en sistemas de control de ingreso y salida de personas en aeropuertos plantea un dilema crucial cómo garantizar la seguridad y eficiencia en la movilidad internacional sin vulnerar derechos fundamentales como la privacidad y la autodeterminación informativa.

La LOPDP constituye el marco jurídico principal para enfrentar estos desafíos. Sin embargo, la aplicación práctica de esta normativa en proyectos de gran escala como los

aeroportuarios revela tensiones entre la necesidad de seguridad y la protección de derechos ciudadanos.

En el Ecuador, al igual que en otros países, se ha incorporado tecnologías avanzadas para optimizar la gestión aeroportuaria. El uso de datos biométricos e inteligencia artificial permite agilizar procesos de ingreso y salida de pasajeros, reducir riesgos de suplantación y fortalecer la seguridad nacional. Sin embargo, estas innovaciones plantean desafíos jurídicos y éticos relacionados con la privacidad, el consentimiento y la proporcionalidad en el tratamiento de datos personales.

Fundamento Teórico

Para entender los desafíos de la privacidad y protección de datos personales, es importante conocer los diferentes conceptos que engloban el caso objeto de estudio, tales como: los datos biométricos, que constituyen información inherente e irrenunciable de cada individuo, pues a diferencia de una contraseña o un documento de identidad, no pueden ser modificados ni sustituidos en caso de vulneración; huellas dactilares, geometría facial, iris y patrones de voz permiten una identificación inequívoca, lo que los convierte en activos de alto valor para sistemas de control migratorio, pero también en objetivos privilegiados de ataques y usos indebidos. La LOPDP en su artículo 25 clasifica a los datos biométricos como categorías especiales de datos precisamente porque su exposición o tratamiento inadecuado puede afectar de forma grave la intimidad, la dignidad y la seguridad personal de sus titulares, con consecuencias que, a diferencia de otras vulneraciones, son irreversibles.

Por otro lado, se encuentran los sistemas de inteligencia artificial aplicados al reconocimiento biométrico, que procesan volúmenes de datos en tiempo real mediante modelos de aprendizaje automático que comparan rasgos capturados con bases de

datos de referencia. Esta capacidad optimiza los procesos de verificación de identidad en entornos de alta afluencia como los aeropuertos, pero introduce riesgos que no pueden ser ignorados desde una perspectiva jurídica, los sesgos algorítmicos, especialmente frente a personas de determinadas etnias o géneros, pueden generar errores de identificación que deriven en restricciones injustificadas al ejercicio de derechos. A esto se suma el riesgo de vigilancia masiva, pues un sistema diseñado para verificar identidades puede, si no está debidamente ajustado en su finalidad, convertirse en un instrumento de seguimiento continuo de la población. El análisis jurídico de estos sistemas no puede limitarse a constatar su eficiencia técnica; debe evaluar si su diseño y operación son compatibles con los principios de proporcionalidad, minimización y limitación de finalidad.

Asimismo, la LOPDP recoge, en buena medida, la arquitectura normativa del Reglamento General de Protección de Datos de la Unión Europea (RGPD), mediante principios como: legalidad, finalidad, minimización, exactitud, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva, los cuales constituyen obligaciones que condicionan la validez jurídica de cualquier operación de tratamiento. En el contexto del tratamiento biométrico para control migratorio en aeropuertos, estos principios operan como límites que el responsable del tratamiento debe observar desde la fase de diseño del sistema (privacy by design), no como controles posteriores a su implementación.

Fundamento Jurídico en Ecuador

El artículo 66, numeral 19 de la Constitución de la República del Ecuador (CRE, 2008) reconoce el derecho a la protección de datos personales como un derecho fundamental autónomo, distinto del derecho a la privacidad. Esta distinción implica que

el Estado no solo debe abstenerse de vulnerar la intimidad de las personas, sino que está obligado a garantizar activamente que cualquier tratamiento de datos, incluso el realizado por entidades públicas en ejercicio de potestades legítimas, respete los principios, derechos y garantías que la ley establece.

En el marco normativo ecuatoriano, la LOPDP constituye el eje normativo central de este análisis. Las disposiciones más relevantes para el caso estudiado son: la calificación de los datos biométricos como categorías especiales que requieren medidas reforzadas de seguridad y una base de legitimación específica; la habilitación del tratamiento en contextos de interés público o ejercicio de potestades públicas, conforme al artículo 7, numeral 4, que desplaza, pero no elimina, la exigencia del consentimiento individual; el principio de proporcionalidad, que exige que el tratamiento sea estrictamente necesario para la finalidad declarada; y, la obligación de realizar las EIPD previas al tratamiento de categorías especiales de datos. Estos elementos constituyen un sistema integrado que el responsable del tratamiento, en el presente caso la entidad pública de control migratorio debe implementar, gestionar y supervisar de manera continua para garantizar la licitud del tratamiento de datos personales y la protección efectiva de los derechos de sus titulares.

En el Ecuador, la SPDP es el órgano encargado de supervisar el cumplimiento de la LOPDP y su reglamento, emitir lineamientos técnicos y sancionar el cometimiento de infracciones de responsables y encargados del tratamiento o terceros relacionados. En el contexto del tratamiento biométrico mediante sistemas de inteligencia artificial para control migratorio en aeropuertos, su rol es relevante porque los sistemas involucrados operan sobre categorías especiales de datos, procesan información de forma masiva y

continua, y participan en ellos múltiples actores, tales como: responsables, encargados y subencargados, cuya cadena de responsabilidad debe ser claramente delimitada.

Desafíos de la Privacidad en Aeropuertos

En los aeropuertos, la lógica del consentimiento libre e informado enfrenta una tensión para los derechos y libertades del titular, ya que el pasajero que desea ejercer su derecho a la movilidad no tiene, en la práctica, una alternativa real al sometimiento al sistema biométrico. Esta situación plantea la pregunta de si el consentimiento prestado en ese contexto cumple los requisitos de libertad, especificidad e inequivocidad que exige la LOPDP. Cuando el tratamiento se fundamenta en el interés público o en el ejercicio de potestades legales, como ocurre en el control migratorio, el consentimiento deja de ser la base legitimadora, lo que no exime al responsable de garantizar transparencia, proporcionalidad y respeto a los derechos de los titulares.

Las bases de datos biométricas representan un riesgo de seguridad distinto al de otros tipos de datos personales. Una filtración de datos financieros puede mitigarse cambiando cuentas o tarjetas; una filtración de datos biométricos es, por definición, irreparable. Este carácter irreversible del daño justifica que la LOPDP imponga medidas de seguridad reforzadas y que los principios de privacidad desde el diseño y privacidad por defecto no sean opcionales, sino exigibles desde la arquitectura misma del sistema, considerando el principio de privacidad desde el diseño y por defecto.

Los aeropuertos operan en un entorno de interconexión global que implica de manera frecuente la transferencia de datos biométricos a sistemas de otros países o a proveedores de infraestructura tecnológica ubicados en el extranjero. La LOPDP establece condiciones específicas para las transferencias internacionales, exigiendo

que el país receptor ofrezca niveles de protección equivalentes o que se adopten garantías adecuadas. En la práctica, verificar el cumplimiento de estas condiciones cuando intervienen subencargados en múltiples jurisdicciones es uno de los desafíos más complejos de la gobernanza de datos dentro de las organizaciones.

Los sistemas de reconocimiento facial han sido objeto de cuestionamientos técnicos y jurídicos a nivel internacional por presentar tasas de error significativamente altas en personas de determinadas etnias, géneros o edades. Desde una perspectiva jurídica, estos sesgos no son únicamente un problema técnico que deba resolver el proveedor del sistema, sino que, constituyen un riesgo de vulneración al derecho de igualdad y no discriminación. El responsable del tratamiento tiene la obligación de verificar, antes de implementar el sistema y de forma periódica durante su operación, que los modelos utilizados no introducen ni propagan sesgos discriminatorios.

El desafío más relevante, desde la perspectiva de derechos fundamentales es el riesgo de que un sistema diseñado para un fin legítimo derive, por la progresividad de su uso en un instrumento de vigilancia masiva de la población. Este fenómeno, conocido en la doctrina como función creep o expansión de finalidad, constituye una de las amenazas más serias para el derecho a la protección de datos en entornos de tratamiento biométrico a gran escala, y es precisamente el tipo de riesgo que la obligación de realizar EIPD pretende anticipar y controlar.

El Ecuador enfrenta un reto crucial de armonizar la eficiencia y seguridad aeroportuaria con la protección de derechos fundamentales. La LOPDP ofrece un marco robusto, pero su aplicación práctica requiere, estrategias claras de minimización de datos, protocolos de auditoría y transparencia algorítmica, cooperación internacional

con estándares equivalentes y campañas de educación ciudadana y sensibilización sobre derechos digitales.

En definitiva, el desafío no es tecnológico, sino jurídico y ético, ya que los actores del sistema de protección de datos deben garantizar que la innovación para la actividad de control migratorio de los ciudadanos en aeropuertos no erosione la privacidad de los titulares de los datos personales.

3.3. Evolución Tecnológica y Protección de Datos:

El Papel de la Inteligencia Artificial en el Tratamiento de Datos Personales

La acelerada evolución tecnológica ha transformado la manera en que los Estados gestionan los flujos de control migratorios. En aeropuertos internacionales, los sistemas de control de ingreso y salida de personas se han sofisticado mediante el uso de biometría, reconocimiento facial, análisis predictivo, todo ello con inteligencia artificial. Estos avances, aunque prometen eficiencia y seguridad, conllevan desafíos jurídicos y técnicos en materia de protección de datos personales.

En este contexto, la LOPDP y las directrices emitidas por la SPDP conforman el marco normativo aplicable al tratamiento de datos sensibles en los procesos de control migratorio. Este marco proporciona el sustento teórico y jurídico para examinar la interacción entre las tecnologías basadas en inteligencia artificial y el tratamiento de datos personales, así como para analizar los principios de protección de datos que rigen estas actividades, los riesgos derivados de su utilización en los controles migratorios aeroportuarios y las obligaciones legales que deben cumplir tanto las entidades operadoras como los proveedores de servicios tecnológicos.

Evolución Tecnológica en el Control Migratorio

El control migratorio ha experimentado una transformación significativa a nivel global, pasando de procesos manuales basados en documentos físicos a sistemas digitales interconectados. Entre las tecnologías que han impulsado esta evolución se encuentran: el uso de huellas dactilares, iris y reconocimiento facial permite verificar identidades con rapidez y precisión; el análisis masivo de información sobre viajes, antecedentes y perfiles de riesgo facilita la toma de decisiones en tiempo real y, los algoritmos capaces de predecir patrones de movilidad, detectar anomalías y optimizar procesos de seguridad.

A efectos del presente estudio, se propone como caso de análisis el supuesto en que una entidad pública competente en materia de control migratorio adoptara estas tecnologías en aeropuertos de Ecuador, integrando bases de datos nacionales e internacionales. Este escenario hipotético, permite examinar las exigencias jurídicas que derivarían de un tratamiento de datos personales a gran escala bajo el marco de la LOPDP.

Fundamento Teórico de la Protección de Datos Personales

La protección de datos personales se fundamenta en el derecho a la privacidad y a la autodeterminación informativa. Desde una perspectiva teórica, la privacidad es el derecho fundamental que garantiza el control sobre la información propia y la autodeterminación informativa, es la capacidad de decidir cómo, cuándo y para qué se usan los datos personales.

La inteligencia artificial introduce un reto adicional, donde los algoritmos pueden generar perfiles y predicciones que exceden la finalidad original del tratamiento de datos, lo que exige mecanismos de supervisión y auditoría.

Marco Jurídico Ecuatoriano

La LOPDP establece los principios y obligaciones para el tratamiento de datos en Ecuador. Sus aspectos más relevantes para proyectos migratorios son:

Datos Sensibles: biométricos, de salud y origen étnico requieren protección reforzada.

Consentimiento: debe ser libre, informado y explícito, salvo excepciones legales como seguridad nacional.

Responsabilidad Proactiva: las autoridades deben demostrar cumplimiento mediante evaluaciones de impacto.

Derechos: acceso, rectificación, eliminación, oposición y las demás constantes en la LOPDP.

La SPDP supervisa el cumplimiento de estas normas, emite directrices y puede imponer sanciones por vulneraciones.

El Papel de la Inteligencia Artificial en el Tratamiento de Datos Personales

La inteligencia artificial en aeropuertos ecuatorianos puede desempeñar varios roles: reconocimiento facial, que agiliza el paso de pasajeros, pero implica riesgos de vigilancia masiva; análisis predictivo, identifica patrones sospechosos, aunque puede generar sesgos discriminatorios; automatización de procesos, que reduce tiempos de espera y errores humanos; y, la interoperabilidad, que conecta sistemas nacionales e internacionales, aumentando la exposición de datos.

El desafío jurídico es garantizar que estos usos respeten los principios de proporcionalidad y finalidad, evitando que la IA se convierta en un mecanismo de control desmedido.

Riesgos y Desafíos

El uso de inteligencia artificial en el tratamiento de datos personales en aeropuertos presenta riesgos como: sesgos algorítmicos, que involucra discriminación por género, raza o nacionalidad; vigilancia masiva, que erosiona la privacidad de los ciudadanos; ciberseguridad, donde se podría presen; así como, la dificultad para auditar decisiones automatizadas.

La legislación ecuatoriana exige la EIPD para proyectos de alto riesgo, como los sistemas migratorios basados en inteligencia artificial.

Perspectiva Comparada

Otros países han enfrentado desafíos similares, por ejemplo: en la Unión Europea, el Reglamento General de Protección de Datos (RGPD) establece límites claros al uso de inteligencia artificial en datos sensibles; en Estados Unidos, la ausencia de una ley federal integral ha generado debates sobre el uso de reconocimiento facial en aeropuertos.

Ecuador, al adoptar la LOPDP, se alinea con estándares internacionales; sin embargo, enfrenta retos de implementación y capacitación institucional.

La evolución tecnológica en el control migratorio ofrece beneficios indiscutibles en eficiencia y seguridad, pero también plantea riesgos significativos para la protección de datos personales. La inteligencia artificial, como herramienta de tratamiento masivo de

información, debe ser regulada bajo principios de legalidad, proporcionalidad y transparencia. En Ecuador, la LOPDP y la supervisión de la SPDP constituyen un marco sólido, aunque su efectividad dependerá de la capacidad institucional para auditar algoritmos, garantizar derechos y prevenir abusos.

El equilibrio entre seguridad nacional y protección de derechos fundamentales será el eje central de los debates futuros. La clave está en diseñar sistemas de control migratorio que aprovechen la inteligencia artificial sin sacrificar la privacidad y la dignidad de las personas.

3.4. Biometría: aproximación conceptual y jurídica

3.4.1. Sistemas y datos biométricos

La biometría es definida según la Real Academia Española (RAE), como el estudio mensurativo o estadístico de fenómenos biológicos. De igual manera, el Instituto Nacional de Tecnologías de la Comunicación (INTECO), señala que la misma constituye un método de reconocimiento de personas basado en características fisiológicas o de comportamiento.

En concordancia con ello el Biometrics Institute la define como el uso de características biológicas y conductuales únicas para identificar o verificar la identidad de una persona. Así pues, desde un enfoque práctico, la biometría permite identificar o autenticar a una persona mediante el análisis de rasgos físicos o conductuales.

Mientras que, desde una perspectiva técnica, el término proviene de “bio” (vida) y “metría” (medida), por lo que todo sistema biométrico mide y analiza características propias de una persona para reconocer su identidad. En términos operativos, consiste

en utilizar características corporales o conductuales como huella dactilar, iris, voz o firma para determinar o confirmar la identidad de una persona.

Los datos biométricos mantienen las siguientes características:

Único: Corresponde a información única o con alta probabilidad de ser exclusiva de una persona.

Relacionado con la Identidad: Su finalidad principal es identificar o verificar la identidad de su titular.

Sensible: Se considera un dato sensible o de categoría especial, debido a que puede revelar información personal íntima y generar riesgos significativos si se utiliza indebidamente.

Irreemplazable: A diferencia de una contraseña, los datos biométricos no pueden modificarse fácilmente si se ven comprometidos.

Requiere Procesamiento Especializado: Su captura, almacenamiento y comparación requieren tecnologías específicas, algoritmos y plantillas biométricas; normalmente no se conserva la imagen original, sino una representación matemática de ella.

Comprende Características Conductuales: Incluyen patrones como la voz, la firma biométrica (presión, velocidad, inclinación) o determinados hábitos de comportamiento.

Adolece de Limitaciones Técnicas: Algunos datos biométricos pueden verse afectados por factores externos; por ejemplo, la voz puede alterarse por condiciones de salud o calidad del dispositivo, y la firma puede variar por factores físicos o emocionales.

En virtud de lo señalado previamente, resulta necesario mencionar detalladamente la clasificación de esta categoría especial de datos personales. Mismos que se clasifican de la siguiente manera:

- **Fisiológicos:** Derivados de características físicas del cuerpo, como huellas dactilares, iris, retina, rostro, geometría de la mano o ADN.
- **Conductuales:** Relacionados con patrones de comportamiento, como la firma dinámica, la voz, la forma de teclear o la marcha.
- **Derivados o Plantillas Biométricas:** Representaciones matemáticas obtenidas de la muestra biométrica, utilizadas para comparación sin necesidad de conservar el dato original.

Por otro lado, existen distintos tipos de datos biométricos, entre los cuáles se encuentran:

- **Datos Estáticos:** Corresponden a características físicas relativamente permanentes, como huellas, rostro o iris.
- **Datos Dinámicos:** Se relacionan con comportamientos o patrones de acción, como la forma de caminar o de escribir.
- **Datos Mixtos:** Combinan elementos físicos y conductuales, como ocurre con el reconocimiento de voz.

Entre los datos biométricos más utilizados en sistemas de seguridad se

encuentran las huellas dactilares, el reconocimiento facial, el iris y la voz. Destacando entre ellos, los siguientes:

Huellas Dactilares: Ampliamente utilizadas en sistemas de acceso y autenticación.

Reconocimiento Facial: Frecuente en dispositivos electrónicos y sistemas de vigilancia.

Reconocimiento de Iris: Altamente preciso y utilizado en entornos de alta seguridad.

Patrón de Voz: Empleado por su singularidad como mecanismo de autenticación.

Patrones de Tecleo: Menos comunes, utilizados para verificar identidad mediante hábitos de escritura.

De igual forma, es importante destacar la irrevocabilidad y la permanencia de los datos biométricos, que son dos de las características más relevantes de este tipo de datos y, al mismo tiempo, sus principales factores de riesgo. Son permanentes porque, en la mayoría de los casos, no cambian significativamente con el tiempo, como ocurre con las huellas dactilares o el iris.

Son irrevocables porque, una vez comprometidos o expuestos, no pueden sustituirse fácilmente, a diferencia de otros mecanismos de autenticación como una

contraseña. Debido a estas características, su tratamiento exige un nivel reforzado de protección jurídica y técnica.

En virtud de ello, la SPDP y la LOPDP, los reconocen como datos sensibles debido al riesgo que su exposición representa para los derechos del titular.

Por lo cual, su uso únicamente está permitido bajo condiciones específicas y, en la mayoría de los casos mediante consentimiento expreso, libre, específico e informado. De igual manera, su tratamiento debe justificarse; no debe emplearse cuando existan medios menos invasivos para alcanzar la misma finalidad. Por tanto, exige la aplicación de medidas técnicas como cifrado, tokenización, hashing y almacenamiento de plantillas biométricas en lugar de imágenes completas.

Respecto de su almacenamiento, las bases de datos centralizadas pueden representar riesgos elevados, como accesos no autorizados, filtraciones o reutilización indebida de la información, incluso cuando esta se encuentra cifrada. Asimismo, existen riesgos asociados a ataques informáticos durante la captura, transmisión o comparación de los datos biométricos, por lo que normas como el Reglamento General de Protección de Datos (RGPD) y legislación nacional en materia de protección de datos personales como la LOPDP (LOPDP, 2021), el RGLOPDP (RGLOPDP, 2023) y normativa secundaria; exigen que estos datos se conserven únicamente durante el tiempo estrictamente necesario.

Resulta sumamente relevante señalar que, debido a su carácter permanente e irreemplazable, los datos biométricos requieren medidas reforzadas de seguridad, tanto

técnicas como organizativas, incluyendo controles de acceso, cifrado y evaluaciones periódicas de riesgo.

El uso de sistemas biométricos genera riesgos relevantes para la privacidad, la seguridad y el ejercicio de derechos fundamentales, especialmente cuando los datos son recolectados o utilizados sin conocimiento o consentimiento del titular, o para finalidades distintas de aquellas originalmente autorizadas.

Entre los principales riesgos se encuentran la vigilancia no autorizada, el seguimiento masivo, el uso indebido de la información y la interconexión de bases de datos mediante identificadores únicos.

Uno de los principales riesgos surge cuando estos sistemas permiten identificar o rastrear personas sin su consentimiento, vulnerando el principio de consentimiento informado.

El reconocimiento facial representa uno de los mayores desafíos, ya que permite identificar automáticamente a una persona en función de su imagen, ubicación y contexto temporal, facilitando prácticas de monitoreo permanente que pueden afectar la privacidad y la libertad individual. Asimismo, estos sistemas no son infalibles y pueden generar errores de identificación, produciendo consecuencias graves, especialmente en ámbitos de seguridad pública o justicia penal.

Otra preocupación relevante es el uso indebido por parte de quienes controlan los datos, lo que puede generar discriminación, exclusión, limitación en el acceso a servicios o pérdida progresiva del anonimato. Entre los principales riesgos en el tratamiento de datos biométricos, se encuentran: violación de la privacidad, identificación masiva y

seguimiento sin consentimiento, discriminación y sesgo algorítmico, filtración o exposición permanente de datos sensibles, uso secundario o desvío de finalidad, responsabilidad administrativa, civil o reputacional para las organizaciones y, riesgos procesales y afectación de garantías en materia penal.

3.4.2. Tratamiento de Datos Biométricos

El tratamiento de datos biométricos debe sustentarse en una base jurídica válida, puesto que se trata de datos sensibles, el consentimiento constituye una de las bases de legitimación más relevantes.

Para que sea válido, el consentimiento debe ser claro, libre e inequívoco, es decir, no debe existir duda respecto de la voluntad del titular. Así pues, existen dos formas reconocidas de consentimiento:

Consentimiento Expreso: Manifestado mediante una declaración o acción afirmativa clara.

Consentimiento Tácito: Aquel que puede inferirse cuando la persona, pudiendo oponerse, no lo hace; sin embargo, en materia de datos sensibles su aplicación suele ser limitada.

En ambos casos, lo esencial es que exista una manifestación inequívoca de voluntad. Debido a la naturaleza sensible de los datos biométricos, muchas legislaciones exigen un consentimiento explícito para su tratamiento.

Este consentimiento debe ser libre, informado, específico y revocable, por lo que no puede obtenerse mediante presión, condicionamiento o ausencia de alternativas razonables. El titular debe recibir información clara sobre la finalidad del tratamiento, los riesgos asociados, quién tendrá acceso a sus datos y el procedimiento para revocar su consentimiento.

En caso de revocatoria, el responsable del tratamiento deberá garantizar mecanismos alternativos razonables que permitan al titular acceder al servicio sin afectar sus derechos.

3.5. Privacidad desde el Diseño y por Defecto

La privacidad desde el diseño se define como un enfoque preventivo y proactivo que exige la integración de salvaguardas y medidas de protección de datos personales desde las fases iniciales de concepción, arquitectura y desarrollo de cualquier sistema, servicio o producto. En lugar de ser un añadido posterior al desarrollo técnico, este principio busca que la privacidad sea un componente orgánico e inseparable de la ingeniería del sistema, permitiendo identificar y mitigar riesgos de forma anticipada antes de que el tratamiento de datos comience efectivamente.

Por su parte, la privacidad por defecto es el principio que garantiza que, de manera automática y sin intervención del usuario, las organizaciones solo traten los datos personales que sean estrictamente necesarios para cada una de las finalidades específicas del tratamiento. Esto implica la aplicación técnica y organizativa de criterios de minimización de datos, limitación de la finalidad y plazos de conservación reducidos,

asegurando que la configuración inicial del sistema sea siempre la más protectora para el titular de la información.

En el estudio de caso del control migratorio en aeropuertos de Ecuador, la entidad pública asume el rol de responsable del tratamiento, actuando bajo una misión de interés público y seguridad nacional para regular el flujo de personas en las fronteras. Para ejecutar esta labor, utiliza el sistema provisto por BioTrust, quien actúa como encargado del tratamiento, suministrando la plataforma tecnológica de biometría multimodal potenciada por inteligencia artificial para la identificación de viajeros nacionales y extranjeros.

La aplicación de la privacidad desde el diseño en este entorno exige que la entidad pública de control migratorio y BioTrust realicen obligatoriamente una EIPD antes de iniciar el tratamiento masivo de datos biométricos. Desde la ingeniería del sistema BioTrust, esto se traduce en la implementación de medidas robustas como el cifrado de plantillas faciales en tránsito y reposo, y la creación de mecanismos de trazabilidad y auditoría que prevengan accesos no autorizados o filtraciones de información sensible e irreversible.

En cuanto a la privacidad por defecto, el sistema BioTrust debe estar configurado para capturar únicamente los rasgos biométricos indispensables para la verificación de identidad, evitando la recolección de datos excesivos. Asimismo, los datos deben ser objeto de una política de retención limitada, donde se eliminen o anonimicen una vez cumplida la finalidad migratoria, y el acceso a la base de datos debe estar restringido por defecto solo a funcionarios autorizados mediante controles de acceso basados en roles (RBAC) y autenticación de doble factor.

Dado que se emplea inteligencia artificial, la protección desde el diseño debe abordar específicamente la prevención de sesgos algorítmicos que puedan derivar en decisiones discriminatorias o errores de reconocimiento masivos. Esto requiere que los algoritmos de BioTrust sean sometidos a auditorías de precisión y que el sistema incluya, por diseño, interfaces que faciliten una supervisión humana significativa, asegurando que ninguna decisión con efectos jurídicos sobre un viajero sea tomada de forma exclusivamente automatizada sin validación de un funcionario.

A pesar de que el tratamiento se enmarca en la seguridad nacional, las fuentes recalcan que se deben observar los principios de la LOPDP y estándares internacionales como ISO/IEC 27701. La legalidad, necesidad y proporcionalidad son los pilares que deben guiar el diseño del sistema migratorio, garantizando que el uso de tecnologías avanzadas sea compatible con el derecho constitucional a la protección de datos personales y la privacidad de los ciudadanos.

En consecuencia, la integración de estos principios fortalece la resiliencia institucional ante posibles incidentes de seguridad y genera confianza pública en el uso de biometría en las fronteras. Una gestión responsable por parte de la entidad pública de control migratorio y BioTrust, que trascienda el mero cumplimiento formal para adoptar una responsabilidad proactiva, asegura que la innovación tecnológica en los aeropuertos ecuatorianos no se convierta en una amenaza para los derechos fundamentales de las personas viajeras.

El enfoque preventivo en el tratamiento de datos biométricos constituye el pilar fundamental para garantizar que la modernización tecnológica en las fronteras no comprometa los derechos fundamentales. Dado que la biometría utiliza rasgos físicos y

conductuales únicos e irreemplazables, como el rostro o el iris, cualquier vulneración resulta irreversible, lo que eleva el impacto de posibles brechas a un nivel crítico. Este enfoque exige que la entidad pública como responsable del tratamiento y su encargado, BioTrust, adopten una postura de responsabilidad proactiva, integrando salvaguardas desde la concepción misma de los sistemas para mitigar riesgos antes de que estos se materialicen.

Dentro del marco legal ecuatoriano, el tratamiento de datos biométricos para seguridad nacional se rige por un régimen especial. Según el artículo 2 literal e) y el artículo 11 de la LOPDP, aunque existen excepciones regulatorias por el interés público, es obligatorio respetar los principios de la ley y los estándares internacionales de derechos humanos. Esto implica que cualquier sistema implementado en aeropuertos debe superar estrictos juicios de legalidad, necesidad y proporcionalidad, asegurando que la tecnología sea una herramienta de apoyo y no un mecanismo de vigilancia desmedida.

La herramienta preventiva por excelencia es la EIPD. Este análisis debe realizarse de manera previa al inicio de cualquier tratamiento masivo o automatizado que tenga efectos jurídicos sobre los viajeros. La EIPD permite a la entidad pública de control migratorio dentificar amenazas como el acceso no autorizado a bases de datos o la exfiltración de plantillas faciales, permitiendo priorizar medidas correctivas y condicionar el despliegue del sistema BioTrust hasta que los riesgos críticos sean mitigados a niveles aceptables.

La gestión técnica del riesgo se materializa a través de una matriz de valoración que identifica vulnerabilidades específicas, como credenciales débiles o falta de auditoría

algorítmica. Como medida preventiva, se deben implementar controles robustos que incluyan el cifrado de datos en tránsito y reposo, autenticación de múltiples factores (MFA), y el control de accesos basado en roles (RBAC). Estas acciones aseguran que la confidencialidad y la integridad de la información sensible se mantengan protegidas frente a ataques externos o fallos técnicos internos.

En el ámbito de la inteligencia artificial, el enfoque preventivo debe abordar específicamente los sesgos algorítmicos que podrían generar discriminación o errores masivos de reconocimiento. Para evitar que el sistema BioTrust produzca falsos positivos o negativos injustos, es imperativo realizar auditorías de precisión y mantener una supervisión humana efectiva en todas las decisiones automatizadas. La normativa vigente exige que el personal del aeropuerto valide los resultados de la inteligencia artificial, garantizando que el sistema no opere de forma autónoma sin rendición de cuentas.

Asimismo, el principio de privacidad por defecto actúa como una salvaguarda operativa constante. El sistema debe estar configurado para recolectar el mínimo de datos necesarios para la finalidad migratoria y establecer políticas de retención limitada, donde las plantillas biométricas sean eliminadas o anonimizadas una vez cumplido su propósito. Esto previene usos secundarios no autorizados y reduce la superficie de exposición ante posibles incidentes de seguridad que afecten la privacidad de los ciudadanos nacionales y extranjeros.

La gobernanza institucional entre el responsable y el encargado es vital para mantener este ciclo preventivo. La entidad pública de control migratorio debe supervisar que BioTrust cumpla no solo con la LOPDP, sino con reglamentos específicos como la

Resolución SPDP-SPD-2026-0012 (SPDP-SPD-2026-0012-R, 2026) y la Norma General de inteligencia artificial (SPDP-SPD-2026-0009-R, 2026). Una clara definición de roles, articulada en una matriz RACI, asegura que cada departamento sepa cómo actuar proactivamente en la detección de anomalías y en el mantenimiento preventivo de los dispositivos de lectura biométrica.

En consecuencia, la prevención se completa con la preparación ante lo inevitable mediante un plan de respuesta ante incidentes. Este plan no debe ser solo reactivo, sino que debe incluir fases de documentación y aprendizaje que alimenten la mejora continua del sistema. Al mapear escenarios supuestos de riesgo y realizar simulacros, la organización fortalece su resiliencia y genera una cultura de protección de datos que trasciende el cumplimiento formal, consolidando la confianza pública en el uso ético y seguro de la biometría en el Ecuador.

Para garantizar la integridad del control migratorio en el aeropuerto, se deben implementar medidas técnicas robustas que protejan la confidencialidad de las plantillas biométricas y los datos de los viajeros. Estas medidas incluyen el cifrado de datos, la aplicación de controles de acceso basados en roles (RBAC) y la autenticación de múltiples factores (MFA) para todo el personal que interactúa con el sistema BioTrust. Asimismo, es imperativo establecer registros de auditoría detallados y realizar pruebas de penetración periódicas para detectar vulnerabilidades en los activos estratégicos, incluyendo las integraciones con sistemas de entidades nacionales e internacionales.

En el ámbito específico de la inteligencia artificial, las medidas técnicas deben orientarse a la mitigación de fallos algorítmicos. Esto requiere la ejecución de auditorías de sesgo y precisión de forma constante, utilizando métricas de desempeño desglosadas

por grupos para asegurar que el sistema no presente tasas de error desproporcionadas. Además, se deben implementar mecanismos de mantenimiento preventivo y calibración de los dispositivos de lectura biométrica para evitar errores en el cotejo de pasaportes electrónicos que puedan comprometer la seguridad nacional.

Desde la perspectiva organizativa, la piedra angular es la definición de una matriz de roles y responsabilidades (RACI) que vincule a la entidad pública de control migratorio con BioTrust. Esta estructura asegura que el personal operativo, el Delegado de Protección de Datos (DPD), el área de TI y la Alta Dirección sepan exactamente quién debe ejecutar, aprobar o ser consultado ante cualquier tratamiento de datos o incidente. La gobernanza institucional se fortalece con la creación de un Comité de Crisis encargado de validar la clasificación de incidentes y aprobar decisiones críticas antes de cualquier notificación externa.

Otra medida organizativa fundamental es la gestión de la supervisión humana efectiva sobre las decisiones automatizadas. No se trata solo de un requisito técnico, sino de un protocolo operativo que obliga a los funcionarios del aeropuerto a revisar manualmente cualquier coincidencia (match) o alerta generada por la IA antes de tomar una medida con efectos jurídicos sobre el viajero. Esta supervisión actúa como un control de calidad humano que previene discriminaciones y asegura que el sistema BioTrust no opere como una "caja negra" sin rendición de cuentas.

En cuanto a la relación con proveedores, se deben establecer cláusulas contractuales estrictas que obliguen a BioTrust a cumplir con los estándares de seguridad y a facilitar auditorías de cumplimiento. Organizativamente, la institución debe mantener una política de retención de datos claramente definida, programando el borrado o la

anonimización automática de la información biométrica una vez cumplido el plazo necesario para la finalidad migratoria, evitando así la conservación excesiva de datos sensibles.

El plan de respuesta ante incidentes representa una medida organizativa crítica que detalla los pasos concretos para el personal del aeropuerto. Este plan define tiempos de respuesta específicos (por ejemplo, detección y reporte en los primeros 15 minutos) y un flujo de comunicación que debe ser comprendido por todos los niveles de la organización, no solo como una descripción teórica, sino como un manual de acción práctica. El protocolo asegura que el cómputo del plazo legal para notificar a la SPDP inicie correctamente desde el conocimiento del evento.

Por ende, el cumplimiento normativo se integra mediante la adopción de las resoluciones más recientes, como la Resolución SPDP-SPD-2026-0012 (SPDP-SPD-2026-0012-R, 2026) para la gestión de incidentes. Esta disposición exige que la organización mantenga un registro interno y documentación obligatoria de cada incidente, incluyendo lecciones aprendidas y actualizaciones de controles, lo que fomenta una cultura de mejora continua y responsabilidad proactiva en la protección de los datos de los ciudadanos.

CAPÍTULO II

1. Evaluación Normativa

1.1 Requisitos Formales para el Tratamiento de Datos Personales en el Ecuador

La adaptación del sistema de control migratorio en Ecuador al marco legal vigente no es un proceso meramente formal, sino una exigencia de responsabilidad proactiva que traduce los principios generales en acciones operativas concretas. En este contexto, la evaluación normativa parte del reconocimiento de que, si bien el tratamiento de datos biométricos para la seguridad nacional se rige por un régimen especial según el artículo 2 literal e) y el artículo 11 de la LOPDP, esto no exime a la entidad pública de control migratorio de cumplir con los principios de licitud, necesidad y proporcionalidad. Esta adaptación exige que la tecnología no sea vista como un fin en sí misma, sino como una herramienta sujeta a estándares mínimos éticos y jurídicos que garanticen la inviolabilidad de los derechos de los viajeros.

Para lograr una adaptación efectiva, el marco regulatorio debe integrarse de manera jerárquica y técnica. Es obligatorio incluir en esta evaluación el RGLOPDP, la Resolución SPDP-SPD-2026-0012 (SPDP-SPD-2026-0012-R, 2026) que expide la Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales. Estas normas imponen obligaciones específicas de trazabilidad, supervisión humana y transparencia algorítmica, especialmente cuando se emplean sistemas como BioTrust que realizan procesamiento masivo y automatizado de datos sensibles. A nivel constitucional, el artículo 66 numeral 19 y el artículo 92 actúan como el límite supremo para evitar que el control fronterizo derive en una vigilancia masiva desproporcionada.

2. La Necesidad de un Inventario de Datos

La necesidad de un inventario de datos radica en que permite a la entidad pública de control migratorio identificar con precisión qué datos se recolectan, para qué fines específicos se utilizan y quiénes intervienen en cada etapa del ciclo de vida del dato. Sin un inventario detallado, la organización no puede garantizar el principio de minimización de datos ni cumplir con la obligación de informar a la autoridad de control sobre la escala y profundidad de sus tratamientos biométricos.

En el estudio de caso planteado, el inventario desglosa actividades críticas como la AT-01 (Identificación facial en tiempo real mediante IA) y la AT-02 (Verificación de pasaportes biométricos mediante IA). Este registro documenta no solo la captura en el aeropuerto, sino también la interoperabilidad con bases de datos de entidades externas, especificando los flujos de datos que gestiona el encargado BioTrust. Documentar estos intercambios es esencial para evaluar los riesgos de transferencias internacionales y asegurar que existan garantías contractuales suficientes para proteger la integridad de las plantillas faciales fuera del control directo de la institución.

El inventario de datos se extiende a los activos estratégicos del sistema, incluyendo las plataformas de reconocimiento facial con IA, las bases de datos de plantillas biométricas y los módulos de lectura de documentos. Esta catalogación técnica es fundamental para el Plan de Respuesta ante Incidentes, ya que permite al personal de TI y al DPD identificar rápidamente qué sistemas se han visto comprometidos ante un ataque o fallo algorítmico. La evaluación normativa exige que este inventario se mantenga actualizado como un documento vivo que refleje cualquier cambio en la arquitectura del sistema BioTrust.

La utilidad práctica de este inventario culmina en la realización de la EIPD, la cual es obligatoria para tratamientos de alto riesgo que involucren biometría e IA a gran escala. El inventario proporciona los insumos necesarios para que la EIPD identifique amenazas como sesgos algorítmicos o accesos no autorizados, permitiendo establecer medidas de mitigación previas al despliegue operativo. La concurrencia de factores como el uso de datos sensibles e inteligencia artificial hace que este análisis sea indispensable para validar la licitud del tratamiento.

Finalmente, la adaptación normativa a través del inventario refuerza la resiliencia institucional y la confianza pública. Al sistematizar las obligaciones legales y los detalles técnicos del tratamiento, la entidad pública de control migratorio demuestra una gestión responsable y transparente que trasciende el mero cumplimiento de la seguridad nacional. Este enfoque estructurado asegura que la modernización tecnológica en los aeropuertos ecuatorianos se realice bajo un estándar de mejora continua, protegiendo la identidad irreversible de los ciudadanos mientras se optimiza la agilidad del control migratorio.

3. Gobernanza de la Protección de Datos Personales

3.1 Políticas, Instrucciones de Trabajo y Flujogramas

POLÍTICA INSTITUCIONAL DE PROTECCIÓN DE DATOS PERSONALES

La Política Institucional de Protección de Datos Personales de la entidad pública de control migratorio del Ecuador que consta en el Anexo 1, establece las reglas básicas para el uso y cuidado de los datos personales de ciudadanos nacionales, extranjeros, funcionarios, proveedores y usuarios del portal web institucional. Su objetivo es

garantizar que toda la información que se maneja en los servicios de migración y extranjería se trate conforme a la Constitución, la LOPDP, su Reglamento y la normativa de la SPDP. Para ello define conceptos clave (datos personales, datos sensibles, bases de datos, encargados del tratamiento, transferencias internacionales) y fija principios como legalidad, finalidad, minimización, calidad, seguridad, transparencia y responsabilidad proactiva. La política aplica a todas las bases de datos de la entidad, en cualquier soporte, y obliga a todos los funcionarios y terceros a cumplirla. El documento también describe la forma en que se organiza la gestión de datos personales (Delegado, Comité y responsables por áreas), las finalidades concretas de tratamiento propias del control migratorio (por ejemplo: el uso de datos biométricos para identificación, video-vigilancia y control de acceso a áreas críticas) y los procedimientos para que los titulares ejerzan sus derechos. Además, la Política regula las transferencias internas y externas de información, el flujo transfronterizo de datos, el tratamiento de datos sensibles, las medidas de seguridad técnicas y organizativas, las obligaciones de los encargados, la eliminación o anonimización de datos, la realización de evaluaciones de impacto, la notificación de brechas de seguridad y la interacción con la autoridad de protección de datos personales.

FLUJOGRAMAS DE LAS ACTIVIDADES DE TRATAMIENTO DE DATOS PERSONALES

AT-01 - Identificación de entrada y salida del país de personas naturales para el control migratorio: Identificación en tiempo real de personas naturales mediante reconocimiento facial e IA, para el registro de entrada y salida del país, control de impedimentos, identificación de personas requeridas por la justicia nacional e

internacional, prevención del delito de trata de personas o localización y protección de menores en el punto de control migratorio de aeropuertos.

Figura 1 - AT-01 (Actividad de Tratamiento 01)

AT-02 - Verificación de pasaportes biométricos: Cotejar mediante IA los datos biométricos del pasaporte biométrico para la identificación de personas con impedimentos de salida del país ante autoridades nacionales.

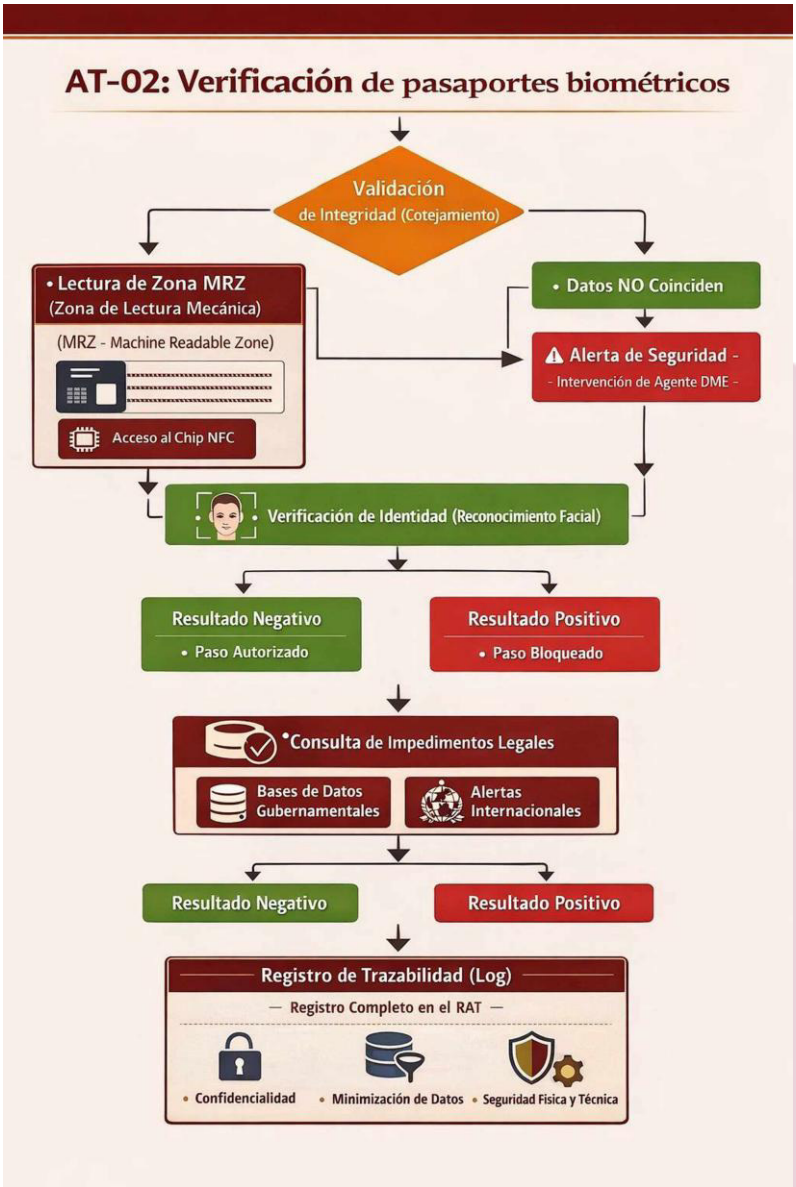

Figura 2 - AT-02 (Actividad de Tratamiento 02)

AT-03 - Control de acceso de los funcionarios de la entidad pública de control migratorio o terceros autorizados a las salas de videovigilancia: Reconocimiento del iris de los funcionarios de la entidad pública de control migratorio o terceros autorizados para el control de acceso a las salas de videovigilancia del aeropuerto.

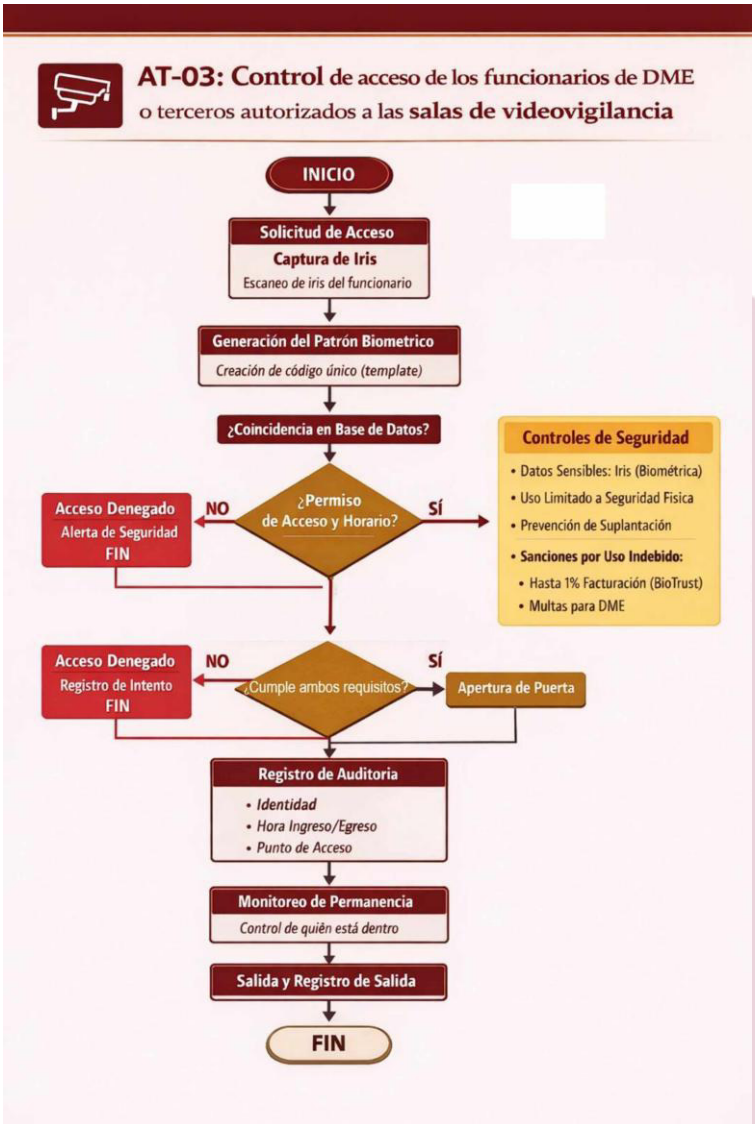

Figura 3 - AT-03 (Actividad de Tratamiento 03)

AT-04 - Control de acceso a oficinas institucionales mediante reconocimiento de voz de los empleados de la entidad pública de control migratorio: Gestionar y controlar el acceso del personal autorizado a las oficinas de la entidad pública de control migratorio en las instalaciones ubicadas en el aeropuerto, mediante sistemas de autenticación biométrica por reconocimiento de voz, con el fin de fortalecer la seguridad institucional y proteger instalaciones, información y bienes institucionales.

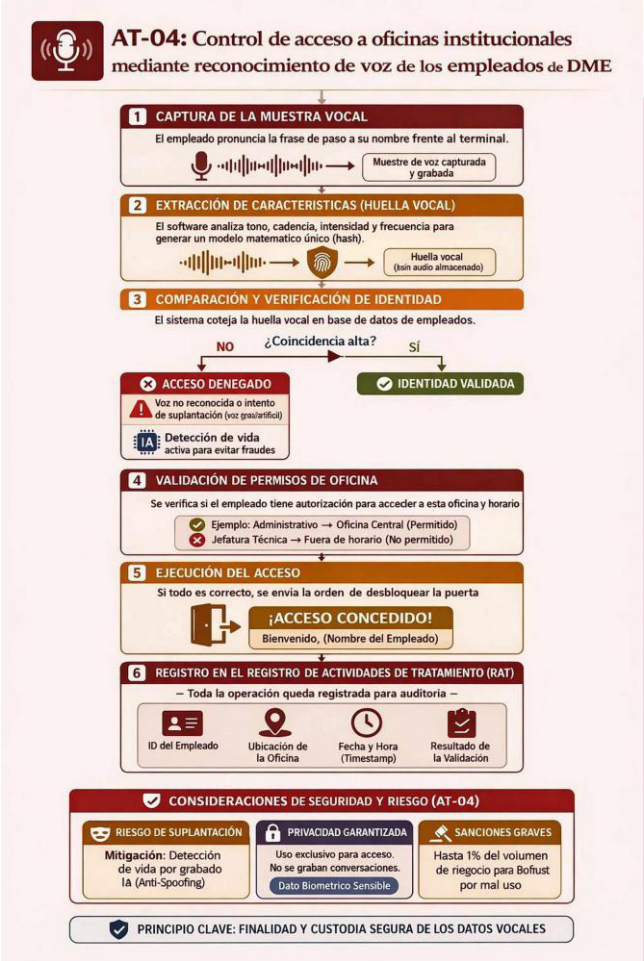

Figura 4 - AT-04 (Actividad de Tratamiento 04)

AT-05 - Control de acceso al Data Center mediante reconocimiento de huellas dactilares de los empleados de la entidad pública de control migratorio: Gestionar y controlar el acceso de personal autorizado al Data Center de la entidad pública de control migratorio, mediante un sistema de autenticación biométrica por reconocimiento de huellas dactilares, con el fin de fortalecer la seguridad y proteger información y bienes institucionales.

Figura 5 - AT-05 (Actividad de Tratamiento 05)

3.2 Matriz RACI

El Anexo 2 corresponde a una matriz RACI que organiza las tareas o actividades clave de la entidad pública de control migratorio frente a la protección de datos personales y otros procesos asociados, cruzándolas con los distintos roles o actores internos (direcciones, unidades, responsables de sistemas, DPD, etc.). Se identifica, para cada actividad, quién es Responsable de ejecutarla (R), quién tiene la autoridad o rinde cuentas por su resultado (A), quién debe ser Consultado por su conocimiento especializado (C) y quién debe ser Informado del avance o decisiones (I), lo que permite eliminar ambigüedades y solapamientos en la gestión. De este modo, este documento funciona como un mapa claro de responsabilidades para la implementación operativa de procesos críticos de la entidad de control migratorio, facilitando la coordinación entre áreas y la rendición de cuentas. En esta matriz se identifica claramente quién lidera la elaboración y actualización de políticas, quién aprueba el registro de actividades de tratamiento, quién debe ser consultado en evaluaciones de impacto, o quién debe ser informado ante incidentes de seguridad, auditorías o requerimientos de la autoridad de control. Esta herramienta es especialmente útil cuando intervienen múltiples actores (áreas operativas, jurídicas, tecnológicas y de seguridad) y se requiere claridad sobre las funciones en cada fase del ciclo de vida del dato personal, desde la recolección hasta la eliminación. Este documento actúa como un instrumento de gobernanza y de gestión de proyectos que traduce los deberes legales y las obligaciones internas en responsables concretos, contribuyendo a una implementación ordenada y verificable del sistema de protección de datos personales de la entidad pública de control migratorio.

3.3 El Cumplimiento del Derecho a la Información: Avisos de Privacidad y Protección de Datos Personales

AVISO INTERNO DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

El Aviso Interno de Privacidad y Protección de Datos Personales que consta en el Anexo 3, dirigido a los trabajadores y demás personal vinculado a la entidad pública de control migratorio del Ecuador, explica en lenguaje accesible que el documento es de uso interno y desarrolla cómo la entidad cumple la Constitución y la LOPDP en el tratamiento de datos personales dentro de la relación laboral, define conceptos clave (datos personales, datos sensibles, tratamiento, trabajadores) y fija el ámbito de aplicación sobre todas las bases de datos institucionales que contienen información de servidores públicos, contratistas y demás personal. Además, describe las finalidades del tratamiento: gestión integral de la relación laboral, cumplimiento de obligaciones legales y reglamentarias, y seguridad institucional mediante control de accesos físicos y lógicos, detalla la base legal del tratamiento, los tipos de operaciones que se realizan sobre los datos (recolección, almacenamiento, uso, actualización, supresión), y regula de forma específica el consentimiento para el uso de datos biométricos del personal, exigiendo que sea libre, específico, informado e inequívoco, así mismo informa sobre los plazos de conservación, otras finalidades como auditorías y estadísticas, las posibles transferencias a entidades públicas, organismos de control y proveedores, y las consecuencias de no entregar datos o entregarlos erróneos, también enumera los derechos de los titulares (acceso, rectificación, eliminación, oposición, portabilidad, entre otros), los canales de contacto con el responsable y el delegado de protección de datos personales, el derecho a reclamar ante la autoridad y el modelo de consentimiento.

AVISO EXTERNO DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

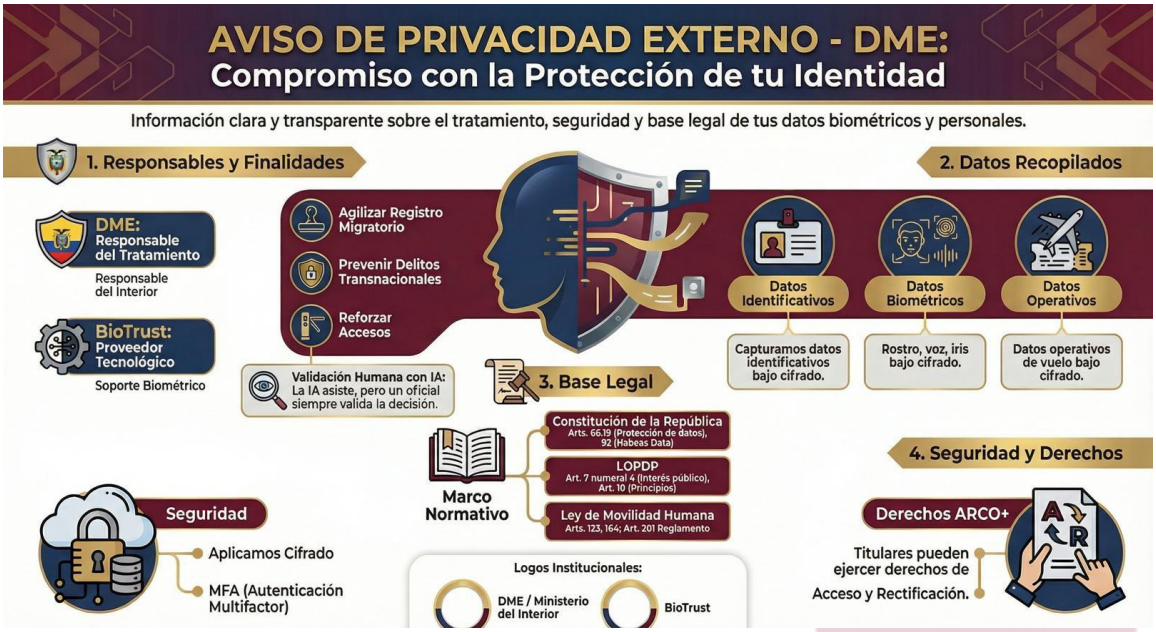

Figura 6 - Aviso Externo de Privacidad y Protección de Datos Personales

3.4 Cláusulas Contractuales entre los Agentes de Tratamiento de Datos Personales

Modelo de cláusula contractual de protección de datos personales, entre responsable y encargado del tratamiento

"CLÁUSULA CONTRACTUAL. - Tratamiento de Datos Personales entre Responsable y Encargado del Tratamiento:

Para el presente contrato se considera a la entidad pública como responsable del tratamiento de datos personales y, a BioTrust como encargado del tratamiento de datos

personales. La presente cláusula no exime a las partes de suscribir un contrato de encargo de tratamiento de acuerdo con la LOPDP.

x.1. Finalidad del Tratamiento

El encargado del tratamiento se compromete a tratar los datos personales de conformidad con las finalidades previstas, siendo estas:

- Gestionar el ingreso y salida en el territorio nacional de ciudadanos nacionales y extranjeros mediante la verificación automatizada de su identidad.
- Validar la identidad a través de lectores biométricos integrados con documentos de viaje electrónicos (e-passports), aplicando un cotejo (matching) 1:1 y 1:N asistido por Inteligencia Artificial.
- Ejecutar el reconocimiento facial, de iris y otros identificadores biométricos directamente en el flujo operativo del puesto fronterizo aeroportuario.
- Controlar el acceso físico a las salas de video-vigilancia y a las áreas de seguridad restringidas del aeropuerto, limitado estrictamente al personal funcionario autorizado.
- Prevenir delitos como la suplantación de identidad, detectar de forma oportuna a personas requeridas por la justicia, proteger a los menores de edad y garantizar la seguridad del Estado, buscando siempre equilibrar estos controles con la agilización del tránsito de los viajeros.

El encargado del tratamiento solo podrá tratar los datos personales para las finalidades mencionadas y no podrá utilizarlos para fines distintos a los expresamente autorizados por el responsable.

x.2. Compromiso del Responsable

El responsable del tratamiento declara y garantiza que los datos personales proporcionados al encargado de tratamiento han sido recabados de manera lícita y legítima de acuerdo con la normativa de datos personales vigente. El responsable es el único que responderá ante los titulares de los datos por el cumplimiento de la ley y los derechos de estos.

x.3. Obligaciones del Encargado del Tratamiento

Las obligaciones específicas del encargado del tratamiento se detallarán específicamente en el Contrato de encargo de tratamiento de acuerdo con la LOPDP y demás artículos correspondientes de su Reglamento. Sin embargo, se recalcan las siguientes obligaciones en relación con tratamiento de los datos personales:

- Tratar los datos personales únicamente conforme a las instrucciones del responsable del tratamiento y dentro del marco de la finalidad establecida en el presente Contrato.
- Adoptar las medidas físicas, técnicas, legales, administrativas y organizativas necesarias para garantizar la seguridad de los datos personales y protegerlos en su integridad, disponibilidad y confidencialidad.
- No transferir los datos personales a terceros, salvo que se cuente con la autorización previa y escrita del responsable o en caso de que lo exija la ley.

• Informar de inmediato al responsable en caso de que se detecte alguna vulneración de seguridad que pueda comprometer los datos personales, a más tardar en el término de dos (2) días término desde que tuvo conocimiento de la vulneración de seguridad.

• Notificar e informar al responsable del tratamiento en el término de dos (2) días sobre la solicitud de atención a derechos de protección de datos personales, así como la información pertinente a fin de garantizar la respuesta dentro del término establecido en la Ley.

• Permitir y contribuir con las auditorías o inspecciones que el responsable considere necesarias para garantizar el cumplimiento de las obligaciones en materia de protección de datos.

En caso de que el encargado de tratamiento destine los datos personales para otras finalidades de tratamiento determinando este los fines y medios, se considerará, responsable del tratamiento en lo que respecta a dicho tratamiento.

x.4. Subcontratación del Tratamiento

El encargado del tratamiento no podrá subcontratar el tratamiento de los datos personales sin la autorización previa y por escrito del responsable del tratamiento. En caso de subcontratación, el encargado del tratamiento se compromete a asegurar que el subcontratista cumpla con las mismas obligaciones de protección de datos que tiene con el responsable del tratamiento, estableciendo un acuerdo que regule dicha subcontratación.

En caso de realizar subcontratación, el tercero asumirá las mismas obligaciones establecidas para el encargado de tratamiento establecidas en el contrato de encargo y las contempladas en la normativa de protección de datos personales vigente, es así que el subcontratado/sub-encargado de tratamiento deberá cumplir con las instrucciones de tratamiento de datos dadas por el responsable y encargado del tratamiento.

En caso de que el sub-encargado de tratamiento sufra una vulneración de seguridad a los datos personales, el encargado de tratamiento seguirá siendo plenamente responsable de la misma frente al responsable de tratamiento debiendo cumplir con la notificación de la vulneración dentro del término de dos (2) días al responsable.

x.5. Derecho de Repetición Contra el Encargado

Las partes reconocen que, conforme con lo establecido en la normativa aplicable en materia de protección de datos personales, el responsable del tratamiento asume la responsabilidad frente al titular de los datos por cualquier daño que se derive del tratamiento ilícito de los datos personales.

No obstante, cuando el incumplimiento de las obligaciones legales, contractuales o técnicas en materia de protección de datos sea atribuible al encargado del tratamiento, este deberá asumir la responsabilidad por los daños y perjuicios causados y mantener indemne al responsable por cualquier reclamación, sanción, multa, daño o gasto que se derive directa o indirectamente de dicho incumplimiento.

Asimismo, se acuerda expresamente que el responsable de tratamiento tendrá derecho a repetir contra el encargado de tratamiento por los importes que haya debido

asumir frente a terceros (incluidos titulares, autoridades o tribunales) como consecuencia de actuaciones u omisiones imputables al encargado de tratamiento.

Ambas partes se comprometen a delimitar claramente sus respectivas obligaciones y responsabilidades mediante el correspondiente contrato de encargo del tratamiento.

x.6. Derechos de los Titulares de los Datos

El encargado de tratamiento se compromete a cooperar con el responsable de tratamiento para garantizar que los titulares de los datos puedan ejercer sus derechos. El encargado de tratamiento notificará al responsable del tratamiento cualquier solicitud que reciba directamente del titular de los datos, y deberá prestar su apoyo en el cumplimiento efectivo de la solicitud dentro del plazo de quince (15) días establecido en la LOPDP.

x.7. Devolución o Eliminación de los Datos

Al finalizar el tratamiento de los datos personales, el encargado del tratamiento deberá devolver todos los datos personales al responsable del tratamiento tanto los que ha tenido acceso para realizar el tratamiento como los que surjan como resultado del procesamiento de estos o, si así lo solicita este último, la eliminación segura de todos los datos personales tratados, de acuerdo con lo establecido en la normativa de protección de datos.

De manera excepcional el encargado de tratamiento podrá conservar los datos personales tratados con la finalidad de dar cumplimiento a una obligación legal, datos los cuales deberán mantenerse alojados en una base de datos distinta a la inicial y deberán

estar bloqueados con todas las medidas de seguridad necesarias que garanticen la integridad, disponibilidad y confidencialidad de la información.

x.8. Plazo de Conservación

El encargado de tratamiento solo podrá conservar los datos personales durante el tiempo estrictamente necesario para cumplir con las finalidades del tratamiento y conforme a las instrucciones del responsable.

x.9. Confidencialidad

El encargado del tratamiento se compromete a mantener la confidencialidad sobre los datos personales tratados y a no divulgarlos a terceros sin la autorización expresa y por escrito del responsable del tratamiento, salvo que sea requerido por una obligación legal o por orden judicial. En este sentido, el encargado del tratamiento se compromete y garantiza que cuenta con convenios de confidencialidad o cláusulas de confidencialidad con todo su personal especialmente con quienes tienen acceso o que llegaren a conocer sobre los datos personales objeto de tratamiento. Asimismo, declara que cuenta con todas las medidas de seguridad necesarias para garantizar la seguridad de la información (SPDP-SPD-2025-0006-R, 2025).

CAPÍTULO III

1. Nivel Mínimo Aceptable para el Tratamiento Ético, Responsable y Estratégico de Datos Personales y el Uso de estos en Sistemas de IA

En el contexto de la modernización tecnológica de las fronteras en los aeropuertos internacionales del Ecuador, el Nivel Mínimo Aceptable (NMA) constituye el umbral crítico e infranqueable de controles que el responsable y BioTrust, como encargado, deben garantizar para el tratamiento lícito de datos biométricos mediante sistemas de Inteligencia Artificial. Se debe analizar como mínimo, desde la dimensión ética, este estándar exige mitigar los sesgos algorítmicos que provocan falsos positivos o negativos, garantizando la no discriminación de flujos masivos de pasajeros, especialmente de colectivos de atención prioritaria. Asimismo, se debe tener total control para evitar la adopción de decisiones restrictivas plenamente automatizadas, mediante un esquema de supervisión humana efectiva donde la validación final de una alerta o un impedimento de salida dependa exclusivamente de la revisión técnica de un funcionario calificado.

En lo que respecta a la responsabilidad proactiva (accountability), la gestión institucional debe alinearse con la normativa de la materia y, de manera imperativa, con la resolución SPDP-SPD-2026-0009-R, emitida el 12 de febrero de 2026 por la SPDP, la cual norma la garantía de derechos en el uso de sistemas de Inteligencia Artificial. Esta regulación dictamina que todo tratamiento sistemático y automatizado de datos biométricos sensibles a gran escala requiere de una EIPD previa y específica antes de cualquier despliegue operativo. Bajo este marco, el NMA demanda una gobernanza contractual estricta que delimite funciones mediante herramientas como la matriz RACI, prohibiendo expresamente al proveedor tecnológico cualquier tratamiento secundario o

transferencia ilícita de datos personales hacia fines comerciales o de marketing sin base legal.

La dimensión estratégica aborda la seguridad técnica avanzada necesaria para neutralizar los riesgos identificados en el servicio de BioTrust. Para evitar escenarios catastróficos, como fugas de información de usuarios o caídas del sistema en horas pico, resulta obligatorio implementar controles de cifrado y reposo, control de accesos basados en roles, autenticación multifactor y mecanismos de prevención de pérdida de datos. Ante cualquier vulnerabilidad que afecte la confidencialidad, integridad o disponibilidad de la información, el protocolo exige activar la notificación obligatoria en un término de 5 días ante la SPDP y ARCOTEL, y de 3 días para los pasajeros afectados. Finalmente, ante fallos técnicos o actualizaciones defectuosas que provoquen la caída del servidor principal, el sistema debe garantizar la continuidad del servicio mediante la suspensión inmediata de la automatización y la activación del protocolo de contingencia de paso migratorio de manera manual, salvaguardando el flujo de viajeros sin afectar la seguridad nacional del Estado.

2. Matriz Integrada de Riesgos de Tratamientos de Datos Personales Biométricos, incluyendo Tratamientos con Uso de IA

La Matriz de valoración de riesgos (Anexo 4) identifica y evalúa los principales riesgos asociados al uso de sistemas de reconocimiento facial, IA y bases de datos biométricas en una entidad pública de control migratorio. Se organiza, para cada actividad de tratamiento como la identificación en tiempo real de personas mediante reconocimiento facial o cotejo de pasaportes biométricos; un código de riesgo; el activo afectado sean las plataformas, bases de datos o los sistemas interoperables con

entidades externas; las amenazas relevantes y una descripción clara de cómo estas pueden materializarse como, por ejemplo: accesos no autorizados, filtraciones, sesgos algorítmicos, fallos de verificación, etc. La matriz valora para cada riesgo la probabilidad de ocurrencia y el impacto en distintas dimensiones: confidencialidad, integridad, disponibilidad, privacidad y, de forma destacada, los derechos y libertades de las personas, generando un nivel de riesgo inherente y un riesgo residual tras aplicar controles. Asimismo, clasifica los controles (preventivos o disuasorios) y detalla medidas concretas como cifrado en tránsito y reposo, control de accesos basado en roles (RBAC), autenticación multifactor (MFA), registros de auditoría, pruebas de penetración, auditorías de sesgo algorítmico, revisión humana obligatoria y políticas de retención y anonimización de datos biométricos. En conjunto, este documento es una herramienta de gestión de riesgos de protección de datos personales orientada a los procesos críticos del control migratorio, permitiendo priorizar riesgos altos y definir tratamientos alineados con la LOPDP y la seguridad nacional.

3. Plan de Respuesta a Incidentes de Seguridad de la Información que involucren Datos Personales (Brechas).

3.1. Marco Normativo Aplicable

3.1.1. Marco Legal Principal

- La Constitución de la República del Ecuador (CRE, 2008) garantiza: Derecho a Protección de Datos (art. 66) y Habeas Data (art. 92).
- La Ley Orgánica de Protección de Datos Personales (LOPDP, 2021) es la norma central. Establece:
    - Medidas de Seguridad Obligatorias (art. 10 y 25)

- Responsabilidad Proactiva (art. 11)
- Notificación de Brechas a la Autoridad y Titulares (arts. 32 y 33)
- Evaluación de impacto (EIPD) en Tratamientos de Alto Riesgo (art. 26)

- Reglamento General a la Ley Orgánica de Protección de Datos Personales (RGLOPDP, 2023)
- Resolución Nro. SPDP-SPD-2026-0009-R Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial (SPDP-SPD-2026-0009-R, 2026).
- Resolución Nro. SPDP-SPD-2026-0012-R Guía de Gestión de Riesgos y Evaluación de Impacto V2 (SPDP-SPD-2026-0012-R, 2026).

3.1.2. Normativa Sectorial (Migración)

- La Ley Orgánica de Movilidad Humana (LOMH, 2018), exige confidencialidad de datos (art. 11) e Implica tratamiento masivo y sensible en control migratorio.

3.1.3. Estándares Internacionales

- **ISO/IEC 27001:** Gestión de riesgos, incidentes, controles y mejora continua. Evaluación y tratamiento de riesgos (6.1.2 y 6.1.3), Gestión de incidentes (A.5.24–A.5.27), Control de accesos, monitoreo y trazabilidad.
- **ISO/IEC 27701:** Extiende ISO 27001 hacia protección de datos personales. Evaluación de riesgos de privacidad (5.4.1.2), Privacy by design (7.3.1), Gestión y notificación de incidentes (7.4.5 y 7.4.6).

3.1.4. Evaluación de Impacto en la Protección de Datos (SPDP) – Eje Central del Cumplimiento

- Basada en la Resolución Nro. SPDP-SPD-2026-0012-R (SPDP-SPD-2026-0012-R, 2026)
- Obligatoria en Migración por: Uso de datos biométricos, tratamiento masivo, interoperabilidad internacional.
- Evalúa: Riesgos (acceso indebido, fuga, alteración), impacto (alto o muy alto).

3.2. Definición de incidente de seguridad biométrica con IA

El art. 4 de la LOPDP menciona los términos y definiciones que se aborda en determinado cuerpo normativo. Por lo que, se indica que la vulneración de la seguridad de los datos personales es “el incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales”.

Por otra parte, la AEPD determina que “una brecha de datos personales es un incidente de seguridad que ocasiona la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos”.

Un incidente de seguridad biométrica con IA es una vulneración que afecta la confidencialidad, integridad o disponibilidad de las plantillas faciales. Según la LOPDP y la AEPD, esto incluye el acceso no autorizado o la filtración de datos gestionados por BioTrust en el aeropuerto. Estas brechas comprometen la identidad del titular, generando riesgos de suplantación de identidad bajo un impacto calificado como crítico. La IA añade complejidad al ser el núcleo que procesa y, eventualmente, expone estos datos sensibles.

Bajo esta definición, la IA actúa como un factor de riesgo cuando presenta sesgos algorítmicos o errores de reconocimiento facial sistemáticos. Un incidente ocurre no solo

por ataques externos, sino por la alteración accidental o intencional de los datos de entrenamiento o de los resultados. La falta de supervisión humana significativa puede derivar en decisiones injustas y discriminatorias. Esto constituye una afectación directa a la integridad del tratamiento y a los derechos de los titulares. Para BioTrust, un error en la plataforma de IA que genere falsos positivos es, técnicamente, un incidente de seguridad.

3.3. Fases del protocolo de respuesta

El protocolo de respuesta ante un incidente de seguridad biométrica con inteligencia artificial se estructura en siete fases que buscan garantizar una reacción ordenada, transparente y eficaz. La primera es detección y notificación, donde se registra la anomalía, se informa de inmediato al equipo de seguridad y a la dirección, y se documenta el hecho en el sistema de gestión. Luego sigue la contención, que implica aislar el sistema afectado, suspender procesos críticos como validaciones en aeropuertos si hay riesgo de fuga de datos, y aplicar medidas de mitigación urgentes para frenar la propagación.

La tercera fase es el análisis y evaluación, que consiste en investigar la causa raíz del incidente, valorar el impacto sobre los datos biométricos comprometidos y clasificar la gravedad según la normativa vigente. Posteriormente se aborda la comunicación, tanto a los titulares afectados como hacia la SPDP dentro de los términos legales, además de coordinarse con instituciones como aeropuertos y policía de migración. La quinta fase, remediación, busca corregir vulnerabilidades mediante actualización de algoritmos, reforzar mecanismos de autenticación y cifrado, revisar proveedores y contratos, y restablecer el servicio de forma segura.

En la sexta etapa, documentación y aprendizaje, se elabora un informe final con cronología, acciones y lecciones aprendidas, se revisan políticas internas y se capacita al personal en buenas prácticas. Finalmente, la fase de prevención y mejora continua contempla simulacros periódicos, monitoreo proactivo de anomalías en IA y auditorías de cumplimiento con estándares internacionales como ISO/IEC 27001 y GDPR. En conjunto, este protocolo asegura una respuesta integral que no solo atiende la emergencia, sino que fortalece la resiliencia institucional frente a futuros incidentes.

3.4. Roles y responsabilidades

La participación de cada actor en el Plan de Respuesta ante Incidentes de Seguridad biométrica con IA, se muestra en una matriz RACI (responsable, aprobador, consultado e informado).

Actividad / Tarea	DME						BioTrust
	Área de PDP	DPD	Alta Dirección	Área de TI / Seguridad de la Información	Área Jurídica	Personal operativo	DPD
Detección y reporte inicial del incidente	I	I	I	I	I	R	I
Validación y clasificación del incidente	R	A	C	C	C	I	C
Activación formal del Plan de Respuesta ante Incidentes de Seguridad y del Equipo de Respuesta	R	A	C	C	C	I	C
Coordinación técnica de contención y preservación de evidencias	R	C	I	R	I	I	R
Análisis de impacto en derechos y libertades de titulares	R	A	C	C	C	I	C
Decisión sobre necesidad de notificación a la SPDP	R	A	C	I	C	I	C
Redacción y envío de la notificación a la SPDP	R	A	I	I	C	I	C
Definición del contenido de la comunicación a titulares	R	A	C	I	C	I	C
Emisión de comunicaciones a titulares afectados	R	I	I	I	I	C	C
Coordinación con BioTrust sobre medidas técnicas correctivas	I	R	I	C	I	I	R
Implementación de medidas correctivas en la infraestructura propia	I	I	I	R	I	I	C
Actualización del registro interno de incidentes	R	A	I	C	I	I	C
Decisión sobre realización o actualización de la EIPD	R	A	C	C	C	I	C
Revisión de lecciones aprendidas y aprobación del cierre del incidente	I	R	A	C	C	I	C

Leyenda RACI: R = Responsable de ejecutar la actividad; A = Aprobador final; C = Consultado; I = Informado.

Tabla 1 - Matriz RACI (para incidentes de seguridad)

Esta matriz permite al personal de la entidad pública de control migratorio y al proveedor BioTrust identificar con rapidez quién debe ejecutar, aprobar o apoyar cada actividad dentro del protocolo.

3.5. Protocolo de respuesta y notificación de incidentes

El protocolo se estructura en cinco fases secuenciales, cuya activación depende de la naturaleza y magnitud del incidente detectado.

Fase 1: Detección y clasificación (Tiempo real). Constituye el punto de entrada del protocolo. Comprende la identificación de anomalías o vulnerabilidades en el sistema de IA o en las bases de datos biométricas. Los datos biométricos son calificados por el artículo 4 de la LOPDP como datos personales únicos relativos a características físicas o fisiológicas de una persona natural que permiten confirmar su identificación, como imágenes faciales o datos dactiloscópicos. Por su naturaleza, se encuadran además dentro de las categorías especiales de datos sensibles previstas en el artículo 25 de la LOPDP, lo que impone al responsable del tratamiento obligaciones reforzadas de seguridad conforme al artículo 37 de la norma ibídem.

Fase 2: Comité de crisis y contención (Inmediato). Activado el sistema de alerta, se procede al aislamiento de los activos comprometidos, que en el contexto del protocolo incluye los sistemas de IA e INTERPOL, y a la activación del paso migratorio manual como medida operativa de continuidad. Esta fase corresponde al deber del responsable y del encargado del tratamiento de implementar medidas de seguridad técnicas, organizativas y de cualquier otra índole para garantizar la confidencialidad, integridad y disponibilidad de los datos personales, estipulado en el artículo 10, literal j), en concordancia con el artículo 37 de la LOPDP.

Fase 3: Transparencia hacia los titulares (Término 3 días / según impacto). Esta fase distingue dos obligaciones:

La notificación al titular se activa cuando la vulneración conlleva un riesgo para sus derechos fundamentales y libertades individuales. El artículo 46 de la LOPDP fija en *tres (3) días* el término para notificar al titular, contados desde que el responsable del tratamiento tuvo conocimiento del riesgo. El contenido de la notificación deberá observar lo señalado en el artículo 43, el cual exige describir la naturaleza de la vulneración, las categorías y volúmenes aproximados de datos y titulares afectados, los datos de contacto del responsable o delegado de protección de datos, las consecuencias probables, y las medidas adoptadas o propuestas para remediar la vulneración.

La gestión de derechos, activada según el impacto, consiste en informar a los titulares sobre las medidas de mitigación y protección de derechos disponibles. Ello incluye el ejercicio de los derechos de acceso, rectificación, eliminación, suspensión del tratamiento y oposición reconocidos en los artículos 13 a 19 de la LOPDP, cuya atención debe producirse en el plazo de quince (15) días desde la solicitud del titular.

Fase 4: Notificaciones legales. Esta fase articula dos canales paralelos de notificación:

El artículo 43 de la LOPDP establece expresamente que el responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la SPDP y ARCOTEL tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, salvo que sea improbable que la violación constituya un riesgo para los derechos y libertades de las personas físicas. La misma

disposición precisa que, si la notificación no tiene lugar en ese plazo, deberá ir acompañada de indicación de los motivos de la dilación.

El segundo canal corresponde a la comunicación a con las demás entidades vinculadas, orientada al refuerzo de la sincronización de datos. Este canal refleja la obligación de coordinación interinstitucional para salvaguardar la integridad de los datos tratados en el contexto de la función migratoria, coherente con el artículo 36, numeral 1 y 3, que permite la transferencia de datos personales sin consentimiento del titular cuando los datos deban proporcionarse a autoridades administrativas en virtud de competencias atribuidas por la normativa vigente.

Fase 5: Análisis Post-Incidente (Finalizado). Concluido el ciclo de respuesta, el protocolo contempla la elaboración de un informe detallado, la actualización de la EIPD y la remediación de la vulnerabilidad. La EIPD es exigida por el artículo 42 de la LOPDP cuando el tratamiento, por su naturaleza o contexto, conlleve un alto riesgo para los derechos y libertades del titular, siendo obligatoria en particular cuando se trata de evaluación sistemática de aspectos personales basada en tratamiento automatizado. Adicionalmente, el artículo 47, numerales 3 y 7, obliga al responsable a implementar procesos de verificación, evaluación y valoración periódica de la eficacia de las medidas adoptadas, así como a tomar medidas para prevenir, impedir, reducir, mitigar y controlar las vulneraciones identificadas.

3.6. Registro de incidentes y documentación

El registro de incidentes referenciado en el Anexo 5 documenta cinco escenarios de violaciones de seguridad supuestos, construidos sobre la base del perfil tecnológico, normativo y organizacional del sistema biométrico objeto de análisis. Cada incidente

identifica los elementos exigidos por los artículos 4, 37, 43 y 46 de la LOPDP, la metodología de gestión de riesgos de la Guía SPDP 2025.

El cuadro integrado refleja: la cronología de detección, la naturaleza e impacto del incidente, los datos afectados, las consecuencias reales y potenciales, las medidas adoptadas, el estado de las notificaciones obligatorias a la SPDP y a los titulares, y la necesidad de EIPD.

CAPÍTULO IV

1. Ponderación de Derechos: Intimidad, Protección de Datos Personales y otros Derechos Fundamentales

El caso plantea un conflicto jurídico entre el derecho fundamental a la protección de datos personales y los derechos a la seguridad nacional e interés público, derivado de la implementación de un sistema de biometría multientidad que hace uso de inteligencia artificial para el control migratorio de viajeros, detectar alertas judiciales y prevenir delitos como la trata de personas y la suplantación de identidad. De esta manera, se garantiza el interés público (seguridad nacional) sobre el interés individual (protección de datos biométricos del titular). Sin embargo, surge la necesidad de precisar si dicho interés individual debe entenderse como la protección de los datos biométricos en particular por su carácter sensible, único e irreemplazable o como la manifestación del derecho general a la protección de datos personales. En efecto, los datos biométricos, al ser considerados categorías especiales de datos, requieren un nivel reforzado de garantías, lo que intensifica el conflicto frente a la prevalencia del interés público. Además, dicho conflicto radica en determinar si el tratamiento de datos biométricos realizado por la entidad pública de control migratorio a través de los sistemas de inteligencia artificial proporcionados por la empresa BioTrust, cumple con los principios, garantías, obligaciones y medidas establecidas en la normativa vigente. En este contexto, surge la necesidad de analizar si la seguridad en control migratorio constituye una base de legitimación suficiente para el tratamiento de datos personales, sin desconocer que la protección de datos biométricos representa un interés individual de mayor intensidad dentro del derecho general a la protección de datos.

La protección de datos personales de los titulares es el derecho directamente afectado, el cual garantiza que cada persona mantenga control sobre su información personal, especialmente cuando se trata de datos sensibles como los biométricos, exigiendo que el tratamiento de datos se realice de manera lícita, transparente y limitada a una finalidad específica, además del derecho a la intimidad y privacidad, así como a la dignidad humana. Por lo que se contrapone al derecho a la seguridad nacional, el cual protege a las personas frente amenazas, resguardando bienes jurídicos como la vida, la integridad personal y el orden público, lo que puede justificar la implementación de herramientas tecnológicas destinadas a prevenir delitos o fortalecer controles migratorios, siempre que dichas medidas sean necesarias y proporcionales. Por último, el interés público se fundamenta en la prevención del delito mediante el uso de tecnologías de reconocimiento facial por parte de la entidad pública de control migratorio. Los titulares de los datos personales son los viajeros, especialmente niñas, niños y adolescentes; y, personas con discapacidad.

A continuación, realizaremos un análisis de ponderación respecto a la idoneidad, necesidad y proporcionalidad:

Idoneidad. - Tomando en consideración de que la finalidad legítima es garantizar la seguridad nacional y la eficiencia en el control migratorio, por parte de la institución pública encargada de este control, consideramos que la implementación de un sistema de biometría que hace uso de inteligencia artificial en una medida idónea para el control migratorio de viajeros, detectar alertas judiciales y prevenir delitos como la trata de personas y la suplantación de identidad. La idoneidad de la medida se verifica en la capacidad de la biometría y la IA para identificar de manera precisa y rápida a las personas, reduciendo riesgos de suplantación de identidad y

fortaleciendo la seguridad aeroportuaria. Sin embargo, este análisis exige considerar alternativas menos invasivas con la privacidad, como el uso de documentos electrónicos con chips, códigos QR o sistemas de verificación basados en contraseñas dinámicas. Estas opciones, aunque útiles, no alcanzan el mismo nivel de certeza y rapidez que los datos biométricos, lo que demuestra que el uso de biometría e inteligencia artificial son las opciones más idóneas para cumplir el fin legítimo.

Necesidad. - El control migratorio implica el tratamiento masivo y continuo de datos personales y biométricos de ciudadanos nacionales y extranjeros, incluidos grupos vulnerables como menores de edad. En este contexto, los sistemas de IA permiten verificar identidades con mayor precisión, detectar alertas judiciales y prevenir delitos como la trata de personas y la suplantación de identidad. Además, facilitan respuestas inmediatas frente al alto flujo de pasajeros en terminales aéreas internacionales. No obstante, resulta imprescindible preguntarse si se ha valorado o confirmado que no existan otros tratamientos que permitan alcanzar los fines declarados sin incurrir en un nivel tan alto de riesgo. Dentro de los análisis realizados hemos valorado los métodos tradicionales de verificación migratoria, basados exclusivamente en la revisión manual de documentos y validaciones humanas, resultan insuficientes frente al volumen, velocidad y complejidad de las operaciones aeroportuarias actuales. Esto posibilita identificar alertas migratorias, documentos fraudulentos, suplantaciones de identidad y posibles casos de trata de personas de manera más eficiente que los mecanismos convencionales. En consecuencia, el uso de reconocimiento facial mediante IA constituye una medida necesaria y razonable para cumplir la finalidad pública de seguridad nacional y control migratorio, siempre que su implementación se realice bajo criterios minimización de datos, supervisión

humana y respeto a los derechos fundamentales reconocidos en la Constitución (CRE, 2008) y la normativa de protección de datos personales.

Proporcionalidad. - En este último análisis, se determina que el grado de satisfacción del interés público perseguido (la seguridad colectiva y prevención del delito) sí compensa la elevada afectación al derecho a la protección de datos personales de los viajeros, incluidos grupos vulnerables como menores de edad, cuyos datos biométricos son sensibles. Sin embargo, esta compensación no es automática; la proporcionalidad se mantiene únicamente si el beneficio obtenido para la sociedad supera el riesgo individual mediante la aplicación de salvaguardas obligatorias: la realización previa de una EIPD, responsabilidad proactiva entre la entidad pública de control migratorio y BioTrust, pero sobre todo supervisión humana efectiva en las decisiones automatizadas para evitar que sesgos de la IA deriven en discriminación, sesgos algorítmicos o detenciones injustas.

En conclusión, el control migratorio en aeropuertos para el tratamiento masivo de datos biométricos potenciado por inteligencia artificial, y bajo las condiciones de una implementación que garantice obligatoriamente la realización previa de una EIPD, la minimización de la información y una supervisión humana efectiva para mitigar sesgos algorítmicos, el derecho a la protección de datos personales sufre una restricción admisible en favor del interés público y la seguridad nacional. En consecuencia, esta restricción resulta constitucionalmente idónea, necesaria y proporcional, siempre que la entidad pública de control migratorio y BioTrust ejerzan responsabilidad proactiva que garantice la eficiencia tecnológica en la detección de delitos graves y no vulnere derechos fundamentales a la privacidad y dignidad de los viajeros.

2. Evaluación de Impacto a la Privacidad y Protección de Datos Personales

Descripción Sintética del Tratamiento

El tratamiento analizado consiste en gestionar las funciones de control migratorio, administración institucional y seguridad integral mediante el tratamiento de datos biométricos, con el fin de verificar identidades, cumplir obligaciones legales, proteger personas, instalaciones y sistemas institucionales, y prevenir riesgos que afecten la seguridad nacional, el orden público o el funcionamiento de la institución. Dicho tratamiento comprende biometría fisiológica (huella dactilar, reconocimiento facial e iris) y biometría conductual (reconocimiento de voz), utilizadas para identificación, autenticación y control de acceso. En este tratamiento, se emplean plataformas de reconocimiento facial con IA, sistemas de control migratorio, servicios de consulta biométrica y demográfica, integraciones con bases de datos nacionales e internacionales, y mecanismos biométricos de autenticación mediante huella, rostro, iris y voz. La IA fortalece la identificación de personas y la gestión de la seguridad, optimizando procesos migratorios; sin embargo, su uso requiere la aplicación de medidas de supervisión, auditoría y EIPD para mitigar riesgos relacionados con privacidad, sesgos algorítmicos, seguridad de la información y transparencia. Los sujetos afectados en este tratamiento corresponden a pasajeros nacionales y extranjeros, incluidos grupos de atención prioritaria, así como a funcionarios, servidores públicos, personal operativo, técnico, de seguridad y terceros autorizados vinculados a la entidad de control migratorio.

Justificación de la Obligatoriedad de la EIPD

La EIPD es obligatoria en este caso ya que el sistema de IA para control migratorio captura la biometría facial de titulares de forma masiva, asegurando el derecho a la seguridad en el ámbito migratorio. Eso es lo que la LOPDP (LOPDP, 2021) y el RGLOPDP (RGLOPDP, 2023), identifican como tratamientos de alto riesgo, ya que involucra el tratamiento de datos biométricos, decisiones automatizadas que tienen consecuencias jurídicas sobre los titulares. En ese sentido, el uso de IA para control migratorio es necesario porque reduciría el tiempo para verificar los datos biométricos de entrada y salida del país, facilitar operaciones logísticas, evitar el error humano mediante la automatización. Asimismo, es proporcional a la finalidad del tratamiento porque a través del uso de la IA se puede minimizar los datos de los titulares y en consecuencia se garantizaría la seguridad nacional y el interés público; es decir, el Estado otorgaría un servicio de calidad sin obviar su responsabilidad de proteger los datos personales de ciudadanos nacionales o extranjeros.

El tratamiento de datos biométricos en aeropuertos ecuatorianos se debería realizar con el apoyo de IA debido a que mejoraría en gran magnitud el servicio migratorio. Sin embargo, al hacerlo de forma manual no sería opcional por el volumen de personas que ingresan y salen del país a diario, lo que hace que el control migratorio de forma manual sea inviable, lento y propenso a errores. Un funcionario revisando documentos y rostros durante horas seguidas comete equivocaciones que un sistema de IA puede evitar. Sin embargo, toda decisión que afecte derechos de una persona debe pasar por la revisión de un funcionario que pueda contextualizar, cuestionar y corregir lo que el sistema arroje. En ese sentido, la ley no deja margen de duda ni de elección al responsable del tratamiento en este caso, la entidad de control migratorio, de que antes de poner en marcha este sistema de IA, debe hacer la EIPD, siendo este el único

mecanismo que la normativa diseñó específicamente para que se analice, documenten y reduzcan riesgos antes de que se materialicen en daños irreparables a los titulares o afectaciones a sus derechos.

Identificación de Riesgos Relevantes

Riesgos para los Derechos y Libertades. - La observación sistemática y masiva en zonas de acceso público mediante reconocimiento facial (biometría) genera un monitoreo persistente que puede restringir a los ciudadanos, afectando al derecho a la protección de datos personales, intimidad personal y familiar (Art. 66 num. 19 y 20, CRE).

Riesgos Tecnológicos. - Una vulneración de la confidencialidad en las bases de datos biométricas del proveedor BioTrust expondría rasgos físicos únicos e inalterables, facilitando la suplantación de identidad de forma irreversible, afectando al derecho a la protección de datos de carácter personal (Art. 66 num. 19 CRE) y al derecho a la seguridad integral (Art. 3 num. 8 CRE).

Riesgos de Sesgo y Discriminación. - El uso de algoritmos de Inteligencia Artificial (IA) para la identificación automática puede presentar tasas de error diferenciadas (falsos positivos/negativos) según el grupo étnico o género, derivando en retenciones migratorias arbitrarias, afectando al derecho a la igualdad y no discriminación (Art. 11 num. 2 CRE).

Riesgos para Grupos de Atención Prioritaria. - El tratamiento sistemático de datos faciales de niñas, niños y adolescentes que transitan por los aeropuertos sin medidas reforzadas de protección ante la IA, afectando al derecho del interés superior de niños, niñas y adolescentes (Art. 44 CRE).

Medidas de Mitigación Previstas o Propuestas

Las medidas de mitigación propuestas son las siguientes: en cuanto a los riesgos relacionados con derechos y libertades, se propone como medida técnica y organizativa, recolectar solo los datos estrictamente necesarios, aplicar técnicas de anonimización y cifrado, garantizar transparencia mediante avisos claros y habilitar mecanismos de supervisión independiente que permitan ejercer derechos como acceso y rectificación. Frente a los riesgos tecnológicos, las medidas técnicas que se plantean son las siguientes: un sistema de seguridad reforzado con cifrado avanzado, servidores certificados, autenticación multifactor, auditorías externas y planes de respuesta inmediata a incidentes, limitando el acceso únicamente a personal autorizado. Para prevenir el riesgo de sesgos y discriminación, como medidas organizativas se recomienda un plan de gobernanza algorítmica con evaluaciones de impacto, entrenamiento de modelos con datos diversos, supervisión humana en decisiones críticas, auditorías externas y canales de reclamo efectivos.

Finalmente, para riesgos relacionados con grupos de atención prioritaria, como medidas jurídicas, se requiere un plan de protección reforzada que aplique el principio del interés superior del niño, protocolos diferenciados para menores, anonimización de datos faciales, consentimiento informado de representantes legales, supervisión especializada con participación de la Defensoría del Pueblo y auditorías periódicas de la IA. De esta manera, las medidas son suficientes, realistas y efectivas, porque en conjunto, buscan equilibrar la seguridad migratoria con la protección de los derechos fundamentales, asegurando un tratamiento legítimo, proporcional y confiable.

Evaluación del Riesgo Residual

A pesar de la implementación de medidas técnicas, organizativas y jurídicas destinadas a mitigar los riesgos asociados al tratamiento de datos biométricos mediante IA, subsisten riesgos residuales relacionados con la afectación potencial de los derechos y libertades de los titulares, incidentes de ciberseguridad, sesgos algorítmicos, deficiencias en la gobernanza de datos y posibles impactos sobre grupos de atención prioritaria, especialmente niñas, niños y adolescentes. No obstante, dichos riesgos no permanecerían en un nivel alto, sino que se reducirían a un nivel medio o medio-bajo gracias a la aplicación de controles como cifrado de la información, limitación de accesos, supervisión humana de las decisiones automatizadas, auditorías periódicas y mecanismos de transparencia y rendición de cuentas. En consecuencia, el riesgo residual se considera jurídicamente aceptable, en la medida en que el tratamiento responde a una finalidad legítima de interés público vinculada al control migratorio y la seguridad nacional, cuenta con una base legal habilitante y observa los principios de necesidad, proporcionalidad y responsabilidad proactiva. Asimismo, estos riesgos pueden mitigarse razonablemente mediante la mejora continua de los controles de seguridad, la revisión permanente de los sistemas de IA, la capacitación del personal y el fortalecimiento de la gobernanza institucional, garantizando que la protección de los derechos fundamentales se mantenga como un elemento central durante todo el ciclo de vida del tratamiento de datos personales.

Conclusión

La EIPD permite concluir que el tratamiento es de riesgo aceptable condicionado. Esta determinación se fundamenta en que, si bien el uso de biometría (fisiológica y conductual) e inteligencia artificial para el control migratorio conlleva riesgos iniciales

para la privacidad, la intimidad y la protección de datos personales, la implementación rigurosa de las medidas de mitigación técnicas, organizativas y jurídicas, la anonimización, la supervisión humana y los protocolos diferenciados para grupos vulnerables logra reducir el impacto de un nivel alto a un nivel medio o medio-bajo.

El tratamiento se considera jurídicamente tolerable y proporcional dado que responde a una finalidad legítima de interés público y de seguridad nacional, siempre que se mantenga el cumplimiento estricto de las garantías previstas para salvaguardar los derechos de los titulares enfocándose en los grupos de atención prioritaria, evitando sesgos discriminatorios. La aceptabilidad del riesgo está supeditada a la ejecución permanente de los planes de gobernanza algorítmica y a la mejora continua de los controles de seguridad para evitar vulneraciones en las bases de datos que comprometan la identidad digital de los ciudadanos.

Fecha	Acciones	Nombres, Apellidos y Cargos	Firmas
01 de junio del 2026	Elaborado por:	• Jefe de TI. • Jefe Legal. • Analista de Protección de Datos Personales.	
01 de junio del 2026	Revisado por:	• Delegado de Protección de Datos Personales. • Oficial de Seguridad de la Información.	
02 de junio del 2026	Aprobado por:	• Responsable del Tratamiento (Representante Legal o Delegado de la Entidad de Control Migratorio).	

Tabla 2 - Firmas de Responsabilidad EIPD

3. Análisis de Viabilidad Jurídica, Decisión Final y Recomendaciones frente al Uso de Sistemas Biométricos

El presente dictamen jurídico analiza la viabilidad del uso de un sistema de biometría apoyado en inteligencia artificial para el control aeroportuario y migratorio, con base en la ponderación de derechos desarrollada en el documento de análisis constitucional y en los resultados de la Evaluación de Impacto relativa a la Protección de Datos Personales (EIPD). Su finalidad es emitir una decisión jurídica expresa, motivada y profesional sobre la licitud y viabilidad de la implementación, así como formular recomendaciones jurídicas y organizacionales acordes con el nivel de riesgo identificado.

Toma de Decisión Jurídica

A la luz del análisis normativo, la ponderación de derechos realizada y los resultados de la Evaluación de Impacto relativa a la Protección de Datos Personales, se concluye que el uso del sistema de biometría con inteligencia artificial para el control aeroportuario y migratorio es viable de manera condicionada. Esta viabilidad no es absoluta ni irrestricta. Su validez jurídica depende de que el tratamiento se mantenga estrictamente vinculado a la finalidad pública de control migratorio y seguridad nacional, que se apliquen de forma efectiva las medidas técnicas, organizativas y jurídicas de mitigación identificadas en la EIPD, y que se preserve de manera continua el equilibrio entre el interés público perseguido y los derechos fundamentales de los titulares de los datos personales, en particular cuando se trate de datos biométricos y de grupos de atención prioritaria.

Fundamentos de la Decisión

La presente decisión se fundamenta en que el tratamiento analizado recae sobre datos biométricos, una categoría especialmente sensible de datos personales, cuyo uso en contextos de observación sistemática y control masivo exige un estándar reforzado de licitud, finalidad, minimización, proporcionalidad, seguridad y responsabilidad proactiva. Desde la ponderación constitucional desarrollada en el análisis previo, existe una tensión entre el derecho a la protección de datos personales, la intimidad y la dignidad humana, por un lado, y la seguridad nacional, el orden público y el interés público, por otro, concluyéndose que la restricción al derecho fundamental solo puede considerarse admisible si supera de manera estricta los juicios de idoneidad, necesidad y proporcionalidad. En ese marco, la biometría con inteligencia artificial resulta idónea para fortalecer la verificación de identidad, detectar alertas y prevenir riesgos relevantes en el control migratorio, y se presenta como necesaria frente al alto volumen de tránsito aeroportuario y las limitaciones de los métodos exclusivamente manuales, aunque su uso no queda liberado de la obligación de aplicar salvaguardas reforzadas ni de valorar alternativas menos intrusivas cuando sean materialmente viables.

A ello se suma que la EIPD concluye que el tratamiento es de alto riesgo, pero que el mismo puede reducirse a un nivel medio o medio-bajo mediante medidas técnicas, organizativas y jurídicas como cifrado, limitación de accesos, auditorías, gobernanza algorítmica, transparencia, supervisión humana efectiva y protocolos diferenciados para grupos de atención prioritaria. Por tanto, la viabilidad jurídica se sostiene en la convergencia de tres elementos: la existencia de una finalidad legítima constitucionalmente relevante, la superación condicionada del test de proporcionalidad y la constatación de que el riesgo residual es jurídicamente aceptable solo si el

responsable del tratamiento mantiene un cumplimiento continuo y verificable. En consecuencia, la decisión favorable no es absoluta, sino estrictamente condicionada a que las garantías identificadas en la EIPD operen de forma real y permanente durante todo el ciclo de vida del tratamiento.

Recomendaciones Jurídicas y Organizacionales

Dado que la decisión adoptada es de viabilidad condicionada, la implementación del sistema no debe autorizarse en términos generales o irrestrictos, sino bajo condiciones de despliegue progresivo, controlado y verificable. En consecuencia, se formulan las siguientes recomendaciones jurídicas y organizacionales.

Reducción del Alcance

El sistema debe limitarse estrictamente a operaciones de control migratorio y seguridad aeroportuaria debidamente definidas, evitando usos secundarios incompatibles, ampliaciones funcionales no evaluadas previamente o reutilización de datos biométricos para finalidades distintas a las justificadas en la EIPD. Asimismo, debe aplicarse una lógica de necesidad reforzada para determinar en qué puntos del proceso migratorio la biometría resulta verdaderamente indispensable y en cuáles pueden emplearse mecanismos menos intrusivos. Esta reducción del alcance es coherente con el análisis de ponderación, que admite la restricción del derecho únicamente cuando el tratamiento se mantenga dentro de parámetros estrictos de minimización y finalidad legítima. También se recomienda segmentar el uso del sistema respecto de categorías de titulares y escenarios de riesgo. Para grupos de atención prioritaria, especialmente niñas, niños y adolescentes, deben establecerse protocolos diferenciados, controles

reforzados y restricciones adicionales de tratamiento, conforme al riesgo específico identificado en la EIPD.

Alternativa No Biométrica Obligatoria

La alternativa no biométrica es la vía manual para el control migratorio, esta vía debe reposar en procedimientos documentales y de verificación humana suficientemente robustos, como: revisión presencial de documentos de viaje, contrastación visual de identidad, consultas a bases de datos por canales tradicionales, de modo que no implique una desventaja irrazonable, un trato discriminatorio ni dilaciones excesivas frente al canal automatizado con biometría. En términos organizacionales, la aplicación de esta vía alternativa exige dotar de recursos y capacitación específica al personal encargado, y establecer criterios claros para activar esta vía alternativa (manual).

Reevaluación Periódica

La EIPD no debe entenderse como un acto único de cumplimiento formal, sino como una herramienta dinámica de gobernanza que debe actualizarse cuando existan cambios tecnológicos, normativos, operativos o contextuales que modifiquen el nivel de riesgo o la proporcionalidad del tratamiento o de forma periódica cada 12 meses. En el plano jurídico y organizacional, esta actualización implica revisar periódicamente la precisión del sistema, los sesgos algorítmicos, la eficacia de las medidas de seguridad, la suficiencia de los controles de acceso, la trazabilidad de las decisiones, los incidentes de seguridad registrados y el funcionamiento de los canales de reclamo y tutela de derechos. También exige auditorías independientes y mecanismos de rendición de

cuentas que permitan demostrar que el riesgo residual sigue siendo jurídicamente aceptable y que no se ha producido un desvío funcional del sistema.

Cierre Jurídico

La decisión adoptada no implica una valoración abstracta de la biometría ni una habilitación general e incondicionada de su uso por parte de la administración pública. Se trata, más bien, de una conclusión contextual, concreta y jurídicamente fundada, construida a partir de la finalidad perseguida, de la intensidad de la injerencia en derechos fundamentales, del juicio de proporcionalidad aplicado y de los resultados de la EIPD. En consecuencia, la viabilidad jurídica reconocida "viable de manera condicionada" permanece sujeta a revisión ante cambios tecnológicos, normativos o fácticos que alteren el equilibrio entre seguridad nacional, interés público y protección de datos personales. Si las condiciones de necesidad, minimización, supervisión humana, alternativa no biométrica, protección reforzada para grupos vulnerables, seguridad de la información o gobernanza algorítmica dejan de cumplirse de forma efectiva, la base jurídica de admisibilidad también debe ser reconsiderada.

CAPÍTULO V

1. CONCLUSIONES GENERALES

1. La investigación determinó que el uso de sistemas biométricos con inteligencia artificial en el control migratorio es factible desde el punto de vista jurídico, siempre que se garantice el cumplimiento de la normativa de protección de datos personales. Además, se concluyó que una adecuada gestión de riesgos y la aplicación de medidas preventivas de privacidad son esenciales para proteger los derechos de los ciudadanos y asegurar un equilibrio entre la seguridad nacional y la protección de datos.
2. La implementación de sistemas biométricos con inteligencia artificial en las entidades públicas de control migratorio de los aeropuertos del Ecuador es jurídicamente viable, siempre que se sustente en una base legal válida y cumpla los principios de protección de datos personales previstos en la normativa ecuatoriana.
3. El uso de biometría puede fortalecer la seguridad nacional y eficiencia de los procesos operativos, en lo relativo al control migratorio en aeropuertos del país, por lo cual, resulta recomendable; sin embargo, debido a la naturaleza sensible e irreversible de estos datos, su utilización debe estar acompañada de medidas reforzadas de seguridad, transparencia y gobernanza.
4. La Evaluación de Impacto en la Protección de Datos constituye un requisito fundamental para identificar, evaluar y mitigar los riesgos asociados al tratamiento de datos biométricos, permitiendo determinar si la implementación del sistema biométrico resulta necesaria, proporcional y justificable.

1.2 CONCLUSIONES ESPECÍFICAS

2.1. Utilidad de la Propuesta en un Entorno Específico

La propuesta constituye una referencia práctica para entidades públicas que implementen sistemas biométricos con inteligencia artificial, facilitando la identificación de riesgos, el cumplimiento normativo y la aplicación de medidas de protección de datos personales.

2.2. Análisis del Cumplimiento de los Objetivos de la Investigación

La investigación cumplió su objetivo general y los objetivos específicos al determinar la viabilidad jurídica condicionada del uso de biometría en el control migratorio, analizar el marco normativo aplicable e identificar los riesgos e impactos sobre los derechos fundamentales de los titulares.

2.3. Contribución a Nivel Académico

El estudio aporta al desarrollo académico de la protección de datos personales, especialmente en materia de privacidad desde el diseño y por defecto (SPDP-SPD-2025-0040-R, 2025) aplicada a sistemas biométricos e inteligencia artificial, generando un referente para futuras investigaciones.

2.4. Contribución a Nivel Personal

La investigación fortaleció competencias jurídicas, técnicas y analíticas relacionadas con la protección de datos personales, promoviendo una visión interdisciplinaria para abordar los desafíos legales y éticos de las tecnologías emergentes.

2.5. Limitaciones de la Investigación

Las principales limitaciones fueron la escasa casuística nacional sobre biometría e inteligencia artificial y el carácter predominantemente jurídico-documental del estudio, sin incluir pruebas técnicas o evaluaciones operativas de sistemas reales.

BIBLIOGRAFÍA NACIONAL

CRE. (20 de octubre de 2008). *Constitución de la República del Ecuador*.

LOGJCC. (22 de octubre de 2009). *Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional*.

LOMH. (23 de octubre de 2018). *Ley Orgánica de Movilidad Humana*.

LOPDP. (26 de mayo de 2021). *Ley Orgánica de Protección de Datos Personales*.

RGLOPDP. (13 de noviembre de 2023). *Reglamento General a la Ley Orgánica de Protección de Datos Personales*.

SPDP-SPD-2025-0006-R. (30 de abril de 2025). *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, Resolución Nro. SPDP-SPD-2025-0006-R*.

SPDP-SPD-2025-0040-R. (13 de noviembre de 2025). *Guía de Protección de Datos Personales Desde el Diseño y por Defecto, Resolución Nro. SPDP-SPD-2025-0040-R*.

SPDP-SPD-2026-0005-R. (25 de febrero de 2026). *Norma General sobre el Tratamiento de Datos Personales a Gran Escala, Resolución Nro. SPDP-SPD-2026-0005-R*.

SPDP-SPD-2026-0009-R. (12 de febrero de 2026). *Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial, Resolución Nro. SPDP-SPD-2026-0009-R*.

SPDP-SPD-2026-0012-R. (30 de marzo de 2026). *Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales V2, Resolución Nro. SPDP-SPD-2026-0012-R*.

BIBLIOGRAFÍA INTERNACIONAL

LFPD. (6 de julio de 2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. México.

LGPD. (8 de septiembre de 2020). *Ley General de Protección de Datos*. Brasil.

OEA. (2015). *LMPDP*. Obtenido de https://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo.asp?utm_source

ANEXOS

1. **Anexo 1:** Política Institucional de Protección de Datos Personales
2. **Anexo 2:** Matriz RACI
3. **Anexo 3:** Aviso Interno de Privacidad y Protección de Datos Personales
4. **Anexo 4:** Matriz de Riesgos
5. **Anexo 5:** Registro de Incidentes

Anexo 1

Política Institucional de Protección de Datos Personales

POLÍTICA INSTITUCIONAL DE PROTECCIÓN DE DATOS PERSONALES

ENTIDAD PÚBLICA DE CONTROL MIGRATORIO

2026

ELABORACION:	APROBACION:	REVISION:	APROBACION:
Departamento Legal	Director Nacional de Migración y Extranjería	Delegado de Protección de Datos Personales	Ministro del interior

1. Objetivo

Cumplir con la legislación vigente en materia de protección, manejo y el tratamiento adecuado de los datos personales a los que tiene acceso en la operación regular de sus servicios migratorios y de extranjería, ya sean datos de ciudadanos nacionales o extranjeros, funcionarios, proveedores, usuarios del sitio web de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO del Ecuador, Organismo Adscrito al Ministerio del Interior a fin de asegurar el respeto por los derechos de sus titulares, así como el cumplimiento del marco normativo vigente.

2. Alcance

El presente documento es aplicable a todas las bases de datos personales o información destinada a estar contenida en bases de datos de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, así como al tratamiento de dichas bases de datos por parte de este Organismo o por parte de terceros encargados.

Todos los funcionarios de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO se encuentran obligados a conocer y cumplir todas y cada una de las disposiciones de esta Política.

3. Documentos de referencia

El artículo 66, numeral 19 de la Constitución de la República del Ecuador, la Ley Orgánica de Protección de datos personales y su Reglamento y normativa técnica emitida por la Superintendencia de Datos Personales.

4. Definiciones

- **Datos personales:** toda información sobre una persona natural que la identifica o la hace identificable a través de medios que puedan ser razonablemente utilizados.
- **Datos sensibles:** datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; pasado judicial; condición migratoria; identidad cultural; afiliación sindical e información relacionada a la salud o a la vida sexual e identidad de género.
- **Bases de datos:** conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.
- **Tratamiento de datos personales:** cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

- **Titular de datos personales:** persona natural a quien corresponden los datos personales. En el caso de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO podrán ser ciudadanos nacionales o extranjeros que hagan uso de los servicios de migración y extranjería, los funcionarios, proveedores personas naturales y terceros cuyos datos hayan llegado a una base de datos de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO.
- **Titular de la base de datos:** persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido de la base de datos personales, el tratamiento de estos y las medidas de seguridad.
- **Transferencias Internacionales de Datos Personales:** Envío de datos personales desde un país a otro, sujeto a regulaciones para garantizar un nivel adecuado de protección de la información en el destino.
- **Encargado del tratamiento:** persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando juntamente con otra, realiza el tratamiento de los datos personales por encargo del titular de la base de datos personales o el responsable de tratamiento.
- **Cedente:** es aquella persona que entrega o transfiere un bien o un derecho a otra.
- **Cesionario:** es la persona que recibe un derecho de parte de otra
- **Normas institucionales vinculantes:** Reglas internas adoptadas por el Estado Ecuatoriano para permitir transferencias internacionales de datos personales dentro del mismo, cumpliendo con estándares de protección de datos.
- **Autoridad nacional de protección de datos personales:** Se refiere, en Ecuador, a la Superintendencia de Protección de Datos Personales o SPDP.

5. Disposiciones Generales

5.1. Confidencialidad

La Información personal a la que los funcionarios de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO y/o terceros tengan acceso tiene carácter confidencial y no podrá ser divulgada, comunicada ni compartida con terceros sin contar con el consentimiento previo del titular de la información, salvo las excepciones establecidas en la Ley.

Todas las personas que intervengan en el tratamiento de la información están obligadas a guardar el secreto profesional y a mantener la confidencialidad respecto de estos. Dicha obligación se mantendrá aún después de finalizada la relación que une a esas personas con LA ENTIDAD PÚBLICA DE CONTROL MIGRATORIO.

5.2. Principios

LA ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, a través de la presente política tiene por principio básico garantizar que la información personal de todas las personas naturales cuyos datos maneje sean protegidas bajo los preceptos de la norma vigente, así como los mejores estándares aplicados al sector.
LA ENTIDAD PÚBLICA DE CONTROL MIGRATORIO se preocupa por que toda persona tenga el derecho a controlar la información que comparte con terceros, así como el derecho a que ésta se

utilice de forma apropiada. Por este motivo, en sus actividades regulares de negocio, la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO respeta los principios establecidos en la legislación:

- **Actuamos con legalidad:** El tratamiento de la Información realizado por la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO se realizará conforme a lo establecido en la Ley, demás normativa y jurisprudencia aplicable. Se encuentra prohibida la recopilación de información por medios fraudulentos, desleales o ilícitos.

- **Tratamiento legítimo, siempre:** La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO no podrá tratar Información si no cuenta con el consentimiento previo, expreso, inequívoco y libre de su titular, o una justificación legal, contractual o de interés del titular o de la empresa que amerite su tratamiento.

- **Tratamiento con finalidades reales:** La Información debe ser recopilada y utilizada por la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, para una finalidad determinada al inicio de nuestros procesos y alineado a nuestra estrategia institucional. El tratamiento de dichos datos no se extenderá a cuestiones ajenas a los servicios de migración y extranjería, para fines personales o de terceros que no hayan sido previamente informados o que no formen parte de nuestros procedimientos normales.

- **Utilizamos los datos de manera ordenada y proporcional a las necesidades institucionales:** Todo tratamiento de la Información realizado por la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, deberá ser adecuado, necesario, oportuno, relevante y no excesivo a la finalidad para la que la información hubiese sido recopilada

- **Aseguramos la calidad de los datos que manejamos:** La Información que vaya a ser tratada por la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, debe ser veraz, exacta, íntegra, precisa, completa, comprobable, clara y en la medida de lo posible, actualizada, necesaria, pertinente y adecuada respecto de la finalidad para la que fue recopilada. Dicha Información deberá conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan, salvo dichos datos hayan sido obtenidos de fuentes accesibles al público o del mismo titular

- **Nos alineamos con el mejor estándar de seguridad de la información:** La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO y todos los aliados estratégicos que intervengan en el ciclo de vida de los datos personales, incluyendo los terceros que actúen como encargados del tratamiento de bases de datos personales deberán adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de la información y proteger los datos personales frente a cualquier riesgo, amenaza o vulnerabilidad. Éstas deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de la información que se trate. La empresa asegurará que esto conste como parte de las relaciones contractuales y comerciales vigentes y procurará evaluar continuamente su cumplimiento, dependiendo de la criticidad.

- **Transferencias internacionales:** La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO realizará transferencias internacionales de la Información personal solo a aquellos proveedores que garanticen un nivel suficiente de protección para la información que se vaya a tratar o por lo menos equiparable a lo establecido en esta política y la normativa ecuatoriana vigente.

- **Somos leales a los titulares de los datos personales:** El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados.
En ningún caso los datos personales podrán ser tratados a través de medios o para fines ilícitos o desleales.

- **Somos transparentes con los titulares de los datos:** Para asegurar la transparencia, toda información o comunicación relativa a los tratamientos que ejecuta la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO deberán ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro. Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la Ley de Protección de Datos Personales, su reglamento y demás normativa atinente a la materia.

- **Datos pertinentes y mínimamente requeridos:** Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento.

- **Conservamos los datos únicamente mientras sea necesario:** Los datos personales se conservarán solo durante el tiempo en que exista una necesidad o justificación válida para su almacenamiento. Esta necesidad estará determinada por la finalidad específica de cada proceso y por lo establecido en la normativa vigente.

- **Responsabilidad proactiva y demostrada:** La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO apoyará y participará activamente en la implementación y mejora de estándares, mejores prácticas, esquemas de auto y co-regulación, como códigos de conducta en protección de datos, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo aplicable a sus servicios de migración y extranjería. Además, mantendrá buena relación y rendirá cuentas sobre el tratamiento a los titulares y a la Autoridad de Protección de Datos Personales, cuando sea necesario. Adicionalmente, a fin de demostrar cumplimiento a largo plazo, la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO realizará procedimientos de auditoría interna para asegurar la mejora continua del esquema de protección de datos personales.

5.3. Bases de datos

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, llevará un Registro de Actividades de Tratamiento y conforme los procedimientos que determine la Autoridad de Protección de Datos Personales, misma que presentará ante el Registro Nacional de Datos Personales.

6. Gobierno de protección de datos personales

En cumplimiento de la Ley Orgánica de Protección de Datos Personales, LA ENTIDAD PÚBLICA DE CONTROL MIGRATORIO implementará un sistema integral de gobernanza de datos personales que comprenderá, entre otros elementos:

- La designación de un Delegado de Protección de Datos Personales.
- La creación de un Comité de Protección de Datos Personales, encargado de documentar sus deliberaciones mediante actas formales.
- La conformación de un equipo de Responsables de Protección de Datos Personales (PDP) en las áreas clave de la institución o por proceso, acorde con las definiciones de los Data Owners.
- La capacitación continua a los funcionarios en materia de protección y gestión de datos personales.

7. Finalidades Generales para el Tratamiento de Datos Personales

7.1. Identificación de entrada y salida del país de personas naturales para el control migratorio.- La finalidad para el tratamiento de datos personales de los usuarios de los servicios de migración y extranjería, será la identificación en tiempo real de personas naturales mediante reconocimiento facial e IA, para el registro de entrada y salida del país, control de impedimentos, identificación de personas requeridas por la justicia nacional e internacional, prevención del delito de trata de personas o localización y protección de menores en el punto de control migratorio del Aeropuerto Internacional Mariscal Sucre.

7.2. Verificación de pasaportes biométricos.- La finalidad para el tratamiento de datos personales de los usuarios de los servicios de migración y extranjería, será realizar el cotejamiento de datos del pasaporte biométrico para la identificación de personas con impedimentos de salida del país ante autoridades nacionales.

7.3. Control de acceso de los funcionarios de la DME o terceros autorizados a las salas de video vigilancia. - La finalidad para el tratamiento de datos personales de los funcionarios de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO será el reconocimiento del iris de dichos funcionarios o terceros autorizados para el control de acceso a las salas de videovigilancia del del Aeropuerto Internacional Mariscal Sucre.

7.4. Control de acceso a oficinas institucionales mediante reconocimiento de voz de los empleados de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO.- La finalidad para el tratamiento de datos personales de los funcionarios de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO será la de gestionar y controlar el acceso del personal autorizado a las oficinas de la Dirección de Migración del Ecuador en las instalaciones ubicadas en el Aeropuerto Internacional Mariscal Sucre, mediante sistemas de autenticación biométrica por reconocimiento de voz, con el fin de fortalecer la seguridad institucional y proteger instalaciones, información y bienes institucionales.

7.5. Control de acceso al Data Center mediante reconocimiento de huellas dactilares de los funcionarios de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO.- La finalidad para el tratamiento

de datos personales de los funcionarios de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO será la de gestionar y controlar el acceso de personal autorizado al Data Center de la mencionada institución, mediante un sistema de autenticación biométrica por reconocimiento de huellas dactilares, con el fin de fortalecer la seguridad y proteger información y bienes institucionales.

7.6. Postulantes a cargos en la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO. - La información recopilada sobre los postulantes a puestos de trabajo se utilizará para gestionar su candidatura a los puestos de trabajo ofrecidos por LA ENTIDAD PÚBLICA DE CONTROL MIGRATORIO y en los casos que amerite, para conservarla, según la autorización del postulante, para próximas postulaciones.

7.7. Funcionarios de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO.- La información recopilada sobre los funcionarios de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO se utilizará para gestionar la relación laboral que sostienen con la mencionada institución, para evaluar el nivel de productividad y cumplimiento de las políticas y estándares internos, incluyendo mediciones de rendimiento, para cumplir con la normativa aplicable en materia laboral así como para auditorías internas, externas y controles realizados por autoridades públicas.

7.8. Proveedores de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO. - La información recopilada sobre proveedores se utilizará para gestionar su relación comercial de prestación de servicios o comercialización de bienes a favor de ENTIDAD PÚBLICA DE CONTROL MIGRATORIO y asegurar cumplimiento con la normativa aplicable o con políticas y estándares definidos por la mencionada institución.

7.9. Sistemas de video vigilancia. - La información recopilada por medio de nuestros sistemas de videovigilancia será utilizada a fin de preservar la seguridad de los establecimientos, bienes muebles e infraestructura de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO.

8. Derechos de los titulares de la información

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, contará con un procedimiento sencillo y gratuito de atención de los derechos de los titulares de la Información contemplados en la Ley, entre ellos el derecho de información, acceso, actualización, inclusión, supresión, oposición y portabilidad, entre otros.

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO realizará las acciones necesarias para informar al titular de la información sobre los derechos conferidos por la legislación, atendiendo de manera oportuna y dentro de los plazos todas las solicitudes y requerimientos relacionados con dichos derechos.

En los procesos de atención de derechos de titulares de la información serán de aplicación las siguientes directrices:

- La supresión o rectificación de la Información no procederá cuando ello afecte derechos o intereses legítimos de LA ENTIDAD PÚBLICA DE CONTROL MIGRATORIO o cuando exista una obligación legal de conservación de la información.

- La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, podrá rechazar determinados requerimientos cuando la divulgación de la información pueda comprometer u obstaculizar actuaciones judiciales o administrativas en curso.
- La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, podrá rechazar actuaciones que sean desproporcionadas e inejecutables, analizando caso por caso con asesoría del Delegado de Protección de Datos.

Los titulares de los derechos podrán iniciar sus solicitudes por medio del llenado y entrega del formulario de ejercicio de derechos de datos personales de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, exclusivamente a través de los canales oficiales autorizados en el portal web de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO o de forma presencial en sus oficinas a nivel nacional. El trámite de dichas solicitudes se sujetará a la normativa vigente en materia de protección de datos personales y al procedimiento interno establecido por la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO para su gestión.

9. Transferencias de la información

La información personal transferida entre áreas se limitará a las medidas de seguridad de la información determinadas en las políticas internas de la institución, respetando mecanismos seguros y autorizados, privilegios mínimos y necesidad proporcional. Las áreas no podrán compartir información entre ellas por aplicaciones, plataformas, dispositivos o aplicativos no autorizados que puedan comprometer la integridad de la información

La información objeto de tratamiento por parte de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO sólo podrá ser cedida o transferida a terceros para el cumplimiento de los fines relacionados con el interés legítimo del cedente y del cesionario, siempre que cuenten con el consentimiento previo, expreso, libre, inequívoco e informado del titular de la Información o concurra una base legal para su tratamiento. Dicho consentimiento no será requerido en los supuestos permitidos por la normativa en materia de protección de datos personales.

Como regla general, la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO no transferirá o comunicará la Información a terceros, salvo en los siguientes casos:

- Cuando sea necesario para la finalidad para la que la información fue recopilada.
- Cuando se le informe al titular de la información antes de la divulgación o al momento de la recopilación de la Información y se obtenga su consentimiento previo y expreso.
- Cuando el consentimiento no sea exigido.
- Cuando la información sea requerida por entidades públicas en el ámbito de sus competencias y en el ejercicio de sus funciones y atribuciones.
- Cuando la información sea solicitada en virtud de órdenes judiciales o disposiciones legales.
- Cuando se trate de acceso a la información por parte de auditores, abogados y demás profesionales en ejercicio de sus funciones, obligados a guardar el secreto profesional.
- Cuando los datos han sido recogidos de fuentes accesibles al público;

- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica entre el responsable de tratamiento y el titular, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con base de datos.
- Cuando la comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando dichos datos se encuentren debidamente disociados o a lo menos anonimizados.
- Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que implique intereses vitales de su titular y este se encontrare impedido de otorgar su consentimiento.
- Cuando la comunicación de datos de carácter personal sea necesaria para realizar estudios epidemiológicos de interés público, dando cumplimiento a los estándares internacionales en la materia de derechos humanos.

10. Flujo transfronterizo o transferencia internacional de datos

Para todas las actividades de transferencia internacional de datos personales sin excepción se ha de cumplir con los siguientes requerimientos legales y organizativos:

- Identificar las fuentes y receptores de información vía cesión o transferencia que involucren a la compañía.
- Incluir cláusulas contractuales estándar en contratos o acuerdos con proveedores extranjeros.
- Suscribir adendas con todos los proveedores internacionales.
- Realizar la transferencia bajo normas corporativas vinculantes.

Todas las actividades de transferencia de datos personales han de ser registradas apropiadamente.

Todas las actividades de transferencias internacionales de datos personales han de cumplir con las siguientes obligaciones con relación a la Autoridad nacional de protección de datos personales:

- Revisión de que el país conste como de nivel adecuado de protección para la transferencia de datos acorde con la Superintendencia de Protección de Datos Personales.
- Solicitar autorización a la autoridad para realizar transferencias de datos en caso de ser necesario.
- Aplicar el procedimiento apropiado en casos excepcionales reconocidos por la norma.

11. Tratamiento de datos sensibles y de categoría especial

LA ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, recopila y trata información y/o datos sensibles como parte de sus servicios institucionales tanto de usuarios como de funcionarios de la institución, particularmente información biométrica (huellas, rostro, iris), datos de salud, antecedentes judiciales y detalles sobre nacionalidad o condición migratoria. Estos tratamientos respetarán los principios de finalidad y proporcionalidad y, ocurrirán únicamente bajo los supuestos que habilitan el tratamiento de datos sensibles de conformidad con la Ley.

LA ENTIDAD PÚBLICA DE CONTROL MIGRATORIO se compromete al tratamiento responsable de datos de categoría especial mantenido medidas de seguridad que incluyen, pero no se limitan a:

- Restringir el acceso a los datos únicamente a funcionarios autorizados.
- Utilizar la información únicamente para la finalidad para la cual fueron recogidos.
- Anonimizar o seudonimizar datos según amerite.

12. Medidas de seguridad

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO implementará las medidas de seguridad técnicas y organizativas necesarias para garantizar la protección de la información y evitar su alteración, pérdida, tratamiento y/o acceso no autorizado conforme a las políticas internas de seguridad informática.

En este sentido, la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO cumplirá con la legislación vigente en materia de medidas de seguridad para la protección de datos personales, específicamente en lo concerniente a los siguientes puntos:

- Control y registro de accesos y privilegios, así como su verificación periódica.
- Registro de eventos, interacciones lógicas,
- Identificación y autenticación de usuarios por medio de la gestión y uso de contraseñas.
- Copias y backups de la información de forma controlada y autorizada.
- Seguridad en los ambientes de procesamiento de datos personales.
- Registro de Bases de Datos/Ficheros manuales y físicos (Excel, archiveros, etc.).
- Depurar archivos no necesarios o duplicados que contengan información personal.
- Implementar medidas seguras de transferencia de información interna y con terceros.
- Depurar accesos y restringir descargas desde sistema que contenga Información personal.
- Mantener procedimientos de actualización de datos.
- Definir estrategias de buen uso de información personal en Gobierno de Datos.

En general la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO y todos sus funcionarios que trabajen con datos personales cumplirán con las medidas de seguridad correspondientes a la naturaleza de la información objeto de tratamiento de conformidad con lo establecido en la legislación.

13. LA ENTIDAD PÚBLICA DE CONTROL MIGRATORIO Tratamiento por terceros – encargados del tratamiento

Toda vez que la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO encargue o sub encargue el tratamiento de una base de datos a un tercero o permita el acceso de terceros a sus bases de datos para la prestación de algún servicio específico, se deberán tener en cuenta las siguientes especificaciones:

- Todo tratamiento de la información realizado por un tercero distinto a la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, deberá estar regulado en un contrato,

estableciéndose expresamente que el tratamiento de la Información se realizará siguiendo las instrucciones de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO o las del cliente corporativo a cargo y, que únicamente se tratará la Información para los fines autorizados o establecidos en el contrato, por lo que el encargado no los utilizará con una finalidad distinta, ni los comunicará indebidamente a otras personas.

- Se identificará a todos los encargados de tratamiento y se precalificará la criticidad del proveedor según las actividades de tratamiento que ejecute en uno o varios servicios.
- El contrato deberá estipular las medidas de seguridad que el encargado del tratamiento está obligado a implementar, tales como la devolución o destrucción de la información una vez finalizado el encargo.
- El contrato deberá establecer que, en caso de incumplimiento el infractor responderá ante el titular y ante las autoridades por todo tratamiento o uso no autorizado de la información.
- Si el encargado del tratamiento necesita subcontratar con terceros para brindar parte de los servicios que se obligó a ofrecer, deberá contar con la autorización previa de la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO y ésta sólo procederá siempre que el subcontratista asuma las mismas obligaciones que el encargado del tratamiento.
- El contrato deberá establecer además obligaciones de confidencialidad respecto a la información a la que accede el encargado del tratamiento, manteniéndose dichas obligaciones en vigor aún después de finalizado el plazo de vigencia del contrato.
- Se mantendrá un registro actualizado de encargados de tratamiento y se ejecutarán evaluaciones continuas del cumplimiento para los proveedores determinados como críticos.

14. Eliminación, bloqueo, disociación o anonimización de la información

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO, procederá a bloquear o eliminar la información de sus registros una vez que haya finalizado el tratamiento de la información, se haya cumplido con el principio de finalidad y no exista obligación legal, contractual, requerimiento de autoridad competente, necesidades técnicas y organizativas u otra razón que justifique la conservación de la información.

Alternativamente, se podrá aplicar procesos de anonimización, seudonimización, disociación o equivalentes cuando por alguna razón institucional, de estadística o de análisis se justifique la conveniencia de conservar la información. La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO definirá oportunamente los procedimientos respectivos que resulten necesarios para la eliminación de la información.

15. Análisis de riesgos y Evaluaciones de impacto en la Privacidad (EIP)

Como regla general la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO se compromete a realizar la pertinente Evaluación de Impacto respecto del tratamiento de datos personales cuando estos impliquen:

- Evaluación sistemática y exhaustiva de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles cuyas decisiones sean jurídicamente vinculantes para el titular.
- Tratamiento a gran escala de categorías especiales de datos o datos relativos a condenas e infracciones penales.
- Observación sistemática a gran escala de una zona de acceso público.

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO posee y aplica procedimientos de identificación, mitigación y reporte de riesgos conforme la normativa nacional vigente.

16. Registro de Actividades de Tratamiento

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO en concordancia con las obligaciones establecidas en la normativa vigente mantendrá un registro anualmente actualizado de las actividades de tratamiento realizadas que detalle:

- Categorías de Titulares.
- Destinatarios y Encargados del tratamiento de datos.
- Transferencias Internacionales.
- Bases Legitimadoras (consentimiento, interés legítimo, obligación).

Para cumplir cabalmente con la obligación se procederá con la descentralización del registro y se realizaran capacitaciones a los responsables del registro.

17. Interacción con la Autoridad de Protección de Datos Personales

En cumplimiento de la normativa nacional y sus obligaciones frente a la autoridad nacional de protección de datos personales la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO acata sus obligaciones respecto a:

- Mantener un registro de sus comunicaciones con la autoridad.
- Mantener al día sus entradas en el Registro Nacional de Protección de Datos.
- Registrar las transferencias internacionales de datos personales.

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO en los casos pertinentes se compromete a acatar las medidas correctivas impuestas por la autoridad en el contexto de medidas preventivas o después de una sanción.

18. Violaciones de seguridad de datos personales

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO mantendrá procedimientos para la notificación de vulneraciones de seguridad tanto al titular como a la Autoridad de Protección de Datos Personales y a la ARCOTEL cuando sea pertinente.

En relación con la respuesta y detección temprana de brechas de seguridad la ENTIDAD PÚBLICA DE CONTROL MIGRATORIO implementará procesos, controles técnicos y organizativos.

19. Legitimación , Información y Consentimiento.

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO identificará y documentará todos los canales de recepción de datos personales, tanto propios como de terceros en calidad de Encargados, incluyendo medios físicos y digitales.

Se garantizará que todos los canales digitales de recolección de datos incluyan los Avisos de Privacidad en lenguaje claro, visible y fácilmente accesible; y se informará presencialmente en eventos o espacios físicos de contacto con titulares.

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO informará de forma activa y oportuna a los titulares y demás aliados estratégicos sobre cualquier cambio sustancial en sus Avisos de Privacidad.

Se implementarán mecanismos de obtención de consentimiento para clientes actuales y nuevos, incluyendo avisos legales digitales y cláusulas en formularios físicos dirigidos a clientes, proveedores y funcionarios.

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO mantendrá registros detallados de los consentimientos otorgados, incluyendo fecha, hora, medio de obtención y categoría del titular; así como un registro de solicitudes de retirada de consentimiento y listas de no contacto segmentadas por sistema.

Cuando aplique, se realizará y documentará un análisis de interés legítimo como base de legitimación para actividades específicas.

20. Privacidad desde el diseño y por defecto

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO adoptará medidas para garantizar la aplicación del principio de Privacidad desde el Diseño y por Defecto (PbDyd), incluyendo la emisión de lineamientos internos, la implementación de controles en tecnologías y un proceso de consultas al Delagado de Protección de Datos Personales en nuevos proyectos institucionales.

21. Responsabilidad proactiva

La ENTIDAD PÚBLICA DE CONTROL MIGRATORIO desarrollará e implementará una estrategia empresarial integral para el tratamiento de datos personales conforme a los principios normativos aplicables, que incluirá:

- La elaboración de directrices internas y externas orientadas a áreas y aliados estratégicos de alto riesgo.
- La realización de auditorías internas con metodología definida y la apertura a auditorías externas.
- La adopción de métricas de seguimiento del cumplimiento, tanto cuantitativas como cualitativas.

- La promoción o adhesión a códigos de conducta, certificaciones, cláusulas tipo y sellos de protección de datos.
- La suscripción de acuerdos de confidencialidad y obligaciones de protección de datos con proveedores y colaboradores.

22. Cambios a la política

Cualquier cambio o excepción a la política deberá ser autorizada por la Dirección General y el Ministro del Interior.

Todo incumplimiento a lo indicado en la presente política será sancionado conforme a la Ley.

23. Anexos

Plazos de Conservación de información.
Procedimiento para garantizar el ejercicio de derechos del titular de datos personales.

Anexo 2

Matriz RACI

ENTIDAD PÚBLICA DE CONTROL MIGRATORIO

SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES

MATRIZ DE ROLES Y RESPONSABILIDADES (RACI)

Versión 1.0 | 2026

Código:	EPCM-PDP-RACI-001
Versión:	1.0
Fecha:	2026
Estado:	VIGENTE
Elaborado por:	Implementador de PDP
Revisado por:	Delegado de Protección de Datos Personales
Aprobado por:	Comité de Protección de Datos Personales
Normativa:	LOPDP | RGLOPDP | EGSI v3.0 | ISO 27001:2022

LEYENDA RACI
R — RESPONSIBLE — Ejecuta. Puede haber más de uno por actividad.
A — ACCOUNTABLE — Rinde cuentas. ÚNICO por actividad.
C — CONSULTED — Aporta antes de la actividad. Bidireccional.
I — INFORMED — Recibe información después. Unidireccional.
S — SOPORTE — Apoya sin ser el responsable principal.
N/A — NO APLICA — La actividad no corresponde a este rol/área.

NIVELES DE APROBACIÓN DOCUMENTAL	
NIVEL 1 — Máxima Autoridad de la EPCM	Política Institucional de PDP | Actos administrativos de designación de roles clave en la institución
NIVEL 2 — Comité de Protección de Datos Personales	Políticas específicas | Metodologías | Planes estratégicos | Protocolos y Políticas técnicas operativas | Procedimientos | Avisos legales | Documentos de implementación

MATRIZ RACI	
CÓDIGO: GEPCM.03.02.P01.F04	**VERSIÓN: 01**
FECHA: 15-12-2025	
MACROPROCESO: GESTIÓN DE CUMPLIMIENTO NORMATIVO	
PROCESO: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
SUBPROCESO: GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES	

ENTIDAD PÚBLICA DE CONTROL MIGRATORIO — MATRIZ RACI: ROLES Y RESPONSABILIDADES EN PROTECCIÓN DE DATOS PERSONALES

Ley Orgánica de Protección de Datos Personales (LOPDP) | Versión 1.0 | 2026

			AUTORIDADES Y DIRECCIONES INSTITUCIONALES							UNIDADES ADMINISTRATIVAS Y DE APOYO								ROLES ESPECIALIZADOS EN SI Y PDP				
#	GRUPO	ACTIVIDAD / OBLIGACIÓN	Director EPCM	Dir. Jurídica	Dir. Planificación	Dir. TIC	Dir. Administrativo	Dir. Financiero	Dir. TH	Secretaría General	Coord. Salud Inst.	Coord. Comunicación	Coord. Infraestructura	Coord. Bienes	Coord. Comp. Públicas	Coord. Des. Sistemas	Facultades	Comité de PDP	OSI	Oficial de Privacidad	DPDP	Auditores Internos
1. GOBERNANZA Y PLANIFICACIÓN																						
1	1	Aprobar la Política Institucional de Protección de Datos Personales [NIVEL 1]	A	C	I	N/A	N/A	N/A	I	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C	I	R	C	I
2	1	Constituir formalmente el Comité de PDP	A	C	C	I	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	R	I	I	I	N/A
3	1	Designar formalmente al Oficial de Privacidad	A	C	I	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	R	N/A	I	C	N/A
4	1	Designar formalmente al Delegado de Protección de Datos (DPD)	A	C	I	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	R	N/A	C	I	N/A
5	1	Designar formalmente al Oficial de Seguridad de la Información (OSI)	A	C	C	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	R	I	I	I	N/A
6	1	Aprobar el Plan de Proyecto de adecuación a la LOPDP [NIVEL 2]	I	C	C	I	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A	S	R	C	I
7	1	Establecer objetivos de PDP alineados a objetivos institucionales	I	C	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A	S	R	C	I
8	1	Informar semestralmente a la máxima autoridad los avances LOPDP	I	N/A	I	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A	I	R	C	I
2. DIAGNÓSTICO Y ANÁLISIS																						
9	2	Realizar el GAP Analysis del nivel de cumplimiento de la LOPDP	I	C	C	C	I	I	C	I	I	I	I	I	I	I	I	A	N/A	R	C	C
10	2	Elaborar el inventario/mapa de datos personales y flujos de información	I	C	C	S	C	C	C	C	C	C	C	C	C	C	C	A	S	R	C	N/A
11	2	Identificar base legal para cada tratamiento de datos personales	I	C	C	C	C	C	C	C	C	C	C	C	C	C	C	A	N/A	R	C	N/A
12	2	Identificar transferencias internacionales de datos personales	I	C	N/A	S	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A	N/A	R	C	I
13	2	Reportar al Oficial de PDP cualquier nuevo tratamiento o cambio en tratamientos	I	R	N/A	R	R	R	R	R	R	R	R	R	R	R	R	I	N/A	A	I	N/A
3. EVALUACIÓN DE RIESGOS Y EIPD																						
14	3	Aprobar la Metodología de Análisis de Riesgos PDP [NIVEL 2]	I	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A	S	R	C	C
15	3	Elaborar Matrices de Riesgos de tratamientos de datos personales	I	C	N/A	S	N/A	C	C	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	A	S	R	C	C
16	3	Realizar Evaluación de Impacto en PDP — EIPD (cuando proceda)	I	C	N/A	S	N/A	N/A	C	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	A	S	R	C	C
17	3	Aprobar el Plan de Tratamiento y Mitigación de Riesgos PDP [NIVEL 2]	I	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A	S	R	C	C
18	3	Dar seguimiento a implementación del Plan de Tratamiento de Riesgos PDP	I	C	N/A	R	R	R	R	R	R	R	R	R	R	R	R	I	S	A	C	C
4. REGISTRO DE ACTIVIDADES DE TRATAMIENTO (RAT)																						

19	4	Elaborar y mantener actualizada la Matriz RAT institucional	I	C	C	S	C	C	C	C	C	C	C	C	C	C	C	A	S	R	C	N/A
20	4	Actualizar el RAT ante cambios en procesos o sistemas	I	C	N/A	R	R	R	R	R	R	R	R	R	R	R	R	I	S	A	C	N/A
5. DOCUMENTOS LEGALES Y CONTRACTUALES																						
21	5	Aprobar Avisos de Privacidad y PDP (interno y externo) [NIVEL 2]	I	C	C	S	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	A	N/A	R	C	N/A
22	5	Aprobar Avisos Legales para plataformas y sistemas [NIVEL 2]	I	C	N/A	S	N/A	N/A	N/A	N/A	N/A	I	N/A	N/A	N/A	S	N/A	A	N/A	R	C	N/A
23	5	Aprobar Modelos de Contratos de Encargo de Tratamiento [NIVEL 2]	I	C	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	A	N/A	R	C	N/A
24	5	Aprobar Modelos de Consentimientos Informados [NIVEL 2]	I	C	N/A	N/A	N/A	N/A	C	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	A	N/A	R	C	N/A
25	5	Aprobar Modelos de Clausulado jurídico conforme SPDP [NIVEL 2]	I	R	N/A	N/A	C	N/A	C	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	A	N/A	S	C	N/A
26	5	Aprobar Política de Cookies y Aviso de Cookies [NIVEL 2]	I	C	N/A	S	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	S	N/A	A	N/A	R	C	N/A
27	5	Aprobar Acuerdo de Confidencialidad para colaboradores [NIVEL 2]	I	C	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A	N/A	R	C	N/A
6. DERECHOS DE LOS TITULARES (ARCO+PP)																						
28	6	Diseñar y aprobar el Protocolo de Atención de Derechos ARCO+ [NIVEL 2]	I	C	N/A	S	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	A	N/A	R	C	N/A
29	6	Recibir y registrar solicitudes de derechos ARCO+	I	C	N/A	N/A	N/A	N/A	N/A	R	N/A	N/A	N/A	N/A	N/A	N/A	N/A	I	N/A	A	C	N/A
30	6	Analizar y gestionar solicitudes de derechos ARCO+	I	R	N/A	S	N/A	N/A	S	S	N/A	N/A	N/A	N/A	N/A	S	N/A	I	N/A	A	C	N/A
31	6	Dar respuesta formal al titular dentro del plazo legal	I	R	N/A	N/A	N/A	N/A	N/A	S	N/A	N/A	N/A	N/A	N/A	N/A	N/A	I	N/A	A	S	N/A
32	6	Supervisar cumplimiento de plazos en atención de derechos	I	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	I	N/A	R	A	C
33	6	Escalar solicitudes complejas que requieran decisión institucional	I	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A	N/A	R	C	N/A
7. GESTIÓN DE VIOLACIONES DE SEGURIDAD DE DATOS PERSONALES																						
34	7	Aprobar Procedimiento de Gestión y Notificación de Violaciones a la Seguridad de Datos Personales [NIVEL 2]	I	C	N/A	S	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A	S	R	C	N/A
35	7	Detectar y reportar internamente una violación de datos personales	I	N/A	N/A	R	R	R	R	R	R	R	R	R	R	R	R	I	R	A	I	N/A
36	7	Evaluar el riesgo y clasificar la violación de datos personales	I	C	N/A	S	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A	S	R	C	C
37	7	Notificar la violación a la SPDP y ARCOTEL en plazos legales	I	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A	N/A	R	S	N/A
38	7	Notificar la violación a los titulares afectados cuando corresponda	I	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	S	N/A	N/A	N/A	N/A	N/A	A	N/A	R	S	N/A
39	7	Supervisar cumplimiento del proceso y plazos de notificación	I	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	I	N/A	R	A	C
40	7	Documentar la violación, acciones tomadas y lecciones aprendidas	I	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	I	R	A	C	C
8. MEDIDAS DE SEGURIDAD TÉCNICAS																						
41	8	Aprobar Informe de Medidas de Seguridad para datos personales [NIVEL 2]	I	N/A	N/A	S	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A	S	R	C	C
42	8	Implementar controles técnicos de seguridad para datos personales [NIVEL 2]	I	N/A	N/A	R	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	R	N/A	A	S	C	C	N/A
43	8	Implementar gestión de accesos e identidad para sistemas con datos personales [NIVEL 2]	I	N/A	N/A	R	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	R	N/A	A	S	C	C	N/A
44	8	Implementar cifrado y pseudonimización para datos personales sensibles [NIVEL 2]	I	N/A	N/A	R	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	R	N/A	A	S	C	C	N/A
45	8	Verificar eficacia de los controles técnicos implementados	I	N/A	N/A	I	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	I	C	R	A	C
9. CAPACITACIÓN Y SENSIBILIZACIÓN																						
46	9	Aprobar el Plan de Capacitaciones en PDP [NIVEL 2]	I	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	S	N/A	N/A	N/A	N/A	N/A	A	N/A	R	C	I

47	9	Ejecutar capacitaciones sobre LOPDP a personal administrativo	I	N/A	N/A	S	I	I	S	I	I	**R**	I	I	I	I	I	I	N/A	**A**	C	N/A
48	9	Ejecutar campañas de sensibilización en PDP para toda la institución	I	N/A	N/A	S	N/A	N/A	I	N/A	N/A	**R**	N/A	N/A	N/A	N/A	N/A	I	N/A	**A**	C	N/A
49	9	Registrar asistencia y evidencias de capacitaciones en PDP	I	N/A	N/A	N/A	N/A	N/A	**R**	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	I	N/A	**A**	C	I
50	9	Evaluar la efectividad de las capacitaciones en PDP	I	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	I	N/A	**A**	C	**R**
10. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO																						
51	10	Aprobar lineamientos de privacidad desde el diseño en nuevos sistemas [NIVEL 2]	I	C	N/A	S	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	S	N/A	**A**	S	**R**	C	N/A
52	10	Revisar nuevos tratamientos de datos desde perspectiva LOPDP antes de implementar	I	C	N/A	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	I	N/A	**A**	C	N/A
53	10	Asesorar a áreas sobre obligaciones LOPDP en proyectos nuevos	I	S	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	I	N/A	**R**	**A**	N/A
11. GESTIÓN DE PROVEEDORES Y ENCARGADOS DE TRATAMIENTO																						
54	11	Identificar proveedores/encargados que traten datos personales	I	C	N/A	S	**R**	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**R**	N/A	N/A	I	N/A	**A**	C	N/A
55	11	Incorporar cláusulas de PDP en contratos con proveedores/encargados	I	**R**	N/A	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	C	N/A	N/A	**A**	N/A	S	C	N/A
56	11	Supervisar cumplimiento PDP de encargados externos	I	C	N/A	N/A	S	N/A	N/A	N/A	N/A	N/A	N/A	N/A	S	N/A	N/A	I	N/A	**A**	**R**	C
57	11	Gestionar medidas de seguridad en transferencias internacionales de datos	I	C	N/A	S	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**A**	N/A	**R**	C	N/A
12. AUDITORÍA INTERNA Y MEJORA CONTINUA																						
58	12	Aprobar el Instructivo de Auditoría Interna PDP [NIVEL 2]	I	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**A**	S	C	C	**R**
59	12	Planificar y ejecutar la Auditoría Interna de PDP	I	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**A**	S	C	C	**R**
60	12	Emitir informe de resultados de la Auditoría Interna PDP	I	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**A**	N/A	I	C	**R**
61	12	Gestionar acciones correctivas derivadas de la auditoría interna PDP	I	N/A	N/A	S	S	S	S	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**A**	S	**R**	C	C
62	12	Elaborar el Informe de Nivel de Madurez SGSI + PDP	I	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**A**	S	**R**	C	C
63	12	Cooperar con la SPDP en auditorías e inspecciones externas	**A**	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	I	N/A	S	**R**	N/A
64	12	Elaborar y aprobar el Plan de Mejora Continua del Sistema de PDP [NIVEL 2]	I	N/A	C	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	**A**	N/A	**R**	C	C

Elaborado por:	Revisado por:	Aprobado por:
F/. **Nombre:** **Fecha:**	F/. **Nombre:** **Fecha:**	F/. **Nombre:** **Fecha:**

REFERENCIA DE ROLES — ABREVIATURAS Y NOMBRES COMPLETOS

ABREVIATURA	NOMBRE COMPLETO DEL ROL / ÁREA
Director EPCM	Director/a de la Entidad Pública de Control Migratorio
Dir. Jurídica	Dirección Jurídica
Dir. Planificación	Dirección de Planificación Institucional
Dir. TIC	Dirección de Tecnologías de la Información y Comunicación
Dir. Administrativo	Dirección Administrativa
Dir. Financiero	Dirección Financiera
Dir. TH	Dirección de Talento Humano
Secretaría General	Secretaría General
Coord. Salud Inst.	Coordinación de Salud Institucional
Coord. Comunicación	Coordinación de Comunicación Institucional
Coord. Infraestructura	Coordinación de Gestión de Infraestructura y Mantenimiento
Coord. Bienes	Coordinación de Bienes e Inventarios
Coord. Comp. Públicas	Coordinación de Gestión de Compras Públicas
Coord. Des. Sistemas	Coordinación de Desarrollo de Sistemas Informáticos
Comité de PDP	Comité de Protección de Datos Personales
OSI	Oficial de Seguridad de la Información
Implementador de PDP	Implementador de PDP
DPD	Delegado de Protección de Datos Personales
Auditores Internos	Equipo de Auditores Internos

DESCRIPCIÓN DE ROLES — PROTECCIÓN DE DATOS PERSONALES | EPCM | 2026			
#	ROL	RESPONSABILIDADES PRINCIPALES	BASE NORMATIVA
1	**Máxima Autoridad de la EPCM**	Aprueba documentos NIVEL 1 (políticas generales) mediante acto administrativo. Designa roles clave. Garante de recursos para el cumplimiento normativo.	LOPDP Art. 47 | EGSI v3 | Estatuto DME | Reglamento del Comité de PDP
2	**Comité de Protección de Datos Personales**	Órgano colegiado estratégico. Presidente aprueba NIVEL 2. Seguimiento a incidentes de alto impacto. Informa semestralmente al Director.	Reglamento del Comité de PDP | EGSI v3 | ISO 27001:2022
3	**Implementador de PDP**	Responsable operativo de implementar el sistema LOPDP: RAT, EIPD, derechos ARCO+, riesgos, capacitaciones, informes. Coordina con todas las áreas institucionales.	LOPDP | Reglamento LOPDP | Reglamento del Comité de PDP
4	**Delegado de Protección de Datos Personales (DPD)**	Rol INDEPENDIENTE de supervisión, asesoría y control. Punto de contacto con SPDP y ARCOTEL. NO implementa operativamente. Actúa sin instrucciones jerárquicas.	LOPDP Art. 48 y 49 | Reglamento LOPDP | SPDP | Reglamento del Comité de PDP
5	**Oficial de Seguridad de la Información (OSI)**	Coordina implementación SGSI/EGSI. Apoya controles técnicos con impacto en datos personales. Colabora con el Oficial de Privacidad en gestión de riesgos integrada.	EGSI v3 | ISO/IEC 27001:2022 | Reglamento del Comité de PDP
6	**Auditores Internos**	Planifican y ejecutan auditorías internas de PDP y SGSI. Emiten informes independientes. Operan sin relación jerárquica con las áreas auditadas.	ISO 19011 | ISO 27001:2022 Cláusula 9.2 | EGSI v3
7	**Dirección TIC / Desarrollo de Sistemas**	Implementan controles tecnológicos de seguridad. Gestionan incidentes técnicos. Apoyan en sistemas y plataformas que tratan datos personales.	Reglamento del Comité de PDP | EGSI v3 | LOPDP Art. 38
8	**Dirección Jurídica**	Asesora jurídicamente sobre normativa PDP. Elabora y revisa contratos, clausulados y documentos legales. Participa en notificaciones a la autoridad de control.	LOPDP | Reglamento LOPDP | Estatuto DME
9	**Dirección de Talento Humano**	Trata datos del personal (contratos, nómina, evaluaciones). Cumple LOPDP en selección y desvinculación. Coordina capacitaciones y registros de personal.	LOPDP | Reglamento LOPDP | Código del Trabajo
10	**Coordinación de Salud Institucional**	Trata datos de salud (categoría especial LOPDP Art. 26). Requiere EIPD obligatoria y medidas reforzadas. Gestiona consentimientos informados de usuarios.	LOPDP Art. 26 | Reglamento LOPDP | Código Orgánico de Salud
11	**Secretaría General**	Gestiona datos de solicitudes y respuestas de información. Principal punto de recepción de solicitudes ARCO+.	LOPDP | Reglamento LOPDP | LOES

12	**Todas las Unidades / Áreas**	Reportar nuevos tratamientos o cambios al Oficial de Privacidad. Participar en capacitaciones obligatorias. Cumplir políticas internas. Notificar incidentes de inmediato.	LOPDP | Reglamento LOPDP | Políticas internas DME

Anexo 3

Aviso Interno de Privacidad y Protección de Datos Personales

AVISO INTERNO DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES
ENTIDAD PÚBLICA DE CONTROL MIGRATORIO

I. ÁMBITO DE APLICACIÓN

Como parte de su compromiso con el cumplimiento del Régimen de Protección de Datos Personales, la Entidad Pública de Control Migratorio, en adelante la ENTIDAD, ha elaborado el presente documento, el cual es de manejo interno.

En este documento se detallan las acciones necesarias para dar cumplimiento a lo establecido en la Política de Tratamiento de Datos Personales de la ENTIDAD, cuyo objetivo es garantizar el derecho constitucional a la protección de datos personales, que incluye el acceso y la decisión sobre información y datos de esta naturaleza, así como su correspondiente protección.

En este sentido, la recolección, almacenamiento, uso, procesamiento, circulación o cualquier otra forma de tratamiento de datos personales requerirá la autorización del titular o el cumplimiento de una obligación legal, de conformidad con lo dispuesto en el artículo 66 numeral 19 de la Constitución de la República del Ecuador, en concordancia a lo dispuesto en el artículo 10 y 12 de la Ley Orgánica de Protección de Datos Personales (LOPDP).

Por lo que, la Entidad Pública de Control Migratorio pone en conocimiento de sus trabajadores el presente Aviso Interno de Privacidad y Protección de Datos Personales.

II. DEFINICIONES

DATOS PERSONALES:

Se refiere a cualquier información relativa a una persona física identificada o identificable (por ejemplo, un Empleado). Una persona identificable es aquella cuya identidad pueda inferirse directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos específicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona física. Algunos ejemplos de Datos personales: nombres, fotografías, direcciones de correo electrónico, datos de cuentas bancarias, información médica, direcciones IP y otros identificadores en línea.

TRATAMIENTO:

Cualquier operación o conjunto de operaciones realizadas sobre Datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. “Datos personales sensibles”: toda información sobre un Empleado relativa a su raza u origen étnico, opiniones políticas o filosóficas, creencias religiosas, salud o estado físico o mental, vida, preferencias u orientación sexual, pertenencia o afiliación sindical, datos biométricos, información genética, comisión o presunta comisión de infracciones penales y otras acciones legales relacionadas o condenas en el pasado.

TRABAJADORES:

Trabajadores actuales o antiguos trabajadores, incluidos aquellos que trabajan de forma no permanente, como trabajadores eventuales, temporales y a contrata, contratistas independientes, consultores, asesores profesionales, suplentes y personal en prácticas.

III. OBJETO DE ESTE AVISO INTERNO DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES.

El presente Aviso Interno de Privacidad y Protección de Datos Personales tiene como finalidad establecer los principios, lineamientos y obligaciones que rigen el tratamiento de los datos personales de los trabajadores, servidores públicos y demás personal vinculado a la ENTIDAD.

La ENTIDAD reconoce y respeta el derecho a la privacidad y a la protección de los datos personales de su personal, y asume el compromiso de tratarlos de manera lícita, leal, transparente y responsable, en cumplimiento de la normativa vigente, en particular la Ley Orgánica de Protección de Datos Personales (LOPDP) y demás disposiciones aplicables.

Este Aviso describe las categorías de datos personales que son objeto de tratamiento en el marco de las actividades identificadas más adelante como finalidades del tratamiento, su base legal, así como los derechos que asisten a los titulares de los datos y los mecanismos disponibles para su ejercicio.

En caso de dudas, consultas, solicitudes o reclamos relacionados con el presente Aviso o con el tratamiento de datos personales, los titulares podrán comunicarse con la ENTIDAD a través de los canales institucionales establecidos para tal efecto, conforme al procedimiento que se detalla en las secciones correspondientes del presente documento.

La ENTIDAD incorporará en los contratos de trabajo o mediante la plantilla indicada en el ANEXO 1, una cláusula de autorización expresa y explícita del trabajador, permitiendo que la ENTIDAD en su calidad de empleador/responsable del tratamiento pueda tratar sus datos personales incluyendo datos biométricos, en el marco de la relación laboral y sólo para fines del desarrollo de esa relación laboral. En ella, para el otorgamiento de la autorización el trabajador debe ser debidamente informado del propósito del tratamiento de sus datos personales y en concreto de su posible comunicación a terceros.

EXISTENCIA DE BASE DE DATOS

Los datos personales de los trabajadores de la ENTIDAD forman parte de bases de datos institucionales administradas por la ENTIDAD, las cuales cuentan con medidas de seguridad técnicas, jurídicas, físicas, administrativas y organizativas adecuadas, conforme a la Ley Orgánica de Protección de Datos Personales y su reglamento.

IV. FINALIDADES DEL TRATAMIENTO DE DATOS PERSONALES

Los datos personales de los trabajadores de la ENTIDAD serán tratados para las siguientes finalidades:

- Gestionar y administrar la relación laboral, que incluye la administración de procesos de contratación, registro, control de asistencia, evaluación, desarrollo, cumplimiento de obligaciones laborales, pago de remuneraciones y beneficios y demás obligaciones laborales.
- Cumplimiento de obligaciones legales, reglamentarias y administrativas aplicables a la ENTIDAD.
- Garantizar la seguridad institucional mediante la gestión y control de accesos a instalaciones, áreas restringidas y sistemas institucionales de la ENTIDAD, utilizando mecanismos tecnológicos adecuados, con el fin de proteger al personal, la información y los bienes institucionales.

V. BASE LEGAL PARA EL TRATAMIENTO DE DATOS PERSONALES

El tratamiento de los datos personales se fundamenta en:

- La ejecución de la relación laboral entre el trabajador y la ENTIDAD.
- El cumplimiento de obligaciones legales aplicables al sector público.
- El interés público en el ejercicio de competencias institucionales.
- El consentimiento del titular, cuando corresponda.

VI. TIPOS DE TRATAMIENTO DE DATOS PERSONALES

En el marco de las finalidades de tratamiento previamente descritas, la ENTIDAD realiza las siguientes operaciones sobre los datos personales de sus trabajadores:

- Recolección, registro y organización de datos.
- Almacenamiento en bases de datos físicas y digitales.
- Consulta, uso y circulación interna de la información.
- Actualización, rectificación, supresión o eliminación cuando corresponda.

VII. CONSENTIMIENTO PARA TRATAMIENTO DE DATOS BIOMÉTRICOS

Sin perjuicio de las excepciones previstas en la normativa aplicable, la ENTIDAD se compromete a tratar los datos biométricos de sus trabajadores, únicamente cuando cuente con la manifestación de voluntad del titular, conforme a lo establecido en la Ley Orgánica de Protección de Datos Personales.

El consentimiento del titular será considerado válido cuando reúna las siguientes condiciones:

- Libre: otorgado sin error, fuerza o dolo.
- Específico: referido de manera concreta a las finalidades determinadas del tratamiento, particularmente aquellas relacionadas con el control de accesos y seguridad institucional.
- Informado: emitido previa comunicación clara, suficiente y transparente sobre el tratamiento de sus datos personales, conforme al principio de transparencia.
- Inequívoco: expresado de forma clara mediante una acción afirmativa que no deje lugar a dudas sobre el alcance de la autorización otorgada.

La recolección de datos biométricos podrá realizarse por medios físicos o electrónicos, mediante sistemas tecnológicos implementados para la autenticación y control de accesos a instalaciones, áreas restringidas o sistemas institucionales.

No será necesario recabar el consentimiento del titular cuando el tratamiento o la comunicación de datos personales se sustente en una base legal distinta, de conformidad con la Ley Orgánica de Protección de Datos Personales, entre ellas:

- Cuando el tratamiento sea necesario para el cumplimiento de obligaciones legales o el ejercicio de competencias atribuidas a la ENTIDAD.
- Cuando el tratamiento sea necesario para la ejecución de la relación laboral o para garantizar la seguridad institucional.
- Cuando los datos deban ser proporcionados a autoridades administrativas o judiciales en ejercicio de sus competencias legales.

- Cuando la comunicación se realice entre entidades del sector público para el cumplimiento de fines legítimos, respetando los principios de protección de datos personales.

En todos los casos, la ENTIDAD garantizará que el tratamiento de datos biométricos se realice bajo estrictas medidas de seguridad, confidencialidad y proporcionalidad, limitándose a las finalidades previamente informadas.

El almacenamiento, uso, circulación, supresión o cualquier otro tratamiento aplicado a los datos biométricos constará en el inventario de bases de datos institucional, cuya actualización será responsabilidad de las unidades competentes, bajo supervisión del responsable o delegado de protección de datos personales, cuando corresponda.

La ENTIDAD conservará la prueba del consentimiento otorgado por los trabajadores para su tratamiento, para lo cual adoptará las acciones necesarias para mantener registros o mecanismos técnicos o tecnológicos idóneos con el fin de determinar cuándo y cómo obtuvo ésta, de acuerdo con lo establecido por la ley. La ENTIDAD obtendrá del trabajador un nuevo consentimiento cuando en la Política de Tratamiento haya un cambio sustancial respecto a la finalidad.

VIII. TIEMPO DE CONSERVACIÓN DE LOS DATOS PERSONALES

Los datos personales serán conservados durante el tiempo necesario para cumplir con las finalidades descritas y conforme a los plazos establecidos en la normativa aplicable y políticas de archivo institucional.

IX. OTRAS FINALIDADES DEL TRATAMIENTO

- Auditorías internas y externas.
- Generación de estadísticas institucionales.
- Mejora de procesos administrativos.
- Cumplimiento de requerimientos de organismos de control.

X. RESPONSABLE DEL TRATAMIENTO Y DELEGADO DE PROTECCIÓN DE DATOS PERSONALES

RESPONSABLE DEL TRATAMIENTO

Entidad Pública de Control Migratorio.
Av. Amazonas y La Granja
(02)276394 Ext. 1023
servicios.migratorios@ministeriodelinterior.gob.ec

DELEGADO DE PROTECCIÓN DE DATOS PERSONALES

Av. Amazonas y La Granja
(02)276394 Ext. 1024
delegado.datos@ministeriodelinterior.gob.ec

XI. TRANSFERENCIAS O COMUNICACIONES DE DATOS PERSONALES

Los datos personales podrán ser comunicados a:

- Entidades públicas competentes.
- Organismos de control.
- Proveedores de servicios vinculados a la gestión institucional, bajo acuerdos de confidencialidad.
- Las transferencias internacionales, de existir, se realizarán cumpliendo las garantías establecidas en la normativa vigente.

XII. CONSECUENCIAS DEL TRABAJADPR DE LA NO ENTREGA DE DATOS PERSONALES

La entrega de los datos personales es obligatoria para la gestión de la relación laboral. La negativa a proporcionarlos puede impedir la vinculación, permanencia o acceso a beneficios laborales.

XIII. EFECTO DE SUMINISTRAR DATOS ERRÓNEOS O INEXACTOS

El suministro de datos incorrectos o incompletos puede generar afectaciones en la gestión administrativa, pagos, beneficios y cumplimiento de obligaciones legales.

XIV. REVOCATORIA DEL CONSENTIMIENTO

El trabajador podrá revocar su consentimiento en cualquier momento, cuando el tratamiento se base en este, sin afectar la legalidad del tratamiento previo.

XV. DERECHOS DEL TITULAR

El titular podrá ejercer sus derechos de:

- Información
- Acceso
- Rectificación y actualización
- Eliminación
- Oposición
- Portabilidad.
- Suspensión del tratamiento
- No ser objeto de decisiones automatizadas
- Consulta

Mediante solicitud dirigida al responsable, al siguiente correo electrónico: privacidadyprotección@ entidadmigracion.gob.ec

XVI. DERECHO A LA PORTABILIDAD

El titular podrá solicitar la portabilidad de sus datos cuando corresponda, conforme a la normativa vigente.

XVII. RECLAMOS

El titular podrá presentar reclamos ante:

- El responsable del tratamiento, a través de los canales indicados.
- La autoridad de Protección de Datos Personales.

XVIII. DECISIONES AUTOMATIZADAS Y PERFILES

La ENTIDAD no adopta decisiones basadas únicamente en tratamientos automatizados ni elabora perfiles sin intervención humana. En caso de implementarse, se informará oportunamente.

XIX. CONSULTAS

Si tiene cualquier consulta sobre el modo en que tratamos Datos personales, o para más información acerca de este Aviso, o si desea ejercitar sus derechos en relación con Datos personales que le incumban, póngase en contacto con el responsable del tratamiento de datos personales: privacidadyprotección@entidadmigracion.gob.ec

XX. ACTUALIZACIONES DE ESTE AVISO

Este Aviso puede actualizarse periódicamente para reflejar los cambios oportunos en nuestras prácticas de privacidad y protección de datos personales. En estos casos, le informaremos a través de la intranet e indicaremos al principio de este Aviso la fecha de la actualización más reciente. Le recomendamos que consulte nuestra intranet periódicamente para estar al tanto de la versión más reciente de este Aviso.

XXI. LEGISLACIÓN APLICABLE Y RESOLUCIÓN DE CONFLICTOS

Los términos del presente Aviso de Privacidad y protección de datos personales se rigen y se interpretan de acuerdo con las leyes vigentes en la República del Ecuador, sujetándose a la competencia y jurisdicción de los Jueces de Quito Ecuador; y, en el ámbito administrativo a la Superintendencia de Protección de Datos Personales.

ANEXO I
CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES Y BIOMÉTRICOS DE TRABAJADORES

Yo, _____, con cédula de ciudadanía número _____, declaro que he recibido, leído y comprendido el documento denominado “Aviso Interno de Privacidad y Protección de Datos Personales” de la Entidad Pública de Control Migratorio.

En este sentido:

1. Autorizo de manera libre, específica, informada e inequívoca a la Entidad Pública de Control Migratorio para el tratamiento de mis datos personales en el marco de la relación laboral, conforme a los fines, condiciones y alcances establecidos en dicho Aviso.
2. Autorizo expresamente el tratamiento de mis datos personales, incluidos datos biométricos, tales como aquellos obtenidos mediante mecanismos tecnológicos de autenticación: huella dactilar, reconocimiento de voz, iris, con la finalidad de:
    - Gestionar y controlar el acceso a instalaciones institucionales, oficinas, áreas restringidas y dependencias estratégicas.
    - Fortalecer la seguridad institucional, la protección de la información, los bienes y el personal de la ENTIDAD.
    - Verificar la identidad del personal autorizado en el ejercicio de sus funciones.

3. Declaro que he sido informado/a de que el tratamiento de mis datos biométricos se realizará conforme a la Ley Orgánica de Protección de Datos Personales, bajo principios de proporcionalidad, minimización, seguridad y confidencialidad, y únicamente para las finalidades previamente señaladas.
4. Reconozco que mi consentimiento podrá ser revocado en los casos en que sea aplicable, sin afectar la legalidad del tratamiento realizado con anterioridad, de conformidad con la normativa vigente.
5. Entiendo que el tratamiento de mis datos personales y biométricos podrá estar sustentado, además del consentimiento, en otras bases legales relacionadas con la relación laboral y el cumplimiento de obligaciones legales y de seguridad institucional.

El presente documento forma parte de los derechos y obligaciones derivados de mi relación laboral con la Entidad Pública de Control Migratorio.

_____

CC:

DIRECCIÓN DE MIGRACIÓN DEL ECUADOR

AVISO INTERNO DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

DIRECCIÓN DE MIGRACIÓN DEL ECUADOR

ÁMBITO DE APLICACIÓN

Este documento es de manejo interno y establece las directrices para el tratamiento de datos personales de los trabajadores, servidores y personal vinculado a la Dirección de Migración del Ecuador, en cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) y demás normativa aplicable.

FINALIDADES DEL TRATAMIENTO

Gestión de la Relación Laboral

Administración de procesos de contratación, registro, asistencia, evaluación, desarrollo, pagos y beneficios laborales.

Cumplimiento Legal

Atención de olgaciones legales, reglamentarias y administrativas aplicables a la Dirección y al Ministerio del Interior.

Seguridad Institucional

Gestión y control de accesos a instalaciones, áreas restringidas y sistemas institucionales para proteger al personal, la información y los bienes institucionales.

BASE LEGAL

- Ejecución de la relación laboral.
- Cumplimiento de obligaciones legales.
- Interés público en el ejercicio de competencias institucionales.
- Consentimiento del titular, cuando corresponda, en particular para el tratamiento de datos biométricos.

TIPOS DE TRATAMIENTO

- ✓ Recolección, registro y organización.
- ✓ Almacenamiento en medios físicos y digitales.
- ✓ Consulta, uso y circulación interna.
- ✓ Actualización, rectificación, supresión o eliminación.

DERECHOS DEL TITULAR

- Información
- Acceso
- Rectificación y actualización
- Eliminación
- Oposición
- Portabilidad
- Suspensión del tratamiento
- No ser objeto de decisiones automatizadas
- Consulta

Para ejercer sus derechos, escriba a:
privacidadyprotección@direcciónmigración.gob.ec

CONSENTIMIENTO DE DATOS BIOMÉTRICOS

- ✓ **Libre**, específico, informado e **inequívoco.**
- ✓ **Finalidad:** control de accesos y seguridadinstitucional.
- ✓ **Medios:** sistemas de huella dactilar, reconocimiento de voz, iris u otros tecnológicos.
- ✓ **Conservación:** por el tiempo necesario y bajo estrictas medidas de seguridad y confidencialidad.

RECLAMOS

Puede presentar sus reclamos ante:

- El Responsable del Tratamiento:
  privacidadyprotección@direcciónmigración.gob.ec
- Autoridad de Protección de Datos Personales.

CONSULTAS

Para consultas sobre el tratamiento de sus datos personales:

privacidadyprotección@direcciónmigración.gob.ec

Puede consultar actualizaciones en la intranet institucional.

LEGISLACIÓN APLICABLE

Ley Orgánica de Protección de Datos Personales y demás normativa vigente en la República del Ecuador.

Competencia y jurisdicción: Jueces de Quito y Superintendencia de Protección de Datos Personales.

Anexo 4

Matriz de Riesgos

Matriz de Valoración de Riesgo

Proyecto	Aeropuerto XYZ
ID	RIESGOS-001
Fecha de inicio	24/4/2026
Fecha de fin	28/4/2026

ID de Riesgo	RAT/Tratamiento	Activo	Amenazas	Descripción	Vulnerabilidad	Probabilidad	IMPACTO EN LAS DIMENSIONES AFECTADAS					Impacto (valor más Alto)	Riesgo Inherente	Tipo de Controles	Controles	Riesgo Residual
							C - Confidencialidad	I - Integridad	D - Disponibilidad	P - Privacidad	DL - Derechos y Libertades					
AT-01-R01	AT-01 Identificación en tiempo real de personas naturales mediante reconocimiento facial e IA, para el registro de entrada y salida del país, control de impedimentos, identificación de personas requeridas por la justicia nacional e internacional, prevención del delito de trata de personas o localización y protección de menores en el punto de control migratorio del Aeropuerto	Plataforma de reconocimiento facial con IA	Acceso no autorizado o filtración de datos biométricos de viajeros	Posible exfiltración, acceso indebido o uso no autorizado de plantillas biométricas y datos identificativos de viajeros, con impacto sobre la confidencialidad, privacidad y riesgo de suplantación de identidad.	Exposición en redes, credenciales débiles, controles de acceso insuficientes, concentración de grandes volúmenes de datos sensibles.	Muy Probable	Crítico	Irrelevante	Irrelevante	Crítico	Crítico	Crítico	Crítico	Preventivo	Cifrado en tránsito y reposo, RBAC, MFA, registros de auditoría, segregación de funciones, pruebas de penetración y monitoreo continuo.	Medio
AT-01-R02			Sesgos algorítmicos o errores de reconocimiento facial	El sistema de IA podría presentar mayores tasas de falsos positivos o negativos para determinados grupos, generando decisiones injustas en controles migratorios.	Datos de entrenamiento no representativos, falta de auditoría algorítmica, ausencia de supervisión humana significativa.	Probable	Crítico	Irrelevante	Irrelevante	Moderado	Crítico	Crítico	Alto	Preventivo	Auditorías de sesgo y precisión, revisión humana obligatoria de coincidencias, métricas de desempeño por grupo, política de no uso exclusivo automatizado.	Bajo
AT-01-R03		Base de datos biométrica de viajeros (plantillas faciales)	Acceso no autorizado o filtración de datos biométricos de viajeros	Posible exfiltración, acceso indebido o uso no autorizado de plantillas biométricas y datos identificativos de viajeros, con impacto sobre la confidencialidad, privacidad y riesgo de suplantación de identidad.	Exposición en redes, credenciales débiles, controles de acceso insuficientes, concentración de grandes volúmenes de datos sensibles.	Muy Probable	Crítico	Irrelevante	Irrelevante	Crítico	Crítico	Crítico	Crítico	Preventivo	Cifrado en tránsito y reposo, RBAC, MFA, registros de auditoría, segregación de funciones, pruebas de penetración y monitoreo continuo.	Medio
AT-01-R04			Sesgos algorítmicos o errores de reconocimiento facial	El sistema de IA podría presentar mayores tasas de falsos positivos o negativos para determinados grupos, generando decisiones injustas en controles migratorios.	Datos de entrenamiento no representativos, falta de auditoría algorítmica, ausencia de supervisión humana significativa.	Probable	Crítico	Irrelevante	Irrelevante	Moderado	Crítico	Crítico	Alto	Preventivo	Auditorías de sesgo y precisión, revisión humana obligatoria de coincidencias, métricas de desempeño por grupo, política de no uso exclusivo automatizado.	Bajo
AT-01-R05		Sistema de Control Migratorio (registros de entradas y salidas)	Acceso no autorizado o filtración de datos biométricos de viajeros	Posible exfiltración, acceso indebido o uso no autorizado de plantillas biométricas y datos identificativos de viajeros, con impacto sobre la confidencialidad, privacidad y riesgo de suplantación de identidad.	Exposición en redes, credenciales débiles, controles de acceso insuficientes, concentración de grandes volúmenes de datos sensibles.	Muy Probable	Crítico	Irrelevante	Irrelevante	Crítico	Crítico	Crítico	Crítico	Preventivo	Cifrado en tránsito y reposo, RBAC, MFA, registros de auditoría, segregación de funciones, pruebas de penetración y monitoreo continuo.	Medio
AT-01-R06			Sesgos algorítmicos o errores de reconocimiento facial	El sistema de IA podría presentar mayores tasas de falsos positivos o negativos para determinados grupos, generando decisiones injustas en controles migratorios.	Datos de entrenamiento no representativos, falta de auditoría algorítmica, ausencia de supervisión humana significativa.	Probable	Crítico	Irrelevante	Irrelevante	Moderado	Crítico	Crítico	Alto	Preventivo	Auditorías de sesgo y precisión, revisión humana obligatoria de coincidencias, métricas de desempeño por grupo, política de no uso exclusivo automatizado.	Bajo
AT-01-R07		Servicios interoperables con Registro Civil (datos demográficos y biométricos)	Acceso no autorizado o filtración de datos biométricos de viajeros	Posible exfiltración, acceso indebido o uso no autorizado de plantillas biométricas y datos identificativos de viajeros, con impacto sobre la confidencialidad, privacidad y riesgo de suplantación de identidad.	Exposición en redes, credenciales débiles, controles de acceso insuficientes, concentración de grandes volúmenes de datos sensibles.	Muy Probable	Crítico	Irrelevante	Irrelevante	Crítico	Crítico	Crítico	Crítico	Preventivo	Cifrado en tránsito y reposo, RBAC, MFA, registros de auditoría, segregación de funciones, pruebas de penetración y monitoreo continuo.	Medio
AT-01-R08			Sesgos algorítmicos o errores de reconocimiento facial	El sistema de IA podría presentar mayores tasas de falsos positivos o negativos para determinados grupos, generando decisiones injustas en controles migratorios.	Datos de entrenamiento no representativos, falta de auditoría algorítmica, ausencia de supervisión humana significativa.	Probable	Crítico	Irrelevante	Irrelevante	Moderado	Crítico	Crítico	Alto	Preventivo	Auditorías de sesgo y precisión, revisión humana obligatoria de coincidencias, métricas de desempeño por grupo, política de no uso exclusivo automatizado.	Bajo
AT-01-R09		Interfaces de integración con INTERPOL (alertas y coincidencias)	Acceso no autorizado o filtración de datos biométricos de viajeros	Posible exfiltración, acceso indebido o uso no autorizado de plantillas biométricas y datos identificativos de viajeros, con impacto sobre la confidencialidad, privacidad y riesgo de suplantación de identidad.	Exposición en redes, credenciales débiles, controles de acceso insuficientes, concentración de grandes volúmenes de datos sensibles.	Muy Probable	Crítico	Irrelevante	Irrelevante	Crítico	Crítico	Crítico	Crítico	Preventivo	Cifrado en tránsito y reposo, RBAC, MFA, registros de auditoría, segregación de funciones, pruebas de penetración y monitoreo continuo.	Medio
AT-01-R10			Sesgos algorítmicos o errores de reconocimiento facial	El sistema de IA podría presentar mayores tasas de falsos positivos o negativos para determinados grupos, generando decisiones injustas en controles migratorios.	Datos de entrenamiento no representativos, falta de auditoría algorítmica, ausencia de supervisión humana significativa.	Probable	Crítico	Irrelevante	Irrelevante	Moderado	Crítico	Crítico	Alto	Preventivo	Auditorías de sesgo y precisión, revisión humana obligatoria de coincidencias, métricas de desempeño por grupo, política de no uso exclusivo automatizado.	Bajo
AT-02-R01	AT-02 Cotejar mediante IA los datos biométricos del pasaporte biométrico para la identificación de personas con impedimentos de salida del país ante autoridades nacionales	Módulo de lectura de pasaportes biométricos	Fallo en la verificación biométrica de pasaportes o fraude documental no detectado	El sistema podría no detectar pasaportes alterados o suplantación de identidad, comprometiendo el control migratorio y la seguridad nacional.	Dependencia de dispositivos de lectura, fallos de actualización de listas de documentos, falta de pruebas de robustez.	Probable	Irrelevante	Severo	Irrelevante	Moderado	Severo	Severo	Alto	Preventivo	Mantenimiento preventivo, calibración de dispositivos, actualización de listas de documentos, doble verificación manual en casos de duda.	Bajo
AT-02-R02			Reutilización o conservación excesiva de datos biométricos de pasaportes	Los datos biométricos podrían conservarse más tiempo del necesario o reutilizarse para fines distintos al control migratorio, afectando principios de minimización y limitación de la finalidad.	Políticas de retención poco claras, ausencia de borrado/anonimización, controles débiles sobre usos secundarios.	Probable	Crítico	Irrelevante	Irrelevante	Crítico	Severo	Crítico	Alto	Disuasorio	Políticas de retención definidas, anonimización/borrado programado, revisiones de cumplimiento, cláusulas contractuales con proveedores.	Medio
AT-02-R03		Base de datos de pasaportes biométricos y registros de control	Fallo en la verificación biométrica de pasaportes o fraude documental no detectado	El sistema podría no detectar pasaportes alterados o suplantación de identidad, comprometiendo el control migratorio y la seguridad nacional.	Dependencia de dispositivos de lectura, fallos de actualización de listas de documentos, falta de pruebas de robustez.	Probable	Irrelevante	Severo	Irrelevante	Moderado	Severo	Severo	Alto	Preventivo	Mantenimiento preventivo, calibración de dispositivos, actualización de listas de documentos, doble verificación manual en casos de duda.	Bajo
AT-02-R04			Reutilización o conservación excesiva de datos biométricos de pasaportes	Los datos biométricos podrían conservarse más tiempo del necesario o reutilizarse para fines distintos al control migratorio, afectando principios de minimización y limitación de la finalidad.	Políticas de retención poco claras, ausencia de borrado/anonimización, controles débiles sobre usos secundarios.	Probable	Crítico	Irrelevante	Irrelevante	Crítico	Severo	Crítico	Alto	Disuasorio	Políticas de retención definidas, anonimización/borrado programado, revisiones de cumplimiento, cláusulas contractuales con proveedores.	Medio
AT-02-R05		Plataforma de reconocimiento facial/huellas asistida por IA para pasaportes	Fallo en la verificación biométrica de pasaportes o fraude documental no detectado	El sistema podría no detectar pasaportes alterados o suplantación de identidad, comprometiendo el control migratorio y la seguridad nacional.	Dependencia de dispositivos de lectura, fallos de actualización de listas de documentos, falta de pruebas de robustez.	Probable	Irrelevante	Severo	Irrelevante	Moderado	Severo	Severo	Alto	Preventivo	Mantenimiento preventivo, calibración de dispositivos, actualización de listas de documentos, doble verificación manual en casos de duda.	Bajo
AT-02-R06			Reutilización o conservación excesiva de datos biométricos de pasaportes	Los datos biométricos podrían conservarse más tiempo del necesario o reutilizarse para fines distintos al control migratorio, afectando principios de minimización y limitación de la finalidad.	Políticas de retención poco claras, ausencia de borrado/anonimización, controles débiles sobre usos secundarios.	Probable	Crítico	Irrelevante	Irrelevante	Crítico	Severo	Crítico	Alto	Disuasorio	Políticas de retención definidas, anonimización/borrado programado, revisiones de cumplimiento, cláusulas contractuales con proveedores.	Medio
AT-02-R07		Servicios interoperables con Registro Civil para validación de pasaportes	Fallo en la verificación biométrica de pasaportes o fraude documental no detectado	El sistema podría no detectar pasaportes alterados o suplantación de identidad, comprometiendo el control migratorio y la seguridad nacional.	Dependencia de dispositivos de lectura, fallos de actualización de listas de documentos, falta de pruebas de robustez.	Probable	Irrelevante	Severo	Irrelevante	Moderado	Severo	Severo	Alto	Preventivo	Mantenimiento preventivo, calibración de dispositivos, actualización de listas de documentos, doble verificación manual en casos de duda.	Bajo
AT-02-R08			Reutilización o conservación excesiva de datos biométricos de pasaportes	Los datos biométricos podrían conservarse más tiempo del necesario o reutilizarse para fines distintos al control migratorio, afectando principios de minimización y limitación de la finalidad.	Políticas de retención poco claras, ausencia de borrado/anonimización, controles débiles sobre usos secundarios.	Probable	Crítico	Irrelevante	Irrelevante	Crítico	Severo	Crítico	Alto	Disuasorio	Políticas de retención definidas, anonimización/borrado programado, revisiones de cumplimiento, cláusulas contractuales con proveedores.	Medio
AT-02-R09		Integraciones con INTERPOL para cotejo de documentos y personas requeridas	Fallo en la verificación biométrica de pasaportes o fraude documental no detectado	El sistema podría no detectar pasaportes alterados o suplantación de identidad, comprometiendo el control migratorio y la seguridad nacional.	Dependencia de dispositivos de lectura, fallos de actualización de listas de documentos, falta de pruebas de robustez.	Probable	Irrelevante	Severo	Irrelevante	Moderado	Severo	Severo	Alto	Preventivo	Mantenimiento preventivo, calibración de dispositivos, actualización de listas de documentos, doble verificación manual en casos de duda.	Bajo
AT-02-R10			Reutilización o conservación excesiva de datos biométricos de pasaportes	Los datos biométricos podrían conservarse más tiempo del necesario o reutilizarse para fines distintos al control migratorio, afectando principios de minimización y limitación de la finalidad.	Políticas de retención poco claras, ausencia de borrado/anonimización, controles débiles sobre usos secundarios.	Probable	Crítico	Irrelevante	Irrelevante	Crítico	Severo	Crítico	Alto	Disuasorio	Políticas de retención definidas, anonimización/borrado programado, revisiones de cumplimiento, cláusulas contractuales con proveedores.	Medio

Anexo 5

Registro de Incidentes

REGISTRO DE INCIDENTES Y DOCUMENTACIÓN - VIOLACIONES DE SEGURIDAD DE DATOS PERSONALES

N°	Denominación del incidente	Descripción del hecho	Fecha / hora detección	Datos afectados	Consecuencias reales y potenciales	Medidas adoptadas	Notif. SPDP (art. 43)	Notif. titular (art. 46)	reDPIA requerida
01	**Acceso no autorizado a la base de plantillas biométricas**	Un agente externo logra acceder, mediante credenciales de servicio comprometidas, a la base de datos centralizada de plantillas biométricas del sistema BioTrust en el servidor del aeropuerto. Se exfiltran registros de huellas dactiloscópicas e imágenes faciales de aproximadamente 12.000 viajeros.	Martes 14-01-2026, 02:37 h. Detectado por el sistema de monitoreo de accesos al día siguiente a las 08:15 h. Reportado al responsable del tratamiento a las 10:00 h del 15-01-2026.	Datos biométricos (huellas dactiloscópicas e imágenes faciales): 12.000 titulares. Condición migratoria e historial de movimientos asociados. Categoría especial sensible (art. 4 y 25 LOPDP).	REALES: Exfiltración confirmada de datos sensibles irreemplazables. POTENCIALES: Suplantación de identidad biométrica; uso en fraude documental transnacional; imposibilidad del titular de revocar sus datos biométricos (son permanentes); investigación penal (art. 234 COIP - acceso no consentido a sistema informático).	Bloqueo de credenciales comprometidas (inmediato). Aislamiento del servidor afectado. Análisis forense iniciado. Notificación interna a la Dirección de Migración. Registro del incidente en el libro de incidentes. Inicio de auditoría de accesos.	OBLIGATORIA. Plazo: 5 días hábiles desde conocimiento (15-01-2026). Vencimiento: 22-01-2026. Contenido mínimo: art. 43 LOPDP. Autoridad: SPDP y ARCOTEL.	OBLIGATORIA. Plazo: 3 días desde conocimiento del riesgo (art. 46 LOPDP). Requiere canal de comunicación masiva por ser 12.000 titulares. Excepciones del art. 46 no aplican.	SÍ — INMEDIATA. Cambio sustancial en el perfil de riesgo. Concurre supuesto art. 42 lit. b (gran escala, categoría especial). Debe incluir análisis de arquitectura centralizada vs. distribuida.
02	**Comunicación indebida de datos biométricos a tercero no autorizado**	Un funcionario de BioTrust transfiere, mediante correo electrónico corporativo, un archivo comprimido con imágenes faciales y datos de identidad de 3.500 viajeros de vuelos internacionales a una empresa de marketing digital, invocando un supuesto contrato de análisis de	Jueves 06-02-2026, 16:45 h (envío del correo). Detectado por el sistema DLP (Data Loss Prevention) el 07-02-2026 a las 09:00 h. Comunicado al responsable a las 11:30 h del 07-02-2026.	Imágenes faciales (dato biométrico) y datos de identidad de 3.500 viajeros internacionales. Condición migratoria implícita. Categoría: datos sensibles (art. 4 y 25 LOPDP).	REALES: Transferencia ilícita consumada a destinatario no habilitado. Posible elaboración de perfiles comerciales. POTENCIALES: Uso publicitario de datos sensibles; transferencia internacional no controlada; multa grave a BioTrust (0.7%-1% volumen	Revocación inmediata de accesos del funcionario. Requerimiento de destrucción certificada de datos a la empresa receptora. Inicio de proceso disciplinario interno. Preservación del correo como evidencia digital.	OBLIGATORIA. Plazo: 5 días desde conocimiento (07-02-2026). Vencimiento: 14-02-2026. La transferencia a tercero no autorizado constituye vulneración de seguridad por pérdida de confidencialidad (art. 4 y 43 LOPDP).	OBLIGATORIA. Afectación directa a derechos de 3.500 titulares. El uso comercial no autorizado de datos biométricos constituye riesgo a derechos fundamentales (art. 46 LOPDP). Plazo: 3 días desde 07-02-2026.	SÍ. El incidente revela ausencia de controles de transferencia y de cláusulas contractuales mínimas (Res. SPDP-2025-0006-R). La reDPIA debe incorporar evaluación del flujo de datos y controles DLP.

		afluencia aeroportuaria que no cuenta con autorización del responsable del tratamiento ni base legal LOPDP.			negocio, art. 72 LOPDP); responsabilidad penal del funcionario (art. 229 COIP - revelación ilegal de bases de datos).	Consulta a asesoría jurídica.			
04	**Pérdida de disponibilidad del sistema: caída del servidor biométrico en hora pico**	Una actualización de firmware defectuosa en el servidor principal del sistema BioTrust provoca la caída total del servicio biométrico durante 3 horas y 40 minutos en el Aeropuerto Mariscal Sucre. Los controles migratorios se paralizan parcialmente, generando aglomeración de 800 viajeros. Se activa el proceso manual de verificación documental.	Viernes 03-04-2026, 17:15 h (inicio de la caída). Detección: 17:18 h por monitoreo automatizado. Restauración del servicio: 20:55 h. Reporte al responsable: 03-04-2026, 21:30 h.	Registros de movimiento migratorio de 800 viajeros pendientes de control. Potencial pérdida de integridad en registros procesados manualmente durante la contingencia. Afectación a la disponibilidad del sistema (art. 4 LOPDP — dimensión de disponibilidad).	REALES: Interrupción del servicio de control migratorio. Registros procesados manualmente sin garantía de integridad. Riesgo de duplicación o pérdida de registros. POTENCIALES: Incumplimiento de art. 201 Regl. LOMH (registro en sistemas informáticos oficiales); responsabilidad administrativa ante la Contraloría General del Estado; hallazgos negativos en auditoría OACI.	Rollback de la actualización (3h 40min). Verificación manual de pasajeros durante la contingencia. Revisión de integridad de registros post-restauración. No se activó el plan de continuidad del negocio (PCN) formalmente. No se convocó al Delegado de Protección de Datos.	EVALUACIÓN NECESARIA. La caída del sistema con impacto en la disponibilidad de datos personales puede constituir vulneración de seguridad (art. 4 LOPDP). Si se confirma pérdida o corrupción de registros: notificación obligatoria en 5 días (art. 43 LOPDP).	CONDICIONAL. Obligatoria si se acredita pérdida o alteración de datos de titulares identificables durante el procesamiento manual (art. 46 LOPDP). Plazo: 3 días desde confirmación.	SÍ. El incidente evidencia ausencia de plan de continuidad del negocio con escenarios de datos personales, inexistencia de entorno de prueba para actualizaciones, y falta de redundancia del sistema.