Maestría en

Protección de Datos

Trabajo de investigación previo a la obtención del título de Magíster en Protección de Datos

AUTORES:

ALDAS ONOFRE MARTIN ELIAS

ANCHATUÑA CHANGO JORGE RODRIGO

GUAMÁN GUAMÁN MARIA LOURDES

LÓPEZ CÓRDOVA JUAN CARLOS

PARRA ALVAREZ GEOMARA JACQUELINE

TUMIPAMBA CAÑAR JHORSHUA FERNANDO

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 aseguradora"

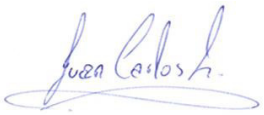
Quito, junio 2026

Certificación de autoría

Nosotros, Aldas Onofre Martin Elias, Anchatuña Chango Jorge Rodrigo, Guamán Guamán María Lourdes, López Córdova Juan Carlos, Parra Álvarez Geomara Jacqueline y Tumipamba Cañar Jhorshua Fernando, 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.

Firma del graduando

GUAMÁN GUAMÁN MARIA LOURDES



Firma del graduando

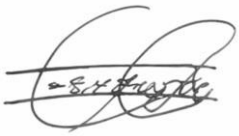
LÓPEZ CÓRDOVA JUAN CARLOS

Firma del graduando

ANCHATUÑA CHANGO JORGE RODRIGO

Firma del graduando

ALDAS ONOFRE MARTIN ELIAS



Firma del graduando

TUMIPAMBA CAÑAR JHORSHUA FERNANDO

Firma del graduando

PARRA ALVAREZ GEOMARA JACQUELINE

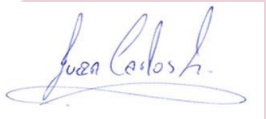
Autorización de Derechos de Propiedad Intelectual

Nosotros, Aldas Onofre Martin Elias, Anchatuña Chango Jorge Rodrigo, Guamán Guamán María Lourdes, López Córdova Juan Carlos, Parra Álvarez Geomara Jacqueline y Tumipamba Cañar Jhorshua Fernando, 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 aseguradora”, 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.

Firma del graduando

GUAMÁN GUAMÁN MARIA LOURDES



Firma del graduando

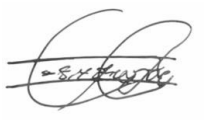
LÓPEZ CÓRDOVA JUAN CARLOS

Firma del graduando

ANCHATUÑA CHANGO JORGE RODRIGO

Firma del graduando

ALDAS ONOFRE MARTIN ELIAS



Firma del graduando

TUMIPAMBA CAÑAR JHORSHUA FERNANDO

Firma del graduando

PARRA ALVAREZ GEOMARA JACQUELINE

Aprobación de dirección y coordinación del programa

Nosotros, **Nombre del Director/a EIG y Jacqueline Guerrero Carrera, Coordinadora UIDE,** declaramos que los graduandos: ALDAS ONOFRE MARTIN ELIAS, ANCHATUÑA CHANGO JORGE RODRIGO, GUAMÁN GUAMÁN MARÍA LOURDES, LÓPEZ CÓRDOVA JUAN CARLOS, PARRA ÁLVAREZ GEOMARA JACQUELINE Y TUMIPAMBA CAÑAR JHORSHUA FERNANDO, 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 Victoria, Camila, David y Sebastián: aprender no tiene fecha de vencimiento. A mis padres, raíz de todo lo que soy. A mis compañeros de trabajo, por hacer más liviano el camino. Y a cada titular de datos que aún no sabe que la ley lo protege: este trabajo existe para que algún día lo sepa, y lo exija.

Jorge Anchatuña

Dedico este trabajo a mi familia, por ser mi mayor inspiración y el motivo para continuar creciendo; a mis amigos, por acompañarme y animarme en los momentos difíciles; y a mis compañeros, con quienes compartí aprendizajes, retos y experiencias durante este camino. A todas las personas que, de una u otra manera, creyeron en mí y aportaron a mi formación, les dedico este logro con mucho cariño.

Martin Aldas

Dedico este logro a mis padres, Juan Carlos y Rosa, por ser mi ejemplo y apoyo constante; a mis hermanos, Madelaine y Declan, por acompañarme y motivarme; a mi novia, Tabatha, por darme ánimo y estar a mi lado en todo momento; y a mi mejor amigo, Martín, por compartir conmigo cada desafío y cada nueva meta.

Fernando Tumipamba

El presente trabajo lo dedico a mi familia, quienes han sido el soporte para culminar esta etapa, a mi esposo, que siempre ha estado alentándome para no decaer; a mis hijos Samantha, Mathias y Emily, quienes son mi inspiración y motivación. A mi madre por siempre darme la mano en los momentos que más la necesito. Este logro es de quienes me rodean, porque su presencia en mi vida me inspira a ser mejor cada día.

María Guamán

El presente trabajo está dedicado, ante todo, a Dios, quien me otorgó la sabiduría, la fortaleza y la perseverancia para culminar este proceso. A mis padres, por su amor incondicional, su sacrificio y el apoyo brindado en cada etapa de mi formación. A mis hermanos, por su compañía y aliento constante a lo largo de este camino.

Juan Carlos López

Dedico este trabajo a mi esposo David y a mi hija Paula, quienes han sido mi refugio, inspiración y apoyo incondicional a lo largo de este camino académico y profesional. Con su amor, paciencia y fortaleza me han impulsado a superar cada desafío y alcanzar esta meta. Que este trabajo refleje mi compromiso como abogada con la construcción de una sociedad más justa, ética y respetuosa de la privacidad y los derechos fundamentales.

Jacqueline Parra Alvarez.

AGRADECIMIENTOS

A Dios, primero y siempre. A Fénix Corp, a mis socios y compañeros de Arest Consulting, gracias por el apoyo que hizo posible este esfuerzo. A mis tutores y a la primera promoción de la Maestría en Protección de Datos Personales, por el privilegio de aprender juntos. Este logro lleva la huella de cada uno de ustedes.

Jorge Anchatuña

Agradezco profundamente a mis padres, Mauricio y Sylvia, por su esfuerzo, ejemplo y apoyo constante; a mi hermano Mateo, por motivarme a seguir creciendo a pesar del cansancio y las dificultades; y a Daniela, por escucharme, acompañarme y confiar en mí durante todo este proceso. Gracias por ser parte fundamental de este logro.

Martin Aldas

Agradezco profundamente a mis padres, Juan Carlos y Rosa, por su esfuerzo, confianza y apoyo incondicional; a mis hermanos, Madelaine y Declan, por su compañía y motivación; a mi novia, por su paciencia, comprensión y palabras de aliento; y a mi mejor amigo, Martín, por acompañarme siempre y avanzar conmigo hacia nuevas metas. Gracias por ser parte fundamental de este logro.

Fernando Tumipamba

En primer lugar, agradezco a Dios por permitirme haber llegado hasta esta etapa, por demostrarme que no existen barreras para aprender y crecer personal y profesionalmente. En segundo lugar, agradezco a mi familia por ser el pilar fundamental y creer en mí. En tercer y último lugar, agradezco a los docentes y compañeros, quienes con su experiencia y aportes han consolidado un conocimiento amplio en lo que es la protección de datos.

María Guaman

Expreso mi más sincero agradecimiento a Dios, por guiarme y sostenerme a lo largo de esta investigación. A mis padres, cuyo esfuerzo y dedicación han sido el pilar fundamental de mi crecimiento personal y profesional. A mis hermanos, por su apoyo incondicional y por acompañarme en cada momento de este proceso académico.

Juan Carlos López

Agradezco profundamente a la Universidad Internacional del Ecuador (UIDE), mi casa de estudios y desarrollo profesional durante más de diez años, por brindarme las herramientas para crecer académica y personalmente. Mi gratitud a sus autoridades, docentes y jefes por su confianza y apoyo constante. A mi familia, especialmente a David y Paula, por acompañarme en este camino. Este logro también les pertenece.

Jacqueline Parra Alvarez.

RESUMEN

El presente trabajo de titulación analiza la aplicación del principio de privacidad desde el diseño y por defecto en el uso de datos biométricos dentro del sector asegurador en Ecuador. El problema central identificado radica en que las aseguradoras, al incorporar tecnologías biométricas apoyadas en inteligencia artificial como el reconocimiento facial y dactilar para el control de acceso de sus empleados, frecuentemente lo hacen sin evaluar los riesgos que ello supone para los derechos fundamentales de los titulares, y sin cumplir plenamente con las exigencias de la Ley Orgánica de Protección de Datos Personales (LOPDP), vigente en el país desde 2021.

El objetivo general del estudio es proponer un marco de gobernanza integral que permita a una aseguradora implementar sistemas biométricos de forma ética, proporcional y conforme a derecho, incorporando los principios de privacidad desde el diseño y por defecto como eje transversal del tratamiento. Para ello, se plantean objetivos específicos que incluyen: identificar las bases de legitimación aplicables al contexto laboral, evaluar los riesgos del tratamiento biométrico potenciado por inteligencia artificial, diseñar mecanismos de gobernanza alineados con la LOPDP y estándares internacionales, y formular recomendaciones técnicas y jurídicas para una implementación responsable.

Metodológicamente, el trabajo adopta un enfoque cualitativo con perspectiva jurídico-analítica. Se realiza un análisis normativo de la LOPDP y su Reglamento General, complementado con el estudio de estándares internacionales como ISO/IEC 27701, el NIST Privacy Framework y las directrices del Comité Europeo de Protección de Datos (CEPD). La investigación se articula a través de un caso práctico ficticio que simula la implementación de un sistema biométrico con inteligencia artificial en una aseguradora ecuatoriana, lo que permite aterrizar el análisis teórico en un escenario organizacional concreto y reproducible.

Los principales hallazgos evidencian que los datos biométricos, por su carácter sensible e irrevocable, exigen condiciones más estrictas que los datos personales ordinarios. Se constata que el consentimiento, en relaciones laborales marcadas por la subordinación, no puede considerarse libremente otorgado, lo que obliga a la aseguradora a explorar bases alternativas de legitimación y a garantizar opciones equivalentes no biométricas. Asimismo, se identificaron riesgos críticos asociados a la desviación de la finalidad, el sesgo algorítmico y la falta de control sobre los encargados del tratamiento. Frente a ello, el trabajo diseñó herramientas prácticas de gobernanza: un registro de actividades de tratamiento, una matriz RACI, avisos de privacidad, cláusulas contractuales con proveedores tecnológicos, una matriz integrada de riesgos y un plan de respuesta a incidentes de seguridad.

Se concluye que la privacidad desde el diseño y por defecto no es una mera aspiración voluntaria, sino una obligación jurídica exigible en Ecuador. Su aplicación al uso de biometría en el sector asegurador requiere que la protección de datos se integre desde la concepción del sistema, priorizando arquitecturas descentralizadas, minimización de datos, transformación criptográfica irreversible de las plantillas biométricas y supervisión humana de las decisiones automatizadas. La investigación demuestra que es posible armonizar innovación tecnológica y protección de derechos fundamentales, siempre que la gobernanza de datos sea proactiva, documentada y centrada en el titular.

Palabras clave: biometría, privacidad, LOPDP, inteligencia artificial, tratamiento.

ABSTRACT

This thesis examines the application of the Privacy by Design and by Default principle to the use of biometric data in Ecuador's insurance sector. The central problem identified is that insurance companies, when adopting biometric technologies powered by artificial intelligence such as facial and fingerprint recognition for employee access control, frequently do so without rigorously assessing the risks these technologies pose to data subjects' fundamental rights, and without fully complying with the requirements of the Organic Law on Personal Data Protection (LOPDP), in force in the country since 2021.

The general objective of the study is to propose a comprehensive governance framework that enables an insurance company to implement biometric systems in an ethical, proportionate, and legally compliant manner, embedding the Privacy by Design and by Default principles as a transversal axis of data processing. To this end, specific objectives are established, including: identifying the lawful bases applicable to the employment context, assessing the risks of biometric processing enhanced by artificial intelligence, designing governance mechanisms aligned with the LOPDP and international standards, and formulating technical and legal recommendations for responsible implementation.

Methodologically, the study adopts a qualitative approach with a legal-analytical perspective. A normative analysis of the LOPDP and its General Regulation is conducted, complemented by the examination of international standards such as ISO/IEC 27701, the NIST Privacy Framework, and the guidelines of the European Data Protection Board (EDPB). The research is structured around a fictional case study that simulates the deployment of an AI-powered biometric system in an Ecuadorian insurance company, allowing the theoretical analysis to be grounded in a concrete and reproducible organizational scenario.

The main findings demonstrate that biometric data, given its sensitive and irrevocable nature, demands stricter conditions than ordinary personal data. It is established that consent, in employment relationships characterized by subordination, cannot be considered freely given, which requires the insurance company to explore alternative lawful bases and to guarantee equivalent non-biometric options. Critical risks were also identified in relation to purpose limitation creep, algorithmic bias, and insufficient control over data processors. In response, the study designed practical governance tools: a record of processing activities, a RACI matrix, privacy notices, contractual clauses with technology providers, an integrated risk matrix, and a personal data breach response plan.

It is concluded that Privacy by Design and by Default is not merely a voluntary best practice, but a legally enforceable obligation in Ecuador. Its application to the use of biometrics in the insurance sector requires that data protection be integrated from the very conception of the system, prioritizing decentralized architectures, data minimization, irreversible cryptographic transformation of biometric templates, and meaningful human oversight of automated decisions. The research demonstrates that technological innovation and the protection of fundamental rights can be reconciled, provided that data governance is proactive, well documented, and centered on the rights of the data subject.

Keywords: biometrics, privacy, LOPDP, artificial intelligence, data processing.

TABLA DE CONTENIDOS

LISTA DE TABLAS

CAPITULO I

1. INTRODUCCION

El avance tecnológico ha hecho que las industrias busquen mejorar sus procesos y así ser más competitivos en el mercado, sin embargo, este configura a que un activo muy preciado como los datos personales se vean cada vez más involucrados dentro del giro del negocio, por lo que, es indispensable observar y aplicar los principios y obligaciones que emana la normativa en protección de datos, su reglamento y normativa conexa.

En el presente trabajo de investigación se aborda el análisis de la implementación de un sistema biométrico y potenciado con Inteligencia Artificial para el control de accesos a los empleados de una aseguradora ubicada en Ecuador, cuyo proveedor externo seria Biotrust.

En el ámbito laboral ecuatoriano, se ha vuelto habitual el uso de tecnologías que recolecten datos biométricos, como huellas dactilares o reconocimiento facial para el control de asistencia y seguridad, sin embargo, esta aplicación desmedida a ocasionado que se generan preocupaciones legales y éticas en torno a la protección de los derechos fundaméntales de los trabajadores, específicamente el derecho a la privacidad y autodeterminación informativa.

En Ecuador, la Constitución de la Republica de 2008 en su artículo 66, numeral 16, reconoce como derecho fundamental a la protección de datos personales, otorgando al titular la facultad de conocer, actualizar, rectificar y decidir sobre su información, quienes la tratan y para que finalidad. La Ley Orgánica de Protección de Datos Personales, expedido en el año 2021, refuerza esta garantía y desarrolla los principios, obligaciones, derechos y sanciones derivadas del tratamiento de datos personales. Con respecto a los datos biométricos, la normativa los cataloga como sensibles, siendo asi que su tratamiento se encuentra

prohibido, salvo que se cuente siempre con el consentimiento del titular, o en los casos que la ley lo habilite, observando los principios de legitimidad, proporcionalidad y finalidad.

La Superintendencia de Protección de Datos Personales, entidad encargada de regular, auditar y supervisar el tratamiento de datos personales en los ámbitos públicos y privados, en base a una consulta realizada se ha pronunciado indicando que, el consentimiento para el uso de sistemas biométricos en el control de asistencia laboral debe cumplir con los criterios de ser libre, específico, informado e inequívoco. Sin embargo, en el contexto laboral, y a su criterio, la relación de subordinación entre empleador y trabajador puede generar presiones implícitas que invalidan el consentimiento, ya que su negativa podría acarrear consecuencias negativas en su estabilidad laboral. En este sentido, la SPDP considera que el consentimiento en estas circunstancias no puede considerarse plenamente válido, ya que el trabajador se encuentra en una posición de vulnerabilidad.

En base a este preámbulo, la investigación se centra en cuatro capítulos: El primer capítulo aborda el planteamiento del problema, los objetivos generales y específicos, su justificación y fundamentación teórica. El segundo capítulo abarca el marco legal aplicable, las políticas internas y externas, matriz de roles y responsabilidades. El tercer capítulo contempla el análisis de riesgos en torno al uso de datos biométricos e IA y la propuesta del plan de respuesta ante incidentes de seguridad. Finalmente, en el capítulo cuarto se realiza el análisis de ponderación de derechos de protección de datos personales y otros derechos fundamentales, así como, el impacto a la privacidad y la viabilidad jurídica de su implementación.

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.

La aseguradora recolecta biometría de empleados: aquí se suma el riesgo de “función secundaria” (usarlo para productividad, control horario o vigilancia), lo cual ampliaría la finalidad y puede ser incompatible si no se justifica.

A nivel operacional, BioTrust debe decidir el modelo de tratamiento: ¿centraliza plantillas biométricas para todos los clientes o permite almacenamiento local por cliente? Centralizar

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

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

2.1.2 Delimitación del problema

El problema de investigación se basa en el análisis jurídico y normativo, centrado en el ámbito de protección de datos personales frente a la implementación de sistemas biométricos potenciados con inteligencia artificial para el control horario de trabajadores en una entidad aseguradora ubicada en Ecuador, con el riesgo de uso de datos para fines secundarios. Con respecto a la delimitación temporal, el estudio abarca el periodo comprendido desde la plena vigencia y exigibilidad de la Ley Orgánica de Protección de Datos Personales en el año 2023 hasta mayo de 2026. Finalmente, en cuanto a la delimitación espacial, la investigación se circunscribe al territorio ecuatoriano, considerando

la normativa vigente aplicable, incluyendo la Constitución de la República del Ecuador, LOPDP y su reglamento, normativa sectorial y directrices emitidas por la Autoridad de Control.

2.2. Justificación

La presente investigación está enfocada en la necesidad de analizar críticamente la implementación de tecnologías biométricas e inteligencia artificial en entornos laborales, donde convergen altos niveles de riesgo para la privacidad, la seguridad de la información y los derechos fundamentales de los trabajadores.

Con respecto al ámbito jurídico, se evalúa la base legitimadora del consentimiento del titular para el tratamiento de datos biométricos y los principios de la LOPDP como proporcionalidad, minimización, licitud, transparencia, ya que este se consideraría invalido debido a la asimetría de poder. El bagaje de fuentes jurídicas coincide en que "el consentimiento en relaciones de dependencia está "contaminado" por el riesgo de represalias o pérdida de oportunidades laborales" (Holland y Tham, 2022).

En el ámbito tecnológico, se evalúa la seguridad de la información, permitiendo integrar marcos internacionales como ISO/IEC 27001, 27005 y 27701, promoviendo un enfoque basado en riesgos que articule la protección de datos personales con la gestión de seguridad de la información. Finalmente, la investigación tiene relevancia social, ya que busca garantizar la protección de los derechos fundamentales de los trabajadores frente al uso potencialmente invasivo de tecnologías biométricas e inteligencia artificial, promoviendo un equilibrio adecuado entre innovación tecnológica y respeto a la dignidad humana.

2.3. Problemas jurídicos

¿Es jurídicamente viable la implementación de un sistema de biometría en la aseguradora, 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 aseguradora 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 jjurídica y la conveniencia del uso de sistemas de biometría en la aseguradora, a la luz de la normativa y principios de protección de datos personales, a fin e formular una conclusión jurídica fundamentada sobre la viabilidad, no viabilidad o viabilidad condicionada y elaborar recomendaciones conforme al principio de privacidad desde el diseño y por defecto, incluso para el supuesto de que la organización decida avanzar pese a un resultado negativo de la EIPD.

2.4.2 Objetivos específicos

- Evaluar el marco normativo aplicable al tratamiento de datos biométricos mediante sistemas de biometría, identificando las bases jurídicas que podrían legitimar su uso por parte de la aseguradora, considerando tanto la legislación general de protección de datos como la normativa sectorial correspondiente.
- Identificar la naturaleza de los datos biométricos como datos personales sensibles o de categoría especial, y determinar las implicaciones jurídicas derivadas de su tratamiento en un modelo multidentidad, especialmente en cuanto a restricciones, garantías reforzadas y deberes del responsable.

- Establecer las implicaciones jurídicas del uso de inteligencia artificial en sistemas de biometría, en particular en relación con riesgos de sesgo algorítmico, errores de identificación, discriminación indirecta y transparencia del tratamiento.
- Identificar y ponderar los posibles impactos del uso de biometría en los derechos fundamentales de los titulares de los datos, incluyendo el derecho a la privacidad, la protección de datos personales, la no discriminación y la autodeterminación informativa.

3. FUNDAMENTOS TEÓRICOS

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

El vertiginoso avance de la sociedad digital ha masificado la recopilación, el almacenamiento y el procesamiento de información personal, impactando de forma directa en la esfera íntima de los individuos, al tratar datos personales de manera indiscriminada, sin control alguno.

En este contexto, según Mendoza (2024) el derecho a la protección de datos personales se ha consolidado como un derecho humano autónomo, estrechamente vinculado a la evolución de los derechos a la intimidad y a la privacidad.

Frente a esta realidad, en el ámbito internacional se han adoptado diversos instrumentos jurídicos que sirven como parámetros de referencia para los ordenamientos locales. Entre estos instrumentos destaca el Reglamento General de Protección de Datos de la Unión Europea (RGPD), aplicable desde 2018, el cual introdujo un marco riguroso de obligaciones para responsables y encargados del tratamiento, dotándolos además de un alcance extraterritorial en supuestos específicos. El RGPD reconoce principios rectores fundamentales como la licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva. Asimismo, fortalece el control de los titulares sobre su información

mediante el reconocimiento de los derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad. En este mismo escenario, existen marcos de cooperación internacional como el Convenio 108+ del Consejo de Europa, orientados a garantizar la protección efectiva de las personas y a viabilizar flujos transfronterizos seguros de información.

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

Ecuador enfrenta grandes desafíos en la privacidad y protección de datos personales, a pesar de los esfuerzos realizados por la autoridad de control, aún hay cierta recesión en cuanto al cumplimiento de la normativa e ir más allá de lo que indica la norma. Se han identificado ciertos factores estructurales que aún deben fortalecerse tales como: Cultura y educación; existe una baja conciencia de las personas en cuanto a su información y lo que se comparte, desconocen de la normativa en protección de datos y los derechos que les asiste como titulares. Por parte de las organizaciones, falta capacitación en programas de protección de datos y cumplir con la ley de manera proactiva, lo que provoca que se incrementen los riesgos y negligencia para el tratamiento que realicen.

En cuanto a los desafíos institucionales y de supervisión, si bien es cierto, Ecuador cuenta con una autoridad de control, esta tiene limitaciones presupuestarias y de personal, que impide realizar sus actividades de manera óptima como auditorias, inspecciones y gestión de procesos sancionatorios. Por otro lado, las organizaciones poseen infraestructuras tecnológicas débiles lo cual impide salvaguardar la información, provocando vulneraciones de seguridad.

Con respecto a los desafíos tecnológicos y de ciberseguridad; el avance de la tecnología como la inteligencia artificial implica graves riesgos para los titulares, ya que al entrenarlos puede haber sesgos u opacidad en el sistema, donde la falta de supervisión humana podría generar discriminación a los ciudadanos. En cuanto a la ciberseguridad, en los últimos

tiempos se ha evidenciado un aumento en los ataques a bases de datos de instituciones públicas y privadas, como filtración de datos incluyendo datos biométricos, poniendo de manifiesto el riesgo para la libertad y derechos de los titulares.

Finalmente, los desafíos legales y regulatorios: La sociedad digital encamina al desarrollo del país, sin embargo, plantea riesgos legales y éticos en el tratamiento de datos personales, por lo que es necesario que las organizaciones acaten las regulaciones que se expidan en torno a la privacidad y protección de datos personales. Finalmente, es necesario que el Ecuador se alinee con estándares internacionales para facilitar el flujo transfronterizo de datos de forma segura, mejorando la competitividad en el mercado digital.

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

La constante evolución tecnológica ha transformado radicalmente la forma en que se recopila y procesa la información, generando un impacto directo sobre los derechos fundamentales de las personas. En este contexto, “la IA, con su capacidad para emular procesos de razonamiento humano, y el big data, con su enfoque en la gestión de grandes volúmenes de datos, han demostrado ser una combinación poderosa que mejora la eficiencia y competitividad en múltiples sectores (Gandomi & Haider, 2021).

Este fenómeno plantea un desafío estructural para los principios clásicos de la protección de datos establecidos en el artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021), especialmente los relativos a la finalidad, pertinencia y minimización de datos, proporcionalidad y conservación. Dado que los sistemas de IA requieren con frecuencia grandes volúmenes de información para su funcionamiento y procesamiento, el tratamiento de datos puede exceder los propósitos originalmente declarados.

En el marco normativo ecuatoriano, la LOPDP reconoce expresamente los retos que imponen estas tecnologías. El artículo 20 consagra el derecho del titular a no ser objeto de

decisiones basadas única o parcialmente en valoraciones automatizadas que produzcan efectos jurídicos o le afecten de manera significativa. Al perfilar a los titulares de datos, la IA puede generar sesgos algorítmicos que deriven en discriminación sistémica; por ello, la legislación exige que las organizaciones garanticen la transparencia algorítmica, entendida como la obligación de permitir al titular conocer la lógica aplicada en el tratamiento y de solicitar la intervención humana cuando una decisión automatizada incida sobre sus derechos. Esta exigencia conecta directamente con el principio de lealtad y transparencia del artículo 10, literales b) y c) de la ley referida, en el cual se indica que el tratamiento sea leal y que toda información relativa a este sea fácilmente accesible y comprensible para el titular.

Para cumplir con la norma, el papel de la IA en el tratamiento de datos personales debe estar supeditado al principio de responsabilidad proactiva, que obliga al responsable del tratamiento a demostrar de manera continua el cumplimiento de las disposiciones legales. Esto implica que el uso de tecnologías disruptivas no exime de la obligación de garantizar la licitud en cada fase del tratamiento. En consecuencia, resulta imperativa la ejecución de Evaluaciones de Impacto en la Protección de Datos (EIPD), reguladas en el artículo 42 de la LOPDP, previas a la implementación de cualquier sistema de IA, con el fin de identificar y mitigar los riesgos de vulneración a la privacidad antes de que el sistema entre en funcionamiento productivo.

3.4. Biometría: aproximación conceptual y jurídica

La biometría se define como el conjunto de técnicas automatizadas orientadas al reconocimiento de individuos a partir de sus características físicas, fisiológicas o conductuales. Desde una perspectiva conceptual, dichas características permiten la identificación unívoca de una persona natural, convirtiendo al cuerpo humano en un identificador inherente e intransferible (Agencia Española de Protección de Datos [AEPD], 2020). En la actualidad, las tecnologías biométricas se han masificado, empleándose tanto

en dispositivos de uso personal como en sistemas corporativos de seguridad y control de acceso, lo que genera un impacto significativo sobre la privacidad de los ciudadanos y exige un marco jurídico robusto que regule su tratamiento (AEPD, 2023).

Desde la perspectiva jurídica ecuatoriana, el artículo 4 de la LOPDP define expresamente al dato biométrico como dato personal único relativo a características físicas, fisiológicas o conductuales que permiten la identificación única del titular; y el artículo 25 los clasifica como categorías especiales de datos personales.

Esta categorización reconoce que su tratamiento indebido puede originar riesgos graves para los derechos y libertades fundamentales del titular. En consecuencia, el ordenamiento jurídico impone una protección reforzada que se traduce en tres mandatos concretos: (i) prohibición del tratamiento como regla general; (ii) excepciones taxativas previstas en el artículo 26 de la LOPDP; y (iii) obligación de realizar una EIPD previa, conforme al artículo 42 de la misma ley. A nivel reglamentario, el Decreto Ejecutivo 684 de 2021, que aprueba el Reglamento a la LOPDP, desarrolla estas exigencias y refuerza las obligaciones del responsable del tratamiento en relación con los datos sensibles.

Esta aproximación jurídica exige que cualquier entidad que pretenda implementar sistemas biométricos se someta a un escrutinio riguroso de proporcionalidad. La recolección de datos biométricos no puede justificarse por mera conveniencia administrativa o eficiencia operativa; debe superar un estricto test tripartito de idoneidad, necesidad y proporcionalidad en sentido estricto, garantizando que no existan medios menos lesivos para la intimidad del titular que permitan alcanzar la misma finalidad legítima perseguida (Comité Europeo de Protección de Datos [CEPD], 2022). La Autoridad de Protección de Datos Personales (APDP), creada por la LOPDP, tiene plena competencia sancionatoria para fiscalizar el cumplimiento de estas exigencias e imponer las medidas correctivas que correspondan.

3.4.1. Sistemas biométricos y datos biométricos

Un sistema biométrico es una arquitectura tecnológica diseñada para capturar, extraer, almacenar y comparar datos biométricos con el fin de identificar o autenticar a un individuo; cada una de estas fases constituye un tratamiento autónomo sujeto a las disposiciones del artículo 4 de la LOPDP. El dato biométrico posee cuatro características esenciales que lo distinguen de cualquier otro tipo de información personal: universalidad (toda persona lo posee), unicidad (es irrepetible en cada individuo), permanencia (se mantiene estable a lo largo del tiempo) y mensurabilidad (puede ser capturado y procesado cuantitativamente mediante sistemas automatizados) (Kindt, 2013). Existen dos grandes categorías: la biometría fisiológica, que analiza rasgos anatómicos como la huella dactilar, el reconocimiento facial o el escáner de iris; y la biometría conductual, que analiza patrones de comportamiento, como la dinámica de tecleo o la firma grafométrica (AEPD, 2020).

La característica más crítica del dato biométrico desde la perspectiva jurídica es su irrevocabilidad y permanencia. A diferencia de una contraseña alfanumérica que, en caso de vulneración, puede ser reemplazada de forma inmediata por el usuario, un dato biométrico comprometido queda expuesto de por vida (Kindt, 2013). Esta inmutabilidad determina que la filtración de una base de datos biométrica genere un daño irreversible para el titular, imposibilitando cualquier forma de restitución de su seguridad y exponiéndolo a vulnerabilidades perpetuas en todos los sistemas que utilicen dicha característica biométrica. Desde el marco de la LOPDP, este riesgo refuerza la exigencia de aplicar el principio de pertinencia y minimización de datos personales consagrado en el artículo 10, literal e), que dispone que los datos deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento.

Los riesgos jurídicos específicos de la biometría son excepcionalmente elevados e incluyen tres amenazas principales. En primer lugar, la suplantación de identidad profunda mediante técnicas de inteligencia artificial generativa (deepfakes), que permiten falsificar rasgos

biométricos con creciente fidelidad. En segundo lugar, el riesgo de vigilancia masiva no autorizada, habilitada por la capacidad de los sistemas biométricos para identificar individuos en espacios públicos de forma subrepticia. En tercer lugar, el riesgo de función ampliada o function creep, que ocurre cuando datos recolectados para un fin legítimo inicial como el control de acceso físico en una empresa son posteriormente empleados para finalidades distintas y no autorizadas, como la evaluación del rendimiento laboral o la inferencia del estado de salud del trabajador, vulnerando el principio de limitación de la finalidad consagrado en la LOPDP (CEPD, 2022).

3.4.2. Tratamiento de datos biométricos

Las bases de legitimación para el tratamiento de datos biométricos en Ecuador están estrictamente limitadas en razón de su naturaleza de datos sensibles. El artículo 26 de la LOPDP establece que dicho tratamiento está prohibido por regla general, salvo que se configure alguna de las excepciones taxativas previstas: la protección de intereses vitales del titular cuando este se encuentre física o jurídicamente imposibilitado de otorgar su consentimiento; el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito laboral, siempre que una disposición legal lo exija o lo autorice expresamente; o la existencia de razones de interés público esencial. La excepción laboral merece especial atención: su aplicación requiere que una norma legal específica imponga o autorice el uso de biometría, no siendo suficiente la mera conveniencia organizacional del empleador ni la práctica generalizada en el sector.

Dentro de estas bases de legitimación, el consentimiento adquiere una relevancia particularmente reforzada. Para que sea válido, el artículo 8 de la LOPDP exige que sea libre, específico, informado, inequívoco y, al tratarse de datos sensibles, explícito mediante una acción afirmativa clara del titular. No se admiten consentimientos tácitos, casillas premarcadas ni fórmulas genéricas incorporadas en contratos de adhesión. Adicionalmente, el responsable del tratamiento asume la carga probatoria de demostrar que el titular

comprendió cabalmente la naturaleza de la información que entregó, los riesgos específicos asociados a su irrevocabilidad y los plazos de conservación aplicables. Este estándar probatorio estricto conecta directamente con el principio de responsabilidad proactiva y demostrada del artículo 10, literal k), de la LOPDP, que obliga al responsable a acreditar haber implementado mecanismos para la protección de datos personales.

Sin embargo, fundamentar el tratamiento biométrico exclusivamente en el consentimiento presenta riesgos jurídicos severos en relaciones asimétricas, como el ámbito laboral, donde la libertad del empleado puede verse viciada por la posición de subordinación frente al empleador (AEPD, 2023). La doctrina especializada y las autoridades de control consideran que, en estos contextos, el consentimiento raramente puede ser calificado de libre. Por ello, incluso cuando se obtenga consentimiento explícito, se exige que el responsable del tratamiento ofrezca alternativas no biométricas equivalentes como tarjetas de proximidad o claves alfanuméricas que no penalicen, estigmaticen ni condicionen al titular que decida no otorgar su autorización biométrica (CEPD, 2022). Esta exigencia de alternativas se fundamenta, además, en el principio de pertinencia y minimización del artículo 10, literal e), de la LOPDP, que impone seleccionar siempre el medio menos intrusivo para alcanzar la finalidad legítima perseguida.

3.5. Privacidad desde el diseño y por defecto

La privacidad desde el diseño y por defecto es un principio rector consagrado en el artículo 39 de la LOPDP, que define la protección de datos desde el diseño como el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, los riesgos para los derechos de los titulares, implementando las medidas técnicas, organizativas y de cualquier otra índole necesarias. Este principio tiene sus fundamentos teóricos en los siete principios fundacionales formulados por Cavoukian (2009), entre los cuales destacan Privacy Embedded into Design que postula que la privacidad debe ser parte integral de la arquitectura del sistema, no un complemento

opcional y Full Functionality que rechaza las soluciones de suma cero y exige que privacidad y funcionalidad coexistan sin sacrificio de ninguna. Aplicados a la biometría, estos principios se materializan en la obligación de realizar una EIPD antes de implementar cualquier sistema biométrico, conforme al artículo 42 de la LOPDP, con el fin de identificar riesgos y diseñar salvaguardas desde el origen.

El enfoque preventivo en el tratamiento de datos biométricos exige privilegiar arquitecturas tecnológicas descentralizadas. La medida más efectiva consiste en almacenar la plantilla biométrica exclusivamente en el dispositivo del propio usuario como el enclave seguro de un teléfono móvil o una tarjeta inteligente en lugar de crear bases de datos centralizadas, las cuales se convierten en objetivos de alto valor para ciberataques y en fuentes de riesgo sistémico para los titulares (AEPD, 2020). Esta opción arquitectónica no solo reduce la superficie de ataque, sino que también refuerza el control del titular sobre su propia información, en línea con los derechos de acceso, rectificación y supresión reconocidos en la LOPDP. Desde el punto de vista de la configuración por defecto, el sistema debe establecer el nivel más restrictivo posible de acceso y tratamiento sin necesidad de acción del titular, garantizando la minimización de los datos tratados en cada interacción.

Las medidas técnicas y organizativas deben ser robustas, proporcionales al nivel de riesgo del tratamiento y revisadas periódicamente atendiendo al estado de la técnica, conforme lo exige el artículo 37 de la LOPDP, que impone a los responsables implementar medidas de seguridad aceptadas por el estado de la técnica, sean organizativas, técnicas o de cualquier otra índole. En el plano técnico, se requiere la transformación del dato biométrico en un código matemático irreversible mediante funciones hash criptográficas, de modo que sea imposible reconstruir el rasgo biométrico original a partir del valor almacenado, complementado con técnicas de cifrado fuerte y protocolos de pseudonimización (Agencia de la Unión Europea para la Ciberseguridad [ENISA], 2021). En el plano organizativo, son exigibles políticas estrictas de control de acceso basadas en el principio de mínimo privilegio, auditorías periódicas de los sistemas y planes formales de respuesta ante incidentes de

seguridad. En suma, la privacidad desde el diseño no constituye una opción voluntaria de buenas prácticas, sino una obligación jurídica exigible bajo la LOPDP: el artículo 47, numeral 9, establece expresamente entre las obligaciones del responsable del tratamiento la de implementar la protección de datos personales desde el diseño y por defecto, cuyo incumplimiento puede acarrear la intervención correctiva y sancionatoria de la Autoridad de Protección de Datos Personales.

CAPITULO II

4. Evaluación normativa

La promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Registro Oficial Suplemento 459 el 26 de mayo de 2021, junto con su Reglamento General expedido en noviembre de 2023, consagró en el ordenamiento jurídico ecuatoriano las reglas punitivas, preventivas y de control sobre el flujo de activos de información. De conformidad con el artículo 1 de la LOPDP, el objeto y finalidad de la ley es garantizar el derecho a la protección de datos personales, lo cual incluye el acceso y decisión sobre información de este carácter.

En el ecosistema de una empresa aseguradora, que realiza un tratamiento masivo y continuo de información sensible, la normativa impone obligaciones de cumplimiento proactivo. De manera particular, el artículo 26 de la LOPDP categoriza explícitamente a los datos biométricos como datos sensibles, definiéndolos como aquellos que se refieren a características físicas, fisiológicas o conductuales de una persona natural que permiten su identificación única. Debido a esta naturaleza irreversible y de alto riesgo, el tratamiento de datos biométricos mediante sistemas de inteligencia artificial queda condicionado al cumplimiento riguroso de las bases de licitud y los principios del régimen normativo ecuatoriano.

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

Para que el procesamiento de datos en el territorio nacional posea validez jurídica, el responsable debe estructurar sus operaciones sobre las bases de legitimación descritas en la ley. De acuerdo con el artículo 7 de la LOPDP, el tratamiento será legítimo únicamente si se cumple con alguna de las condiciones tasadas en la norma, tales como el cumplimiento de una obligación legal, la ejecución de medidas contractuales o el consentimiento del titular.

En el escenario propuesto por la aseguradora para el control de sus trabajadores, el análisis formal encuentra un obstáculo crítico en el artículo 8 de la LOPDP, el cual determina los requisitos esenciales para la validez del consentimiento. La ley señala expresamente que la manifestación de la voluntad del titular debe ser libre, específica, informada e inequívoca. En el contexto laboral, la relación de subordinación intrínseca fractura la condición de "consentimiento libre". Debido a la asimetría de poder, el empleado carece de una libertad real de elección si la alternativa de no entregar su huella o rostro conlleva repercusiones implícitas sobre la estabilidad de su puesto de trabajo.

Por consiguiente, todo diseño tecnológico implementado en la aseguradora debe subordinarse formalmente a los principios rectores consagrados en el artículo 10 de la LOPDP. Para la integración de la biometría, los siguientes principios actúan como requisitos formales obligatorios e insustituibles:

- Finalidad (Art. 10, literal b): Establece que los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados de manera incompatible con dichos fines. En el caso analizado, si la plantilla biométrica se captura para el control de acceso a áreas críticas, la aseguradora tiene prohibido redirigir de forma secundaria dichos datos para la vigilancia de la productividad laboral o la monitorización algorítmica conductual sin una base legal independiente.
- Proporcionalidad (Art. 10, literal c): Dictamina que el tratamiento debe ser adecuado, pertinente y limitado a lo estrictamente necesario en relación con las finalidades para las que son tratados. La aseguradora está obligada a documentar de manera formal que el uso de biometría e inteligencia artificial es la medida idónea y que no existen mecanismos alternativos tradicionales (como tarjetas de proximidad o contraseñas) menos intrusivos para los derechos del titular que alcancen el mismo nivel de seguridad.
- Confidencialidad y Seguridad (Art. 10, literales g e i): El tratamiento de datos debe

realizarse garantizando una seguridad adecuada mediante la aplicación de medidas técnicas y organizativas. Al tratarse de datos sensibles del artículo 26, el umbral técnico de protección debe incorporar cifrado de vectores criptográficos y la imposibilidad de reconstrucción de la imagen original desde la base de datos de almacenamiento.

- Transparencia y Lealtad (Art. 10, literal e): En concordancia con el artículo 12 (Derecho a la información), obliga al responsable a comunicar de forma clara y accesible al titular sobre los fines del tratamiento, la existencia de decisiones automatizadas (si el sistema de IA aprueba o deniega accesos sin intervención humana) y el periodo de retención de la información.

El cumplimiento formal se complementa de forma obligatoria con las garantías para la atención de los derechos contenidos en el Capítulo III de la norma. La aseguradora, en su calidad de Responsable del Tratamiento, debe desplegar canales simplificados para que los titulares puedan ejercer eficazmente sus derechos ARCO+: Acceso (Art. 13), Rectificación y actualización (Art. 14), Eliminación (Art. 15), Oposición (Art. 16), y en especial, el derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas (Art. 18), lo cual restringe el uso de algoritmos de inteligencia artificial para auditar o sancionar al personal sin una supervisión humana significativa.

5. La necesidad de un inventario de datos

Dentro del marco del principio de responsabilidad demostrada (*accountability*), la implementación de un sistema de gestión de privacidad es inviable si la organización no conoce con precisión qué datos posee, dónde residen, quién accede a ellos y cómo fluyen a lo largo de su ciclo de vida. Es aquí donde radica la necesidad imperativa de diseñar y mantener actualizado un Inventario de Datos, formalizado jurídicamente bajo la figura obligatoria del Registro de Tratamientos, estipulado en el artículo 42 de la LOPDP. Aunque la ley no impone un formato informático rígido, la norma determina que este registro debe

mantenerse permanentemente actualizado a disposición de la Autoridad de Protección de Datos Personales. En sintonía con estándares internacionales como la norma ISO/IEC 27701 y el *NIST Privacy Framework*, este inventario constituye la columna vertebral técnica del cumplimiento.

El Inventario de Datos actúa como una radiografía operativa que permite a la aseguradora mapear el flujo del dato desde su captura inicial hasta su eliminación definitiva. Para el caso de los sistemas biométricos, el inventario no se limita a registrar de manera general la existencia de "datos de empleados", sino que debe desglosarse de forma granular de acuerdo con las exigencias del artículo 42. Debe especificar que se recolectan imágenes faciales o de huellas dactilares, detallar que dichas imágenes pasan por un proceso de vectorización matemática para generar una plantilla biométrica (la cual constituye el dato sensible real según el artículo 26), y precisar con exactitud la ubicación física y lógica de los servidores locales o infraestructuras en la nube donde se almacenan, identificando además las categorías de destinatarios a quienes se pretende comunicar dichos datos.

La utilidad práctica del inventario de datos abarca tres dimensiones críticas:

- Identificación de Riesgos y Puntos de Fuga: Permite mapear de forma exacta las interfaces donde los datos biométricos entran en contacto con sistemas de terceros o proveedores de servicios de inteligencia artificial.
- Garantía de Derechos ARCO+: Si un trabajador o cliente solicita la supresión de sus datos de conformidad con el artículo 15 de la LOPDP, la aseguradora solo podrá garantizar este derecho de manera efectiva si el Registro de Tratamientos detalla con precisión cada base de datos y sistema donde la plantilla biométrica ha sido replicada o indexada.
- Sustento ante Auditorías de la Autoridad de Control: El inventario constituye la primera prueba documental que exigirá la Superintendencia para verificar que la organización comprende, identifica y gobierna sus activos de información bajo un

enfoque de Privacidad desde el Diseño.

6. Gobernanza de la protección de datos personales

La gobernanza de la protección de datos personales es el marco estructural, organizativo y operativo mediante el cual una institución define sus políticas, asigna responsabilidades claras y establece los mecanismos de control necesarios para garantizar el cumplimiento normativo a largo plazo. No se trata de un esfuerzo aislado del departamento legal o del área de ciberseguridad, sino de una estrategia corporativa transversal coordinada por la alta gerencia.

En el ecosistema de una aseguradora, y en estricto cumplimiento del artículo 48 de la LOPDP que vuelve obligatoria esta figura para entidades que traten datos sensibles de forma masiva, esta gobernanza se materializa mediante la designación formal de un Delegado de Protección de Datos (DPD). Las funciones de este oficial, alineadas detalladamente al artículo 49 de la norma, incluyen informar y asesorar al responsable, supervisar el cumplimiento de la ley y de las políticas internas, y actuar como el nexo y punto de contacto exclusivo con la Autoridad de Protección de Datos Personales.

La gobernanza efectiva asegura que la privacidad sea integrada de forma nativa (Privacy by Design) en cada nuevo producto, servicio o despliegue tecnológico, mitigando los riesgos reputacionales y financieros derivados del severo régimen sancionatorio de la ley.

6.1. Políticas, instrucciones de trabajo y flujogramas

En el desarrollo del análisis en cuanto a la implementación de sistemas biométricos con inteligencia artificial, se han generado políticas y flujogramas que permiten cumplir con el deber de informar, demostrar responsabilidad proactiva y una adecuada gobernanza en protección de datos, los cuales han sido considerados como anexos en el presente trabajo de investigación.

6.2. Matriz RACI

	DPO	SGSI	TI	Negocio	TH	Usuarios
Actualizar RAT	Aprobador / Autoridad	Responsable	Responsable	Consultado	Responsable	Informado
Evaluación de Impacto	Aprobador / Autoridad	Responsable	Consultado	Consultado	Consultado	Informado
Derechos Titulares	Aprobador / Autoridad	Consultado	Consultado	Informado	Responsable	Responsable
Gestión de Incidentes	Consultado	Aprobador / Autoridad	Responsable	Informado	Informado	Informado
Cláusulas Contractuales	Aprobador / Autoridad	Consultado	Informado	Consultado	Informado	Informado

Tabla 1: Matriz RACI.

La presente matriz RACI refleja un esquema de gobernanza estructurado para el tratamiento de datos biométricos dentro de la aseguradora, alineado con los principios de la LOPDP, su reglamento y estándares internacionales como ISO/IEC 27701, bajo un enfoque de responsabilidad proactiva.

En este contexto, se evidencia que el delegado de Protección de Datos (DPO) asume un rol transversal como Aprobador/Autoridad en las actividades críticas del tratamiento, lo cual garantiza la supervisión independiente, la validación normativa y el cumplimiento de las obligaciones legales, especialmente en procesos de alto riesgo como la Evaluación de Impacto (DPIA) y la gestión del Registro de Actividades de Tratamiento (RAT).

Por su parte, el área de Seguridad de la Información (SGSI) se posiciona como un actor clave en la ejecución operativa de controles, asumiendo principalmente el rol de responsable, particularmente en la gestión de riesgos, incidentes de seguridad y apoyo en evaluaciones de impacto. Esto responde a la necesidad de implementar medidas técnicas y organizativas robustas frente a la naturaleza sensible de los datos biométricos.

El área de Tecnologías de la Información (TI) complementa esta gestión desde una perspectiva técnica, siendo responsable de la implementación, mantenimiento e integración

de las soluciones biométricas, así como del soporte en la gestión de incidentes y controles de acceso.

Las Áreas de Negocio y Talento Humano (TH) cumplen un rol fundamental en la definición de finalidades y uso legítimo de los datos, siendo especialmente relevante la participación de Talento Humano como responsable en la gestión de derechos de los titulares, considerando la relación directa con los empleados y el contexto laboral del tratamiento.

Finalmente, los Usuarios (empleados) son reconocidos como titulares de los datos personales, con un rol activo en el ejercicio de sus derechos, lo cual fortalece el principio de autodeterminación informativa.

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

El derecho a la información es el pilar de la transparencia proactiva en el ordenamiento jurídico ecuatoriano. El artículo 12 de la LOPDP consagra el Derecho a la información, determinando que el responsable debe comunicar al titular, de manera clara, accesible y en lenguaje sencillo, todos los aspectos del tratamiento antes de recopilar sus datos.

En una aseguradora que implementa biometría apoyada por Inteligencia Artificial, el cumplimiento de este derecho se vuelve estricto debido a que se procesan datos sensibles (Art. 26). Por ello, el Aviso de Privacidad específico para este sistema debe contener puntualmente los siguientes requisitos exigidos por el artículo 12:

Identidad del Responsable: Datos de la aseguradora y de su Delegado de Protección de Datos (Art. 48).

Finalidad Limitada: Declarar el fin exacto (ej. control de acceso físico a áreas críticas), blindando a la empresa contra la desviación de finalidad (Art. 10, literal b).

Tiempo de Conservación: El plazo de retención y los criterios para la eliminación segura de los vectores biométricos.

Decisiones Automatizadas: Informar si el sistema de IA toma decisiones autónomas de acceso y explicar la lógica algorítmica aplicada (Art. 18).

Canales ARCO+: Los medios gratuitos para que el personal pueda ejercer sus derechos de acceso, rectificación, eliminación u oposición (Capítulo III).

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

El tratamiento de datos dentro de una aseguradora raramente ocurre de manera aislada; comúnmente involucra la participación de proveedores externos de software, infraestructura en la nube (SaaS/PaaS) o consultoras de desarrollo de modelos de inteligencia artificial. En la terminología de la LOPDP, es fundamental distinguir y regular contractualmente las relaciones entre el Responsable del Tratamiento (la aseguradora, quien decide sobre los fines y medios del tratamiento) y el Encargado del Tratamiento (el proveedor tecnológico que procesa los datos por cuenta y orden de la aseguradora), figuras definidas formalmente en el artículo 4 de la ley.

El artículo 43 de la LOPDP determina que toda relación entre un responsable y un encargado debe estar estrictamente instrumentada a través de un contrato escrito o acto jurídico que vincule a ambas partes. Este instrumento jurídico debe contener cláusulas contractuales obligatorias y sumamente rigurosas, entre las cuales destacan:

1. Limitación de Objeto e Instrucciones: Con base en el artículo 43, el encargado se compromete por contrato a tratar los datos biométricos únicamente siguiendo las instrucciones explícitas del responsable, quedándole estrictamente prohibido utilizar dicha información para fines propios, comercialización, mejoras autónomas de sus algoritmos de IA o transferencias a terceros no autorizados.
2. Deber de Confidencialidad y Seguridad: Adoptar las medidas de seguridad técnicas

y organizativas necesarias para garantizar la integridad, confidencialidad y disponibilidad de los datos sensibles de conformidad con el artículo 38 y artículo 10, literal g de la LOPDP, aplicando estándares avanzados (como el cifrado robusto de vectores) alineados a la norma ISO/IEC 27701.

3. Subcontratación Regulada: El proveedor no puede delegar o subcontratar la ejecución de los servicios que impliquen el tratamiento de las plantillas biométricas a un sub-encargado sin la autorización previa, expresa y por escrito de la aseguradora, tal como lo dispone el marco regulatorio del artículo 43.
4. Auditoría y Cooperación: Cláusulas que facultan a la aseguradora a realizar auditorías, inspecciones y controles periódicos en los sistemas del proveedor. Adicionalmente, el encargado está obligado a asistir al responsable para que este pueda cumplir con la atención de las solicitudes de derechos ARCO+ (Capítulo III) y en la realización de las Evaluaciones de Impacto (Art. 44).
5. Régimen de Notificación de Brechas de Seguridad: El encargado tiene la obligación contractual y reglamentaria de notificar de forma inmediata al responsable cualquier incidente, filtración o acceso no autorizado a los datos biométricos. Esta celeridad es un requisito indispensable para que la aseguradora pueda cumplir con el artículo 41 de la LOPDP, el cual impone la obligación legal de notificar la vulneración a la Autoridad de Protección de Datos Personales en el término máximo de cinco (5) días desde que tuvo constancia de la misma, bajo riesgo de incurrir en las infracciones graves tipificadas en la ley.

CAPITULO III

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

El despliegue de tecnologías biométricas potenciadas por sistemas de Inteligencia Artificial (IA) dentro del entorno laboral de la aseguradora, introduce riesgos extraordinarios para los derechos y libertades fundamentales de los titulares. Al amparo de la Ley Orgánica de Protección de Datos Personales (LOPDP), los datos biométricos guardan la naturaleza jurídica de datos sensibles (Art. 4 LOPDP), cuya explotación automatizada se encuentra proscrita por regla general, salvo las excepciones taxativas del Art. 14 del mismo cuerpo legal.

Por consiguiente, determinar el "nivel mínimo aceptable" para este tratamiento no puede limitarse a un mero ejercicio de cumplimiento de control técnico (listas de verificación); exige la estructuración de un modelo de gobernanza holístico sustentado en el principio de responsabilidad proactiva y demostrada (Art. 11 LOPDP), la arquitectura de *Cero Confianza* (*Zero Trust*) y las directrices de la Superintendencia de Protección de Datos Personales (SPDP) plasmadas en su *Guía de Protección de Datos desde el Diseño y por Defecto (2025)*.

En el contexto específico de una relación de subordinación laboral, la asimetría de poder inherente entre el empleador y el trabajador despoja al consentimiento de sus características de libertad e idoneidad como base legitimadora (Art. 8 LOPDP). Bajo esta premisa, el nivel mínimo aceptable requiere la coexistencia obligatoria de los siguientes pilares técnico-jurídicos:

- **Mitigación Absoluta de la Desviación de Finalidad (*Function Creep*):** La recolección de vectores y plantillas biométricas faciales con el propósito declarado de garantizar la seguridad física y el control de accesos a áreas restringidas no puede, bajo ninguna circunstancia estratégica o comercial, mutar hacia fines secundarios de

monitoreo de productividad, análisis conductual o control disciplinario. Esto vulneraría flagrantemente los principios de lealtad, proporcionalidad y limitación de la finalidad (**Art. 11 LOPDP**). El nivel mínimo aceptable exige el aislamiento lógico y operativo de los logs de acceso respecto a los sistemas de gestión de talento humano.

- **Gobernanza Algorítmica y Mitigación del Sesgo (Cumplimiento del Art. 20 LOPDP):** El motor de IA provisto por el encargado (*BioTrust*) para los procesos de autenticación (identificación 1:1 o verificación 1:N) y detección de vida (*liveness detection*) no puede operar como una "caja negra". La aseguradora, en su rol de Responsable del Tratamiento, debe exigir auditorías algorítmicas periódicas al proveedor que certifiquen tasas simétricas de *Falso Rechazo* (FRR) y *Falsa Aceptación* (FAR) entre diferentes grupos demográficos (género, edad y etnicidad), mitigando riesgos de discriminación algorítmica. Asimismo, queda prohibida la adopción de bloqueos físicos o suspensiones laborales automatizadas; todo resultado negativo arrojado por la IA debe contar con una intervención humana significativa antes de surtir efectos jurídicos o materiales perjudiciales para el empleado, salvaguardando el derecho a la impugnación y explicación consagrado en el Art. 20 de la LOPDP.

- **Operacionalización de la Privacidad desde el Diseño y por Defecto (*DevPrivOps / DevSecOps*):** En alineación con la metodología de la SPDP (2025), la organización debe integrar la protección de datos en el ciclo de vida del desarrollo y despliegue tecnológico. Esto implica:
- **Estrategia de Minimización y Abstracción:** No almacenar imágenes del rostro en alta resolución (*raw data*). El nivel mínimo exige que el hardware capture la información, la transforme inmediatamente en un vector matemático unidireccional (plantilla biométrica criptográfica) y destruya la imagen origen.

- **Seguridad por Defecto (DevSecOps):** Implementación de cifrado de extremo a extremo (AES-256) tanto en tránsito como en reposo, almacenamiento de claves

criptográficas en módulos de seguridad de hardware (HSM) independientes y la ejecución de evaluaciones de seguridad estáticas (SAST) y dinámicas (DAST) sobre las APIs que conectan la infraestructura híbrida de la aseguradora con la nube de *BioTrust*.

Garantía de Alternativas Equivalentes No Invasivas (*Fallback*): El nivel mínimo de ética y responsabilidad proactiva impone que la biometría no sea un mecanismo obligatorio de acceso generalizado. La aseguradora debe proveer sistemas alternativos equivalentes y sin penalización (como tarjetas de proximidad inteligentes o tokens criptográficos) para aquellos trabajadores que decidan ejercer su derecho de oposición al tratamiento de sus datos sensibles o cuyas condiciones físicas impidan un correcto enrolamiento biométrico

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

Para la estructuración de la matriz de riesgos del proyecto, se adopta un enfoque multidimensional alineado con la *Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales* de la SPDP (2025) y los estándares internacionales ISO/IEC 27701 y el NIST Privacy Framework. A diferencia de los análisis de riesgos de seguridad tradicionales enfocados en los activos de la empresa, esta matriz prioriza el riesgo sobre los derechos y libertades de los titulares.

La escala cualitativa de valoración integrada (Probabilidad x Impacto) define cuatro niveles de riesgo residual: Bajo, Medio, Alto y Crítico.

ID	Activo de Información / Derecho del Titular	Amenaza Identificada	Vulnerabilidad Técnica / Organizacional	Probabilidad	Impacto	Riesgo Inherente	Medidas de Mitigación y Controles de Gobernanza (DevRiskOps)	Riesgo Residual
R-01	Vectores biométricos / Derechos de Autodeterminación e Indemnidad.	Desviación de la finalidad (*Function Creep*): Explotación de datos de acceso para control disciplinario y analítica laboral conductual.	Inexistencia de políticas corporativas segregadas; falta de control de accesos basado en roles (RBAC) entre sistemas de TI y Talento Humano.	Alta	Alto	Crítico	Aplicación de tácticas *DevPrivOps* (Separar y Abstraer). Implementación de auditorías de logs inmutables. Firma de addendums contractuales laborales que prohíban el uso disciplinario de la biometría.	Bajo
R-02	Base de datos centralizada de plantillas / Confidencialidad e Integridad.	Filtración o exfiltración de bases de datos por ataques dirigidos o privilegios mal administrados en la nube híbrida.	Almacenamiento centralizado en servidores del encargado (*BioTrust*) sin hashing unidireccional ni cifrado a nivel de aplicación (*Application-Layer Encryption*).	Media	Muy Alto	Crítico	Tokenización de los vectores biométricos. Cifrado homomórfico o transformación simétrica reversible controlada exclusivamente por la aseguradora (claves del responsable). Despliegue de un SIEM/XDR para correlación de anomalías en tiempo real.	Medio

R-03	Identidad digital del empleado / Derecho a la Igualdad y No Discriminación.	Sesgo algorítmico y exclusión: Falsos rechazos reiterados que impiden el acceso a trabajadores debido a factores demográficos o envejecimiento.	Uso de un modelo de aprendizaje profundo (*Deep Learning*) en la IA entrenado con datasets extranjeros no representativos de la diversidad fenotípica ecuatoriana.	Alta	Alto	Alto	Exigencia contractual a *BioTrust* de la entrega de hojas de datos de equidad (*Datasheets for Datasets*). Monitoreo continuo del *drift* (degradación) del modelo de IA. Establecimiento de umbrales (*thresholds*) dinámicos adaptados al entorno local.	Bajo
R-04	Acceso físico seguro / Derecho al Trabajo y Dignidad Laboral.	Decisiones 100% automatizadas: Bloqueo automatizado del ingreso físico al edificio ante fallos del sistema o falsos rechazos, provocando indefensión.	Configuración de los torniquetes físicos y sistemas de seguridad supeditados exclusivamente a la respuesta binaria de la API de la IA, sin modo de bypass.	Media	Alto	Alto	Despliegue obligatorio de un canal de *fallback* físico y manual controlado por guardias de seguridad humana. Integración de alertas SOC que notifiquen tasas de rechazo inusuales en un mismo nodo de acceso para triaje técnico inmediato.	Bajo
R-05	Flujos transfronterizos / Principio de Información y Responsabilidad.	Pérdida de la cadena de custodia del dato debido a transferencias no autorizadas a subencargados en terceros países sin nivel adecuado de protección.	Cláusulas contractuales genéricas e insuficientes con el proveedor de nube híbrida; ausencia de procesos de debida diligencia de software (*Software*	Media	Medio	Medio	Inclusión obligatoria de Cláusulas Contractuales Tipo (SCC) homologadas por la SPDP. Prohibición expresa de subcontratación en jurisdicciones que no garanticen estándares equivalentes a la LOPDP. Auditorías periódicas basadas en ISO/IEC 27001/27701 al encargado.	Bajo

			Supply Chain Security).					

Tabla 2: Matriz de Riesgos

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

Como parte fundamental del sistema de gobernanza y del principio de responsabilidad proactiva de la aseguradora, se ha diseñado un Plan de Respuesta a Incidentes enfocado de forma especializada en eventos que comprometan datos biométricos. La justificación de un protocolo reforzado radica en la naturaleza sensible e irreversible de la biometría; a diferencia de una credencial alfanumérica, el compromiso de una plantilla facial o dactilar expone al titular a un riesgo perpetuo de suplantación de identidad y discriminación.

El plan adopta un enfoque técnico-jurídico basado en los estándares internacionales NIST SP 800-61 e ISO/IEC 27701, estructurando las acciones organizacionales en fases secuenciales que van desde la detección automatizada en el SOC hasta la remediación post-incidente. Desde la perspectiva normativa, el diseño del plan está estrictamente supeditado al cumplimiento del artículo 41 de la Ley Orgánica de Protección de Datos Personales (LOPDP), el cual impone la obligación perentoria de notificar cualquier brecha de seguridad a la Autoridad de Control en un término máximo de cinco (5) días desde que se tenga constancia de su ocurrencia.

El plan de respuesta ante incidentes de seguridad se encuentra como anexo 4 del presente trabajo de investigación.

CAPITULO IV

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

10.1. Paso 1. Identificación del conflicto jurídico concreto

El caso plantea un conflicto jurídico entre el derecho fundamental a la protección de datos personales y el derecho a la intimidad de los trabajadores, frente al interés del empleador en garantizar la seguridad y el control de accesos en el entorno laboral, derivado de la implementación de un sistema de biometría multidentidad potenciado con IA, con riesgos de funciones secundarias como vigilancia excesiva, evaluación de productividad y control horario.

10.2. Paso 2. Identificación y delimitación de los derechos involucrados

Se identifican como derechos afectados el derecho a la protección de datos personales y el derecho a la intimidad de los trabajadores, debido al uso de datos biométricos mediante sistemas con inteligencia artificial. La Constitución de la República del Ecuador 2008 reconoce el derecho a la protección de datos personales y a la intimidad (art. 66, nums. 19 y 20), mientras que la Ley Orgánica de Protección de Datos Personales (LOPDP) clasifica los datos biométricos como categorías especiales de datos personales (art. 25).

El interés involucrado corresponde a la necesidad del empleador de fortalecer la seguridad física de las instalaciones, prevenir accesos no autorizados, evitar suplantaciones de identidad y proteger áreas críticas mediante mecanismos de autenticación reforzada. Los titulares de los datos son los trabajadores de la aseguradora que serán parte del sistema biométrico, quienes presentan una situación de vulnerabilidad relativa debido a la relación laboral con el empleador.

10.3. Paso 3. Determinación de la intensidad de la afectación

La afectación conjunta a los derechos fundamentales a la protección de datos personales y a la intimidad, reconocidos en el artículo 66, numerales 19 y 20 de la Constitución de la República del Ecuador, es ALTA, fundamentada en los siguientes factores:

Naturaleza e irreversibilidad: Los datos biométricos son considerados categorías especiales de datos personales, conforme al artículo 25 de la Ley Orgánica de Protección de Datos Personales (LOPDP). Al tratarse de rasgos físicos permanentes e insustituibles, cualquier brecha de seguridad, acceso no autorizado o exfiltración de información podría ocasionar un daño irreversible al titular, quien no puede modificar sus características biométricas como sí ocurre con una contraseña o credencial tradicional.

Afectación a la intimidad y riesgo de vigilancia: El uso de sistemas biométricos con inteligencia artificial permite identificar de manera unívoca a los trabajadores y generar registros continuos sobre su ingreso, permanencia y circulación dentro de las instalaciones. Aunque la finalidad declarada sea la seguridad, existe el riesgo de que la información sea utilizada para fines secundarios, como vigilancia excesiva, monitoreo de conductas o evaluación de productividad, afectando la esfera privada y la expectativa razonable de intimidad de los trabajadores, artículo 66, numeral 20, de la Constitución de la República del Ecuador.

Escala y gobernanza de IA: La integración de motores de aprendizaje profundo para verificación continua y detección de vida incrementa el alcance del tratamiento y el riesgo de desviación de la finalidad originalmente prevista. Los registros podrían ser utilizados para finalidades incompatibles con aquellas para las que fueron recolectados, vulnerando los principios de finalidad y minimización previstos en el artículo 10 de la Ley Orgánica de Protección de Datos Personales (LOPDP)

Asimetría laboral y automatización: La relación de subordinación existente entre empleador y trabajador limita la libertad real para aceptar el tratamiento de datos biométricos. Asimismo, el uso de decisiones automatizadas puede generar errores de identificación o falsos rechazos que afecten derechos de los trabajadores, incluyendo su acceso al lugar de trabajo y el ejercicio de sus actividades laborales.

Frente a esta severa restricción de derechos, el grado de satisfacción del interés contrapuesto seguridad corporativa, prevención de accesos no autorizados y protección de áreas críticas es medio. Si bien la biometría puede resultar eficaz para reforzar la seguridad en determinados espacios, su utilización generalizada para el control ordinario de asistencia resulta excesiva, especialmente cuando existen alternativas menos intrusivas, tales como tarjetas de proximidad, credenciales electrónicas o tokens de autenticación.

10.4. Paso 4. Aplicación del test de proporcionalidad

a) Idoneidad

¿El uso de biometría es capaz de alcanzar la finalidad perseguida?

El sistema biométrico resulta idóneo en la medida en que contribuye a prevenir accesos no autorizados, reducir riesgos de suplantación de identidad, fortalecer la seguridad de áreas críticas y garantizar que únicamente personas autorizadas ingresen a determinados espacios. Adicionalmente, la detección de vida, las funcionalidades antifraude y el matching biométrico permiten incrementar la confiabilidad de los mecanismos de autenticación utilizados por la organización (ENISA, 2021).

b) Necesidad

¿Existen medidas alternativas menos intrusivas que permitan alcanzar la misma finalidad?

Se constata que existen medios alternativos menos intrusivos e igualmente aptos para alcanzar la finalidad perseguida, tales como tarjetas de proximidad, credenciales electrónicas, tokens físicos o digitales y sistemas de control de acceso con validación humana. Estas alternativas generan una menor afectación al derecho a la protección de datos personales y a la intimidad de los trabajadores, por lo que la utilización de biometría para fines ordinarios de control laboral no supera plenamente el juicio de necesidad (CEPD, 2022).

c) Proporcionalidad en sentido estricto

¿El beneficio obtenido compensa la intensidad de la afectación al derecho fundamental?

El grado de satisfacción del interés perseguido no compensa la elevada afectación a los derechos a la protección de datos personales y a la intimidad de los trabajadores, especialmente considerando que la biometría implica el tratamiento de datos sensibles y que su aplicación en contextos de uso generalizado genera riesgos relevantes para la privacidad. En consecuencia, su implementación indiscriminada resulta desproporcionada y únicamente podría considerarse admisible de forma condicionada, bajo restricciones estrictas de finalidad, minimización, alternativas no biométricas y controles reforzados (CEPD, 2022).

10.5. Paso 5. Conclusión ponderativa

En consecuencia, en el contexto del uso generalizado de biometría con inteligencia artificial en el entorno laboral, la ponderación realizada permite concluir que los derechos a la protección de datos personales y a la intimidad de los trabajadores prevalecen frente al interés empresarial de seguridad, debido a la alta intensidad de la afectación y a la existencia de medidas alternativas menos intrusivas que permiten alcanzar la finalidad perseguida. No obstante, el tratamiento podría resultar constitucional y legalmente

admisible de forma excepcional cuando se limite a áreas críticas de alta seguridad y se implementen garantías reforzadas de protección de datos, supervisión humana y mecanismos alternativos de acceso (Constitución de la República del Ecuador, art. 66, nums. 19 y 20; Ley Orgánica de Protección de Datos Personales, arts. 10, 25, y 42; CEPD, 2022).

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

11.1. Descripción sintética del tratamiento

El tratamiento consiste en la recopilación y utilización de datos biométricos de los trabajadores de la aseguradora, mediante huella dactilar y reconocimiento facial, con la finalidad exclusiva de verificar su identidad y controlar el acceso a áreas críticas o restringidas.

El sistema utiliza un mecanismo de verificación biométrica uno a uno (1:1), apoyado en inteligencia artificial, aprendizaje automático y detección de prueba de vida para prevenir suplantaciones. La aseguradora actúa como responsable del tratamiento y BioTrust como encargado tecnológico de la solución, sin perjuicio de la posible intervención de proveedores de nube o subencargados.

El sistema no podrá utilizarse para el control general de asistencia, medición de productividad, vigilancia permanente, análisis de conducta o aplicación de medidas disciplinarias. Cualquier modificación de la finalidad requerirá un nuevo análisis de necesidad y proporcionalidad, así como la actualización de la presente EIPD, de conformidad con los principios de finalidad y minimización previstos en el artículo 10 de la Ley Orgánica de Protección de Datos Personales (LOPDP).

11.2. Justificación de la obligatoriedad de la EIPD

La realización de una Evaluación de Impacto en la Protección de Datos (EIPD) es obligatoria debido al alto riesgo que el tratamiento puede representar para los derechos y libertades de los trabajadores, de conformidad con el artículo 42 de la Ley Orgánica de Protección de Datos Personales (LOPDP). Esta necesidad se fundamenta en el uso de datos biométricos para la identificación unívoca de personas; el empleo de inteligencia artificial; la ejecución sistemática del tratamiento dentro de una relación laboral; la naturaleza permanente de las características biométricas; y el desequilibrio existente entre el empleador y el trabajador, que puede afectar la libertad del consentimiento (Comité Europeo de Protección de Datos [CEPD], 2022).

También concurren riesgos de desviación de la finalidad, brechas de seguridad, discriminación algorítmica, decisiones automatizadas y pérdida de control sobre los datos cuando intervienen encargados, subencargados o proveedores internacionales. Estos eventos pueden afectar los derechos a la protección de datos personales, intimidad, privacidad, igualdad, dignidad, trabajo y debido proceso. En consecuencia, el tratamiento se encuentra comprendido en los supuestos del artículo 42 de la Ley Orgánica de Protección de Datos Personales y de los artículos 29 a 31 del Reglamento General a la Ley Orgánica de Protección de Datos Personales.

Como criterio interpretativo, se consideran los Oficios N.os SPDP-IRD-2025-0031-O, SPDP-IRD-2025-0065-O y SPDP-IRD-2025-0108-O de la Superintendencia de Protección de Datos Personales. Aunque estos pronunciamientos analizan principalmente el uso de biometría para el registro de asistencia, resultan aplicables por analogía al establecer la necesidad de realizar un test de proporcionalidad, un análisis de riesgos y una evaluación de impacto, así como de verificar la ausencia de riesgos residuales altos o críticos y la disponibilidad de alternativas menos invasivas para los trabajadores.

11.3. Identificación de riesgos relevantes

R-01. Desviación de la finalidad y vigilancia excesiva

Existe el riesgo de que los datos biométricos o los registros de acceso sean utilizados para control de asistencia, productividad, análisis conductual o medidas disciplinarias. Esta ampliación incompatible de la finalidad podría vulnerar los principios de transparencia, minimización, proporcionalidad y limitación de la finalidad, así como los derechos a la protección de datos personales, intimidad y privacidad. De conformidad con los principios de finalidad y minimización previstos en el artículo 10 de la Ley Orgánica de Protección de Datos Personales (LOPDP) (CEPD, 2022).

R-02. Filtración o exfiltración de plantillas biométricas

El acceso no autorizado, pérdida o filtración de plantillas biométricas puede producir consecuencias graves e irreversibles, debido a que las características biométricas no pueden ser modificadas como una contraseña. Este riesgo afecta la confidencialidad, integridad y seguridad de los datos personales (Kindt, 2013; Ley Orgánica de Protección de Datos Personales, art. 37).

R-03. Sesgo algorítmico, falsos rechazos y discriminación

El sistema puede producir resultados desiguales por factores como edad, características físicas, condiciones médicas, iluminación o calidad de los dispositivos. Los errores reiterados pueden generar discriminación o exclusión injustificada, afectando los derechos a la igualdad, dignidad y trabajo (CEPD, 2022).

R-04. Decisiones automatizadas y bloqueo del acceso

Un falso rechazo o falla técnica puede impedir automáticamente el ingreso de un trabajador sin revisión humana ni mecanismo alternativo. Esto podría causar indefensión

o consecuencias laborales injustificadas y vulnerar los derechos al trabajo, dignidad y debido proceso (Ley Orgánica de Protección de Datos Personales, art. 20; CEPD, 2022).

R-05. Transferencias no autorizadas y pérdida de la cadena de custodia

Existe el riesgo de que BioTrust, sus subencargados o proveedores de nube accedan, transfieran o almacenen datos biométricos sin autorización o garantías adecuadas. Esto puede dificultar el ejercicio de derechos y vulnerar los principios de seguridad, transparencia y responsabilidad proactiva, de conformidad con la Ley Orgánica de Protección de Datos Personales (LOPDP), especialmente los artículos 10 y 37.

La materialización de los riesgos R-01 a R-05 podría producir consecuencias que superan el ámbito tecnológico y afectan directamente los derechos fundamentales de los trabajadores. En particular, podría vulnerar el derecho a la protección de datos personales y el derecho a la intimidad personal y familiar, reconocidos en el artículo 66, numerales 19 y 20, de la Constitución de la República del Ecuador.

11.4. Medidas de mitigación previstas o propuestas

Medidas técnicas: se implementará la separación lógica entre el sistema biométrico y los sistemas de Talento Humano, nómina o productividad; controles de acceso basados en roles; privilegios mínimos; registros de auditoría; cifrado de datos en tránsito y reposo; segregación de bases de datos; gestión segura de claves; eliminación de imágenes originales una vez generada la plantilla; y herramientas de monitoreo para detectar accesos o extracciones anómalas, de conformidad con el artículo 37 de la Ley Orgánica de Protección de Datos Personales (LOPDP).

También se realizarán pruebas periódicas de precisión, falsas aceptaciones, falsos rechazos y posibles sesgos del modelo. Ante fallas o resultados negativos deberá existir intervención humana y un método alternativo de acceso. Ningún rechazo podrá generar automáticamente sanciones o consecuencias laborales, en observancia de la Ley

Orgánica de Protección de Datos Personales y de las directrices del Comité Europeo de Protección de Datos (CEPD, 2022). Asimismo, se mantendrá un inventario de subencargados y controles para impedir transferencias o copias no autorizadas.

Medidas organizativas: se designarán responsables para supervisar el cumplimiento de las obligaciones de protección de datos y seguridad de la información. El personal autorizado recibirá capacitación periódica y accederá únicamente a los datos necesarios para sus funciones.

Se realizarán auditorías sobre los accesos, conservación, eliminación de datos y funcionamiento del modelo de inteligencia artificial. Además, se aplicará un procedimiento de respuesta a incidentes que incluya detección, contención, evaluación, documentación, notificación y remediación.

La EIPD deberá actualizarse cuando cambien la finalidad, la tecnología, el proveedor, la arquitectura, la ubicación de los datos o el nivel de riesgo, de conformidad con el artículo 42 de la Ley Orgánica de Protección de Datos Personales y los artículos 29 a 31 del Reglamento General a la Ley Orgánica de Protección de Datos Personales.

Medidas jurídicas: se adoptará una política específica para el tratamiento de datos biométricos y se informará previamente a los trabajadores sobre la finalidad, base legitimadora, responsable, encargado, plazo de conservación, destinatarios, transferencias, decisiones automatizadas y ejercicio de derechos, de conformidad con el artículo 12 de la Ley Orgánica de Protección de Datos Personales.

Los contratos con BioTrust y otros proveedores deberán regular las medidas de seguridad, confidencialidad, eliminación de datos, atención de derechos, auditorías, incidentes, subencargados y transferencias. Se prohibirá el uso de la biometría para vigilancia permanente, productividad, control disciplinario o decisiones laborales automatizadas, de conformidad con los principios de finalidad, minimización y proporcionalidad previstos en

la Ley Orgánica de Protección de Datos Personales, su Reglamento General y los criterios interpretativos emitidos por la Superintendencia de Protección de Datos Personales.

Cuando se utilice el consentimiento como base legitimadora, este deberá ser libre, específico, informado, inequívoco y demostrable, de conformidad con el artículo 8 de la Ley Orgánica de Protección de Datos Personales (LOPDP). El trabajador deberá disponer de una alternativa no biométrica equivalente, accesible y sin penalizaciones (CEPD, 2022).

11.5. Evaluación del riesgo residual

Una vez aplicadas las medidas propuestas, la matriz del capítulo III determina un riesgo residual bajo para los riesgos R-01, R-03, R-04 y R-05, y medio para el riesgo R-02. Por ello, el riesgo residual global se considera medio, principalmente por el carácter permanente e irreversible de los datos biométricos.

No se identifican riesgos residuales altos o críticos siempre que los controles sean implementados antes del inicio del tratamiento y permanezcan operativos durante todo su ciclo de vida, de conformidad con el artículo 42 de la Ley Orgánica de Protección de Datos Personales y los artículos 29 a 31 del Reglamento General a la Ley Orgánica de Protección de Datos Personales.

12. Conclusión de la DPIA

El tratamiento resulta jurídicamente aceptable únicamente de manera excepcional y condicionada, siempre que se limite al control de acceso a áreas críticas y se demuestre que la finalidad no puede alcanzarse con un nivel equivalente de seguridad mediante mecanismos menos invasivos, de conformidad con la Ley Orgánica de Protección de Datos Personales y las directrices del Comité Europeo de Protección de Datos (CEPD, 2022).

Antes de su implementación, la aseguradora deberá documentar el test de necesidad, idoneidad y proporcionalidad; acreditar una base legitimadora válida; aplicar las medidas correspondientes a los riesgos R-01 a R-05; y verificar que no existan riesgos residuales altos o críticos, de conformidad con el artículo 42 de la Ley Orgánica de Protección de Datos Personales.

El sistema no podrá utilizarse para vigilancia permanente, productividad, control general de asistencia ni consecuencias laborales automatizadas. Todo rechazo deberá ser revisado por una persona y deberá existir un mecanismo alternativo de ingreso. La viabilidad del tratamiento queda condicionada a la supervisión humana, limitación estricta de la finalidad y monitoreo continuo de los riesgos para los derechos a la protección de datos personales, intimidad y privacidad de los trabajadores (CEPD, 2022).

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

13.1. Toma de decisión jurídica

Con base en el análisis normativo, la ponderación de derechos y los resultados de la evaluación de Impacto en Protección de Datos Personales, se concluye que la implementación de un sistema biométrico asistido con Inteligencia Artificial en la institución es jurídicamente viable de manera condicionada.

13.2. Fundamentos de la decisión:

La presente decisión se fundamenta en la Evaluación de Impacto en la Protección de Datos Personales (EIPD), la Ley Orgánica de Protección de Datos Personales, el Reglamento General a la Ley Orgánica de Protección de Datos Personales, la ponderación de derechos realizada y los criterios interpretativos emitidos por la Superintendencia de Protección de Datos Personales (SPDP). El EIPD concluye que el

tratamiento es jurídicamente viable de manera condicionada, restringiendo el uso de la biometría al acceso a zonas críticas por motivos de seguridad. Del ejercicio de ponderación realizado se concluye que el derecho a la protección de datos personales, la intimidad y la autodeterminación informativa de los trabajadores prevalece frente al interés empresarial cuando la biometría se utiliza de manera generalizada para el control de asistencia, debido a la alta intensidad de la afectación y a la existencia de medidas menos intrusivas que permiten alcanzar la misma finalidad. No obstante, el uso de biometría puede resultar admisible de manera excepcional cuando se limite exclusivamente al acceso a zonas críticas de alta seguridad, se encuentre debidamente justificado y se implementen garantías reforzadas de protección de datos y mecanismos alternativos para los trabajadores.

La Superintendencia de Protección de Datos Personales (SPDP) ha establecido que el uso de biometría para el simple registro de asistencia es excesivo e impertinente. Sin embargo, al focalizar el sistema únicamente en áreas de alta seguridad y ofrecer mecanismos alternativos de acceso, se respetan los principios de pertinencia, minimización y limitación de la finalidad, de conformidad con el artículo 10 de la Ley Orgánica de Protección de Datos Personales (LOPDP). Este criterio coincide con el resultado de la ponderación efectuada en el presente trabajo, en la que se determinó que la afectación a los derechos fundamentales de los trabajadores supera el beneficio obtenido cuando la biometría se utiliza para fines ordinarios de control laboral.

- Al preverse métodos alternativos de acceso, se reduce la coacción inherente a la relación laboral y la asimetría de poder que podrían viciar el consentimiento. En tal sentido, el trabajador no sufrirá represalias ni temor a perder su empleo si decide no utilizar el sistema biométrico, evidenciándose así una manifestación de voluntad libre, específica, informada e inequívoca, de conformidad con el artículo 8 de la Ley Orgánica de Protección de Datos Personales (LOPDP).
- Finalmente, la Superintendencia de Protección de Datos Personales (SPDP),

mediante los Oficios N.os SPDP-IRD-2025-0031-O, SPDP-IRD-2025-0065-O y SPDP-IRD-2025-0108-O, ha señalado que quienes utilicen sistemas de inteligencia artificial que impliquen tratamiento de datos personales deben realizar una adecuada gestión de riesgos, garantizar la transparencia y efectuar auditorías periódicas sobre su funcionamiento. En este sentido, al analizar los riesgos, se establece que existe un riesgo residual aceptable, el cual se fortalecerá mediante controles estrictos, supervisión humana y la limitación de las finalidades, evitando que el sistema se desvíe hacia otras funciones como la evaluación de la productividad o la vigilancia sistemática, de conformidad con el artículo 42 de la Ley Orgánica de Protección de Datos Personales y los artículos 29 a 31 del Reglamento General a la Ley Orgánica de Protección de Datos Personales.

13.3. Recomendaciones jurídicas y organizacionales.

Con la finalidad de que la viabilidad condicionada se sostenga, es preciso implementar las siguientes medidas:

- **Reducción del alcance y limitación de finalidades:** La recolección de plantillas biométricas y el uso de la inteligencia artificial debe encontrarse de manera aislada, restringiendo el acceso únicamente al personal autorizado que cumpla funciones relacionadas con la administración del sistema biométrico y la gestión de talento humano, y prohibiendo su utilización para la evaluación de la productividad o la vigilancia excesiva. Su alcance estará limitado exclusivamente a la autenticación para zonas de acceso crítico, de conformidad con el artículo 10 de la Ley Orgánica de Protección de Datos Personales (LOPDP).
- **Alternativas para el control de acceso:** Se debe garantizar en todo momento la voluntariedad real del trabajador, por lo que es necesario proveer mecanismos alternativos como tarjetas de proximidad, credenciales electrónicas o tokens para aquellos trabajadores que no deseen enrolarse en el sistema biométrico, de

conformidad con el artículo 8 de la Ley Orgánica de Protección de Datos Personales (LOPDP).

- **Auditorias periódicas:** Es necesario realizar un monitoreo continuo de los riesgos tecnológicos mediante auditorías técnicas, jurídicas y organizacionales, con la finalidad de mitigar sesgos y riesgos de discriminación, conforme a la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial emitida por la Superintendencia de Protección de Datos Personales.
- **Re-evaluación periódica (re-DPIA):** Se debe mantener un ciclo continuo de revisión de la DPIA. Ante cualquier cambio en la arquitectura del sistema, nuevas zonas físicas de acceso o reformas a la normativa de protección de datos, se debe recalibrar la matriz de riesgos y actualizar los documentos pertinentes, de conformidad con el artículo 42 de la Ley Orgánica de Protección de Datos Personales y los artículos 29 a 31 del Reglamento General a la Ley Orgánica de Protección de Datos Personales.
- **Protección desde el diseño y por defecto:** Mantener sistemas de cifrado sólido de extremo a extremo, garantizar que únicamente se conserven representaciones matemáticas de las plantillas biométricas y establecer políticas de control de acceso basadas en roles, con procesos de auditoría verificables, de conformidad con el artículo 37 de la Ley Orgánica de Protección de Datos Personales (LOPDP).

13.4. Cierre jurídico

El presente dictamen de viabilidad condicionada constituye un pronunciamiento dinámico y estrictamente ligado a los controles técnicos y organizacionales implementados. La licitud del tratamiento de datos personales sensibles mediante inteligencia artificial no es permanente; dependerá del ejercicio continuo del del principio de responsabilidad

proactiva y demostrada (accountability), previsto en la Ley Orgánica de Protección de Datos Personales

Cualquier alteración en el estado de la técnica, el surgimiento de nuevas vulnerabilidades algorítmicas o la emisión de futuras directrices por parte de la Superintendencia de Protección de Datos Personales (SPDP) exigirá la actualización inmediata de la Evaluación de Impacto en la Protección de Datos Personales (EIPD), de conformidad con el artículo 42 de la Ley Orgánica de Protección de Datos Personales y los artículos 29 a 31 del Reglamento General a la Ley Orgánica de Protección de Datos Personales.

Se concluye que el tratamiento analizado no solo puede afectar el derecho a la protección de datos personales, sino también otros derechos fundamentales como la intimidad, la privacidad y la libertad de los trabajadores, reconocidos en el artículo 66, numerales 19 y 20, de la Constitución de la República del Ecuador. No obstante, dichas afectaciones pueden considerarse justificadas y proporcionadas únicamente cuando el tratamiento se limite a finalidades específicas de seguridad, se apliquen medidas de minimización de datos y se garanticen mecanismos alternativos para quienes no deseen utilizar sistemas biométricos, de conformidad con el artículo 10 de la Ley Orgánica de Protección de Datos Personales (LOPDP).

CAPITULO V

14. CONCLUSIONES GENERALES

La presente investigación abordó la tensión entre la eficiencia que ofrecen los sistemas biométricos potenciados con inteligencia artificial y la obligación jurídica de proteger los derechos fundamentales de los trabajadores, reconocidos en el artículo 66, numerales 19 y 20 de la Constitución de la República del Ecuador. A partir del análisis normativo, la ponderación de derechos y la evaluación de impacto realizados, es posible formular respuestas fundadas a los tres problemas jurídicos que estructuraron esta investigación.

Es jurídicamente viable la implementación de un sistema de biometría en la aseguradora, conforme a la normativa de protección de datos personales y a los principios de licitud, necesidad, proporcionalidad y minimización. La investigación concluye que la implementación del sistema biométrico es viable únicamente de manera condicionada. Los datos biométricos, clasificados como categoría especial conforme al artículo 25 de la LOPDP, están sujetos a una prohibición general de tratamiento con excepciones taxativas. En el ámbito laboral, el consentimiento resulta estructuralmente insuficiente como base legitimadora, pues la subordinación entre empleador y trabajador vicia su carácter libre, criterio confirmado por la Superintendencia de Protección de Datos Personales en sus pronunciamientos institucionales. La viabilidad jurídica queda condicionada a que el tratamiento se restrinja al control de acceso en zonas de alta seguridad, supere el test de idoneidad, necesidad y proporcionalidad, y se garanticen alternativas no biométricas reales y sin penalización.

Resulta recomendable el uso de biometría en la aseguradora 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. La investigación concluye que el uso de biometría no es recomendable para finalidades ordinarias de control laboral. La ponderación determinó una afectación de alta intensidad a los derechos fundamentales, debido principalmente al carácter irrevocable del dato biométrico, una plantilla comprometida expone al titular a un riesgo perpetuo que ninguna medida posterior puede remediar íntegramente. La existencia de alternativas equivalentes menos intrusivas desvirtúa además la necesidad de recurrir a datos sensibles para alcanzar la misma finalidad.

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. La EIPD concluye afirmativamente, pero bajo condiciones estrictas. Identificados cinco riesgos a) Desviación de finalidad, b) Filtración de plantillas, c) Sesgo algorítmico, d) Decisiones automatizadas sin supervisión humana, e) Transferencias no autorizadas, el riesgo residual se sitúa en nivel medio una vez aplicadas las medidas de mitigación, sin riesgos altos o críticos, siempre que los controles sean implementados antes del inicio del tratamiento y mantenidos durante todo su ciclo de vida. La privacidad desde el diseño y por defecto, consagrada en el artículo 39 de la LOPDP, no es una aspiración voluntaria; es una obligación jurídica exigible cuyo incumplimiento activa el régimen sancionatorio de la Superintendencia.

15. CONCLUSIONES ESPECÍFICAS

Los cuatro objetivos específicos de la investigación fueron cumplidos integralmente. Se evaluó el marco normativo aplicable y las bases de legitimación disponibles; se identificó la naturaleza jurídica del dato biométrico y sus implicaciones de protección reforzada; se establecieron las consecuencias jurídicas del uso de inteligencia artificial, particularmente en materia de sesgo algorítmico y decisiones automatizadas conforme al artículo 20 de la

LOPDP; y se ponderaron los impactos sobre los derechos fundamentales de los titulares mediante el test de proporcionalidad desarrollado en el Capítulo IV.

A nivel académico, la investigación aporta un modelo de análisis jurídico integrado y replicable, que articula la LOPDP con los estándares ISO/IEC 27701 y el NIST Privacy Framework, y lo traduce en herramientas concretas de gobernanza: registro de actividades de tratamiento, matriz RACI, avisos de privacidad, cláusulas contractuales, matriz de riesgos y plan de respuesta a incidentes. Este aporte llena un vacío identificado en la literatura jurídica ecuatoriana sobre gobernanza operativa en protección de datos.

A nivel personal y profesional, el proceso fortaleció en los autores competencias de análisis jurídico crítico, gestión del riesgo y toma de decisiones en escenarios de alta complejidad técnica y normativa, consolidando su perfil en el ámbito de la privacidad y la gobernanza de datos.

Entre las limitaciones de la investigación se destacan dos aspectos centrales. En primer lugar, el análisis se desarrolló sobre un caso práctico ficticio que, si bien fue diseñado para reflejar fielmente las condiciones del sector asegurador ecuatoriano, no captura la totalidad de variables organizacionales, contractuales y tecnológicas propias de una implementación real. En segundo lugar, la valoración de los riesgos identificados puede variar con el tiempo ante la evolución acelerada de las capacidades de la inteligencia artificial y el perfeccionamiento de las técnicas de ataque cibernético, lo que podría alterar el nivel de riesgo residual estimado en el corto y mediano plazo.

Estas limitaciones, lejos de restar valor a las conclusiones alcanzadas, señalan líneas de investigación futura de considerable relevancia. El ecosistema regulatorio ecuatoriano se encuentra en plena transformación: durante el desarrollo de esta investigación se expidió la Ley de Ciberseguridad, cuya articulación con la LOPDP y su impacto sobre el tratamiento de datos biométricos en entornos laborales constituye un campo de análisis

aún pendiente de desarrollo académico. Asimismo, la consolidación de la Superintendencia de Protección de Datos Personales como autoridad de control activa a través de la emisión de resoluciones, guías interpretativas y el ejercicio efectivo de su potestad sancionatoria redefinirá progresivamente los estándares mínimos exigibles a las organizaciones. Ambos procesos apuntan hacia un escenario en el que la protección de datos dejará de ser percibida como una carga de cumplimiento para convertirse en una condición estructural del ejercicio empresarial responsable, y en el que cada titular podrá ejercer sus derechos con pleno conocimiento y sin temor.

16. Bibliografía

Agencia de la Unión Europea para la Ciberseguridad (ENISA). 2021

Agencia Española de Protección de Datos. (2020). Nota técnica que incluye catorce equívocos relacionados con el uso de la biometría. https://www.aepd.es/media/notas-tecnicas/nota-equivocos-biometria.pdf

Agencia Española de Protección de Datos. (2023). *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*. https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf

Comité Europeo de Protección de Datos [CEPD, 2022).

Constitución de la República del Ecuador. (2008). Registro Oficial No. 449, 20 de octubre de 2008. https://www.asambleanacional.gob.ec/documentos/constitucion_de_bolsillo.pdf

Gandomi, A., & Haider, M. (2021). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 56, 102287.https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face Recognition Vendor Test (FRVT), Part 3: Demographic effects* (NISTIR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales. *2025)*. Resolución No. SPDP-SPD-2025-0003-R, 29 de abril de 2025. Superintendencia de Protección de Datos Personales.

Guía de Protección de Datos desde el Diseño y por Defecto (2025). Resolución No. SPDP-SPD-2025-0040-R, 21 de octubre de 2025. Superintendencia de Protección de Datos Personales.

Holland, P., & Tham, T. L. (2022). Workplace biometrics: Protecting employee privacy one fingerprint at a time. *Economic and Industrial Democracy, 43*(2), 501–515. https://doi.org/10.1177/0143831X20917453

International Organization for Standardization. (2023). *Information technology—Artificial intelligence—Guidance on risk management (ISO/IEC 23894:2023).* https://www.iso.org/standard/77304.html

Ley Orgánica de Protección de Datos Personales. (2021). Quinto Suplemento del Registro Oficial No. 459, 26 de mayo de 2021. https://www.cpccs.gob.ec/wp-content/uploads/2025/07/LEY-ORGANICA-DE-PROTECCION-DE-DATOS.pdf

Mendoza Enríquez, O. A. (2024). Inteligencia artificial y orden internacional: Una mirada desde el derecho a la privacidad y el derecho de protección de datos personales. *Informática y Derecho. Revista Iberoamericana de Derecho Informático (2.ª época), 2*(15), 99–116. https://revistas.fcu.edu.uy/index.php/informaticayderecho/article/view/5085

Norma general para la garantía del derecho de protección de datos personales en el uso de sistemas de inteligencia artificial. (2026). Resolución No. SPDP-SPD-2026-0009-R, 12 de febrero de 2026. Superintendencia de Protección de Datos Personales. https://spdp.gob.ec/resoluciones2/

Reglamento General de la Ley Orgánica de Protección de Datos Personales. (2023). Decreto Ejecutivo No. 904. Suplemento del Registro Oficial No. 435, 13 de noviembre de 2023. https://www.cosede.gob.ec/wp-content/uploads/2023/12/REGLAMENTO-GENERAL-A-LA-LEY-ORG%C3%81NICA-DE-PROTECCION-DE-DATOS-PERSONALES_compressed-1.pdf

17. ANEXOS

Anexo 1, Política de Protección de Datos Personales.

Anexo 2, Aviso interno de privacidad y protección de datos personales.

Anexo 3, Aviso externo de privacidad y protección de datos personales.

Anexo 4, Plan de respuesta ante incidentes de seguridad de datos biométricos e IA.

Anexo 5, Flujograma de atención de derechos ARCO.

Anexo 6, Flujograma de gestión de incidentes en protección de datos personales.

Anexo 7, Flujograma de evaluación de riesgos y DPIA para nuevos proyectos, conforme a los principios de privacidad desde el diseño y por defecto.

Anexo 1. Política de Protección de Datos Personales

Código: PO-SD-DP-01

Versión: 1.0

Clasificación: Interna

Macroproceso: Cumplimiento y Gestión de Riesgos

Proceso: Gestión Normativa de Datos Personales

INDICE

1. OBJETIVO

Establecer los parámetros y lineamientos para el tratamiento adecuado de los datos personales administrados por la Compañía de Seguros, garantizando la confidencialidad, integridad y disponibilidad de la información de asegurados, beneficiarios, corredores, empleados y proveedores.

2. ALCANCE

Desde la obtención o entrega de datos personales por parte del titular, hasta la destrucción o supresión de los datos personales

Aplica a todos los colaboradores del Seguro y proveedores de servicios que traten datos personales, es decir, cualquier acción que implique clasificación, almacenamiento, uso, procesamientos y/o transferencia de datos, entre otros.

3. RESPONSABLES

3.1 Del Cumplimiento

1. Gerencia COE de datos y Analítica

2. Área de Ciberseguridad

3. Área de Servicios Administrativos

4. Área Legal

5. Área infraestructura TI

6. Delegado de Protección de Datos Personales

7. Dueños de Tratamientos de Datos Personales

8. Dueños de Dominios que Gestionan Datos Personales

9. Proveedores de Servicos que traten Datos Personales

10. Empleados de la Aseguradora

- **Gerencia COE de datos y Analítica.**
  Revisar políticas relacionadas con el tratamiento de datos personales y llevar a aprobación del Directorio.
  - **Gerencia de Gobierno y Calidad de Datos Personales**

  Responsable de:

  - Aplicar la metodología para la categorización y evaluación de sensibilidad de los datos personales.

- **Equipo de Protección de Datos Personales**

Responsable de:

- Definir y actualizar las políticas, procesos, procedimientos, metodologías, lineamientos y definiciones relacionadas con el tratamiento de datos personales.
- Definir criterios de asignación de Dueños de Tratamientos de datos personales de la Aseguradora.
- Definir los criterios de asignación de Dueños de Tratamiento de datos personales en la Aseguradora
- Definir los lineamientos para la administración de respuestas a los consentimientos del tratamiento de datos personales por parte de los clientes.
- Definir los lineamientos para la administración de respuestas a los consentimientos del tratamiento de datos personales por parte de los clientes.
- Generar las capacidades que permitan identificar datos personales en los servidores físicos y en la nube de la Aseguradora.

- **Área Ciberseguridad**

Responsable de:

- Establecer los controles de ciberseguridad y seguridad de información que protejan los datos e información creados, procesados y almacenados en la Aseguradora.
- Validar el cumplimiento de los controles mínimos de ciberseguridad y seguridad de información definidos por la Aseguradora.

- **Área de Servicios Administrativos**

Responsable de:

- Validar y actualizar los contratos o acuerdos con proveedores en cumplimiento con la Ley Orgánica de Protección de Datos Personales.
- Validar que en los contratos celebrados con los “Encargados de Tratamiento de Datos Personales” se incorporen los lineamientos legales definidos por la Aseguradora y el “Acuerdo de Encargo para el Manejo de Datos Personales" vigente.

- **Área Legal**

Responsable de:

- Establecer lineamientos legales relativos a protección de datos personales para las relaciones contractuales con clientes, colaboradores, proveedores y otros.
- Informar oportunamente sobre normativa nueva o sus reformas en relación con la legislación en la materia.
- Aprobar el texto y modificaciones al consentimiento de los titulares para el tratamiento de sus datos personales.
- Identificar las bases legales de los tratamientos y tiempos de conservación de los datos personales bajo responsabilidad de la Aseguradora
- Incorporar en las relaciones contractuales con los "Encargados de Tratamiento de Datos Personales el "Acuerdo de Encargo para el Manejo de Datos Personales" vigente

- **Área de Infraestructura TI**

  Responsable de:
  - Canalizar los requerimientos tecnológicos de las diferentes áreas de la Aseguradora relacionados al tratamiento de datos personales.

- **Delegado de Protección de Datos Personales**

  Responsable de:
  - Priorizar las acciones necesarias para dar cumplimiento a la Ley Orgánica de Protección de Datos Personales y demás normativa de la materia
  - Asesorar al responsable y encargado del tratamiento de datos personales, sobre el contenido de las disposiciones legales y reglamentarias aplicables a la materia.
  - Ejercer funciones adicionales establecidas por la Autoridad de Protección de Datos Personales.
  - Actualizar y disponibilizar el inventario de bases de datos, garantizando su pertinencia del dato y considerando la protección de los datos personales con relación a la normativa vigente.

- **Dueños de Tratamientos de Datos Personales**.

  Responsable de:
  - Gestionar con el área de Proceso la actualización o rediseño del flujo del proceso y registrar los cambios en los documentos asociados al mismo.
  - Aprobar la ficha de intervención de procesos por la Ley de Protección de Datos Personales de los procesos a su cargo.

- Implementar las medidas, controles y requerimientos definidos por Ciberseguridad para la protección de datos personales.
- Validar que se cuente con la autorización para el tratamiento de datos personales del titular en los procesos que tengan como base legitimadora el cometimiento.

- **Dueños de Dominios que Gestionan Datos Personales**
  Responsable de:
  - Capturar y gestionar el consentimiento para el tratamiento de datos personales del titular dentro de las fronteras de sus dominios, aplicando los lineamientos y directrices definidos por la Aseguradora.
  - Gestionar los datos personales del titular dentro de las fronteras de sus dominios de acuerdo con la base legitimadora que corresponde a cada tratamiento según la normativa vigente de la Ley de Protección de Datos Personales.

- **Proveedores de servicios que traten datos personales**.
  Responsable de:
  - Custodiar y entregar la información correspondiente al cumplimiento de obligaciones establecidas por la Aseguradora para el ejercicio de sus funciones tratando los datos personales que se encuentran bajo la responsabilidad de la Aseguradora.
  - Cumplir con la normativa vigente relacionada a la protección de datos personales
  - Cumplir con las políticas, procedimientos, estándares y términos contractuales definidos por la Aseguradora, así como las medidas de ciberseguridad y seguridad de información para el tratamiento y protección de datos personales.
- **Empleados de la Aseguradora**
  Responsable de:
  - Conocer y cumplir con las políticas, procesos, procedimientos, metodologías, lineamientos, estándares sobre el tratamiento de datos personales establecidos por la Aseguradora.
  - Realizar anualmente las capacitaciones y actualizaciones que disponga la Aseguradora relacionadas a protección de datos personales.
  - Mantener los datos personales durante el tiempo necesario para cumplir con los fines para los que se recopilaron.
  - Aplicar medidas técnicas y organizativas para dar cumplimiento a la minimización de datos personales.

4. POLÍTICAS

4.1Políticas Generales

Todas la políticas, procesos y procedimientos que la Aseguradora emita referente al tratamiento de datos personales deberán cumplir con la Ley de Protección de Datos Personales y la normativa vigente.

Todos los empleados de la Aseguradora realizarán el tratamiento de datos personales bajo las finalidades y en consideración del marco de bases legitimadoras definidas por el COE de Datos y Analítica.

Las vulneraciones de datos personales deberán notificarse a los titulares de los datos personales y al Organismo Regulador de ser el caso.

El incumplimiento de esta política será sujeto de acuerdo con el Reglamento Interno de Trabajo vigente.

4.2 Políticas Relacionadas

4.2.1 Política de Gobierno de Datos

4.2.2 Política General de Seguridad de la Información y Ciberseguridad

4.2.3 Política de Gestión de Proveedores y Contratos

5. GLOSARIO

Colaboradores: funcionarios de la Aseguradora que acojan esta política, con o sin relación de dependencia laboral, tales como: directores, representantes legales, asesores, funcionarios, apoderados y pasantes.

Datos: Cualquier forma de registro sea este electrónico, óptico, magnético, impreso o en otros medios susceptible de ser capturado, almacenado, procesado y distribuido.

Dato Personal: Es el dato que identifica o hace identificable a una persona natural, directa o indirectamente. Ley Orgánica de Protección de Datos Personales (art.4).

Delegado de protección de datos: Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento

normativo al respecto, y de cooperar con la autoridad de Protección de Datos Personales.

Incidente: Es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de los datos personales en el Banco.

Titular: Persona natural cuyos datos son objeto de tratamiento.

Dueño de tratamiento de datos personales: Colaborador de la Aseguradora que se le haya asignado el rol de Process Responsible.

Encargado del tratamiento de datos personales: Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.

Principios: Los principios que rigen la Ley de Protección de Datos Personales son; Juridicidad, Lealtad, Transparencia, Finalidad, Pertinencia y Minimización de Datos Personales, Proporcionalidad del Tratamiento, Confidencialidad, Calidad y Exactitud, Conservación, Seguridad de Datos Personales, Responsabilidad Proactiva y Demostrada, Aplicación Favorable a Titular, Independencia del Control.

Tratamiento de datos: Cualquier operación o conjunto de operaciones realizada sobre datos, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tal como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso.

ANEXO 2

AVISO INTERNO DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

El presente Aviso Interno de Protección de Datos Personales (en adelante, el "Aviso") establece la forma en que Seguros S.A., sociedad legalmente constituida conforme a las leyes de la República del Ecuador, con domicilio en la ciudad de Quito, provincia de Pichincha, con su matriz ubicada en la Av. 6 de diciembre N15-28 y Portugal, en adelante denominada OCSE S.A, recopila, accede, procesa, almacena, utiliza, protege, comparte y, en general, trata los datos personales proporcionados por sus colaboradores durante la vigencia de la relación laboral y en cualquier actividad que desarrollen para OCSE S.A.

Se recomienda leer atentamente este Aviso, así como sus eventuales modificaciones.

INTRODUCCIÓN

Al incorporarse como colaborador de OCSE S.A, usted entrega a la empresa diversa información personal. Somos conscientes de la responsabilidad que ello implica y adoptamos las medidas necesarias para garantizar la confidencialidad, seguridad y el ejercicio de sus derechos como titular de datos personales.

El presente Aviso tiene por objeto informarle de manera clara y transparente:

- Qué datos personales tratamos
- Con qué finalidad los tratamos
- Con quiénes pueden ser compartidos
- Cuáles son sus derechos y cómo ejercerlos

Todo ello conforme a la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP).

Para cualquier consulta relacionada con este Aviso o con el tratamiento de sus datos personales, puede comunicarse con nuestro Delegado de Protección de Datos Personales (DPO) a través del correo electrónico: proteccion.datos@ocse.ec

¿QUÉ DATOS PERSONALES TRATAMOS?

Tratamos los datos personales necesarios para la gestión de la relación laboral, el cumplimiento de obligaciones legales y el adecuado funcionamiento de la empresa.

Entre los datos que pueden ser tratados se incluyen:

Datos de identificación: Nombres y apellidos, número de cédula de identidad, estado civil, fecha y lugar de nacimiento, nacionalidad, sexo, número de cargas familiares.

Datos de contacto: Dirección domiciliaria, ciudad, teléfono convencional, teléfono móvil, correo electrónico personal.

Datos económicos y financieros: Entidad financiera, número de cuenta, remuneración, ingresos mensuales y anuales, beneficios laborales, décimo tercero y décimo cuarto sueldo, aportes a la seguridad social, retenciones tributarias.

Datos laborales y profesionales: Nivel de instrucción, fecha de ingreso, cargo, modalidad contractual, jornada laboral, control de asistencia, historial disciplinario, evaluaciones de desempeño, fecha de terminación de la relación laboral.

Datos de dependientes: Nombres, apellidos, edad y número de identificación de cargas familiares declaradas.

Datos sensibles: Datos relativos a la salud (certificados médicos, aptitud ocupacional), discapacidad, afiliación sindical, y demás datos considerados sensibles como la huella dactilar y/o reconocimiento facial, conforme a la LOPDP, los cuales serán tratados únicamente cuando sea estrictamente necesario y bajo las garantías reforzadas previstas en la ley.

¿CON QUÉ FINALIDAD TRATAMOS SUS DATOS PERSONALES?

Los datos personales de los colaboradores son tratados para las siguientes finalidades legítimas:

- **Gestión del talento humano:** Procesos de reclutamiento y selección, contratación, administración de la relación laboral, movilidad interna y desvinculación.
- **Pago de remuneraciones y beneficios:** Gestión de nómina, pagos salariales, beneficios legales y contractuales, afiliación y aportes al Instituto Ecuatoriano de Seguridad Social (IESS).
- **Capacitación y desarrollo profesional:** Ejecución de programas de formación, evaluaciones de desempeño y planes de carrera.
- **Seguridad Física:** Control de acceso a instalaciones físicas y sistemas informáticos, uso de credenciales, cámaras de videovigilancia y, cuando corresponda, mecanismos biométricos, con fines de seguridad y prevención de fraudes.
- **Seguridad Industrial y Salud Ocupacional:** Medición del clima organizacional y riesgos laborales y psicosociales; y, realización de exámenes preocupacionales, ocupacionales o postocupacionales mediante terceros autorizados.
- **Cumplimiento de obligaciones legales:** Atención de requerimientos de autoridades administrativas, judiciales, laborales, tributarias o de control, incluyendo el Ministerio del Trabajo, el Servicio de Rentas Internas (SRI), el IESS y autoridades judiciales competentes.
- **Ejercicio de derechos y defensa jurídica:** Uso de datos personales para la formulación, ejercicio o defensa de derechos de OCSE S.A en procesos judiciales, administrativos o arbitrales.
- **Operación y continuidad del negocio:** Gestión interna, auditorías, cumplimiento normativo, control interno, comunicaciones corporativas y administración de sistemas tecnológicos.

Sus datos personales no serán utilizados para otras finalidades que sean incompatibles con las que motivaron su recogida.

¿CUAL ES LA BASE LEGAL DEL TRATAMIENTO?

El tratamiento de los datos personales se fundamenta, según corresponda, en:

- La ejecución del contrato de trabajo
- El cumplimiento de obligaciones legales y regulatorias
- El interés legítimo de la empresa, debidamente ponderado
- El consentimiento expreso del titular sobre el tratamiento de datos biométricos, en el cual se determinará de manera clara su finalidad.

¿CÓMO OBTENEMOS LOS DATOS PERSONALES?

Los datos personales son obtenidos principalmente:

- Directamente del colaborador, mediante formularios, documentos, correos electrónicos o sistemas internos
- De forma automática, a través del uso de sistemas informáticos corporativos
- De terceros legalmente habilitados, como autoridades públicas o judiciales

¿CUÁL ES EL PLAZO DE CONSERVACIÓN?

Los datos personales se almacenarán durante el tiempo legalmente requerido o necesario para la consecución de la finalidad al momento de su captura, la finalización de la relación laboral y posterior por causas legítimas de tratamiento.

Una vez cumplida la finalidad, los datos serán eliminados, anonimizados o bloqueados, según corresponda.

¿CON QUIÉN COMPARTIMOS LOS DATOS PERSONALES?

Los datos personales podrán ser compartidos, cuando sea estrictamente necesario, con:

- Autoridades públicas y judiciales del Ecuador
- Proveedores de servicios (tecnología, nómina, auditoría, seguros, salud ocupacional)
- Instituciones financieras
- Empresas del mismo grupo empresarial

En caso de transferencias internacionales de datos, OCSE S.A garantizará que se realicen conforme a la LOPDP, adoptando medidas contractuales y técnicas adecuadas para proteger los derechos del titular.

¿CUALES SON LOS DERECHOS DEL TITULAR DE DATOS?

Usted, como titular de datos personales, tiene derecho a:

- Acceder a sus datos
- Solicitar la rectificación y actualización
- Solicitar la eliminación de datos
- Oponerse al tratamiento
- Solicitar la limitación del tratamiento
- Solicitar la portabilidad
- Revocar el consentimiento, cuando sea aplicable
- Presentar reclamos ante la Autoridad de Protección de Datos Personales del Ecuador

Para ejercer sus derechos, puede escribir a: proteccion.datos@ocse.ec

Las solicitudes serán atendidas dentro de los plazos establecidos por la ley.

SEGURIDAD DE LA INFORMACIÓN

OCSE S.A aplica medidas técnicas, organizativas, administrativas y legales razonables para proteger los datos personales contra accesos no autorizados, pérdida, alteración o divulgación indebida.

Cada colaborador es responsable de mantener la confidencialidad de sus credenciales de acceso a los sistemas corporativos.

MARCO NORMATIVO APLICABLE

Este Aviso se rige por la Ley Orgánica de Protección de Datos Personales del Ecuador, su Reglamento y demás normativa aplicable.

CONTACTO

Para consultas, comentarios o ejercicio de derechos, contáctenos en: proteccion.datos@ocse.ec

MODIFICACIONES AL AVISO

OCSE S.A se reserva el derecho de modificar este Aviso en cualquier momento, en cumplimiento de la normativa vigente. Las modificaciones serán oportunamente comunicadas.

Fecha de emisión: 23 de marzo de 2026.

Aprobado por el Departamento de Proteccion de Datos de OCSE S.A.

ANEXO 3

AVISO EXTERNO DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES.

En cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador, su reglamento y normativa diversa en la materia, te presentamos el Aviso Externo de Privacidad para clientes y usuarios mediante el cual te informamos sobre el tratamiento de tus datos personales.

1. Términos Definidos

Aviso de Privacidad: Se refiere al presente documento, el cual es puesto a disposición del Titular, previo al tratamiento de sus datos personales, de conformidad con la LOPDP.

Datos Personales: Cualquier información concerniente a una persona física identificada o identificable.

Datos Personales Sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Derechos ARCO: Derechos de Acceso, Rectificación, Cancelación y Oposición.

Encargado de Tratamiento: Persona física o jurídica que sola o conjuntamente trate los Datos Personales, por cuenta de OCSE .S.A. como Responsable.

Responsable del Tratamiento: OCSE .S.A., Persona física y jurídica que determina **por qué** (fines) y **cómo** (medios) se tratan los datos personales.

Titular: Persona natural y física a quien corresponden los Datos Personales.

Transferencia: Toda comunicación de datos realizada a persona distinta del Responsable o Encargado del Tratamiento.

Tratamiento: Abarca cualquier operación, como recolección, almacenamiento, uso o eliminación, realizada sobre información que identifica a individuos, ya sea manual o automatizadamente.

2. Identidad y domicilio del Responsable

Seguros S.A., sociedad legalmente constituida conforme a las leyes de la República del Ecuador, con domicilio en la ciudad de Quito, provincia de Pichincha, con su matriz ubicada en la Av. 6 de diciembre y Portugal, en adelante denominada OCSE S.A, puede obtener, usar y almacenar los Datos Personales de usted como Titular de los mismos en su carácter de cliente o potencial cliente del Responsable y este a su vez, será el responsable de su protección y tratamiento conforme la normativa vigente.

3. Obtención de los Datos Personales

El Responsable recabará los Datos Personales a través de la aplicación móvil OCSE (la “Aplicación”), así como también podrá realizarlo a través de su sitio web www.occidentalseguros.ec (la “Página Web”), otras aplicaciones, redes sociales propias y de terceros o nuestros eventos en línea, así como de manera directa del Titular por la contratación del Responsable para brindar cualesquiera de sus servicios o por cualquier tipo de operación que celebre con el Responsable.

4. Datos Personales de Terceros

En caso de que el Titular haya proporcionado datos de contacto de terceros como referencias, autorizados, cotitulares, cónyuges, beneficiarios, coacreditados, garantes, obligados solidarios,

avales, fiadores, tutores, proveedores y demás figuras legales relacionadas con servicios del Responsable, el Titular garantiza que cuenta con su previa autorización para proporcionar dichos datos, incluyendo en su caso los Datos Personales aplicables, y es responsable de comunicar a dichas personas sobre los términos y razones por las cuales los contactaremos y, en su caso, el Tratamiento de sus Datos Personales conforme al presente Aviso de Privacidad, así como los medios para conocer el contenido íntegro del mismo.

Adicionalmente, mediante su consentimiento al presente Aviso de Privacidad, el Titular ratifica su autorización para que el Responsable contacte a dichas personas. El Responsable cumplirá en todo momento con las disposiciones de la normativa vigente respecto a los Datos Personales que obtengamos de forma indirecta.

5. Datos Personales que serán recabados

El Responsable recabará y tratará del Titular las siguientes categorías de Datos Personales:

- Datos de identificación.
- Datos de contacto.
- Datos contenidos cuando se comunica con nosotros mediante redes sociales.
- Datos patrimoniales y financieros.
- Datos vinculados a su número celular.
- Datos relacionados con los servicios contratados.
- Datos biométricos (exclusivamente huella dactilar y/o reconocimiento facial).

La información deberá ser veraz y completa. El Titular será responsable de las consecuencias de proporcionar información falsa o inexacta.

6. Datos Personales Sensibles

Con el fin de poder identificarlo correctamente en atención al servicio contratado, podemos recabar datos biométricos, exclusivamente huellas dactilares o reconocimiento facial, que son catalogados como datos personales sensibles. No recabaremos ningún otro dato personal sensible.

Para esto es necesario contar previamente con su consentimiento expreso y por escrito mediante la aceptación expresa al presente Aviso de Privacidad.

7. Finalidad del Tratamiento de los Datos Personales

Finalidades Primarias

Incluyen, entre otras: identificación, contratación de servicios, verificación de información, cumplimiento legal, prestación y administración de servicios, facturación, atención a clientes, soporte técnico, cobranza, prevención de fraudes, cumplimiento contractual, atención de emergencias, defensa legal y actividades complementarias.

Finalidades Secundarias

Incluyen: mercadotecnia, publicidad, análisis de perfiles, encuestas, promociones, eventos, fortalecimiento de marca, uso de comentarios en redes sociales, material fotográfico o de video, análisis de hábitos y personalización de la experiencia.

El Titular puede negar su consentimiento para las finalidades secundarias sin que ello afecte la prestación de los servicios contratados.

8. Uso de Cookies y Tecnologías Similares

La Página Web utiliza cookies y tecnologías similares para mejorar la experiencia del usuario, medir tráfico y prevenir actividades fraudulentas. El Titular puede deshabilitarlas desde su navegador, aunque ello puede afectar el funcionamiento del sitio.

9. Transferencia de Datos Personales

Los Datos Personales podrán ser transferidos a autoridades, afiliadas, subsidiarias, terceros estratégicos y otros supuestos permitidos por la LOPDP, tanto en territorio nacional como en el extranjero.

Al no manifestar negativa expresa, el Titular consiente determinadas transferencias con fines mercadológicos, promocionales, financieros, turísticos y de eventos.

10. Departamento de Datos Personales

Domicilio principal en la ciudad de Quito, provincia de Pichincha, con su matriz ubicada en la Av. 6 de diciembre N15-28 y Portugal.

Correo electrónico: proteccion.datos@ocse.ec

11. Medios para ejercer derechos

El Titular podrá ejercer derechos ARCO, revocar consentimiento, limitar el uso o manifestar negativa para finalidades secundarias mediante solicitud al Responsable de Tratamiento a través de los canales establecidos.

12. Derechos ARCO

La solicitud deberá incluir identificación, descripción clara del derecho a ejercer y documentación de soporte.

Respuesta: Conforme los plazos legales establecidos en la normativa.

13. Revocación o limitación del consentimiento

El Titular puede revocar o limitar el tratamiento de sus datos, sujeto a obligaciones legales vigentes.

14. Modificaciones al Aviso de Privacidad

Las modificaciones estarán disponibles en la Página Web y en la Aplicación de OCSE .S.A.,

15. Tratamiento indebido de Datos Personales

El Titular puede presentar quejas ante el Responsable del Tratamiento o ante la Superintendencia de Protección de Datos Personales.

16. Aceptación

El titular otorga el consentimiento para el tratamiento de sus datos conforme el aviso externo de privacidad, el cual será otorgado por medios electrónicos y/o firma electrónica, con plena validez legal.

Última fecha de actualización del Aviso de Privacidad: 23 de marzo de 2026.

Aprobado por el Departamento de ´Protección de Datos de OCSE S.A.

ANEXO 4

PLAN DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD DE DATOS BIOMETRICOS E IA

1. Descripción

Este plan define el procedimiento interno que seguirá la aseguradora ficticia ante brechas de seguridad relacionados con datos biométricos de empleados tratados mediante IA. Incluye detección, contención, análisis, notificación, remediación, documentación y cierre.

Su finalidad es responder ante brechas que afecten huellas, rostros, plantillas biométricas, registros de acceso o resultados generados por IA, especialmente si existe uso secundario para control horario, productividad o vigilancia laboral.

2. Objetivo

Establecer un protocolo para gestionar brechas que afecten datos biométricos tratados con IA, garantizando el cumplimiento de plazos y la obligación de notificar a la Autoridad y titulares de datos, protegiendo los derechos y libertades de los trabajadores y demostrando responsabilidad proactiva.

3.1. Marco normativo aplicable

El presente plan se fundamenta en la normativa ecuatoriana y referencia internacional respecto a la obligación de reportar brechas de seguridad, en este contexto tenemos: la Constitución de la República del Ecuador (2008) que en su artículo 66 garantiza el derecho a la protección de datos de carácter personal y a la intimidad, la LOPDP en su artículo 43 y 46 establecen la obligación de notificación de vulneración de seguridad ante la autoridad; y, al titular, respectivamente, el Reglamento General de la LOPDP en sus artículos 24 al 28 establecen los plazos, supuestos y procedimientos de la notificación de vulneraciones, la Resolución SPDP-SPD-2026-0009-R establece la obligación de aplicar medidas técnicas y organizativas, auditar sistemas de IA y realizar gestión de riesgos en tratamientos automatizados, concordando con lo establecido en la Guía de Gestión de la Riesgos de la SPDP expedida a través de la Resolución SPDP-SPD-2026-0012 el cual analiza de manera escalonada las fases del riesgo, los modelos de matrices, valoraciones cuantitativas y cualitativas; finalmente, los estándares internacionales como al ISP/TEC 27035 sobre gestión de incidentes y el RGPD de la Unión Europea como marco referencial.

Estas normas exigen proteger datos personales, aplicar principios de finalidad, minimización, proporcionalidad, seguridad y responsabilidad proactiva, así como gestionar adecuadamente brechas que puedan afectar derechos de los titulares.

3.2. Incidente de seguridad biométrica con IA

Es fundamental diferenciar conceptualmente entre un incidente y una vulneración para escalar la respuesta adecuadamente:

- **Incidente de seguridad:** Cualquier evento confirmado o sospechado que comprometa o pueda llegar a comprometer la confidencialidad, integridad,

disponibilidad o uso legítimo de los sistemas de IA o bases de datos biométricas.

- **Vulneración de seguridad (Brecha):** Un incidente de seguridad confirmado que ha ocasionado la destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales biométricos.

Tipo de evento	Descripción
Acceso no autorizado	Ingreso indebido a bases, plantillas o registros biométricos.
Filtración	Exposición de huellas, rostros o plantillas.
Pérdida o destrucción	Eliminación, corrupción o indisponibilidad de datos.
Error algorítmico	Falsos positivos, falsos negativos o bloqueos injustificados.
Uso secundario	Uso para control horario, productividad o vigilancia.
Transferencia no autorizada	Envío o acceso a datos sin garantías suficientes.

Todo incidente con biometría debe tratarse con prioridad alta, por tratarse de datos sensibles e irreversibles.

3.3. Fases del protocolo

Fase 1: Detección e identificación

Cualquier miembro de la organización que detecte o sospeche de una brecha de seguridad deberá reportarlo inmediatamente al DPD.

Correo DPD: dpd@aseguradora-ficticia.ec
Extensión: 0012
Canal: “Incidente de datos personales / biometría”

Actividad	Responsable	Plazo
Detectar incidente	Personal en general	Inmediato
Reportar al DPD	Personal en general	Máx. 2 horas
Registrar incidente	DPD	Máx. 2 horas
Identificar sistemas afectados	Tecnología / Sistemas	Máx. 4 horas
Clasificar gravedad inicial	DPD, Tecnología y Jurídica	Máx. 4 horas
Activar protocolo	DPD	Máx. 4 horas

Fase 2: Contención y análisis

El objetivo principal de esta fase es frenar la afectación de manera inmediata para que el evento no siga propagándose, y posteriormente confirmar si el incidente se materializó en una vulneración de datos.

Acción	Responsable
Contención inmediata: Ejecutar acciones técnicas urgentes para frenar la vulneración (ej. desconectar equipos de la red, apagar interfaces, bloquear puertos o bajar temporalmente el sistema de IA).	Tecnología / Sistemas

Aislar sistemas comprometidos y suspender accesos sospechosos.	Tecnología / Sistemas
Preservar logs y evidencias.	Tecnología / Sistemas
Confirmar vulneración: Analizar la evidencia para verificar y confirmar si el incidente constituye efectivamente una vulneración (brecha) de datos personales.	DPD y Tecnología
Identificar datos afectados y determinar titulares involucrados.	DPD y Tecnología
Evaluar consecuencias jurídicas y verificar uso secundario.	DPD y Jurídica
Elaborar acta inicial.	DPD

Fase 3: Evaluación del riesgo

El DPD evaluará, junto con Tecnología y Jurídica, si la vulneración representa un riesgo alto para los derechos y libertades de los titulares.

Riesgo alto	Ejemplo
Datos biométricos afectados	Filtración de huellas o rostros.
Uso secundario	Uso no consentido para productividad o vigilancia.
Acceso no autorizado	Ingreso indebido a la base biométrica central.
Decisión automatizada perjudicial	Bloqueo injustificado del trabajador basado en IA.
Discriminación	Error del sistema que afecta desproporcionadamente a ciertos trabajadores.
Transferencia irregular	Envío de datos biométricos sin garantías.
Daño irreversible	Exposición de datos no reemplazables (biometría).

Si no hay riesgo alto, se gestiona internamente. Si existe riesgo alto, se activa la notificación a la SPDP y a los titulares.

Fase 4: Notificación a la autoridad

Para efectos del presente plan, los plazos y términos se computarán conforme a la normativa aplicable. En este sentido, de acuerdo con los artículos 159 y 160 del Código Orgánico Administrativo, los términos se fijan en días y se computan en días hábiles, excluyendo fines de semana y feriados, mientras que los plazos se computan conforme a las reglas de fecha a fecha.

Al presentarse una vulneración de seguridad, la LOPDP en su art 43 y su Reglamento art. 24 establece que, el responsable del tratamiento deberá notificar ante la Autoridad de Protección de Datos Personales y ARCOTEL lo más pronto sea posible, a más tardar en el término de 5 días después de que haya

tenido constancia de ello, salvo que sea improbable que mencionado incidente cause daños en los derechos y libertades de los titulares de datos.

En el caso de no poder reunir toda la información necesaria para la notificación, como principio de responsabilidad proactiva, se recomienda notificar la vulneración de manera escalonada, es decir, en un reporte inicial proveer de la información disponible y comprometerse a complementarla posteriormente conforme avance la investigación. Adicionalmente, la normativa contempla que, si la notificación no se realiza en el término establecido, el responsable de tratamiento deberá indicar de manera motivada el por qué de su dilación.

Los encargados de tratamiento deberán notificar el responsable del tratamiento lo más pronto posible, a más tardar en el término de 2 días contados a partir de la fecha que tenga conocimiento de ello.

Conforme lo determina el art 28 del Reglamento General de la LOPDP, la notificación deberá contener la naturaleza y el tipo de vulneración, identificación de titulares, detalle de los sistemas vulnerados, causa presunta, el volumen y tipo de datos expuestos, las medidas adoptadas, la evaluación de riesgos, entre otros. Mientras que el encargado de tratamiento deberá cumplir con lo mencionado en dicho artículo, a excepción de la evaluación de riesgo.

Fase 5: Notificación a titulares

La LOPDP en su art 46 y su Reglamento artículo 28, establecen la obligatoriedad de notificar al titular sobre la vulneración de seguridad, siempre y cuando exista un riesgo para el titular. Mencionada notificación se lo deberá realizar sin dilación y a más tardar en el término de tres días contados a partir de la fecha en la que tuvo conocimiento del riesgo. La notificación deberá ser emitida en un lenguaje claro y comprensible, observando los derechos de los titulares.

La LOPDP en su artículo 46 determina las excepciones en las cuales no se deberá notificar al titular, siendo los siguientes: 1.- Cuando se haya adoptado medidas de protección técnicas u organizativas apropiadas a los datos afectados que demuestren ser efectivas, 2.- Cuando se haya tomado medidas posteriores que garanticen que el riesgo para los derechos y libertades del titular ya no ocurrirá; y 3.- Cuando se requiera un esfuerzo desproporcionado; en cuyo caso, el responsable deberá realizar una comunicación pública a través de cualquier medio para informar a los titulares sobre la vulneración.

El responsable del tratamiento propone la excepción de los puntos 1 y 2 al reportar el incidente dentro del término de 5 días, sin embargo, es la Autoridad de Protección de Datos Personales, quien valida si esas medidas son suficientes para justificar que no se notifique a los titulares de los datos.

Fase 6: Remediación y cierre

Medida	Responsable
Corregir vulnerabilidad técnica raíz	Tecnología / Sistemas
Revisar accesos y privilegios	Tecnología / Sistemas
Auditar logs	Tecnología / Sistemas
Evaluar implicaciones legales	Jurídica

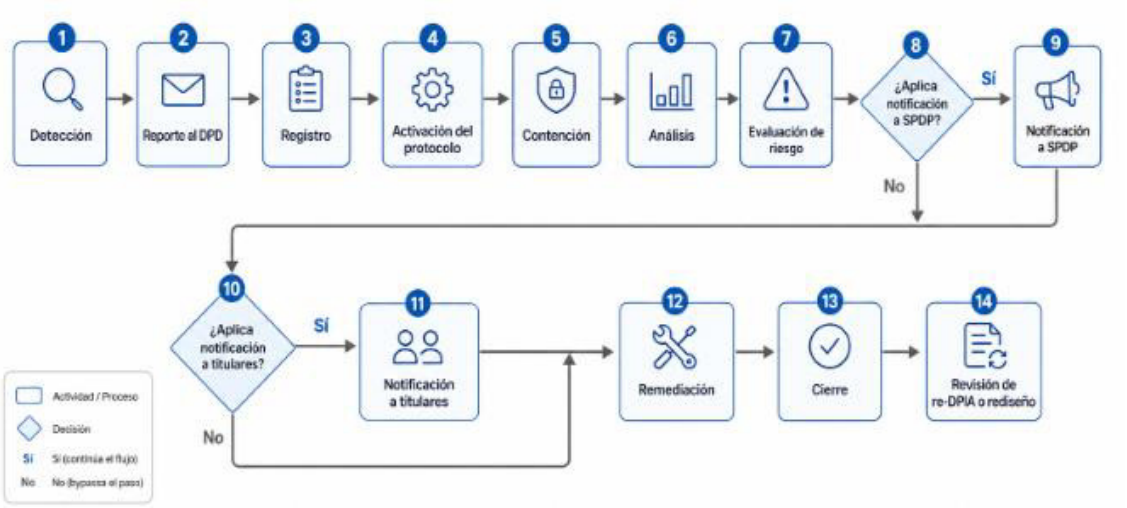
Suspender usos no autorizados de IA	Alta Dirección
Verificar función secundaria	DPD y Jurídica
Actualizar políticas y avisos de privacidad	DPD y Jurídica
Evaluar necesidad de nueva EIPD (re-DPIA)	DPD
Aprobar medidas finales	Alta Dirección
Emitir informe de cierre	DPD

El cierre incluirá causa raíz, impacto, medidas adoptadas, evidencias, notificaciones realizadas, riesgo residual y decisión sobre re-DPIA.

3.4. Roles y responsabilidades

Rol	Responsabilidad
DPD	Coordina el protocolo, evalúa riesgos, documenta, gestiona notificaciones y recomienda medidas.
Tecnología / Sistemas	Ejecuta contención inmediata, analiza técnicamente, preserva evidencias y remedia.
Jurídica	Evalúa implicaciones legales, plazos, responsabilidades y apoya en redacción de notificaciones.
Alta Dirección	Aprueba decisiones críticas, recursos, suspensión de sistemas y aprueba formalmente las notificaciones a la SPDP y titulares.
Personal en general	Detecta y reporta incidentes o sospechas al DPD de forma inmediata.

3.5 Flujograma textual



3.6. Registro de incidentes

El registro interno deberá contener: código del incidente, fechas de detección y conocimiento, confirmación de vulneración, sistemas afectados, datos comprometidos, titulares afectados, gravedad, consecuencias, medidas de

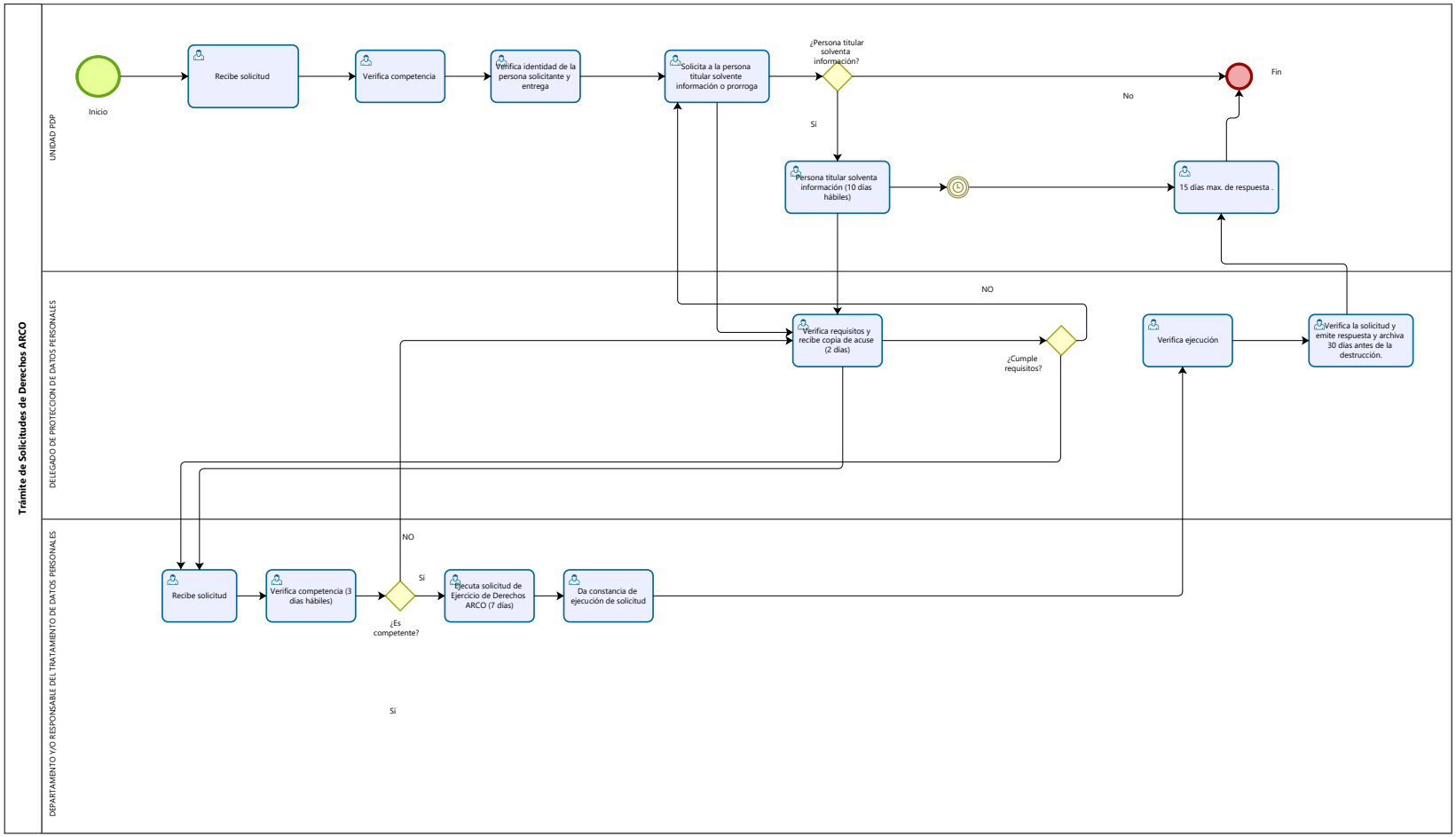
contención adoptadas, aprobaciones de la Alta Dirección, comunicaciones realizadas, acciones correctivas, responsable del cierre, decisión sobre re-DPIA y evidencias.

Trámite de Solicitudes de Derechos ARCO

Bizagi Modeler

Tabla de Contenidos

1 TRÁMITE DE SOLICITUDES DE DERECHOS ARCO



Versión:

1.0

Autor:

cdelgado

1.1 TRÁMITE DE SOLICITUDES DE DERECHOS ARCO

1.1.1 ELEMENTOS DEL PROCESO

1.1.1.1 ¿Persona titular solventa información?

Flujos

Sí

Condición

${solventa == true}

No

Condición

${solventa == false}

1.1.1.2 ¿Cumple requisitos?

Flujos

Sí

Condición

${requisitos == true}

NO

1.1.1.3 ¿Es competente?

Flujos

NO

Sí

Condición

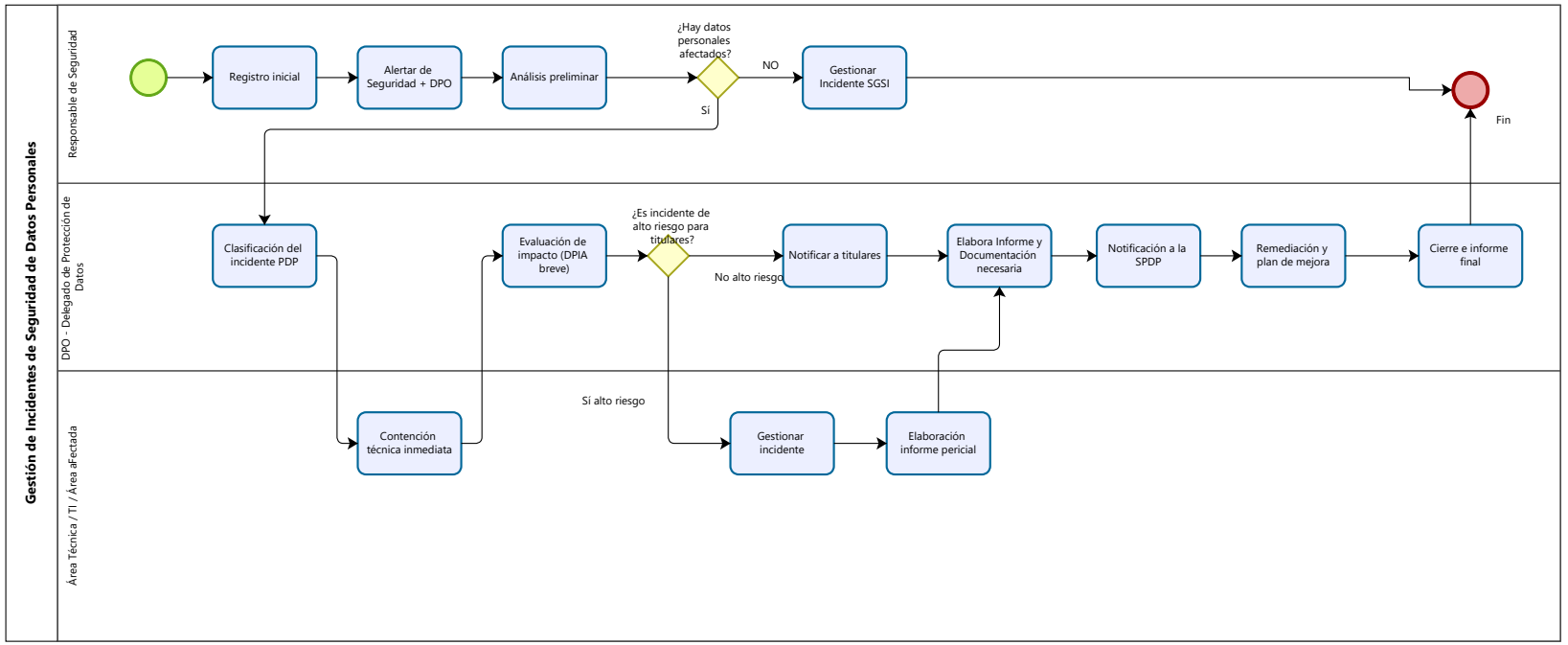
${competente == true}

Gestión de Incidentes de Seguridad de Datos Personales

Bizagi Modeler

Tabla de Contenidos

1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE DATOS PERSONALES



Powered by bizagi Modeler

Versión:

1.0

Autor:

cdelgado

1.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE DATOS PERSONALES

1.1.1 ELEMENTOS DEL PROCESO

1.1.1.1 Inicio Simple

Descripción

Responsabilidad proactiva – Art. 58

1.1.1.2 Registro inicial

Descripción

Art. 59 – Deber de documentar

1.1.1.3 Alertar de Seguridad + DPO

Descripción

Diseño y seguridad por defecto – Art. 47-49

1.1.1.4 Análisis preliminar

Descripción

¿Hay datos personales afectados? (Art. 12)

1.1.1.5 ¿Hay datos personales afectados?

Flujos

NO

Sí

Condición

${datosAfectados == true}

1.1.1.6 Clasificación del incidente PDP

Descripción

Datos sensibles – Art. 27

1.1.1.7 Contención técnica inmediata

Descripción

Medidas de seguridad – Art. 31

1.1.1.8 Evaluación de impacto (DPIA breve)

Descripción

Riesgos altos – Art. 47-49

1.1.1.9 ¿Es incidente de alto riesgo para titulares?

Flujos

Sí alto riesgo

Condición

${altoRiesgo == true}

No alto riesgo

Condición

${altoRiesgo == false}

1.1.1.10 Gestionar incidente

Descripción

Medidas de seguridad – Art. 31

1.1.1.11 Elaboración informe pericial

Descripción

Medidas de seguridad – Art. 31

1.1.1.12 Notificar a titulares

Descripción

Riesgo significativo – Art. 13

1.1.1.13 Elabora Informe y Documentación necesaria

Descripción

Riesgo significativo – Art. 13

1.1.1.14 ☐ Notificación a la SPDP

Descripción

Riesgo significativo – Art. 13

1.1.1.15 ☐ Remediación y plan de mejora

Descripción

Art. 49 – Seguridad por defecto

1.1.1.16 ☐ Cierre e informe final

Descripción

Responsabilidad proactiva – Art. 58-59

1.1.1.17 ☐ Gestionar Incidente SGSI

Descripción

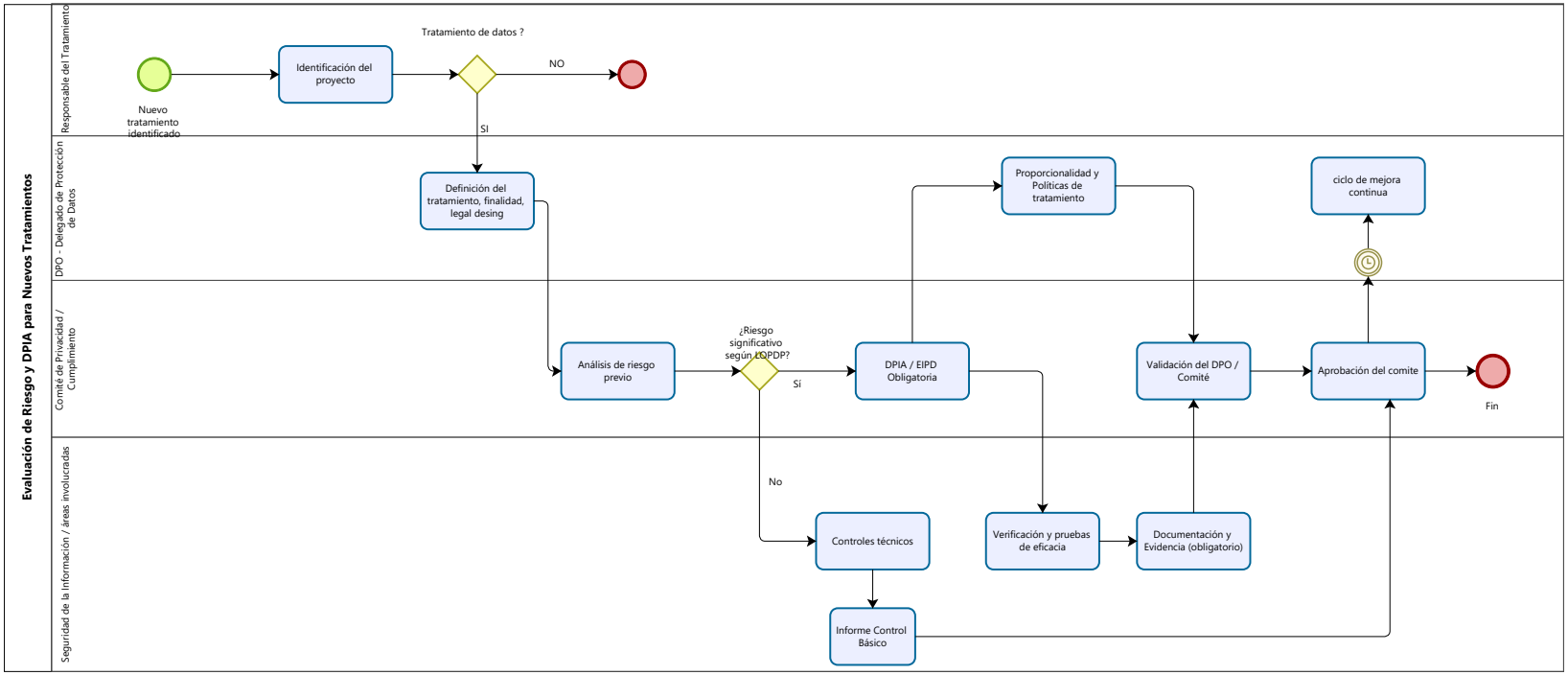
¿Hay datos personales afectados? (Art. 12)

Evaluación de Riesgo y DPIA para Nuevos Tratamientos

Bizagi Modeler

Tabla de Contenidos

1 EVALUACIÓN DE RIESGO Y DPIA PARA NUEVOS TRATAMIENTOS



Powered by bizagi Modeler

Versión:

1.0

Autor:

cdelgado

1.1 EVALUACIÓN DE RIESGO Y DPIA PARA NUEVOS TRATAMIENTOS

1.1.1 ELEMENTOS DEL PROCESO

1.1.1.1 Nuevo tratamiento identificado

Descripción

Nuevo sistema, aplicación, proveedor o tratamiento nuevo

1.1.1.2 Identificación del proyecto

Descripción

Art. 12 – Licitud y transparencia. Registrar: nuevo sistema, aplicación, proveedor o tratamiento nuevo.

1.1.1.3 Definición del tratamiento, finalidad, legal desing

Descripción

Art. 27 y 31 – Finalidad, datos involucrados, flujos, sistemas. ¿Incluye datos sensibles?

1.1.1.4 Análisis de riesgo previo

Descripción

Art. 47-49 – Identificación inicial de riesgos. ¿Existe riesgo significativo?

1.1.1.5 ¿Riesgo significativo según LOPDP?

Flujos

No

Condición

${riesgoSignificativo == false}

Sí

Condición

${riesgoSignificativo == true}

1.1.1.6 ☐DPIA / EIPD Obligatoria

Descripción

Art. 43 – Evaluación completa del impacto. Matriz de riesgos. Proporcionalidad y necesidad.

1.1.1.7 ☐Verificación y pruebas de eficacia

Descripción

Art. 31 y 59 – Seguridad estándar SGSI. Minimización, cifrado, RBAC, avisos.

1.1.1.8 ☐Documentación y Evidencia (obligatorio)

Descripción

Art. 31 y 59 – Seguridad estándar SGSI. Minimización, cifrado, RBAC, avisos.

1.1.1.9 ☐Proporcionalidad y Políticas de tratamiento

Descripción

Art. 43 – Evaluación completa del impacto. Matriz de riesgos. Proporcionalidad y necesidad.

1.1.1.10 ☐Validación del DPO / Comité

Descripción

Art. 48 – Dictamen de proporcionalidad, compatibilidad y necesidad.

1.1.1.11 ☐Controles técnicos

Descripción

Art. 31 y 59 – Seguridad estándar SGSI. Minimización, cifrado, RBAC, avisos.

1.1.1.12 ☐Aprobación del comite

Descripción

Art. 48 – Dictamen de proporcionalidad, compatibilidad y necesidad.

1.1.1.13 ☐ciclo de mejora continua

Descripción

Art. 48 – Dictamen de proporcionalidad, compatibilidad y necesidad.