Maestría en

Protección de Datos

Trabajo de investigación previo a la obtención del título de

Magíster en Protección de Datos

AUTORES:

Montenegro Pozo Angie Paola

Sigcha Morochz Mario David

Reinoso Martínez Gabriel Andrés

Ibarra Flores William Iván

Cajas Torres Dennis Paul

TUTORES:

Profesor PBL1: Humberto Ortiz Rodríguez

Profesor PBL2: Camila Valdez González

Profesor PBL3: Jacqueline Guerrero Carrera

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

Quito, junio 2026

Certificación de autoría

Nosotros, Montenegro Pozo Angie Paola, Sigcha Morochz Mario David, Reinoso Martínez Gabriel Andrés, Ibarra Flores William Iván, Cajas Torres Dennis Paul**,** 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.

Angie Paola Montenegro Pozo
Time Stamping Security Data

Firma del graduando
Montenegro Pozo Angie Paola

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARIO DAVID SIGCHA MOROCHZ

Firma del graduando
Sigcha Morochz Mario David

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
GABRIEL ANDRES REINOSO MARTINEZ

Firma del graduando
Reinoso Martínez Gabriel Andrés

William Ivan Ibarra Flores
Time Stamping Security Data

Firma del graduando
Ibarra Flores William Iván

DENNIS PAUL CAJAS TORRES
Firmado digitalmente por DENNIS PAUL CAJAS TORRES
Fecha: 2026.07.01 20:21:19 -05'00'

Firma del graduando
Cajas Torres Dennis Paul

Autorización de Derechos de Propiedad Intelectual

Montenegro Pozo Angie Paola, Sigcha Morochz Mario David, Reinoso Martínez Gabriel Andrés, Ibarra Flores William Iván y Cajas Torres Dennis Paul, quienes suscribimos en calidad de autores del trabajo de investigación titulado "***Privacidad desde el diseño y por defecto: aplicación del uso de biometría en el escenario de una empresa de seguridad"***, 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.

Angie Paola Montenegro Pozo
Time Stamping Security Data

Firma del graduando
Montenegro Pozo Angie Paola

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
MARIO DAVID SIGCHA MOROCHZ

Firma del graduando
Sigcha Morochz Mario David

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
GABRIEL ANDRES REINOSO MARTINEZ

Firma del graduando
Reinoso Martínez Gabriel Andrés

William Ivan Ibarra Flores
Time Stamping Security Data

Firma del graduando
Ibarra Flores William Iván

DENNIS PAUL CAJAS TORRES
Firmado digitalmente por DENNIS PAUL CAJAS TORRES
Fecha: 2026.07.01 20:20:41 -05'00'

Firma del graduando
Cajas Torres Dennis Paul

Aprobación de dirección y coordinación del programa

Nosotros, **y Jacqueline Guerrero Carrera, Coordinadora UIDE,** declaramos que los graduandos: Montenegro Pozo Angie Paola, Sigcha Morochz Mario David, Reinoso Martínez Gabriel Andrés, Ibarra Flores William Iván, Cajas Torres Dennis Paul, son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.

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

Director/a de la
Maestría en Protección de Datos

Jacqueline Guerrero
Coordinadora de la
Maestría en Protección de Datos

DEDICATORIA

A mi querida mami Carolina, quien ha sido un pilar constante de amor, apoyo y aliento a lo largo de toda mi vida. Gracias por acompañarme, sostenerme y motivarme en cada paso de este camino. Esto es por ti y para ti, mami hermosa.

A Roberta Alegría, tú fuiste, eres y siempre serás el amor de mi vida. Te llevaré eternamente en mi corazón, con todo el amor y la gratitud que dejaste en mí.

Para ustedes con todo mi amor.

MARIO DAVID SIGCHA MOROCHZ

Dedico este trabajo a mis padres, quienes han sido el pilar fundamental sobre el que se sostienen mi vida, mi formación y mi ser. A mi madre, por su amor incondicional, su fortaleza y por haberme sostenido siempre con entrega y ternura, impulsándome a no rendirme y a seguir adelante, incluso en uno de los momentos más duros y difíciles de mi vida.

A mi padre, por enseñarme el valor del amor verdadero, la humildad, el sacrificio y la fortaleza; y por mostrarme, con su ejemplo, que la grandeza de la vida no se mide en lujos, sino en la capacidad de amar y entregarse por quienes se ama. A ambos, porque han sido y serán siempre los amores más grandes de mi vida y la base más firme de todo lo que soy.

Con amor incondicional…

GABRIEL ANDRÉS REINOSO MARTÍNEZ

Dedico este trabajo a la profesional que soy y que he construido con dedicación, esfuerzo y perseverancia. Cada experiencia, desafío y aprendizaje ha sido parte de este logro, que representa no solo la culminación de una etapa académica, sino también el compromiso constante con mi crecimiento y desarrollo profesional.

ANGIE PAOLA MONTENEGRO POZO

Dedico este trabajo a Dios, por ser mi guía y fortaleza en cada paso. A mi familia, por su amor, apoyo y confianza, que me impulsaron a seguir adelante hasta cumplir esta meta.

WILLIAM IVAN IBARRA FLORES

A mi hija Monnik Stefany Cajas Toapanta, por ser la inspiración que me impulsa cada día a crecer, aprender y convertirme en un profesional íntegro. Esta maestría es el resultado de tu apoyo silencioso, tu comprensión en los momentos de dedicación intensa y tu fe en mis capacidades.

Te dedico este trabajo como testimonio de que la perseverancia, la responsabilidad y la excelencia son valores que construyen un mejor futuro. Espero que este logro te inspire a perseguir tus propias metas con la misma dedicación y pasión.

con amor

DENNIS PAULCAJAS TORRES

AGRADECIMIENTOS

Quiero expresar mi principal agradecimiento a Dios, por haberme brindado su bendición, fortaleza y guía para culminar esta maestría, permitiéndome alcanzar una meta muy importante en mi vida personal y profesional.

A mi querida mami Carolina, mi gratitud eterna por su amor, apoyo incondicional y por cada esfuerzo realizado para ayudarme a crecer y convertirme en un excelente profesional. Gracias por estar siempre presente, por creer en mí y por acompañarme en cada paso de este camino.

A todas las personas que estuvieron y están presentes a lo largo de mi vida y durante esta etapa académica, gracias por su apoyo, sus palabras de aliento y por formar parte de este logro.

Muchas Gracias por todo.

MARIO DAVID SIGCHA MOROCHZ

Agradezco a Dios por sostenerme y darme la fuerza necesaria para llegar hasta aquí; a mis padres, por su amor, su apoyo y su presencia incondicional; y a mi hermana, por su cariño y compañía constante. De manera especial, agradezco también a quienes, aun al lado de la eternidad, continúan acompañando mi vida con amor, luz y protección. A todos ellos, mi gratitud más profunda por haber sido refugio, guía y parte esencial de este logro.

GABRIEL ANDRÉS REINOSO MARTÍNEZ

Agradezco a mi equipo de tesis, con quienes compartí este proceso académico, por su compromiso, colaboración y aportes durante el desarrollo de esta investigación. También

agradezco a mis profesores por los conocimientos impartidos, la orientación brindada y el acompañamiento durante mi formación académica. Finalmente, agradezco a mi familia por su apoyo y comprensión durante esta etapa.

ANGIE PAOLA MONTENEGRO POZO

Agradezco a Dios por permitirme culminar esta etapa académica. A mi familia, por su apoyo incondicional, a mis compañeros, docentes y tutores, por compartir sus conocimientos y orientarme durante el desarrollo de este trabajo.

WILLIAM IVAN IBARRA FLORES

Ante todo, expreso mi profundo agradecimiento a Dios por la salud, sabiduría y fortaleza concedidas para alcanzar esta meta importante en mi vida. A mi mami Mónica y mi papi Deni, pilares fundamentales en mi formación personal, por su amor incondicional, sus sacrificios, sus enseñanzas y por haber cultivado en mí los valores de responsabilidad y excelencia. Gracias por creer siempre en mis capacidades y por acompañarme en cada paso de este camino.

A mi esposa Elizabeth, por su amor, paciencia y apoyo incondicional durante todo este proceso. Gracias por entender los momentos de dedicación intensa y por estar a mi lado en cada etapa de esta maestría.

Muchas Gracias por todo.

DENNIS PAUL CAJAS TORRES

RESUMEN

La presente investigación analiza la aplicación del principio de privacidad desde el diseño y por defecto al uso de sistemas biométricos, específicamente de reconocimiento facial apoyado en inteligencia artificial, en el contexto de una empresa de seguridad privada en Ecuador. El problema central se sitúa en determinar si la implementación de este tipo de tecnologías resulta jurídicamente viable y materialmente recomendable a la luz de la Ley Orgánica de Protección de Datos Personales, de los principios de licitud, necesidad, proporcionalidad, minimización y responsabilidad proactiva, así como de los riesgos reforzados que derivan del tratamiento de datos biométricos por su carácter sensible, único e irreversible.

El estudio adopta un enfoque jurídico aplicado, con apoyo en criterios doctrinales, normativa nacional e internacional y herramientas de gestión de riesgos, con el propósito de evaluar la legitimidad del tratamiento biométrico en un escenario de control de acceso a edificios e instalaciones. Para ello, se examina el marco regulatorio ecuatoriano, la gobernanza del tratamiento de datos personales, la necesidad de inventarios y matrices de roles, el cumplimiento del derecho a la información, las cláusulas contractuales entre agentes de tratamiento, los riesgos específicos asociados al uso de biometría con inteligencia artificial y el deber de respuesta frente a incidentes de seguridad. La investigación integra, además, la lógica de la Evaluación de Impacto en la Protección de Datos como herramienta central para determinar si el riesgo residual del tratamiento puede considerarse aceptable.

Los resultados evidencian que el uso de biometría en una empresa de seguridad no es ilícito en abstracto, pero tampoco puede considerarse legítimo de manera automática. Su validez

depende de la concurrencia de condiciones estrictas y acumulativas, entre ellas una base de legitimación suficiente, necesidad real del tratamiento, proporcionalidad verificable, seguridad reforzada, supervisión humana efectiva, auditoría de sesgos, gobernanza clara y mecanismos adecuados de transparencia, impugnación y respuesta ante brechas. Asimismo, se concluye que la privacidad desde el diseño y por defecto no constituye un criterio meramente técnico o complementario, sino una exigencia estructural para traducir los principios de protección de datos en medidas organizativas, jurídicas y tecnológicas concretas. En ese sentido, la investigación sostiene que la viabilidad del sistema biométrico solo puede afirmarse bajo un modelo de implementación condicionado, sujeto a garantías reforzadas, evaluación continua del riesgo y revisión permanente de su impacto sobre los derechos fundamentales de los titulares.

Palabras clave: privacidad desde el diseño; protección de datos personales; biometría; reconocimiento facial; proporcionalidad.

ABSTRACT

This research analyzes the application of the principle of privacy by design and by default to the use of biometric systems, specifically facial recognition supported by artificial intelligence, in the context of a private security company in Ecuador. The central issue lies in determining whether the implementation of this type of technology is legally viable and materially advisable in light of the Organic Law on Personal Data Protection, the principles of lawfulness, necessity, proportionality, minimization, and proactive accountability, as well as the heightened risks arising from the processing of biometric data due to its sensitive, unique, and irreversible nature.

The study adopts an applied legal approach, supported by doctrinal criteria, national and international regulations, and risk management tools, with the purpose of evaluating the legitimacy of biometric processing in an access control scenario for buildings and facilities. To this end, the Ecuadorian regulatory framework, the governance of personal data processing, the need for inventories and role matrices, compliance with the right to information, contractual clauses between data processing agents, the specific risks associated with the use of biometrics with artificial intelligence, and the duty to respond to security incidents are examined. In addition, the research incorporates the logic of the Data Protection Impact Assessment as a central tool to determine whether the residual risk of the processing may be considered acceptable.

The results show that the use of biometrics in a security company is not unlawful in the abstract, but neither can it be considered automatically legitimate. Its validity depends on the concurrence of strict and cumulative conditions, including a sufficient legal basis, a real necessity for the processing, verifiable proportionality, enhanced security, effective human supervision, bias

auditing, clear governance, and adequate mechanisms for transparency, challenge, and breach response. Likewise, it is concluded that privacy by design and by default is not merely a technical or complementary criterion, but rather a structural requirement for translating data protection principles into concrete organizational, legal, and technological measures. In this regard, the research maintains that the viability of the biometric system can only be affirmed under a conditional implementation model, subject to reinforced safeguards, continuous risk assessment, and permanent review of its impact on the fundamental rights of data subjects.

Keywords: privacy by design; personal data protection; biometrics; facial recognition; proportionality.

TABLA DE CONTENIDOS

CAPITULO I 19
1. INTRODUCCION 19
2. MARCO METODOLÓGICO 20
2.1. Presentación y planteamiento del problema 20
2.1.1. Antecedentes 20
2.1.2. Delimitación del problema 22
2.2. Justificación 22
2.3. Problemas jurídicos 24
2.4. Objetivos 25
2.4.1. Objetivo general 25
2.4.2. Objetivos específicos 25
3. FUNDAMENTOS TEÓRICOS 26
2.1. Privacidad y protección de datos personales: una visión global, regional y local 26
2.2. Desafíos de la privacidad y protección de datos personales en el Ecuador 27
2.3. Evolución tecnológica y protección de datos: el papel de la IA en el tratamiento de datos personales 28
2.4. Biometría: aproximación conceptual y jurídica 30
2.4.1. Sistemas y datos biométricos 31
2.4.2. Tratamiento de datos biométricos 32
2.5. Privacidad desde el diseño y por defecto 33
CAPITULO II 35
1. Evaluación normativa 35
1.1. Privacidad desde el diseño y por defecto 35
2. La necesidad de un inventario de datos 38
3. Gobernanza de la protección de datos personales 39
3.1. Políticas, instrucciones de trabajo y flujogramas 39
3.1.1. Políticas de protección de datos personales 40
3.1.2. Instrucciones de trabajo 42

3.1.3. Flujogramas de los procesos 44
3.2. Matriz RACI 50
3.3. El cumplimiento del derecho a la información: avisos de privacidad y protección de datos personales 53
3.4. Cláusulas contractuales entre los agentes de tratamiento de datos personales 56
CAPITULO III 60
1. Nivel mínimo aceptable para el tratamiento ético, responsable y estratégico de datos personales y el uso de estos en sistemas de IA 60
2. Matriz integrada de riesgos de tratamientos de datos personales biométricos, incluyendo tratamientos con uso de IA 64
3. Plan de respuesta a incidentes de seguridad de la información que involucren datos personales (brechas) 65
3.1. Finalidad del plan 65
3.2. Alcance del plan 66
3.3. Marco normativo aplicable 67
3.4. Definición de Incidente de Seguridad Biométrica con IA 69
3.5. Incidentes de seguridad biométrica 69
3.6. Fases del protocolo 71
3.6.1. Fase 1: Detección, reporte y activación del protocolo 71
3.6.2. Fase 2: Contención, preservación de evidencias y análisis preliminar 72
3.6.3. Fase 3: Determinación de la constancia de la vulneración y notificación a la autoridad de control 72
3.6.4. Fase 4: Determinación del riesgo para los titulares y notificación a los afectados 73
3.6.5. Fase 5: Remediación, cierre, registro interno y actualización de controles 74
3.7. Roles y responsabilidades 75
3.8. Flujograma del Protocolo de Notificación 76
3.9. Registro de incidentes y documentación 77
CAPITULO IV 79

1. Ponderación de derechos: intimidad, protección de datos personales y otros derechos fundamentales 79
1.1. Juicio de razonabilidad y proporcionalidad 80
2. Evaluación de impacto a la privacidad y protección de datos personales 83
2.1. Descripción sintética del tratamiento 83
2.2. Justificación de la obligatoriedad de la EIPD 83
2.3. Identificación de riesgos relevantes 84
2.4. Acciones concretas para la gestión de los riesgos identificados 85
2.5. Evaluación de riesgo residual 87
3. Análisis de viabilidad jurídica, decisión final y recomendaciones frente al uso de sistemas biométricos 88
3.1. Toma de decisión jurídica 88
3.2. Fundamentos de la decisión 88
3.3. Recomendación jurídicas y organizacionales 90
CAPITULO V 92
1. CONCLUSIONES GENERALES 92
1.2 CONCLUSIONES ESPECÍFICAS 94
Bibliografía 96
ANEXOS 100
ANEXO A 100

LISTA DE TABLAS

Tabla 1 *Matriz RACI.* 51
Tabla 2 *Marco normativo aplicable.* 67
Tabla 3 *Roles y responsabilidades.* 75

LISTA DE FIGURAS

Figura 1 Flujograma de Enrolamiento Biométrico. 45
Figura 2 Flujograma de Control de Acceso. 46
Figura 3 Flujograma de Atención de Derechos de los Titulares. 48
Figura 4 Flujograma de Atención de Gestión de Brechas de Seguridad. 49
Figura 5 Flujograma de Atención de Gestión de Brechas de Seguridad. 50
Figura 6 Flujograma de Gestión de Incidentes de Seguridad y Violaciones de Datos Personales. 76

CAPITULO I

1. INTRODUCCION

La expansión de tecnologías biométricas apoyadas en inteligencia artificial ha transformado de manera significativa la relación entre innovación, seguridad y derechos fundamentales. Entre estas tecnologías, el reconocimiento facial ocupa un lugar especialmente sensible, en tanto convierte rasgos físicos únicos, permanentes y difícilmente sustituibles en información procesable por sistemas automatizados capaces de autenticar, comparar, clasificar e incluso perfilar a las personas. En este contexto, su uso como mecanismo de control de acceso, verificación de identidad o protección de instalaciones no puede entenderse únicamente desde la eficiencia operativa, sino como un fenómeno que exige un examen jurídico, técnico y organizacional.

En el caso ecuatoriano, este debate adquiere especial relevancia a partir de la vigencia de la Ley Orgánica de Protección de Datos Personales, de su reglamento y de la normativa secundaria emitida por la autoridad de control, que configuran un régimen reforzado de tutela para los datos personales y, con mayor intensidad, para los datos biométricos como categoría especial. Bajo este marco, la biometría no constituye una herramienta neutra ni una simple solución de autenticación, sino un tratamiento de alto impacto potencial sobre la protección de datos personales, la intimidad, la autodeterminación informativa y la igualdad, especialmente cuando incorpora inteligencia artificial, decisiones automatizadas, riesgos de sesgo algorítmico, errores de identificación y posibles expansiones funcionales incompatibles con la finalidad declarada.

La presente investigación se sitúa en ese punto de tensión. Su objeto es analizar la aplicación del principio de privacidad desde el diseño y por defecto al uso de reconocimiento facial con inteligencia artificial en el escenario de una empresa de seguridad privada en Ecuador, a fin de determinar si dicho tratamiento puede sostenerse conforme al ordenamiento ecuatoriano de protección de datos personales y a los derechos fundamentales involucrados. El problema resulta particularmente relevante porque la seguridad física constituye una finalidad legítima, pero no una justificación automática para el tratamiento de datos biométricos, menos aún cuando concurren factores de riesgo como la irreversibilidad del dato facial, la exposición física de los dispositivos, la intervención de terceros encargados y el uso de sistemas algorítmicos cuyo desempeño puede afectar de manera diferenciada a los titulares.

Desde esta perspectiva, el estudio adopta un enfoque técnico-jurídico, aplicado e interdisciplinario. La investigación parte de un examen contextual, crítico y técnicamente informado, orientado a establecer bajo qué condiciones el reconocimiento facial con inteligencia artificial puede resultar compatible con la normativa ecuatoriana de protección de datos personales y con la tutela efectiva de los derechos fundamentales.

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 IA (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 IA.

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. El caso se sitúa en un escenario de uso de reconocimiento facial para el control de acceso a edificios: el riesgo se multiplica por volumen de personas y por la exposición física de los dispositivos (cámaras accesibles, spoofing, ataques de presentación).

El caso plantea como variable crítica el modelo de tratamiento, particularmente entre esquemas de centralización y almacenamiento local por cliente. Centralizar facilita soporte, pero aumenta el “single point of failure” y hace más compleja la segregación. Un incidente afectaría a múltiples entidades. Desde la lógica de privacidad desde el diseño, adquieren relevancia medidas como, cifrar en reposo y tránsito, utilizar hardware seguro, limitar accesos por roles, y cuando sea viable realizar matching en el dispositivo o en el dominio del cliente (especialmente para hospital y banco). La retención de datos biométricos debe examinarse bajo criterios de necesidad y temporalidad, con borrado verificable al finalizar vínculo.

En paralelo aparece la dimensión de IA. 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.

2.1.2. Delimitación del problema

El problema se delimita al análisis jurídico-regulatorio del uso de reconocimiento facial para el control de acceso en edificios por parte de una empresa de seguridad privada en Ecuador. En este contexto, buscamos determinar si el tratamiento de datos biométricos puede ser legítimo, proporcional y seguro conforme a la normativa ecuatoriana de protección de datos personales. Desde una delimitación epistemológica, este estudio analiza el uso de biometría desde el derecho de protección de datos personales y los derechos fundamentales, incorporando criterios complementarios de seguridad de la información, gestión de riesgos y tecnología. La investigación se circunscribe al marco normativo vigente en Ecuador a mayo del 2026 y al contexto operativo de una empresa de seguridad privada que pretende utilizar reconocimiento biométrico para el control de ingreso a edificios o instalaciones. De manera complementaria, el análisis incorpora una comparación referencial con estándares internacionales, normativa internacional en materia de protección de datos personales y normas técnicas aplicables en cuanto permitan valorar mejores prácticas y criterios de cumplimiento.

2.2. Justificación

El presente análisis es muy necesario desde dos perspectivas, la académica, pero más aún, la práctica, toda vez que el tratamiento de datos biométricos constituye una práctica bastante regular y es una de una de las mayores injerencias en la privacidad al procesar información de forma permanente e irrevocable a la identidad de las personas. Es decir, estamos convirtiendo rasgos físicos únicos e individuales en información procesable por máquinas, lo cual genera riesgos críticos y a menudo irreversibles para los derechos fundamentales.

Desde un punto de vista legal, la biometría presenta desafíos en relación al cumplimiento de la Ley Orgánica de Protección de Datos Personales. Esto es relevante en cuanto al principio de legalidad del tratamiento, la restricción general sobre el manejo de datos sensibles sin una base de legitimación, y la necesidad de implementar el principio de responsabilidad proactiva. En este contexto, la privacidad desde el diseño y por defecto actúa como un requerimiento para el cumplimiento de los principios de protección de datos.

El análisis del tratamiento de datos biométricos en el sector de la seguridad privada adquiere especial relevancia en el Ecuador, considerando que, de acuerdo con la información verificada en el sistema institucional del Ministerio del Interior, actualmente constan registradas 1166 empresas de seguridad. Este dato permite dimensionar la amplitud operativa del sector y la incidencia que puede tener la implementación de mecanismos biométricos e inteligencia artificial en actividades vinculadas al control de acceso, verificación de identidad y protección de instalaciones. En ese contexto, el presente estudio responde a una necesidad jurídica y organizacional concreta, que se traduce en determinar si el uso de biometría por parte de las empresas de seguridad puede sostenerse conforme a los principios de licitud, necesidad, proporcionalidad, minimización y responsabilidad proactiva, evitando que la finalidad de

seguridad derive en tratamientos excesivos o en afectaciones injustificadas a los derechos fundamentales de los titulares de los datos personales (Ministerio del Interior, 2026).

Desde una perspectiva tecnológica, examinar el uso de sistemas biométricos en una empresa de seguridad es crucial dado lo intrincadas que son las arquitecturas que combinan inteligencia artificial, procesamiento en tiempo real y almacenamiento de datos sumamente confidenciales, como las plantillas faciales que provienen de características físicas exclusivas.

Estos sistemas funcionan gracias a algoritmos de reconocimiento que pueden incluir métodos de verificación (1:1) o identificación (1:N), lo que aumenta el riesgo de errores, sesgos en los algoritmos y variaciones en su rendimiento dependiendo de las condiciones de operación.

Además, la implementación de infraestructuras en la nube híbrida y dispositivos de captura ubicados físicamente aumenta la superficie de ataque, creando debilidades frente a ataques de suplantación, accesos no autorizados y brechas de seguridad. Desde esta óptica, la suficiencia del tratamiento depende de la existencia de medidas técnicas sólidas como cifrado, gestión de accesos, segmentación y procesamiento en el borde, alineadas con normativas internacionales como ISO/IEC 27001 e ISO/IEC 27701.

2.3. Problemas jurídicos

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

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

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

2.4. Objetivos

2.4.1. Objetivo general

Determinar la viabilidad jurídica y la conveniencia del uso de sistemas de biometría en la empresa de seguridad, 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

1. 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 la empresa de seguridad, considerando tanto la legislación general de protección de datos como la normativa sectorial correspondiente.
2. 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.
3. 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.

4. 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

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

La protección de la privacidad y de la información personal es un derecho esencial en la época digital, relacionado con la dignidad humana, la libertad personal y el dominio sobre los datos individuales. A nivel internacional, entidades como la OCDE han creado directrices que buscan asegurar la recolección restringida, el propósito definido, la seguridad y la rendición de cuentas en el manejo de datos, formando la base de muchos marcos regulatorios actuales. Del mismo modo, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea ha establecido un estándar mundial al introducir principios como la restricción de datos, la limitación de objetivos y la responsabilidad activa, teniendo un gran impacto en la regulación a nivel global (General Data Protection Regulation, 2026; OECD Privacy Principles, 2026).

En la esfera regional, América Latina ha vivido una transformación continua hacia el reconocimiento de la defensa de datos como un derecho independiente, en gran medida gracias al impacto del modelo europeo. Distintos países han formulado normativas completas y organismos de supervisión, mostrando una inclinación hacia la unificación regulatoria y el refuerzo institucional. Este avance pone de manifiesto la necesidad de equilibrar el progreso

tecnológico y económico con la salvaguarda de los derechos de las personas, en un entorno marcado por el aumento en el manejo masivo de información personal y la adopción de nuevas tecnologías (Badillo M; Imran M, 2026).

A nivel local, Ecuador ha fortalecido este derecho a través de la Constitución de 2008 y la Ley Orgánica de Protección de Datos Personales de 2021, que establece un esquema completo basado en pautas como legalidad, proporcionalidad, objetivo y seguridad. Esta legislación, influida por el GDPR, valida el derecho de las personas a gestionar su información, abarcando el acceso, la corrección y la eliminación de datos, además de la responsabilidad de quienes manejan la información para aplicar medidas técnicas y organizativas adecuadas. De esta manera, el sistema ecuatoriano se presenta en concordancia con normativas internacionales, subrayando la necesidad de incorporar la protección de datos en las prácticas tecnológicas y organizacionales actuales (Law R., 2026; Dávila E., 2026).

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

Ecuador enfrenta serios obstáculos en materia de protección de datos personales debido a la reciente promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP). Si bien esta legislación representa un avance significativo, aún se encuentra en proceso de implementación efectiva, tanto a nivel institucional como operativo. Entre los principales desafíos se encuentran los problemas de cumplimiento que enfrentan las entidades públicas y privadas, la falta de madurez en los marcos de gobernanza de datos y la necesidad de fortalecer la cultura de protección de datos, especialmente en las pequeñas y medianas empresas. Además, la introducción de un sistema de sanciones estricto ha incrementado la presión sobre las

organizaciones, evidenciando la brecha entre la normativa y su aplicación efectiva (Espinosa C., 2025).

Desde un enfoque tecnológico y de protección, la nación muestra vulnerabilidades significativas ante amenazas digitales, lo que incrementa los peligros para la privacidad de la población. Ecuador ha sufrido un aumento considerable en ataques cibernéticos, abarcando incidentes de ransomware y grandes filtraciones de información, como el caso que expuso datos de millones de individuos, evidenciando falencias en la seguridad de la información. Estos eventos destacan la urgencia de fortalecer las habilidades en ciberseguridad, optimizar la administración de infraestructuras críticas y adoptar estándares técnicos adecuados para reducir los riesgos relacionados con el manejo masivo de datos personales (CAD, 2025).

Finalmente, en lo que respecta a la estructura, siguen existiendo retos vinculados a la escasa cultura en torno a la protección de datos, la baja alfabetización digital entre las personas y la falta de inversión adecuada en la seguridad de la información. Investigaciones en la región muestran que un porcentaje significativo de las organizaciones no logra adherirse completamente a los estándares de protección y que una gran parte de la ciudadanía ignora sus derechos en este ámbito. En este escenario, la eficacia de la normativa ecuatoriana dependerá no solo de su solidez legal, sino también de su conexión con políticas públicas, habilidades tecnológicas y mecanismos reales de supervisión y ejecución (Vasco J., Ruiz G., Macas B., 2025).

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

El avance tecnológico, especialmente a través de la inteligencia artificial, ha cambiado drásticamente la manera en que se manejan los datos personales, facilitando un análisis extensivo, automatizado y predictivo de información como nunca antes se había visto. A

diferencia de los métodos convencionales, la IA se distingue por su necesidad de grandes cantidades de datos, que incluyen información delicada como características biométricas, patrones de conducta y datos de ubicación, lo que eleva considerablemente las amenazas a la privacidad. En este escenario, la IA no solo manipula datos directos, sino que también produce deducciones y perfiles que pueden descubrir información personal o no obvia sobre los individuos, ampliando así el grado de riesgo más allá del dato que se obtuvo en un principio (Delev Z., 2025; Maiquez J., 2025).

Uno de los retos más significativos en la convergencia de la inteligencia artificial y la protección de datos radica en el conflicto entre el avance tecnológico y la adherencia a principios esenciales como la reducción de datos, la claridad y los propósitos específicos. Los sistemas de inteligencia artificial a menudo funcionan como modelos complejos y difíciles de entender, lo que complica la explicación de las decisiones automatizadas y la efectiva garantía de derechos como el acceso, reproche o eliminación de información. Además, la presencia de sesgos en los algoritmos puede resultar en discriminación indirecta y afectar derechos fundamentales, sobre todo en áreas críticas como el reconocimiento facial, la seguridad, el empleo o los servicios financieros (De Luca S., Federico M., 2025; Baig A., Khan M., 2023).

En este contexto, la salvaguarda de datos en ámbitos de IA requiere un enfoque proactivo y centrado en riesgos, que incluya principios como la privacidad desde el diseño y de manera predeterminada, evaluación de impacto, gestión de datos y monitoreo constante. Organismos internacionales subrayan la importancia de establecer marcos regulatorios y técnicos que faciliten el uso de la IA, sin afectar los derechos de las personas, fomentando sistemas que sean transparentes, auditables y que cumplan con normas éticas. De esta manera, la función de la IA

en el manejo de datos personales no solo transforma los riesgos, sino que requiere una nueva definición de los sistemas de protección y supervisión en el entorno digital (OECD, 2024).

2.4. Biometría: aproximación conceptual y jurídica

La biometría, en el ámbito del manejo de datos personales, implica la utilización de características físicas, fisiológicas o conductuales distintivas para identificar o validar la identidad de un individuo mediante sistemas automáticos, que funcionan con algoritmos que convierten estas características en plantillas digitales que pueden ser comparadas. Desde un enfoque tecnológico y legal, los datos biométricos son considerados datos sensibles por su naturaleza intrínseca, constante e inalterable, lo que significa que, a diferencia de contraseñas u otros identificadores, no pueden ser cambiados en caso de que sean comprometidos, aumentando significativamente los riesgos vinculados a su manejo. Igualmente, la implementación de biometría en sistemas impulsados por inteligencia artificial presenta retos adicionales como fallos en la identificación, sesgos de algoritmos y discriminación indirecta, particularmente en situaciones de identificación masiva o vigilancia, lo que requiere un abordaje fortalecido conforme a principios de legalidad, necesidad y proporcionalidad. En este contexto, los marcos normativos tanto internacionales como nacionales concuerdan en la importancia de implementar garantías rigurosas para su manejo, abarcando fundamentos legales robustos, mecanismos de seguridad sofisticados, restricción de la finalidad y análisis de impacto, especialmente en situaciones de alto riesgo como el control de acceso en áreas públicas o privadas, donde el número de personas, la exposición a la tecnología y la posibilidad de supervisión intensificada aumentan la amenaza potencial a los derechos esenciales (Medrano E., Ruiz E., Ayllon M., 2026; Sen J., 2025).

2.4.1. Sistemas y datos biométricos

Los sistemas biométricos son tecnologías automáticas que permiten reconocer o validar la identidad de un individuo a través del análisis de características físicas, fisiológicas o conductuales singulares, como huellas dactilares, reconocimiento facial, iris o voz, que se convierten en plantillas digitales para su comparación a través de algoritmos específicos. Estos sistemas suelen funcionar mediante una arquitectura que incluye sensores de captura, módulos de procesamiento, creación de plantillas y motores de comparación, los cuales pueden operar en modos de verificación (1:1) o de identificación (1:N), dependiendo de si se pretende validar una identidad o encontrarla en una base de datos. Asimismo, los sistemas biométricos pueden categorizarse según el tipo de característica que emplean, diferenciándose entre biometría fisiológica (cara, iris, huella dactilar, ADN) y biometría conductual (voz, firma, hábitos de comportamiento), lo que incrementa su utilidad en diversos contextos de seguridad y acceso controlado (Sharma N., 2025; Metchik E., 2024).

Los datos biométricos se definen como aquellos datos personales que surgen de un tratamiento técnico específico aplicado a características físicas, fisiológicas o conductuales, permitiendo o confirmando la identificación única de un individuo, lo que les confiere un carácter altamente sensible en los marcos regulatorios de protección de datos. Esta clase de datos exhibe características específicas como singularidad, durabilidad y resistencia a la falsificación, lo que los hace herramientas confiables para la autenticación, aunque también se presentan como elementos de alto riesgo en caso de brechas, puesto que no pueden ser alterados ni sustituidos. Por lo tanto, su manejo se encuentra bajo condiciones rigurosas, exigiendo

fundamentos legales sólidos, protocolos de seguridad fuertes y restricciones definidas en su utilización, sobre todo cuando se utilizan para fines de identificación. (Consumer Law, 2026)

La incorporación de sistemas biométricos en ámbitos de seguridad, como el acceso a edificios, conlleva una interacción complicada entre tecnología, información y derechos básicos, donde la exactitud del sistema, la calidad de la información y la estructura de gestión impactan directamente en los riesgos implicados. Elementos como tasas de error (falsos positivos y negativos), condiciones ambientales y calidad de captura pueden influir en la fiabilidad del sistema, ocasionando posibles repercusiones en la privacidad y en la toma de decisiones automatizadas. Así, la creación y ejecución de sistemas biométricos demanda no solo efectividad técnica, sino también un enfoque holístico que incluya seguridad, ética y adherencia normativa desde su inicio (Metchik E., 2024).

2.4.2. *Tratamiento de datos biométricos*

El manejo de datos biométricos, en el contexto de Ecuador, abarca diversas operaciones que comprenden la recolección, análisis, almacenamiento y utilización de información relacionada con características físicas o comportamentales para identificar o validar la identidad de un individuo, materializándose completamente cuando estos datos son procesados técnicamente para permitir su identificación única. Conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP), estos datos son clasificados como información sensible, por lo que su uso está, en principio, prohibido a menos que haya una base de legalidad adecuada, siendo el consentimiento explícito del interesado la principal autorización jurídica, que debe ser libre, específico, informado y claro, proporcionando al interesado un control real sobre su información personal. Sin embargo, en contextos como la seguridad privada o el control de accesos, la

validez del consentimiento podría verse afectada por la ausencia de opciones verdaderas o por desequilibrios entre las partes, lo que requiere considerar otros fundamentos legales y aplicar rigurosamente los principios de necesidad y proporcionalidad. En este contexto, el manejo de datos tiene que cumplir con requisitos más estrictos, abarcando la reducción de datos, la restricción de objetivos, la adopción de protocolos de seguridad adecuados y la ejecución de análisis de impacto, sobre todo cuando se utilizan tecnologías como la inteligencia artificial, que elevan los riesgos de errores, discriminación o infringir derechos fundamentales. (LOPDP, 2021).

2.5. Privacidad desde el diseño y por defecto

Representa un enfoque anticipado en el manejo de datos personales que requiere incluir la protección de datos desde las etapas iniciales de desarrollo de sistemas, servicios o procesos tecnológicos, en lugar de agregarla de manera reactiva o posterior, lo cual es particularmente importante en el tratamiento de datos biométricos por su naturaleza sensible. Este principio, avalado en normativas como el GDPR, exige establecer medidas técnicas y organizativas apropiadas desde el comienzo y a lo largo de todo el ciclo de vida del tratamiento, teniendo en cuenta aspectos como el riesgo, la naturaleza de los datos y el contexto de uso, garantizando que, por defecto, se procesen únicamente los datos indispensables para cada fin específico.

En el contexto biométrico, esto conlleva implementar medidas técnicas como encriptación, pseudonimización, controles de acceso, reducción de datos y procesamiento en entornos seguros, además de mecanismos para la detección y respuesta a incidentes; por otro lado, desde una perspectiva organizativa, exige la creación de políticas internas, formación del equipo, evaluaciones de impacto, gestión de proveedores y auditorías constantes. Además, la implementación de este método posibilita prever y reducir riesgos como accesos no autorizados,

mal uso de datos, discriminación o fallos en la seguridad, asegurando no solo el cumplimiento de la normativa, sino también la efectiva protección de los derechos de los titulares en contextos tecnológicos de alto riesgo, como los sistemas biométricos, donde la confidencialidad, integridad y disponibilidad de la información son fundamentales (Mishova A., 2025; ;Devergranne T., 2026; European Commission, 2016; GDPR., 2026).

CAPITULO II

1. Evaluación normativa

1.1. Privacidad desde el diseño y por defecto

El tratamiento de datos personales en el Ecuador se encuentra estructurado sobre un sistema normativo jerárquico que parte de la Constitución de la República, se desarrolla a través de la Ley Orgánica de Protección de Datos Personales (LOPDP), su reglamento y normativa secundaria emitida por la autoridad de control, estableciendo un conjunto de requisitos formales que condicionan la licitud, legitimidad y seguridad de cualquier operación sobre datos personales, particularmente cuando se trata de datos biométricos en contextos de alto riesgo como el control de accesos en empresas de seguridad. En primer lugar, la Constitución reconoce el derecho fundamental a la protección de datos personales, así como la autodeterminación informativa, estableciendo que la recolección, tratamiento y difusión de datos requiere autorización del titular o mandato legal, además de garantizar derechos como acceso, rectificación y eliminación de la información, lo cual configura la base jurídica superior que legitima y limita toda actividad de tratamiento.

Sobre este fundamento, la LOPDP establece los requisitos formales específicos que deben cumplir los responsables del tratamiento. En primer lugar, exige la existencia de una base de legitimación válida conforme al artículo 7, siendo el consentimiento del titular la opción más viable en el contexto de datos biométricos, el cual debe reunir características estrictas de ser libre, específico, informado e inequívoco. Esta exigencia se refuerza en el artículo 8, que permite la revocatoria en cualquier momento, lo que implica que el tratamiento debe diseñarse considerando mecanismos efectivos para garantizar el ejercicio de este derecho. Asimismo, el

marco legal establece el cumplimiento obligatorio de principios como minimización, proporcionalidad y finalidad, obligando a que el tratamiento sea adecuado, pertinente y limitado a lo estrictamente necesario para los fines determinados. En el caso de datos biométricos, el artículo 26 establece una prohibición general para su tratamiento, permitiendo excepciones únicamente bajo condiciones estrictas, lo que eleva significativamente el estándar jurídico aplicable

Adicionalmente, la LOPDP impone requisitos formales reforzados en materia de seguridad y gestión del riesgo. En este sentido, el artículo 41 obliga a implementar medidas técnicas y organizativas adecuadas para proteger la información frente a accesos no autorizados, pérdida o destrucción, mientras que el artículo 42 establece la obligatoriedad de realizar una Evaluación de Impacto en Protección de Datos (DPIA) cuando el tratamiento implique un alto riesgo, como ocurre en los sistemas de reconocimiento facial. Asimismo, el artículo 43 establece la obligación de notificar vulneraciones de seguridad a la autoridad competente y, en ciertos casos, a los titulares, lo que introduce un componente formal de responsabilidad y transparencia en la gestión de incidentes

El Reglamento General de la LOPDP desarrolla estos requisitos, operativizando el cumplimiento normativo mediante disposiciones técnicas concretas. Entre ellas, se destaca la exigencia de obtener consentimiento mediante una acción afirmativa verificable, prohibiendo el uso del silencio o la inacción como manifestación de voluntad, así como la obligación de demostrar su obtención en cualquier momento. El reglamento también regula el ciclo de vida del dato, estableciendo la necesidad de definir plazos de conservación, aplicar procedimientos de eliminación o anonimización una vez cumplida la finalidad y garantizar mecanismos accesibles para el ejercicio de derechos por parte de los titulares. Además, introduce obligaciones

adicionales como el registro de actividades de tratamiento, la implementación de canales de atención de derechos, la gestión de transferencias de datos y la adopción de medidas de seguridad basadas en análisis de riesgos

Por su parte, la normativa secundaria emitida por la Superintendencia de Protección de Datos Personales refuerza estos requisitos, especialmente en materia de datos biométricos. En este sentido, se ha establecido que el tratamiento de este tipo de datos se considera automáticamente de “gran escala”, lo que activa obligaciones adicionales como la designación de un Delegado de Protección de Datos, la realización obligatoria de evaluaciones de impacto, la aplicación de privacidad desde el diseño y por defecto, y la implementación de registros reforzados de tratamiento. Asimismo, se ha determinado que el interés legítimo no constituye una base válida para el tratamiento de datos biométricos, lo que limita aún más las posibilidades jurídicas de su utilización y refuerza la necesidad de recurrir al consentimiento como base principal.

En conjunto, estos requisitos formales evidencian que el tratamiento de datos personales en el Ecuador, particularmente en el caso de datos biométricos utilizados en sistemas de seguridad, no puede considerarse una actividad meramente tecnológica u operativa, sino una actividad altamente regulada que exige un cumplimiento integral y documentado. La licitud del tratamiento no depende únicamente de la existencia de una finalidad legítima, sino del cumplimiento estricto de condiciones jurídicas, técnicas y organizativas que garanticen la protección efectiva de los derechos de los titulares. En este contexto, la viabilidad del tratamiento depende si se estructura sobre un modelo de cumplimiento normativo robusto, capaz de demostrar no solo la legalidad del tratamiento, sino también su necesidad, proporcionalidad y control permanente.

2. La necesidad de un inventario de datos

El inventario de datos personales constituye un elemento fundamental dentro del cumplimiento normativo en materia de protección de datos, en la medida en que permite identificar, clasificar y comprender de manera integral las operaciones de tratamiento realizadas por una organización, así como los riesgos asociados a cada fase del ciclo de vida de la información. En el caso analizado, correspondiente a una empresa de seguridad privada que implementa un sistema de reconocimiento facial para el control de acceso a edificios, el inventario revela un tratamiento complejo que integra múltiples categorías de datos personales, incluyendo datos identificativos, datos de acceso, registros de actividad y, especialmente, datos biométricos faciales, los cuales son considerados datos sensibles por su capacidad de identificar de manera única e irreversible a una persona. Este tratamiento se estructura a través de diversas actividades interrelacionadas que comprenden el registro inicial de datos, el enrolamiento biométrico, la generación de plantillas, la verificación de identidad, el monitoreo de eventos y la eliminación de la información una vez cumplida su finalidad.

Desde una perspectiva técnica y operativa, el análisis del Registro de Actividades de Tratamiento (RAT) permite evidenciar que el sistema procesa tanto datos personales básicos, como nombres, apellidos, número de identificación y ubicación dentro del edificio, como datos biométricos derivados de la captura de imágenes faciales, los cuales son transformados en plantillas digitales para su uso en procesos de autenticación. Asimismo, el sistema genera y almacena registros de eventos, tales como fechas, horas y puntos de acceso, así como logs asociados a intentos de autenticación, accesos fallidos y alertas de seguridad, lo que introduce una dimensión adicional relacionada con la trazabilidad del comportamiento de los usuarios. Esta

combinación de datos permite no solo la verificación de identidad, sino también la reconstrucción de patrones de acceso y presencia dentro de las instalaciones, lo cual incrementa el impacto potencial sobre la privacidad de los titulares.

El desarrollo del inventario de datos personales en el caso analizado permitió identificar de manera objetiva la complejidad y el alcance real del tratamiento biométrico implementado por la empresa de seguridad, evidenciando que se trata de un sistema integral que involucra múltiples categorías de datos, actores y flujos de información a lo largo de todo su ciclo de vida. A partir de la matriz de registro de actividades de tratamiento (RAT), se determinó que el sistema no solo procesa datos identificativos y biométricos, sino que también genera información derivada como registros de acceso, logs de eventos y patrones de comportamiento, ampliando significativamente el impacto potencial sobre la privacidad de los titulares.

Asimismo, el inventario permitió evidenciar la existencia de riesgos críticos en fases específicas como el registro, almacenamiento y verificación biométrica, así como la participación de terceros en el tratamiento, lo que incrementa la superficie de exposición y la necesidad de controles reforzados. En este sentido, el ejercicio de inventario no solo facilitó la identificación de los datos tratados, sino que se constituyó en una herramienta clave para demostrar que el sistema biométrico debe ser analizado bajo un enfoque de alto riesgo, validando la necesidad de aplicar principios de minimización, privacidad desde el diseño y gobernanza estricta como condiciones indispensables para su viabilidad jurídica y operativa.

3. Gobernanza de la protección de datos personales

3.1. Políticas, instrucciones de trabajo y flujogramas

La gobernanza de la protección de datos personales en el contexto de un sistema biométrico de reconocimiento facial se expresa en un marco documental compuesto por políticas, instrucciones de trabajo y flujogramas, entendidos como instrumentos operativos a través de los cuales los principios jurídicos de la LOPDP se traducen en prácticas organizativas verificables. Este marco documental no debe entenderse como un mero formalismo administrativo, sino como una herramienta sustantiva de cumplimiento, en tanto permite traducir las exigencias normativas en procedimientos verificables, asignar responsabilidades específicas dentro de la estructura organizacional, y demostrar ante la autoridad de control la implementación efectiva del principio de responsabilidad proactiva consagrado en el artículo 10 de la LOPDP.

3.1.1. Políticas de protección de datos personales

Las políticas constituyen el nivel jerárquico superior dentro del marco documental de gobernanza, en tanto establecen las directrices estratégicas y los compromisos institucionales que orientan el tratamiento de datos personales en toda la organización. En el caso que nos compete, la implementación de reconocimiento facial por una empresa de seguridad privada, las políticas deben ser aprobadas por la máxima instancia de dirección y comunicadas a todos los niveles organizacionales, debiendo incluir como mínimo las siguientes categorías.

Política General de Protección de Datos Personales: Establece el compromiso institucional con el cumplimiento de la LOPDP, define los principios rectores aplicables (licitud, finalidad, minimización, proporcionalidad, calidad, confidencialidad, seguridad y responsabilidad proactiva), identifica al Delegado de Protección de Datos (DPD) como figura responsable, y declara los derechos de los titulares que la organización se compromete a respetar. Esta política debe ser de carácter público, accesible en la página web institucional y comunicada a todos los empleados al momento de su contratación.

Política Específica de Tratamiento de Datos Biométricos: Dado el carácter sensible de los datos biométricos, esta política regula de manera específica las condiciones bajo las cuales se permite su tratamiento, estableciendo los fines autorizados (exclusivamente control de acceso a instalaciones), los plazos de conservación, las medidas de seguridad mínimas, la prohibición expresa de utilización para fines distintos (vigilancia continua, análisis de comportamiento, perfilamiento o transferencia a terceros sin consentimiento), y las condiciones de eliminación segura. Dentro de este marco, adquiere relevancia la previsión de evaluaciones de impacto previas a modificaciones sustanciales del sistema, en tanto el tratamiento biométrico exige una revisión permanente de sus riesgos y de sus condiciones de legitimidad.

Política de Seguridad de la Información: Alineada a los estándares ISO/IEC 27001 e ISO/IEC 27701, establece los controles técnicos y organizativos aplicables al sistema biométrico, incluyendo cifrado de datos en reposo y tránsito, controles de acceso basados en roles, autenticación multifactor para administradores, segmentación de redes, copias de seguridad, gestión de vulnerabilidades, monitoreo continuo y respuesta a incidentes. La eficacia de esta política depende de su revisión periódica y de su actualización frente a cambios significativos en la infraestructura tecnológica o en el panorama de amenazas.

Política de Gestión de Derechos de los Titulares: Regula el procedimiento para atender las solicitudes de acceso, rectificación, eliminación, oposición, portabilidad y revocatoria del consentimiento por parte de los titulares de datos biométricos, estableciendo plazos máximos de respuesta de quince días conforme a la LOPDP, los canales habilitados para presentar solicitudes (correo electrónico, formulario web, atención presencial) y los criterios de verificación de identidad necesarios para garantizar que las solicitudes sean atendidas únicamente al titular legítimo.

Política de Gestión de Brechas de Seguridad: Define el procedimiento institucional para la identificación, contención, evaluación, notificación y remediación de incidentes de seguridad que afecten datos biométricos, estableciendo el deber de notificar a la Superintendencia de Protección de Datos Personales en un plazo máximo de cinco días conforme al artículo 43 de la LOPDP, y a los titulares afectados cuando el incidente entrañe un alto riesgo para sus derechos y libertades.

Política de Gestión de Terceros y Encargados de Tratamiento: Regula los criterios de selección, evaluación y supervisión de proveedores que tengan acceso a datos biométricos, estableciendo la obligatoriedad de suscribir Acuerdos de Tratamiento de Datos (DPA), la realización de auditorías periódicas, la verificación del cumplimiento de estándares de seguridad y la prohibición de subcontrataciones no autorizadas.

3.1.2. Instrucciones de trabajo

Las instrucciones de trabajo constituyen el nivel operativo del marco documental, en la medida en que permiten observar cómo las políticas se proyectan sobre actividades concretas vinculadas al tratamiento de datos biométricos. A diferencia de las políticas, cuyo contenido es estratégico, las instrucciones revelan el modo en que la organización estructura operativamente procesos sensibles como el enrolamiento, la verificación, la atención de derechos, la eliminación segura y la gestión de incidentes. Para el caso analizado, se identifican las siguientes instrucciones de trabajo fundamentales.

Instrucción de Trabajo para el Enrolamiento Biométrico: Este componente permite identificar los elementos críticos del proceso de incorporación de un titular al sistema, entre ellos la verificación previa de identidad, la entrega de información, la obtención de una manifestación válida de voluntad, la captura de la imagen facial, la generación de la plantilla biométrica, su

registro y la trazabilidad del acto realizado. Cada paso debe quedar documentado en el sistema con marca de tiempo y operador responsable.

Instrucción de Trabajo para la Verificación de Identidad: Este componente permite analizar el proceso automatizado de control de acceso y los controles humanos asociados, especialmente en lo relativo a captura facial, contraste con plantillas, definición de umbrales de coincidencia, registro del evento y posibilidad de intervención humana cuando el sistema no arroje un resultado concluyente, incluyendo la captura facial en el punto de ingreso, la comparación con la plantilla almacenada, la aplicación del umbral de coincidencia definido por la organización, el registro del evento (exitoso o fallido), la activación de alertas en caso de intentos repetidos fallidos, y el procedimiento de verificación manual subsidiaria cuando el sistema biométrico no permita identificación concluyente, garantizando el derecho a intervención humana del titular.

Instrucción de Trabajo para la Atención de Derechos de los Titulares: Establece el procedimiento que debe seguir el Delegado de Protección de Datos para recibir, registrar, verificar la identidad del solicitante, evaluar la procedencia, ejecutar la acción correspondiente (acceso, rectificación, eliminación, oposición, portabilidad) y notificar al titular dentro de los plazos legales. Incluye los formatos estandarizados de respuesta, los criterios para denegar fundamentadamente una solicitud y los registros que deben mantenerse como evidencia del cumplimiento.

Instrucción de Trabajo para la Eliminación Segura de Datos Biométricos: Regula el procedimiento técnico de borrado de plantillas biométricas una vez cumplida la finalidad (terminación de la relación laboral, salida definitiva del titular, vencimiento del plazo de conservación o solicitud expresa del titular), incluyendo la eliminación en bases de datos

principales, sistemas de respaldo, copias secundarias y registros de logs vinculados, así como la generación de un certificado de eliminación verificable y la documentación del proceso para fines de auditoría.

Instrucción de Trabajo para la Gestión de Incidentes de Seguridad: Define el procedimiento de respuesta ante eventos como accesos no autorizados, fugas de información, fallos del sistema, suplantación de identidad o ataques externos, estableciendo las fases de detección, contención, erradicación, recuperación y lecciones aprendidas, así como los responsables de cada fase, los plazos máximos de actuación y las plantillas de notificación a la autoridad de control y a los titulares afectados.

3.1.3. Flujogramas de los procesos

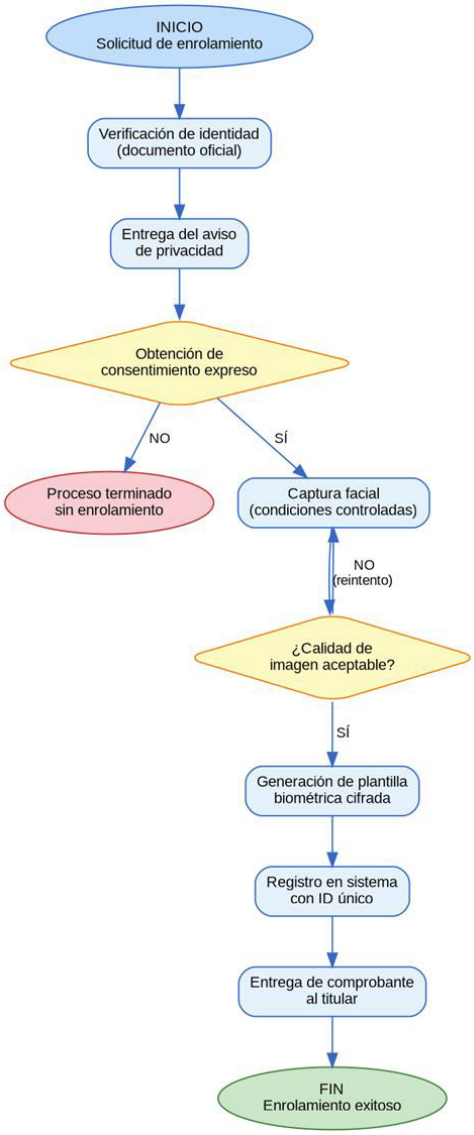
Los flujogramas constituyen representaciones gráficas secuenciales que permiten visualizar los procesos de tratamiento de datos biométricos, facilitando la comprensión del flujo de información, la identificación de puntos críticos de control, la asignación de responsabilidades y la detección de riesgos en cada fase. Su utilidad radica en que complementan las instrucciones escritas con una representación visual que resulta más intuitiva para el personal operativo y más eficaz para fines de capacitación, auditoría y mejora continua, para efectos analíticos, los flujos críticos comprenden.

Flujograma de Enrolamiento Biométrico: Inicia con la solicitud de incorporación del titular, continúa con la verificación de identidad mediante documento oficial, la entrega y aceptación del aviso de privacidad, la obtención del consentimiento expreso, la captura controlada de la imagen facial, la generación de la plantilla biométrica encriptada, el registro en el sistema con identificador único, la confirmación al titular y la finalización del proceso. Desde el punto de vista de gobernanza resulta relevante visualizar los responsables (operador, supervisor, DPD) y los

controles aplicables (calidad de imagen, integridad del consentimiento, validación cruzada con base de datos institucional).

Figura 1

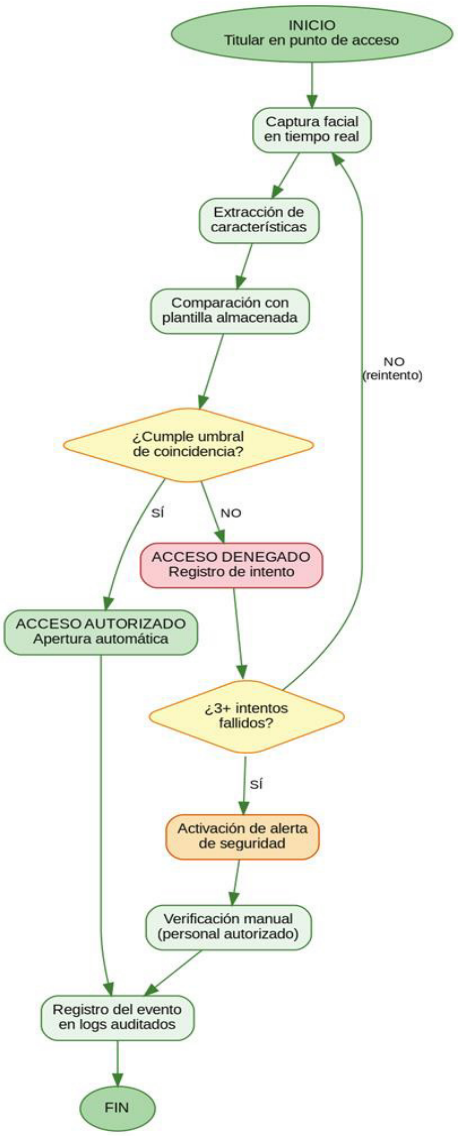
Flujograma de Enrolamiento Biométrico.



Nota. Elaboración Propia

Figura 2

Flujograma de Control de Acceso.



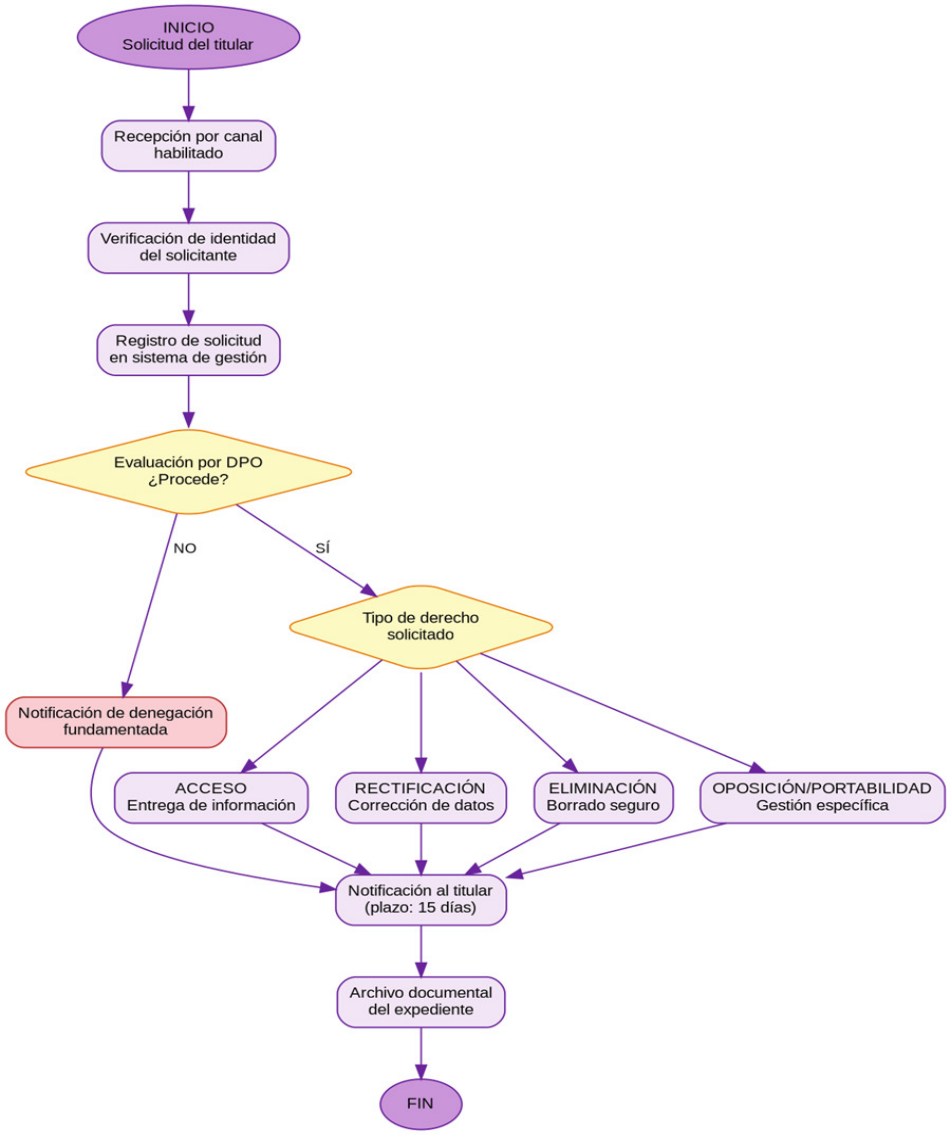
Nota. Elaboración Propia

Flujograma de Control de Acceso: Comienza con la presentación del titular ante el dispositivo biométrico, la captura facial en tiempo real, la extracción de características y comparación con la plantilla almacenada, la evaluación del umbral de coincidencia, la decisión automatizada (acceso autorizado o denegado), el registro del evento en logs auditados, y la activación de procedimientos subsidiarios en caso de denegación (verificación manual por personal autorizado, registro de incidente, atención al titular). L presentación del proceso permite identificar puntos de bifurcación que permitan la intervención humana cuando el sistema arroje resultados inconcluyentes o cuando el titular solicite expresamente esta opción.

Flujograma de Atención de Derechos de los Titulares: Inicia con la recepción de la solicitud por cualquiera de los canales habilitados, la verificación de identidad del solicitante, el registro de la solicitud en el sistema de gestión, la evaluación de procedencia por parte del DPD, la ejecución de la acción correspondiente (acceso, rectificación, eliminación, oposición, portabilidad), la notificación al titular dentro del plazo legal de quince días, y el archivo documental del expediente como evidencia de cumplimiento. La representación del proceso permite identificar rutas alternativas para casos de denegación fundamentada y para escalamiento ante la autoridad de control en caso de inconformidad del titular.

Figura 3

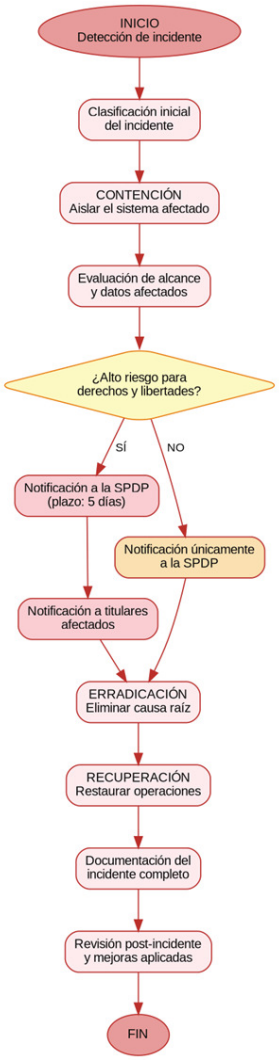
Flujograma de Atención de Derechos de los Titulares.



Nota. Elaboración Propia

Figura 4

Flujograma de Atención de Gestión de Brechas de Seguridad.



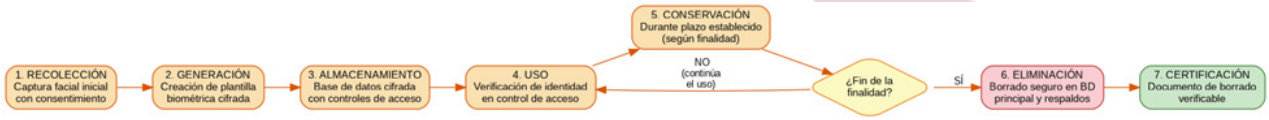
Nota. Elaboración Propia

Flujograma de Gestión de Brechas de Seguridad: Se activa ante la detección de un incidente potencial y comprende las fases de detección y clasificación inicial, contención inmediata para evitar la propagación del daño, evaluación del alcance y categorías de datos

afectados, decisión sobre la necesidad de notificación a la Superintendencia de Protección de Datos Personales en un plazo máximo de cinco días, comunicación a los titulares afectados cuando el riesgo sea elevado, ejecución de medidas correctivas, documentación del incidente y revisión post-incidente para implementar mejoras. Cada fase del flujograma debe identificar a los responsables y los plazos máximos de actuación.

Figura 5

Flujograma de Atención de Gestión de Brechas de Seguridad.



Nota. Elaboración Propia

3.2. Matriz RACI

Alineada a ISO/IEC 27001, ISO/IEC 27701 y la Ley Orgánica de Protección de Datos Personales (Ecuador).

Significado de la Matriz RACI: R → Ejecuta la actividad, A → Responsable final / quien aprueba, C → Consultado (participa técnicamente) e I → Informado

Roles considerados: Oficial de Seguridad de la Información (OSI), Oficial de Protección de Datos (DPD), Administrador de Sistemas (TI), Proveedor del Sistema Biométrico, Auditor Interno y Usuarios / Operadores.

Tabla 1

Matriz RACI.

Actividad / Control	OSI	DPD	TI	Proveedor	Auditor	Usuario
Definición de políticas de monitoreo biométrico	A	R	C	C	C	I
Configuración inicial del sistema biométrico	C	I	R	A	I	I
Monitoreo de disponibilidad del sistema	R	I	A	C	I	I
Supervisión de logs y eventos de autenticación	R	C	A	C	I	I
Detección de accesos no autorizados	R	C	A	C	I	I
Gestión de intentos fallidos y anomalías	R	C	A	C	I	I
Protección de la base de datos biométrica	A	R	C	C	I	I
Aplicación de controles de cifrado	A	R	C	C	I	I
Gestión de vulnerabilidades del sistema	R	I	A	C	C	I
Actualización y parchado del sistema	C	I	R	A	I	I
Gestión de incidentes de seguridad biométrica	R	A	C	C	I	I

Evaluación de impacto en protección de datos (DPIA)	C	A	I	C	C	I
Control de accesos a la plataforma biométrica	R	C	A	C	I	I
Auditoría del sistema biométrico	C	C	I	I	A	I
Generación de reportes de monitoreo	R	C	A	I	I	I
Cumplimiento normativo (LOPDP, ISO)	C	A	I	I	R	I
Capacitación sobre uso seguro del sistema	R	A	C	I	I	C
Eliminación segura de datos biométricos	C	A	R	C	I	I
Control de terceros (proveedor biométrico)	A	R	C	I	C	I
Continuidad del servicio biométrico (BCP/DRP)	R	C	A	C	I	I

Nota. Elaboración propia

La matriz RACI que se presenta a continuación fue elaborada para la empresa de seguridad privada que implementa el sistema de reconocimiento facial, definiendo veinte actividades críticas vinculadas al tratamiento de datos biométricos y asignando responsabilidades específicas a seis roles organizacionales: OSI, DPD, TI, Proveedor del Sistema Biométrico,

Auditor Interno y Usuarios u Operadores. La asignación se realizó conforme a los estándares ISO/IEC 27001, ISO/IEC 27701 y la LOPDP del Ecuador.

Del análisis se desprende que el DPD concentra la responsabilidad final (A) en las actividades de mayor sensibilidad jurídica, mientras que el OSI asume la ejecución (R) en la mayoría de actividades operativas de seguridad. El Administrador de Sistemas (TI) actúa como responsable final (A) en tareas técnicas de infraestructura, y el Proveedor del Sistema Biométrico, en calidad de encargado del tratamiento, asume la responsabilidad final (A) en la configuración y actualización del sistema. El Auditor Interno mantiene un perfil de verificación independiente, y los Usuarios u Operadores aparecen mayoritariamente como informados (I), consistente con su rol operativo.

En conjunto, la matriz refleja un modelo de gobernanza equilibrado que cumple con el principio de segregación de funciones, evitando que un mismo rol concentre simultáneamente la ejecución, aprobación y auditoría de una misma actividad, lo cual constituye un control esencial para mitigar riesgos en el tratamiento de datos biométricos.

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

El derecho a la información del titular de datos personales constituye uno de los pilares estructurales del sistema ecuatoriano de protección de datos y adquiere un carácter más fuerte cuando el tratamiento involucra categorías especiales, como los datos biométricos. Desde una perspectiva constitucional, el artículo 66, numeral 19, de la Constitución de la República del Ecuador reconoce el derecho fundamental a la protección de datos personales, el cual comprende el acceso a información sobre quién trata los datos, con qué finalidad y hacia quién

se dirigen. Complementariamente, el artículo 92 constitucional configura la acción de hábeas data como garantía procesal que presupone, en su lógica interna, la existencia de información previa, veraz y suficiente. Sobre estas bases, el artículo 12 de la Ley Orgánica de Protección de Datos Personales operativiza dicho mandato al establecer un catálogo de diecisiete contenidos mínimos que el responsable del tratamiento debe comunicar al titular.

Desde una perspectiva normativa, el artículo 12 de la LOPDP establece que la información facilitada por el responsable del tratamiento debe incluir, como mínimo: la identidad del responsable, las finalidades específicas del tratamiento, las bases de legitimación, los destinatarios de los datos, la duración del almacenamiento, los derechos que asisten al titular y la existencia de procesos de toma de decisiones automatizadas. En el caso de datos biométricos, se añaden requisitos específicos que exigen mayor claridad y detalle, en particular respecto de la tecnología utilizada, los riesgos asociados, las medidas de seguridad implementadas, y la obligación de mantener acceso permanente a esta información. Adicionalmente, el Reglamento General de la LOPDP establece que esta información debe proporcionarse de manera proactiva, accesible, comprensible y sin demoras injustificadas, preferiblemente al momento del establecimiento de la relación contractual o cuando comience el tratamiento.

En el contexto operativo de una empresa de seguridad privada que implementa reconocimiento facial, el aviso de privacidad y protección de datos personales debe cumplir funciones específicas: informar a los empleados y visitantes sobre la existencia del sistema biométrico, sus finalidades específicas vinculadas al control de acceso, y las bases de legitimación aplicables; detallar técnicamente cómo funcionan los sistemas de captura, verificación y almacenamiento de datos biométricos; explicar los derechos de los titulares,

incluyendo acceso, rectificación, eliminación, oposición y portabilidad; describir los riesgos inherentes al tratamiento de datos biométricos y las medidas técnicas y organizativas implementadas para minimizarlos; identificar a los destinatarios de la información y las condiciones de transferencia a terceros; y establecer los mecanismos para ejercer derechos y presentar reclamaciones ante la Superintendencia de Protección de Datos Personales como autoridad de control.

La estructura del aviso de privacidad debe considerar audiencias diversas dentro del entorno de la empresa de seguridad. Para empleados y personal permanente, el aviso debe integrarse en la documentación contractual y en los manuales de políticas internas, detallando las obligaciones y las garantías que la organización asume frente al tratamiento de sus datos biométricos. Para visitantes y terceros que acceden ocasionalmente a las instalaciones, el aviso debe ser visible mediante carteles informativos colocados de manera estratégica en los puntos de acceso, notificaciones digitales en pantallas o dispositivos biométricos, y comunicaciones claras al momento del registro inicial. En ambos casos, el lenguaje debe ser accesible, evitando tecnicismos innecesarios, pero manteniendo la precisión jurídica y técnica requerida por la normativa, garantizando que cualquier persona pueda comprender el alcance del tratamiento y sus derechos al respecto.

Un aspecto crítico del cumplimiento del derecho a la información en sistemas de reconocimiento facial es la transparencia sobre decisiones automatizadas y sesgos algorítmicos. Conforme a la LOPDP, cuando se utilicen datos personales para tomar decisiones de forma automatizada que produzcan efectos jurídicos o afecten significativamente al titular, este tiene derecho a ser informado sobre esta circunstancia, a obtener una explicación lógica del procesamiento y a solicitar intervención humana. En el contexto de un sistema de control de

acceso basado en biometría, aunque la decisión de permitir o denegar acceso es efectivamente automatizada, debe explicarse claramente al titular cómo se toman estas decisiones, qué criterios técnicos se utilizan, cuáles son las tasas de error reportadas por el sistema, y cómo puede impugnar el resultado si considera que se ha cometido un error de identificación. Asimismo, debe informarse sobre la existencia de auditorías de sesgos algorítmicos y los mecanismos de rendición de cuentas en caso de discriminación indirecta derivada del funcionamiento del sistema.

La obligación de información establecida en el artículo 12 de la LOPDP no puede interpretarse de manera tecnológicamente neutra respecto a los riesgos documentados del reconocimiento facial, pues la dimensión de la transparencia exige que el titular conozca no únicamente el funcionamiento general del sistema sino también sus limitaciones técnicas y sus consecuencias potenciales sobre derechos fundamentales. Desde la perspectiva de los derechos fundamentales, Murray (2024) advierte que el reconocimiento facial amenaza libertades como las de expresión, reunión y movimiento, en tanto actúa como mecanismo de vigilancia que genera un efecto disuasorio sobre el comportamiento de los individuos en sus actividades cotidianas; este impacto expansivo sobre el ejercicio de derechos fundamentales refuerza la lectura de que el aviso de privacidad en contextos biométricos debe ser sustancialmente más detallado y específico que en escenarios de tratamiento ordinario.

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

La implementación de un sistema de reconocimiento facial en una empresa de seguridad privada necesariamente involucra la participación de múltiples agentes de tratamiento de datos personales, cuyas responsabilidades, derechos y obligaciones requieren delimitación contractual

clara y verificable en instrumentos contractuales. Conforme a la LOPDP, el responsable del tratamiento es la persona natural o jurídica que determina los fines y medios del tratamiento de datos personales, mientras que el encargado del tratamiento es quien trata datos personales en nombre y por cuenta del responsable. En el caso analizado, la empresa de seguridad actúa como responsable, en tanto define las finalidades vinculadas al control de acceso, los medios técnicos (equipos, algoritmos, infraestructura) y las políticas de tratamiento; mientras que el proveedor del sistema biométrico, los proveedores de servicios en nube, y potencialmente los integradores de sistemas, actúan como encargados del tratamiento bajo las instrucciones documentadas del responsable.

La Superintendencia de Protección de Datos Personales reforzó la exigencia contractual establecida en la LOPDP mediante la Resolución Nro. SPDP-SPD-2025-0006-R (2025), cuyo artículo 1 establece que la obligación de incorporar cláusulas de protección de datos en las relaciones jurídico-contractuales forma parte del sistema de gestión de cumplimiento y análisis de riesgos, con el carácter de soporte documental y medida de seguridad jurídica.

En el contexto específico de datos biométricos, el contrato entre la empresa de seguridad y el proveedor del sistema biométrico debe contener cláusulas reforzadas que aborden múltiples aspectos críticos. En primer lugar, debe reconocer expresamente la naturaleza sensible de los datos biométricos, su carácter único, irreversible y altamente riesgoso. En segundo lugar, debe establecer límites estrictos en cuanto a los fines permitidos, restringiéndolos exclusivamente al control de acceso a las instalaciones y prohibiendo explícitamente cualquier otra utilización como identificación en bases de datos públicas, vigilancia extensiva, o transferencia a terceros sin consentimiento específico del titular. En tercer lugar, debe definir las medidas técnicas de seguridad mínimas requeridas, incluyendo cifrado robusto en reposo y en tránsito, autenticación

multifactor para el acceso administrativo, segregación lógica de datos por cliente, y aislamiento adecuado de sistemas. En cuarto lugar, debe prohibir cualquier forma de análisis de los datos biométricos más allá de lo necesario para la verificación de identidad, especialmente la prohibición de entrenar modelos de inteligencia artificial adicionales con los datos de la empresa.

Además, debe establecer las obligaciones específicas en materia de auditoría, monitoreo continuo y reporte oportuno de incidentes de seguridad. Asimismo, el contrato debe especificar con claridad las obligaciones del encargado en cuanto a la duración del almacenamiento de los datos biométricos y establecer cláusulas sobre transferencia internacional de datos biométricos, en caso de que el proveedor utilice infraestructura en nube ubicada fuera del Ecuador. Conforme a los artículos relativos a la transferencia internacional contenidos en la LOPDP, dichas transferencias requieren garantías equivalentes a las del ordenamiento ecuatoriano.

Adicionalmente, el contrato debe regular detalladamente la gestión de subencargados, es decir, terceros que el encargado pretenda contratar para apoyar el tratamiento. Es fundamental que el contrato exija autorización previa y por escrito del responsable para la incorporación de cualquier subencargado, prohíba subcontrataciones sin notificación, y establezca que las obligaciones del encargado se trasladen contractualmente a estos subencargados mediante cláusulas equivalentes. Esto resulta especialmente relevante en sistemas biométricos basados en nube, donde múltiples proveedores tecnológicos pueden intervenir en el procesamiento, almacenamiento o transmisión de datos, ampliando significativamente la cadena de responsabilidad y los puntos potenciales de exposición.

En definitiva, las cláusulas contractuales no son el fin del cumplimiento sino su columna vertebral operativa: la herramienta que permite que los principios de la LOPDP, los estándares

internacionales de seguridad y los postulados de la privacidad desde el diseño operen de forma coherente y verificable a lo largo de todo el ciclo de vida del tratamiento biométrico.

CAPITULO III

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

El uso de sistemas biométricos apoyados en inteligencia artificial en contextos de seguridad privada no puede considerarse admisible por la sola invocación de eficiencia operativa, innovación tecnológica o mejora en los controles de acceso. Tratándose de datos biométricos faciales, esto es, de información sensible, única, permanente y de difícil sustitución, el estándar de análisis debe ser reforzado. En consecuencia, el nivel mínimo aceptable para el tratamiento ético, responsable y estratégico de datos personales en sistemas de IA no se agota en la existencia formal de una finalidad legítima, sino que exige la concurrencia de condiciones jurídicas, organizativas y técnicas acumulativas que permitan sostener que el tratamiento se mantiene dentro de límites materialmente compatibles con la protección de datos personales y con los derechos fundamentales de los titulares.

En el caso analizado, ese umbral mínimo parte de una primera exigencia: la finalidad debe ser estricta, determinada y verificable. El uso de reconocimiento facial solo podría considerarse inicialmente admisible si se encuentra limitado al control de acceso físico a edificios o instalaciones y si, además, se excluyen finalidades secundarias o expansivas como vigilancia continua, perfilamiento, control de comportamiento o reutilización de datos biométricos para entrenamiento de modelos. Desde la lógica de la privacidad desde el diseño y por defecto, la finalidad no puede formularse en términos genéricos, sino de modo preciso y operativo, pues de ello depende la posibilidad de controlar la proporcionalidad del sistema y de evitar que la seguridad física se convierta en una justificación abierta para tratamientos excesivos.

La necesidad y la proporcionalidad constituyen un componente central del nivel mínimo aceptable del tratamiento. En el caso analizado, el reconocimiento facial no puede justificarse por razones de conveniencia, rapidez o modernización tecnológica, sino únicamente a partir de una evaluación sustantiva sobre su adecuación frente a la finalidad perseguida. Esto implica examinar si el control de acceso en edificios presenta un nivel de riesgo o exigencia tal que no pueda ser atendido de manera suficiente mediante mecanismos menos intrusivos, como credenciales, tarjetas, códigos, registros manuales o esquemas mixtos de autenticación. Desde esta perspectiva, la proporcionalidad no se agota en verificar que la biometría sea útil, sino en determinar si la intensidad de la injerencia sobre los derechos de los titulares encuentra una justificación suficiente en el contexto concreto. Por la misma razón, el umbral mínimo de aceptabilidad solo puede sostenerse, en principio, bajo esquemas de verificación 1:1, en los que el dato biométrico cumple una función puntual de contraste frente a una identidad previamente declarada, y no bajo modalidades de identificación masiva 1:N, cuyo grado de intrusión, alcance y cercanía con lógicas de vigilancia intensificada resulta cualitativamente superior.

El nivel mínimo aceptable también exige una base de legitimación jurídicamente idónea y materialmente válida. Dado que los datos biométricos constituyen una categoría especial de datos personales, su tratamiento no puede fundarse en bases ambiguas ni en justificaciones amplias. Debe poder sostenerse, antes del inicio del tratamiento, cuál es la base que habilita la operación y por qué esta resulta suficiente en el contexto concreto. En el caso de la empresa de seguridad, ello obliga además a examinar si el consentimiento, aun cuando sea expreso, realmente reúne condiciones de libertad material o si el contexto de acceso genera asimetrías que debilitan su validez. En este punto, el estándar mínimo aceptable no es meramente formal,

exige claridad en la base jurídica, transparencia reforzada y posibilidad real de oposición o alternativa equivalente.

Desde la perspectiva técnica, el tratamiento solo alcanza un umbral mínimo de aceptabilidad si se sustenta en una arquitectura de minimización y seguridad reforzada. Esto supone, al menos, limitar el tratamiento a plantillas biométricas cifradas y evitar la conservación de imágenes faciales crudas salvo necesidad excepcional debidamente documentada; aplicar cifrado en tránsito y en reposo; segmentar información por cliente; restringir accesos por roles; proteger físicamente cámaras, lectores y puntos de captura; y establecer mecanismos robustos de autenticación, trazabilidad y auditoría. Tratándose de sistemas apoyados en inteligencia artificial, ese estándar se amplía e incluye detección de vida, controles antifraude, calibración de umbrales de matching, monitoreo de falsos positivos y falsos negativos, seguimiento del rendimiento en condiciones reales y revisión de sesgos algorítmicos. Sin estas garantías, la tecnología deja de operar como herramienta de seguridad y pasa a constituir una fuente intensificada de riesgo estructural.

No menos importante es la dimensión organizativa de la aceptabilidad mínima. El uso estratégico y responsable de biometría con IA exige una estructura de gobernanza capaz de traducir la normativa en controles efectivos. Esto implica, al menos, roles y responsabilidades claramente definidos entre responsable del tratamiento, delegado de protección de datos, área técnica, área jurídica y proveedor encargado; políticas internas específicas para datos biométricos; procedimientos documentados de enrolamiento, verificación, baja y eliminación; segregación de información entre clientes; capacitación periódica del personal autorizado; revisión humana significativa frente a decisiones automatizadas relevantes; auditorías internas; y reevaluación periódica del riesgo residual y de la EIPD. La privacidad desde el diseño y por

defecto, en este contexto, no puede quedar reducida a un principio programático, sino que debe expresarse en decisiones de arquitectura, documentación, supervisión y control.

A ello se añade una exigencia decisiva, la existencia de una Evaluación de Impacto en la Protección de Datos que no sea formal ni declarativa, sino orientada a la decisión. La EIPD constituye parte del umbral mínimo aceptable porque permite valorar si los riesgos para la protección de datos, la intimidad, la autodeterminación informativa, la igualdad y la no discriminación pueden reducirse a un nivel tolerable. Si, aun después de incorporar medidas técnicas, organizativas y jurídicas, subsiste un riesgo residual elevado, el tratamiento deja de ser estratégicamente defendible. En otras palabras, la aceptabilidad mínima no se define solo antes del despliegue del sistema, sino también a partir de la posibilidad de demostrar que el riesgo residual ha sido efectivamente evaluado, mitigado y sometido a revisión permanente.

El tratamiento solo puede considerarse ético y responsable si incorpora mecanismos reales de respuesta y corrección. Esto comprende la atención de derechos de los titulares, la explicación del funcionamiento general del tratamiento, la posibilidad de impugnación frente a decisiones automatizadas, el registro de incidentes, la notificación de brechas conforme a la normativa aplicable y la revisión periódica de cambios en la finalidad, la tecnología o el contexto de uso. Desde esta óptica, el nivel mínimo aceptable no equivale a una autorización amplia para usar biometría, sino a un umbral estricto de condiciones sin las cuales el tratamiento debe considerarse jurídicamente precario, organizacionalmente deficiente y éticamente insuficiente.

En consecuencia, el nivel mínimo aceptable para el tratamiento ético, responsable y estratégico de datos personales mediante sistemas biométricos con inteligencia artificial en una empresa de seguridad privada solo se alcanza cuando concurren, de manera acumulativa, finalidad estricta, necesidad demostrada, proporcionalidad verificable, base legal idónea,

minimización, seguridad reforzada, gobernanza efectiva, evaluación de impacto, supervisión humana y capacidad real de respuesta frente a errores o incidentes. Fuera de ese umbral, el tratamiento deja de ser una herramienta legítima de control de acceso y pasa a constituir una forma desproporcionada de injerencia sobre los derechos fundamentales de los titulares.

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

El tratamiento de datos personales biométricos mediante sistemas de reconocimiento facial apoyados en inteligencia artificial exige una valoración reforzada del riesgo, debido a la naturaleza sensible, única e irreversible de la información tratada. El sistema opera bajo un esquema de verificación biométrica 1:1 para control de acceso, mediante la captura de imagen facial, generación de plantillas biométricas y comparación automatizada para autorizar o denegar el ingreso a instalaciones. Este tipo de tratamiento no solo compromete dimensiones técnicas de confidencialidad, integridad y disponibilidad, sino también derechos fundamentales como la privacidad, la protección de datos personales, la identidad, la no discriminación y la autonomía de los titulares.

La matriz integrada identifica las actividades críticas del tratamiento, los activos de información involucrados, las amenazas, las vulnerabilidades, la probabilidad de ocurrencia, el impacto, el nivel de riesgo inherente, los controles aplicables y el riesgo residual. Entre las amenazas principales se encuentran la manipulación de software, el acceso no autorizado, el perfilamiento, la falla del servidor de almacenamiento con posible pérdida, corrupción o exposición no autorizada de datos biométricos, el uso indebido de datos o espionaje remoto, y la suplantación de identidad o divulgación de información durante la verificación biométrica. Estas

amenazas se vinculan directamente con activos críticos del sistema, tales como el software de reconocimiento facial, el servidor de procesamiento de IA, las imágenes faciales capturadas, el servidor de almacenamiento, las plantillas biométricas o embeddings faciales, y la API o servicio de autenticación biométrica.

La valoración evidencia la existencia de riesgos inherentes altos y críticos, especialmente en aquellos escenarios relacionados con perfilamiento no autorizado, exposición de plantillas biométricas, acceso indebido a infraestructura de IA y errores o ataques contra el proceso de verificación biométrica. Frente a estos riesgos, se contemplan controles técnicos, organizativos y jurídicos orientados a reducir la probabilidad de materialización y el impacto sobre los titulares.

Entre las medidas principales constan el cifrado robusto de plantillas biométricas, controles de acceso granulares, monitoreo continuo mediante herramientas XDR o SIEM, detección de vivacidad, bloqueo por intentos fallidos, limitación estricta de finalidades, prohibición de usos secundarios, revisión humana ante decisiones automatizadas, auditorías periódicas y cláusulas contractuales frente al uso indebido de datos biométricos. La matriz de riesgos se encuentra en el Anexo A.

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

3.1. Finalidad del plan

El tratamiento de datos biométricos faciales mediante sistemas de reconocimiento facial con IA exige un plan específico de respuesta ante incidentes, debido a la naturaleza sensible, única e irreversible de esta información. En una empresa de seguridad privada, una brecha puede comprometer no solo la confidencialidad de imágenes o plantillas biométricas, sino también la

integridad del sistema, la disponibilidad del servicio, la correcta verificación de identidad y los derechos de los titulares.

La finalidad del plan es establecer un procedimiento ordenado para detectar, reportar, contener, analizar, notificar, remediar y documentar incidentes que involucren datos personales, especialmente datos biométricos tratados mediante IA. Este plan debe cubrir eventos como accesos no autorizados, pérdida o exposición de plantillas biométricas, suplantación de identidad, manipulación del software de reconocimiento facial, extracción de vectores o embeddings, errores sistemáticos de verificación, sesgos algorítmicos y afectaciones a decisiones automatizadas.

Desde la privacidad desde el diseño y por defecto, el plan constituye una garantía estructural del tratamiento biométrico. Su implementación permite demostrar responsabilidad proactiva, trazabilidad, capacidad de respuesta y control del riesgo durante todo el ciclo de vida del dato. Además, facilita la notificación oportuna a la autoridad de control y a los titulares cuando corresponda, así como la actualización de controles técnicos, la EIPD, el RAT y las relaciones con encargados o proveedores tecnológicos.

3.2. Alcance del plan

El plan de respuesta a incidentes aplica a todos los eventos que comprometan o puedan comprometer la confidencialidad, integridad o disponibilidad de datos personales tratados por la empresa de seguridad, con especial énfasis en los datos biométricos faciales utilizados para el control de acceso. Su alcance comprende imágenes faciales, plantillas biométricas, vectores o embeddings, registros de verificación, logs de acceso, credenciales administrativas y demás información asociada al funcionamiento del sistema biométrico.

Asimismo, el plan cubre los componentes tecnológicos que intervienen en el tratamiento, incluyendo cámaras o dispositivos de captura, servidores de almacenamiento, software de reconocimiento facial, módulos de detección de vida, APIs de verificación, infraestructura en nube o híbrida, bases de datos, respaldos y mecanismos de monitoreo. También comprende incidentes que afecten el modelo de inteligencia artificial, sus parámetros, umbrales de coincidencia, exactitud, trazabilidad o decisiones automatizadas de autorización o denegación de acceso.

El alcance subjetivo del plan incluye al responsable del tratamiento, al Delegado de Protección de Datos, al área de TI y seguridad, al área jurídica, a la alta dirección, al personal operativo y a los proveedores o encargados que participen en la operación, soporte, almacenamiento o mantenimiento del sistema biométrico. En consecuencia, cualquier actor que detecte una anomalía o incidente deberá reportarlo conforme al procedimiento interno, a fin de activar oportunamente las medidas de contención, análisis, notificación, remediación y registro.

3.3. Marco normativo aplicable

Tabla 2

Marco normativo aplicable.

Norma / estándar	Aplicación en el protocolo
Constitución de la República del Ecuador	Reconoce derechos vinculados con la intimidad, dignidad y protección de datos personales.
LOPDP, art. 43	Regula la notificación de vulneraciones a la SPDP y ARCOTEL dentro de 5 días desde que el responsable tenga

	constancia de la vulneración; el encargado debe informar al responsable dentro de 2 días.
LOPDP, art. 46	Regula la comunicación a los titulares afectados dentro de 3 días desde que el responsable conozca el riesgo para sus derechos y libertades.
Reglamento General de la LOPDP, arts. 24–28	Desarrolla el contenido, procedimiento, comunicación, actuación del encargado y registro interno de vulneraciones.
Resolución No. SPDP-SPD-2026-0009-R	Complementa el protocolo por tratarse de IA con datos personales; refuerza gestión de riesgos, medidas de seguridad, evaluación de impacto, RAT, auditoría y trazabilidad.
RGPD	Referente internacional sobre responsabilidad proactiva, seguridad del tratamiento y notificación de brechas.
ISO/IEC 27001	Aporta controles de seguridad de la información, gestión de riesgos, control de accesos, trazabilidad y mejora continua.
ISO/IEC 27035	Sirve como estándar técnico para estructurar la gestión de incidentes: detección, análisis, contención, respuesta, documentación y cierre.

Nota. Elaboración propia

3.4. Definición de Incidente de Seguridad Biométrica con IA

Para efectos del presente protocolo, se entenderá por incidente de seguridad biométrica con IA cualquier evento que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de datos biométricos faciales tratados mediante reconocimiento facial, incluyendo afectaciones a imágenes, plantillas, vectores, registros de verificación, software, infraestructura, modelo de IA o decisiones automatizadas, especialmente cuando estos componentes generen impactos acumulativos sobre los derechos de los titulares.

3.5. Incidentes de seguridad biométrica

Se considerarán incidentes de seguridad biométrica, los siguientes:

a) Acceso no autorizado a datos biométricos o a infraestructura asociada: Comprende cualquier acceso indebido a servidores, bases de datos, sistemas de almacenamiento, terminales o repositorios que contengan imágenes faciales, plantillas biométricas o registros de acceso, con capacidad de visualización, extracción, modificación o copia no autorizada de la información.

b) Exposición, pérdida, alteración o corrupción de plantillas biométricas: Incluye incidentes que afecten la integridad o disponibilidad de las plantillas biométricas faciales, ya sea por fallas del servidor de almacenamiento, errores de configuración, ausencia de redundancia, corrupción de datos o pérdida de respaldo, con impacto potencial sobre la continuidad del servicio y la confiabilidad del proceso de verificación.

c) Uso indebido de datos biométricos para fines no autorizados: Se configura cuando las imágenes faciales, plantillas biométricas o registros vinculados al sistema son utilizados para

finalidades distintas del control de acceso, en contravención del principio de finalidad, incluyendo escenarios de reutilización no autorizada o tratamiento secundario incompatible con la finalidad declarada.

Incidentes de seguridad biométrica con inteligencia artificial

Se considerarán incidentes de seguridad biométrica con inteligencia artificial, entre otros, los siguientes:

a) Manipulación no autorizada del software de reconocimiento facial o de sus parámetros: Incluye la alteración indebida del software, del modelo o de sus configuraciones, con capacidad de afectar el funcionamiento del sistema, modificar umbrales de coincidencia, permitir accesos indebidos o generar plantillas biométricas incorrectas.

b) Suplantación de identidad o spoofing en la verificación biométrica: Comprende los eventos en los que un tercero intenta vulnerar el sistema mediante ataques de presentación, manipulación de imágenes, videos, máscaras u otros mecanismos destinados a engañar al motor de verificación biométrica facial.

c) Perfilamiento o inferencia no autorizada a partir de imágenes faciales: Se configura cuando el sistema, sus operadores o terceros utilizan imágenes faciales o datos derivados para analizar, inferir o perfilar características, comportamientos o patrones de los usuarios con fines distintos del control de acceso, sin base jurídica suficiente o sin información adecuada al titular.

d) Sesgos algorítmicos o errores sistemáticos de verificación: Incluye incidentes derivados de limitaciones del modelo de inteligencia artificial que generen diferencias injustificadas de precisión, falsos positivos, falsos negativos o impactos diferenciados sobre determinados titulares, afectando la exactitud del sistema y el ejercicio de derechos.

e) Acceso no autorizado al servidor de procesamiento de IA o a los componentes del modelo: Comprende la intrusión, consulta indebida, modificación o extracción de información desde el entorno donde opera el sistema de inteligencia artificial, incluidos los modelos, parámetros, configuraciones, bases asociadas o registros de procesamiento.

f) Uso indebido, espionaje remoto o extracción de embeddings faciales: Se refiere a la obtención, copia, exfiltración o aprovechamiento no autorizado de plantillas biométricas faciales, embeddings o vectores de características utilizados por el sistema de IA, especialmente cuando ello pueda comprometer la irreversibilidad del dato biométrico o facilitar ataques posteriores.

3.6. Fases del protocolo

3.6.1. Fase 1: Detección, reporte y activación del protocolo

Cualquier colaborador, técnico, administrador, proveedor o mecanismo automatizado que detecte una anomalía en el sistema de reconocimiento facial con IA deberá reportarla de inmediato al DPD y al equipo técnico mediante el correo institucional dpd@empresa-seguridad.ec y la línea directa interna ext. 1000, incluyendo incidentes confirmados o alertas razonables que puedan afectar datos biométricos faciales o el sistema que los procesa. El reporte deberá contener la fecha, hora, componente afectado, descripción preliminar del evento, fuente y evidencias disponibles. Recibido el reporte, el DPD activará el protocolo, convocará al equipo de respuesta, ordenará la apertura del expediente interno y dispondrá las primeras medidas de contención y preservación de evidencias. La clasificación preliminar del incidente como biométrico, biométrico con IA o mixto tendrá carácter inicial y será confirmada o ajustada en la fase de análisis.

3.6.2. Fase 2: Contención, preservación de evidencias y análisis preliminar

Una vez activado el plan, el equipo de respuesta deberá contener de inmediato el incidente en el sistema de control de acceso biométrico facial de la empresa de seguridad, preservando evidencias y asegurando la continuidad operativa mediante el aislamiento de terminales o equipos, desconexión de nodos comprometidos, restricción de accesos, bloqueo de credenciales, suspensión de integraciones con terceros y resguardo forense de logs. Paralelamente, el área técnica identificará la naturaleza del evento, los activos comprometidos, las categorías de datos afectados, el número estimado de titulares, el impacto sobre sus derechos y la posible afectación del sistema de IA, incluyendo plantillas biométricas cifradas, servidor de IA, software de reconocimiento facial, umbrales, API de verificación o decisiones automatizadas de autorización o denegación de acceso. Si interviene el proveedor tecnológico o encargado del tratamiento, este deberá notificar al responsable dentro del término legal de dos días desde que conozca la vulneración.

Como resultado de esta fase, el DPD, con apoyo del área técnica y jurídica, deberá establecer si el evento analizado constituye o no una vulneración de seguridad de datos personales. Si la respuesta es negativa, el incidente continuará en monitoreo, documentación y cierre interno según corresponda. Si la respuesta es afirmativa, se activarán las fases de notificación a la autoridad y de evaluación del riesgo para los titulares, conforme a la Ley Orgánica de Protección de Datos Personales y su Reglamento.

3.6.3. Fase 3: Determinación de la constancia de la vulneración y notificación a la autoridad de control

Concluido el análisis preliminar, el DPD, con apoyo del área técnica y jurídica, deberá determinar si existe constancia de la vulneración, la cual no se configura por una simple

sospecha o alerta no confirmada, sino cuando el responsable cuenta con elementos objetivos para concluir que hubo una afectación real o probable a la confidencialidad, integridad o disponibilidad de datos biométricos faciales tratados mediante reconocimiento facial con IA. Desde ese momento, el responsable deberá notificar a la Superintendencia de Protección de Datos Personales y a la ARCOTEL tan pronto como sea posible y, en todo caso, dentro del término de cinco (5) días desde que tuvo constancia de la vulneración.

La notificación deberá incluir la naturaleza de la vulneración, categorías y número aproximado de titulares afectados, datos de contacto del DPD, sistemas comprometidos, causa presunta, datos biométricos o componentes automatizados involucrados, evaluación preliminar del riesgo y medidas adoptadas o previstas. Si no se cuenta con toda la información, podrá notificarse con los elementos disponibles y completarse de forma escalonada, sin retrasar injustificadamente el cumplimiento legal; además, si el incidente involucra IA, deberá precisarse si afectó el modelo, parámetros, umbrales, lógica de decisión automatizada, exactitud del sistema o posibles sesgos.

3.6.4. Fase 4: Determinación del riesgo para los titulares y notificación a los afectados

Paralelamente o después de notificar a la autoridad, el responsable deberá evaluar si la vulneración genera riesgo para los derechos y libertades de los titulares. Conforme al artículo 46 de la LOPDP, el plazo de tres (3) días para notificar a los titulares se cuenta desde que el responsable conoce dicho riesgo, no desde la simple detección del incidente ni desde la sola constancia de la vulneración. En datos biométricos faciales tratados con IA, esta evaluación debe ser reforzada por tratarse de datos sensibles, únicos e irreversibles, y por posibles efectos como suplantación, perfilamiento, sesgos, errores de verificación o denegaciones indebidas de acceso. Si existe riesgo relevante, la comunicación deberá realizarse sin dilación, de forma clara,

directa e individual, indicando el incidente, datos afectados, consecuencias, medidas adoptadas, contacto del DPD y derechos del titular.

De conformidad con el artículo 46.3 de la Ley Orgánica de Protección de Datos Personales, cuando el responsable considere que no corresponde notificar a los titulares, deberá dejar constancia motivada de esa decisión en el expediente y en el registro interno del incidente, justificando técnica y jurídicamente las razones por las cuales la vulneración no representa riesgo para sus derechos y libertades, o bien identificando las medidas implementadas que neutralizan de manera suficiente dicho riesgo. Esta decisión deberá encontrarse debidamente sustentada y quedar disponible para control posterior de la autoridad competente.

3.6.5. Fase 5: Remediación, cierre, registro interno y actualización de controles

Una vez ejecutadas las notificaciones, la empresa deberá remediar el incidente para restablecer la seguridad, reducir el riesgo residual y evitar su repetición, mediante acciones como restaurar el software, rotar credenciales, reforzar accesos, cifrar información, recalibrar umbrales y revisar el modelo de IA. Además, deberá registrar el incidente, documentar las medidas adoptadas y evaluar si corresponde actualizar el RAT, la EIPD, los controles de seguridad o la relación con el encargado del tratamiento.

3.7. Roles y responsabilidades

Tabla 3

Roles y responsabilidades.

Rol	Responsabilidad en el protocolo	Obligación normativa clave
Delegado de Protección de Datos (DPD)	Coordina el protocolo, notifica a la SPDP, ARCOTEL y a los titulares; documenta el incidente por mandato del responsable del tratamiento.	LOPDP, arts. 43 y 46; Regl., arts. 24–28
BioTrust (Encargado)	Notifica al Responsable dentro de 2 días de conocer la vulneración; preserva evidencias forenses.	LOPDP, art. 43, inc. 2; Regl., art. 27
Área de TI / Seguridad	Detección técnica, contención, análisis forense, preservación de logs y trazabilidad.	LOPDP, art. 37; Regl., art. 24
Área Jurídica	Evalúa base legal, coordina respuesta normativa y gestión de reclamaciones.	LOPDP, art. 43; Regl., art. 26
Alta Dirección	Aprueba decisiones estratégicas, asume responsabilidad institucional.	LOPDP, art. 47

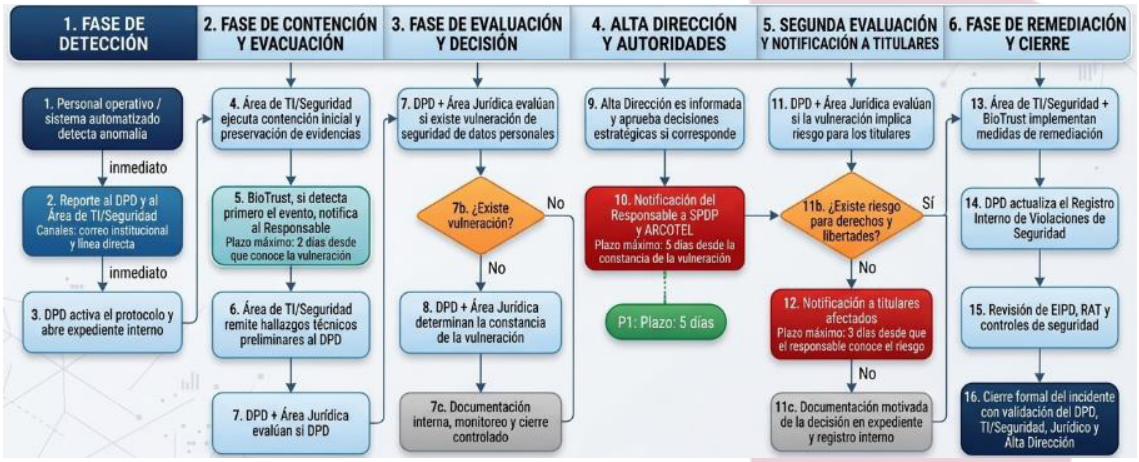
Personal operativo	Detecta y reporta cualquier incidente o anomalía al DPD en el menor tiempo posible.	LOPDP, art. 47, num. 8

Nota. Elaboración propia

3.8. Flujograma del Protocolo de Notificación

Figura 6

Flujograma de Gestión de Incidentes de Seguridad y Violaciones de Datos Personales.



Nota. Elaboración Propia

3.9. Registro de incidentes y documentación

Conforme a la LOPDP y su Reglamento, el responsable del tratamiento deberá mantener un Registro Interno de Violaciones de Seguridad actualizado, verificable y disponible, aun cuando la vulneración no sea notificada a la autoridad o a los titulares. Este registro deberá documentar cronológicamente el incidente desde su detección hasta el cierre, incluyendo actuaciones realizadas, cumplimiento de plazos, fallas identificadas, riesgo residual y medidas correctivas; además, en casos de reconocimiento facial con IA, deberá reflejar afectaciones a datos biométricos, infraestructura, software, modelo, API, decisiones automatizadas o mecanismos de detección de vivacidad. El registro Interno de Violaciones de Seguridad deberá incluir.

- Fechas y horas relevantes: detección del incidente, conocimiento de la vulneración por parte del encargado, constancia de la vulneración por parte del responsable y conocimiento del riesgo para los titulares, cuando corresponda.
- Naturaleza del incidente y clasificación preliminar y final.
- Activos, sistemas, aplicaciones o componentes comprometidos.
- Categorías de datos personales afectados, identificando expresamente los datos biométricos faciales.
- Número estimado o confirmado de titulares afectados.
- Consecuencias reales o potenciales del incidente.
- Evaluación del riesgo sobre los derechos y libertades de los titulares.
- Medidas de contención, remediación y mitigación adoptadas.

- Decisiones sobre notificación a la autoridad y a los titulares, con fechas, medios y contenido esencial.
- Participación del encargado, DPD, área técnica, área jurídica y alta dirección.
- Necesidad de actualizar la EIPD, el RAT y las medidas de seguridad vigentes.
- Fecha de cierre formal y validación final de las áreas competentes.

Cuando el incidente involucre IA, el registro deberá incluir información sobre el comportamiento del sistema, como cambios de configuración, errores de matching, fallas de detección de vivacidad, sesgos o afectación de parámetros, a fin de determinar si la vulneración afectó solo datos biométricos o también el componente algorítmico. Este registro deberá conservarse conforme a las políticas internas, con acceso restringido al DPD, área jurídica, área técnica y alta dirección, y mantenerse disponible para la autoridad de control bajo condiciones de confidencialidad, integridad y trazabilidad.

CAPITULO IV

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

El caso plantea un conflicto jurídico-constitucional entre el derecho fundamental a la protección de datos personales de quienes ingresan a edificios y el interés de seguridad física, control de acceso y protección de bienes, personas e instalaciones. La tensión se configura por la utilización del reconocimiento facial como mecanismo de autorización de ingreso, a través de un sistema que integra captura biométrica, generación de plantillas, verificación con motores de inteligencia artificial, detección de vida, controles antifraude y servicios centralizados de soporte y monitoreo. A ello se suma que el nivel de riesgo se intensifica por el volumen de personas involucradas, la exposición física de cámaras o lectores en los puntos de acceso y la posibilidad de amenazas como spoofing o ataques de presentación.

Los derechos directamente afectados son: i) el derecho a la protección de datos personales, reconocido en el artículo 66 numeral 19 de la Constitución ecuatoriana, cuyo contenido esencial permite al titular decidir y controlar la recolección, uso, conservación, circulación y protección de su información personal; ii) la intimidad personal, vinculada al resguardo de la esfera privada frente a injerencias indebidas; y iii) la igualdad y no discriminación, en la medida en que los sistemas de IA pueden generar tasas de error diferenciadas por edad, rasgos físicos, tonalidades de piel o condiciones particulares de la persona.

La afectación al derecho a la protección de datos personales es alta. Primero, porque el reconocimiento facial utiliza datos biométricos, cuya exposición tiene consecuencias más graves que la pérdida de una credencial, clave o tarjeta. Segundo, porque el tratamiento se produce en

un contexto de acceso físico, donde la persona puede carecer de una alternativa real si necesita ingresar al edificio. Tercero, porque el sistema se apoya en IA, lo que incorpora riesgos de opacidad, sesgo, falsos positivos, falsos negativos, vigilancia indebida y ampliación de finalidad. En consecuencia, el tratamiento puede afectar el núcleo de control constitucional del titular sobre su información si no existen límites estrictos de finalidad, minimización, conservación, seguridad, transparencia y alternativa no biométrica.

1.1. Juicio de razonabilidad y proporcionalidad

Como criterio metodológico aplicable a la ponderación de derechos, la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional establece que, cuando existan contradicciones entre principios o normas y no sea posible resolverlas mediante reglas de antinomias, debe aplicarse el principio de proporcionalidad. Para ello, corresponde verificar que la medida proteja un fin constitucionalmente válido, sea idónea, necesaria y mantenga un debido equilibrio entre la protección y la restricción constitucional. Asimismo, la ponderación exige establecer una relación de preferencia condicionada a las circunstancias del caso concreto, de modo que cuanto mayor sea el grado de afectación de un derecho, mayor debe ser la importancia de la satisfacción del otro. En la Sentencia No. 39-18-IN/22, la Corte Constitucional del Ecuador aplicó este estándar para determinar si una medida restrictiva de derechos era legítima o constituía una restricción injustificada.

En cuanto a la idoneidad, el sistema de reconocimiento facial puede considerarse apto para reforzar el control de acceso, siempre que se limite a verificación 1:1. La captura facial, la comparación con una plantilla previamente registrada y la detección de vida pueden contribuir a prevenir accesos indebidos, suplantaciones o uso fraudulento de credenciales. Sin embargo,

esta idoneidad es restringida: la medida solo resulta apta para una finalidad específica de autenticación en puntos de ingreso, no para vigilancia permanente, monitoreo conductual, identificación masiva ni análisis de patrones de comportamiento. Por tanto, la idoneidad no habilita un uso amplio del sistema, sino únicamente una aplicación funcionalmente limitada al control de acceso.

En cuanto a la necesidad, la medida no supera plenamente este juicio si se implementa como mecanismo único, obligatorio y generalizado para toda persona que ingrese al edificio. La afectación al derecho a la protección de datos personales sería mayor que la generada por alternativas menos intrusivas, como tarjetas de proximidad, códigos temporales, credenciales físicas, registros manuales reforzados, autenticación multifactor para zonas críticas o control biométrico limitado solo a áreas de alto riesgo. Estas alternativas también pueden contribuir a la seguridad física y al control de acceso, pero sin exigir de manera generalizada el tratamiento de datos biométricos faciales. En esta línea, la Corte Constitucional ha sostenido que el análisis de necesidad exige verificar que no exista una medida alternativa menos restrictiva de derechos que sea igualmente idónea para alcanzar el fin constitucionalmente protegido.

En cuanto a la proporcionalidad en sentido estricto, el beneficio obtenido por la empresa, mayor seguridad en el acceso físico, es constitucionalmente relevante, pero no compensa por sí solo la afectación intensa al derecho a la protección de datos personales si el sistema opera de forma masiva, obligatoria, centralizada o sin alternativa. La medida biométrica implica una injerencia reforzada en la protección de datos personales porque transforma el rostro en un identificador técnico permanente y permite decisiones automatizadas de acceso; en la intimidad, porque introduce una forma de observación tecnológica en espacios de ingreso físico; y en la igualdad y no discriminación, porque los errores del sistema pueden impactar de manera

diferenciada a personas según edad, rasgos físicos, tonalidad de piel, discapacidad, cambios faciales o condiciones particulares. En cambio, las medidas alternativas reducen la intensidad de la afectación porque permiten controlar ingresos sin convertir rasgos físicos únicos en datos procesables por IA. Por ello, el equilibrio constitucional solo se alcanza si el sistema incorpora garantías reforzadas: verificación 1:1, almacenamiento local o segregado por cliente, conservación mínima, cifrado, control de accesos, auditorías, evaluación de sesgos, pruebas de liveness, información clara al titular, base de legitimación válida, registro de operaciones, prohibición de usos secundarios y canal no biométrico equivalente.

En el contexto específico de la empresa de seguridad, la implementación de reconocimiento facial para ingreso a edificios puede considerarse jurídicamente viable de forma condicionada, pero no como mecanismo obligatorio, masivo ni indiscriminado. La jerarquía circunstancial favorece al derecho a la protección de datos personales cuando el tratamiento se plantea de forma generalizada, centralizada, sin alternativa no biométrica o bajo esquemas de identificación 1:N. En cambio, el interés de seguridad puede justificar una restricción admisible únicamente si el sistema se limita a verificación 1:1, se aplica a finalidades estrictas de control de acceso, incorpora privacidad desde el diseño y por defecto, y garantiza una alternativa equivalente para los titulares.

Por tanto, la decisión ponderativa no autoriza un despliegue amplio del sistema, sino únicamente un uso limitado, excepcional, documentado y sujeto a revisión periódica. En las condiciones descritas, la verificación 1:1, finalidad estricta, alternativa no biométrica, minimización, seguridad reforzada y control de sesgos, la medida puede superar el juicio de idoneidad, necesidad y proporcionalidad en sentido estricto. Fuera de esas condiciones, la

afectación al derecho a la protección de datos personales sería desproporcionada y correspondería rediseñar la medida o sustituirla por mecanismos menos intrusivos.

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

2.1. Descripción sintética del tratamiento

El tratamiento analizado consiste en el uso de reconocimiento facial apoyado en inteligencia artificial para verificar la identidad de personas que ingresan a edificios o instalaciones administradas por una empresa de seguridad privada en Ecuador. Su finalidad es el control de acceso físico, mediante la comparación del rostro captado con una plantilla biométrica previamente enrolada. Se trata de biometría facial aplicada en un sistema que debe operar preferentemente bajo modalidad de verificación 1:1. La inteligencia artificial interviene en el matching facial, la detección de vida y los controles antifraude frente a intentos de suplantación o ataques de presentación. Los titulares involucrados son, principalmente, residentes, visitantes y trabajadores.

2.2. Justificación de la obligatoriedad de la EIPD

La seguridad física es una finalidad legítima, pero no habilita por sí sola el uso de biometría ni excluye la necesidad de comprobar que el tratamiento sea necesario y proporcional. En este caso concurren varios factores de alto riesgo: se tratan datos biométricos, categoría especial cuyo tratamiento está en principio prohibido salvo las excepciones del artículo 26 de la LOPDP, y se incorpora inteligencia artificial para el cotejo, con decisiones automatizadas de efectos directos sobre el titular. Por ello, el artículo 42 de la LOPDP exige una evaluación de impacto cuando el tratamiento pueda implicar alto riesgo para los derechos y libertades, supuesto que

aquí se configura; esta conclusión se ve además reforzada por criterios de la autoridad de control contenidos en los Oficios SPDP-IRD-2025-0031-O y SPDP-IRD-2025-0065-O. A ello se suma que el dato biométrico es único, permanente e irreversible, de modo que su afectación puede resultar difícil o imposible de reparar. La escala y el contexto del tratamiento, con dispositivos expuestos y registro continuo de accesos, incrementan el riesgo y pueden derivar en formas de monitoreo sistemático. En consecuencia, la EIPD no es opcional, sino el instrumento necesario para valorar necesidad, proporcionalidad y alternativas menos invasivas, ponderando su impacto sobre la intimidad, la imagen, protección de datos personales y seguridad.

2.3. Identificación de riesgos relevantes

La identificación de riesgos que se presenta en esta EIPD constituye una síntesis razonada del análisis desarrollado a detalle en el Capítulo III y en la matriz integrada del Anexo A. Por tanto, los riesgos aquí descritos deben leerse en coherencia con la matriz de riesgos de tratamientos biométricos con IA, especialmente respecto de las relaciones activo/amenaza allí identificadas.

Los riesgos para derechos y libertades se proyectan sobre la protección de datos personales (incluida su dimensión de autodeterminación informativa), la intimidad y la imagen. El riesgo concreto es la pérdida de control sobre un dato permanente e identificador, especialmente si la plantilla se conserva más tiempo del necesario, se reutiliza para finalidades distintas o se emplea de forma funcionalmente expansiva. Los riesgos tecnológicos afectan la confidencialidad, integridad y disponibilidad de los datos por la exposición de cámaras y lectores en puntos físicos de acceso. En este contexto, los principales riesgos son la manipulación de dispositivos, los

ataques de presentación, el spoofing, los accesos no autorizados a plantillas biométricas y las fallas de cifrado, todo lo cual compromete información de difícil sustitución.

Los riesgos organizacionales se relacionan con la responsabilidad proactiva y con el ejercicio efectivo de los derechos de los titulares. Surgen, en particular, si no existe una base legal clara, un aviso de privacidad suficiente, una alternativa no biométrica, reglas de conservación, procedimientos de baja, segregación entre clientes o contratos robustos con encargados y subencargados, lo que podría convertir el tratamiento en una práctica desproporcionada frente a la finalidad declarada.

Los riesgos de sesgo y discriminación afectan la igualdad, la no discriminación, el trabajo, la movilidad y el acceso a servicios. El riesgo concreto consiste en que el sistema genere falsos positivos o falsos negativos por condiciones de iluminación, edad, tonalidad de piel, cambios faciales, discapacidad o condiciones médicas, permitiendo accesos indebidos o impidiendo injustificadamente el ingreso de personas autorizadas.

2.4. Acciones concretas para la gestión de los riesgos identificados

Medidas técnicas: 1) limitar el sistema a verificación 1:1 y excluir identificación masiva 1:N; 2) almacenar únicamente plantillas biométricas y no imágenes faciales crudas; 3) aplicar cifrado en tránsito y en reposo; 4) implementar detección de vida, controles antifraude y pruebas periódicas frente a spoofing o ataques de presentación; 5) proteger físicamente cámaras y lectores ubicados en puntos de acceso; 6) aplicar control de accesos por roles, registros de auditoría, calibración de umbrales y monitoreo de falsos positivos y falsos negativos; y 7) eliminar de forma verificable las plantillas cuando finalice la relación que justifica el acceso.

Medidas organizativas: 1) definir roles y responsabilidades claras entre el responsable del tratamiento, el delegado de protección de datos, el área técnica, el área jurídica y el proveedor encargado; 2) contar con políticas internas y procedimientos documentados sobre enrolamiento, verificación, conservación, eliminación de plantillas biométricas, atención de derechos y gestión de incidentes; 3) segregar los datos por cliente y restringir el acceso únicamente al personal que lo requiera por sus funciones; 4) incorporar supervisión continua, controles de cumplimiento y auditorías internas periódicas; 5) establecer revisión humana significativa frente a decisiones automatizadas relevantes; y 6) realizar reevaluaciones periódicas del riesgo residual y de la EIPD ante cambios tecnológicos, incidentes o ampliación de finalidades.

Medidas jurídicas: 1) definir una base legal válida y documentada; 2) emitir un aviso de privacidad específico, claro y previo; 3) formalizar contratos con BioTrust, encargados y subencargados; 4) establecer cláusulas de confidencialidad, seguridad, eliminación y notificación de incidentes; y 5) dejar constancia de la decisión adoptada por la organización.

En conjunto, las medidas son efectivas porque reducen exposición del dato biométrico, suplantación, accesos no autorizados, errores del sistema, reutilización indebida y falta de control sobre plantillas. También son realistas, porque corresponden a controles técnicos, organizativos y jurídicos aplicables a sistemas biométricos de control de acceso. Sin embargo, su suficiencia es condicionada: solo reducen el riesgo a un nivel jurídicamente tolerable si se implementan antes del despliegue, se documentan, se auditan y se mantienen como obligaciones exigibles. Si falta base legal clara, alternativa no biométrica, limitación de finalidad, verificación 1:1 o eliminación verificable, las medidas dejan de ser suficientes.

2.5. Evaluación de riesgo residual

A pesar de las medidas de mitigación propuestas, subsiste un riesgo residual relevante para los derechos y libertades de los titulares, en especial para la protección de datos personales, la intimidad y la igualdad. Ello se debe a la naturaleza sensible, única e irreversible del dato biométrico facial, así como a la posibilidad persistente de errores de autenticación, ataques de presentación, spoofing y afectaciones derivadas del uso de inteligencia artificial en contextos de control de acceso. No obstante, ese riesgo residual puede considerarse jurídicamente aceptable solo de manera condicionada, siempre que el tratamiento opere bajo límites reforzados de necesidad, proporcionalidad, seguridad y control. En particular, la aceptabilidad del riesgo depende de que se mantengan de forma efectiva la verificación 1:1, la exclusión de identificación masiva 1:N, la existencia de una alternativa no biométrica equivalente, el cifrado de plantillas, la detección de vida, la limitación estricta de finalidad, la eliminación verificable de datos y la supervisión humana frente a incidencias relevantes. Si estas condiciones no se cumplen o no pueden comprobarse, el riesgo residual deja de ser tolerable y el tratamiento se torna desproporcionado frente a los derechos fundamentales comprometidos.

La DPIA permite concluir que el tratamiento presenta un riesgo aceptable condicionado. La finalidad de seguridad física y control de ingreso es legítima; sin embargo, el uso de biometría facial con inteligencia artificial mantiene un riesgo relevante por la naturaleza sensible del dato, la exposición de los dispositivos y la posibilidad de errores, suplantación o afectaciones a la intimidad, la protección de datos y la igualdad. En consecuencia, el tratamiento solo será aceptable si se limita a verificación 1:1, excluye identificación masiva 1:N, ofrece una alternativa no biométrica equivalente, evita conservar imágenes crudas y aplica medidas reforzadas de

seguridad, supervisión y limitación de finalidad. Si estas condiciones no se implementan antes del despliegue, el riesgo se tornará inaceptable por desproporción frente a los derechos fundamentales de los titulares.

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

3.1. Toma de decisión jurídica

A la luz del análisis normativo desarrollado, de la ponderación de derechos realizada y de los resultados de la Evaluación de Impacto en la Protección de Datos, se concluye que el uso de reconocimiento facial apoyado en inteligencia artificial por parte de una empresa de seguridad privada es jurídicamente viable de manera condicionada. Esta conclusión no responde a una aceptación general o automática del tratamiento biométrico, sino a la constatación de que su admisibilidad depende del cumplimiento acumulativo de garantías reforzadas que permitan mantener el tratamiento dentro de límites materialmente compatibles con la protección de datos personales y con los derechos fundamentales de los titulares.

3.2. Fundamentos de la decisión

La presente decisión se fundamenta, en primer lugar, en que la finalidad perseguida, el control de acceso físico a edificios o instalaciones, puede constituir un interés legítimo en términos organizacionales, pero no basta por sí sola para habilitar el tratamiento de datos biométricos. Tratándose de datos personales de categoría especial, sometidos a un régimen reforzado de protección conforme al artículo 26 de la Ley Orgánica de Protección de Datos Personales, la licitud del tratamiento exige una justificación más intensa, basada en necesidad, proporcionalidad, minimización, seguridad reforzada y responsabilidad proactiva. En este punto,

la ponderación constitucional no autoriza reconocer una prevalencia automática del interés de seguridad sobre el derecho a la protección de datos personales y la autodeterminación informativa, garantizados por los artículos 66 numeral 19 y 92 de la Constitución de la República del Ecuador. De acuerdo con la metodología de proporcionalidad reconocida por la Corte Constitucional del Ecuador en la Sentencia No. 39-18-IN/22, la restricción de derechos solo puede considerarse legítima cuando la medida es idónea, necesaria y proporcionada en sentido estricto. Aplicado al caso, ello implica que el reconocimiento facial solo puede sostenerse si no existen medios menos intrusivos igualmente eficaces y si su intensidad de injerencia encuentra una justificación suficiente en el contexto concreto.

En segundo lugar, la decisión se apoya en los resultados de la EIPD, que permiten concluir que, aun con medidas de mitigación técnicas, organizativas y jurídicas, subsiste un riesgo residual relevante para la protección de datos personales, la intimidad, la autodeterminación informativa y la igualdad. Este riesgo deriva de factores estructurales del tratamiento, entre ellos la irreversibilidad del dato biométrico facial, la posibilidad de falsos positivos o falsos negativos, la exposición física de los dispositivos, los ataques de presentación, el spoofing, el uso indebido de plantillas biométricas y los sesgos algorítmicos. No obstante, el análisis también permite sostener que ese riesgo residual puede ser jurídicamente tolerable solo dentro de límites reforzados y bajo una implementación estrictamente condicionada. Fuera de ese marco, el tratamiento dejaría de ser compatible con los principios de protección de datos personales y con el estándar de privacidad desde el diseño y por defecto.

3.3. Recomendación jurídicas y organizacionales

En el escenario de viabilidad condicionada, la primera recomendación consiste en restringir el sistema a verificación 1:1, excluyendo expresamente cualquier modalidad de identificación masiva 1. Esta restricción debe complementarse con una alternativa no biométrica obligatoria, real y funcional, así como con una limitación estricta de finalidad que impida extender el tratamiento a monitoreo continuo, perfilamiento, análisis conductual o entrenamiento de modelos. Del mismo modo, resulta indispensable consolidar un esquema de privacidad desde el diseño y por defecto, que incluya plantillas biométricas cifradas, no conservación de imágenes faciales crudas salvo justificación excepcional, segmentación de la información por cliente, restricción de accesos por roles, protección física de dispositivos, revisión humana significativa, auditorías periódicas y reevaluación continua de la EIPD frente a cambios tecnológicos, incidentes o ampliación de finalidades.

En un escenario de incumplimiento de las condiciones mínimas, la conclusión jurídica es la improcedencia de la implementación del reconocimiento biométrico y la preferencia por mecanismos menos intrusivos de autenticación. Esta conclusión se impone, por ejemplo, cuando no puede sostenerse una base de legitimación válida, no existe alternativa no biométrica, se pretende conservar imágenes crudas sin justificación suficiente, la finalidad se amplía más allá del control de acceso o el riesgo residual permanece elevado aun después de las medidas de mitigación. En tales supuestos, el tratamiento deja de ubicarse en un marco de viabilidad condicionada y pasa a configurarse como una medida incompatible con el estándar mínimo de aceptabilidad desarrollado en esta investigación.

La decisión adoptada no implica una valoración abstracta de la biometría como tecnología, sino una conclusión contextual, fundada y revisable, construida a partir de la estructura normativa nacional, de la ponderación de derechos fundamentales y de los resultados de la Evaluación de Impacto. La viabilidad aquí afirmada es inseparable de las garantías que la sostienen y debe entenderse sujeta a revisión frente a cambios tecnológicos, normativos o fácticos que alteren el equilibrio de derechos analizado.

CAPITULO V

1. CONCLUSIONES GENERALES

La implementación de sistemas de biometría facial apoyados en inteligencia artificial en una empresa de seguridad privada no es jurídicamente inadmisible en abstracto, pero tampoco puede considerarse legítima de manera automática. La respuesta al primer problema jurídico planteado conduce a afirmar que su viabilidad depende del cumplimiento acumulativo de exigencias reforzadas derivadas de la Constitución de la República, de la Ley Orgánica de Protección de Datos Personales y de los principios de privacidad desde el diseño y por defecto. En consecuencia, la licitud del tratamiento no se agota en la existencia de una finalidad de seguridad, sino que exige base de legitimación idónea, necesidad demostrada, proporcionalidad verificable, minimización, seguridad reforzada, supervisión humana y capacidad efectiva de respuesta ante incidentes y errores del sistema.

Respecto al segundo problema jurídico, el uso de biometría en una empresa de seguridad solo puede considerarse recomendable desde la perspectiva de protección de datos y derechos fundamentales cuando se mantiene dentro de un modelo de implementación estrictamente condicionado. Se evidenció que el dato biométrico facial, por su carácter sensible, único, permanente y difícilmente sustituible, incrementa la intensidad de la injerencia sobre la protección de datos personales, la intimidad, la autodeterminación informativa y la igualdad. Por ello, la recomendabilidad del sistema no depende de su conveniencia tecnológica ni de su eficiencia operativa, sino de que el reconocimiento facial se limite a verificación 1:1, excluya

identificación masiva, prohíba usos secundarios y opere bajo una gobernanza robusta capaz de prevenir expansiones funcionales incompatibles con la finalidad declarada.

En relación con el tercer problema jurídico, la Evaluación de Impacto en la Protección de Datos constituye el instrumento decisional central para determinar si el riesgo residual del uso de biometría es aceptable y controlable. El análisis desarrollado permitió establecer que, aun con medidas de mitigación técnicas, organizativas y jurídicas, subsiste un riesgo residual relevante para los derechos y libertades de los titulares, derivado de la irreversibilidad del dato facial, la posibilidad de errores de autenticación, sesgos algorítmicos, ataques de presentación, spoofing y exposición física de los dispositivos. No obstante, dicho riesgo puede ser jurídicamente tolerable solo de manera condicionada, siempre que se mantengan efectivamente límites reforzados de necesidad, proporcionalidad, seguridad y control. Fuera de ese marco, la conclusión jurídica debe modificarse hacia la improcedencia de la implementación y la preferencia por mecanismos menos intrusivos de autenticación.

La privacidad desde el diseño y por defecto no constituye un criterio accesorio o meramente técnico, sino la condición estructural que permite traducir los principios de protección de datos personales en medidas concretas de arquitectura, gobernanza, seguridad, evaluación de impacto y respuesta institucional. Por ello, la decisión final adoptada es la de viabilidad jurídica condicionada del reconocimiento facial con inteligencia artificial dentro de la empresa de seguridad, concluyendo que solo se sostiene mientras permanezcan vigentes y verificables las garantías que la fundamentan.

1.2 CONCLUSIONES ESPECÍFICAS

El análisis jurídico estableció que el reconocimiento facial apoyado en inteligencia artificial no puede reducirse a la verificación aislada de una base de legitimación ni a la constatación formal de una finalidad de seguridad. El análisis desarrollado demuestra que la viabilidad del tratamiento depende de una estructura de garantías acumulativas en la que convergen evaluación normativa, gobernanza, gestión del riesgo, ponderación constitucional y evaluación de impacto. En ese sentido, el problema de la biometría en contextos de seguridad privada no se agota en la licitud abstracta del tratamiento, sino que exige comprobar, en cada caso, si la medida supera estándares reforzados de necesidad, proporcionalidad, minimización, seguridad y control permanente.

Se evidenció que la categoría biométrica posee una singularidad jurídica que intensifica la carga de justificación del tratamiento. El carácter sensible, único, permanente y difícilmente sustituible del dato facial impide equipararlo a mecanismos ordinarios de autenticación y obliga a examinarlo bajo un régimen reforzado de tutela. Desde esta perspectiva, la investigación permitió demostrar que la incorporación de inteligencia artificial no representa únicamente una mejora operativa, sino un factor adicional de complejidad jurídica, por cuanto introduce riesgos de error, opacidad, sesgo algorítmico, decisiones automatizadas y posibles afectaciones diferenciadas sobre los titulares.

En términos académicos, la principal contribución del trabajo radica en haber articulado, dentro de un mismo modelo analítico, dimensiones que con frecuencia se estudian de manera

fragmentada: marco constitucional, normativa de protección de datos, privacidad desde el diseño y por defecto, inventario de datos, gobernanza, matriz de riesgos, protocolo de respuesta a incidentes, ponderación de derechos, evaluación de impacto y decisión jurídica final. Esta integración permitió construir una metodología de análisis aplicable a tratamientos biométricos de alto riesgo en Ecuador, aportando una lectura que no se limita a la descripción normativa, sino que conecta la teoría jurídica con exigencias técnicas y organizacionales concretas.

En el plano profesional y formativo, el proceso investigativo fortaleció una comprensión más rigurosa del papel que cumple la protección de datos personales frente a tecnologías emergentes. El estudio permitió consolidar capacidades de argumentación constitucional, análisis regulatorio, evaluación de impacto, identificación de riesgos y formulación de decisiones jurídicas complejas en escenarios de innovación tecnológica. De igual forma, reforzó la comprensión de que la privacidad desde el diseño y por defecto no constituye una cláusula retórica, sino un criterio operativo indispensable para traducir principios jurídicos en controles verificables a lo largo de todo el ciclo de vida del tratamiento.

Bibliografía

Asamblea Nacional del Ecuador. (2009). Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (Ley s/n). Registro Oficial, Segundo Suplemento No. 52, 22 de octubre de 2009.

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459, 26 de mayo de 2021.

Badillo, M., & Imran, M. (2024). Regulatory strategies and priorities of data protection authorities in Latin America: 2024 and beyond. Future of Privacy Forum. https://fpf.org/wp-content/uploads/2024/05/Final-_-LatAm-DPA-Report-_-2024.pdf

Centro de Autonomía Digital. (2025, 1 de octubre). Data leaks and digital espionage. https://autonomia.digital/en/2025/10/01/data-leaks-and-digital-espionage.html

Cerafor. (2025). Biometric devices: Definition, examples, types, applications. https://cerafor.com/blog/biometric-devices-definition-examples-types-applications/

Comisión Europea. (2021). Cláusulas contractuales tipo para transferencias internacionales (Decisión de Ejecución (UE) 2021/914). https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Constitución de la República del Ecuador. (2008). Registro Oficial 449, 20 de octubre de 2008.

DLA Piper. (2025). Data protection laws of the world: Ecuador. https://www.dlapiperdataprotection.com/index.html?t=law&c=EC

De Luca, S., & Federico, M. (2025). Algorithmic discrimination under the AI Act and the GDPR (PE 769.509). European Parliamentary Research Service.

https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769509/EPRS_ATA(2025)769509_EN.pdf

Devergranne, T. (s. f.). Privacy by design & by default : guide complet RGPD (Art. 25). Données Personnelles. Recuperado el 29 de junio de 2026, de https://www.donneespersonnelles.fr/privacy-by-design-privacy-by-default

Espinosa-Velarde, C. F. (2025). Protección de datos en Ecuador. ECIJA GPA. https://www.ecija.com/actualidad-insights/proteccion-de-datos-en-ecuador/

European Data Protection Board. (2021). Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Versión 2.0). https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

Information Commissioner's Office. (2023). Right to be informed. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-be-informed/

International Organization for Standardization & International Electrotechnical Commission. (2019). ISO/IEC 27701:2019. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management.

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

LegalClarity. (2025). GDPR biometric data: Rules, rights, and penalties. https://legalclarity.org/gdpr-biometric-data-rules-rights-and-penalties/

Medrano-Sánchez, E. J., Ruiz-Ramírez, E., & Ayllon, M. L. (2026). Between innovation and risk: Artificial intelligence and data protection in digital Mexico. Frontiers in Artificial Intelligence, 9, Artículo 1716108. https://doi.org/10.3389/frai.2026.1716108

Murray, D. (2024). Facial recognition and the end of human rights as we know them? The International Journal of Human Rights, 28(4), 1–18. https://doi.org/[verificar DOI: el artículo es de Taylor & Francis, prefijo habitual 10.1080].

OECD. (2024). AI, data governance and privacy: Synergies and areas of international co-operation (OECD Artificial Intelligence Papers No. 22). OECD Publishing. https://doi.org/10.1787/2476b1a4-en

OECD. (2013). The OECD privacy framework. OECD Publishing. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos). Diario Oficial de la Unión Europea, L 119, 4 de mayo de 2016.

Presidencia de la República del Ecuador. (2023). Reglamento General a la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo N.º 904). Registro Oficial Suplemento 435, 13 de noviembre de 2023.

Recording Law. (s.f.). Ecuador data privacy laws. https://www.recordinglaw.com/world-laws/world-data-privacy-laws/ecuador-data-privacy-laws/

Securiti. (2024). The impact of the GDPR on artificial intelligence. https://securiti.ai/impact-of-the-gdpr-on-artificial-intelligence/

Superintendencia de Protección de Datos Personales. (2025a, 20 de mayo). Oficio N.º SPDP-IRD-2025-0065-O [Absolución de consulta sobre el tratamiento de datos biométricos para el registro de asistencia de trabajadores]. https://spdp.gob.ec/consultas2025/

Superintendencia de Protección de Datos Personales. (2025b, 30 de abril). 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 N.º SPDP-SPD-2025-0006-R). https://spdp.gob.ec/resolucion6/

Superintendencia de Protección de Datos Personales. (2026, 12 de febrero). Norma general para la garantía del derecho de protección de datos personales en el uso de sistemas de inteligencia artificial (Resolución N.º SPDP-SPD-2026-0009-R). https://spdp.gob.ec/resol_ia_02_2026/

Vasco Delgado, J. C., Ruiz Muñoz, G. F., Macas Padilla, B. A., & León Quiñónez, V. H. (2025). Ciberseguridad y protección de datos personales: desafíos y perspectivas. GADE: Revista Científica, 5(1), 675–688. https://doi.org/10.63549/rg.v5i1.642

Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer. https://doi.org/10.1007/978-3-319-57959-7

ANEXOS

ANEXO A

Figura A1

Matriz de valoración de riesgos

Nombre de la actividad de tratamiento	Activos de información	Amenazas	Descripción	Dimensión Afectada	Vulnerabilidad	Probabilidad	Impacto	Riesgo Inherente	Tipo de Control	Controles	Riesgo Residual
Registro biometrico de acceso al edificio	Software de reconocimiento facial	Manipulación de software	Alteración no autorizada del software de reconocimiento facial o de sus parámetros, que puede afectar el funcionamiento del sistema y permitir accesos indebidos o generación incorrecta de plantillas biométricas.	Confidencialidad, Integridad	Falta de controles de integridad del software, ausencia de validación de cambios y configuraciones débiles que permiten la modificación no autorizada del sistema.	Poco Probable	Crítico	Medio	Correctivo	Restauración inmediata del software a una versión íntegra y validada, junto con la corrección de configuraciones alteradas y reaplicación de controles de seguridad.	Irrelevante
	Servidor de procesamiento de IA	Acceso no autorizado	Acceso no autorizado que permite la visualización, modificación o extracción de datos biométricos y del modelo, comprometiendo la seguridad del sistema y facilitando accesos indebidos.	Confidencialidad	Configuraciones de acceso débiles, ausencia de autenticación robusta y falta de control de privilegios.	Probable	Crítico	Alto	Detectivo	Monitoreo continuo mediante plataforma XDR (Extended Detection and Response) o solución de ciberseguridad que analice logs y genere alertas ante accesos no autorizados al servidor de procesamiento de IA.	Medio
	Imágenes faciales capturadas	Perfilamiento	Uso de las imágenes faciales capturadas para analizar o inferir características, comportamientos o patrones de los usuarios sin su consentimiento, con fines distintos al control de acceso.	Confidencialidad	Ausencia de controles sobre el uso de datos y falta de limitación de finalidad que permite el tratamiento de imágenes biométricas para fines no autorizados.	Muy Probable	Crítico	Crítico	Disuasorio	Establecimiento de cláusulas de confidencialidad y sanciones administrativas o contractuales ante el uso indebido de imágenes biométricas.	Alto
	Servidor de almacenamiento	Falla del servidor de almacenamiento que puede provocar pérdida, corrupción o exposición no autorizada de datos biométricos.	Interrupción o mal funcionamiento del servidor de almacenamiento que afecta la disponibilidad e integridad de los datos biométricos, pudiendo ocasionar su pérdida, alteración o acceso no autorizado.	Integridad, Disponibilidad	Falta de redundancia y mecanismos de respaldo, así como configuraciones inadecuadas que incrementan el riesgo de falla o pérdida de información.	Poco Probable	Crítico	Medio	Preventivo	Implementación de redundancia y copias de seguridad periódicas, junto con configuraciones seguras y mantenimiento preventivo del servidor de almacenamiento.	Irrelevante
	Plantillas biométricas (embeddings faciales)	Uso indebido de datos / Espionaje remoto	Captura y registro de datos biométricos del titular (rostro) mediante IA, para enrolarlo en el sistema de identificación.	Confidencialidad	Falta de cifrado fuerte; ausencia de Differential Privacy en entrenamiento; almacenamiento de embeddings sin control de acceso granular.	Muy Probable	Crítico	Crítico	Preventivo	Cifrado de embeddings con clave separada (AES-256 por titular) + Differential Privacy en entrenamiento + Federated Learning + verificación de integridad del dataset (SHA-256) + crypto-shredding + DPIA (RGPD Art. 35) + evaluación bajo ISO/IEC 42001	Medio
Verificación biometrica en el acceso	API de verificación biométrica / servicio de autenticación	Suplantación de identidad / Divulgación de información	Comparación en tiempo real del rostro capturado contra los embeddings registrados, mediante IA de matching, para autenticar o identificar al titular.	Confidencialidad, Integridad	Falta de monitoreo y autenticación fuerte de la API; sin detección de vivacidad (liveness detection); umbral de matching mal calibrado; ausencia de rate-limiting.	Probable	Crítico	Alto	Detectivo	Liveness Detection obligatorio (activo + pasivo) + SIEM con monitoreo de scores anómalos + MFA adicional para operaciones críticas + rate limiting + bloqueo por intentos fallidos + re-entrenamiento periódico anti-spoofing + red team IA + cifrado del score en tránsito	Medio

Figura A2

Probabilidad de la ocurrencia dentro de la matriz de valoración de riesgos.

Probabilidad	Ocurrencia
Inminente	La amenaza se materializa diaramente
Muy Probable	La amenaza se materializa una vez a la semana
Probable	La amenaza se materializa una vez al mes
Poco Probable	La amenaza se materializa una vez al año
Improbable	La amenaza se materializa una vez cada 3 años