Maestría en

Protección de Datos

Trabajo de investigación previo a la obtención del título de

Magíster en Protección de Datos

AUTORES:

Faican Jiménez Evelyn Cristina

Moyano Espinoza Luis Enrique

Paredes León Pamela Estefania

Roldán Vallejos Diana Patricia

Rosales Vizcarra Paúl Alejandro

Vaca Villamara Raisa Natalia

TUTORES:

Profesor PBL1: Humberto Ortiz Rodríguez

Profesor PBL2: Camila Valdez González

Profesor PBL3: Jacqueline Guerrero Carrera

"Privacidad desde el diseño y por defecto: Aplicación al uso de biometría en el escenario de una entidad del Sector de la Salud"

Quito, junio 2026

Certificación de autoría

Nosotros, **Rosales Vizcarra Paúl Alejandro; Roldán Vallejos Diana Patricia; Faican Jiménez Evelyn Cristina; Paredes León Pamela Estefania; Vaca Villamara Raisa Natalia y; Moyano Espinoza Luis Enrique,** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
EVELYN CRISTINA FAICAN JIMENEZ

Firma del graduado
Faican Jiménez Evelyn Cristina

Firmado electrónicamente por:
Luis Enrique Moyano Espinoza

Firma del graduado
Moyano Espinoza Luis Enrique

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
PAMELA ESTEFANIA PAREDES LEON

Firma del graduado
Paredes León Pamela Estefania

Firmado electrónicamente por:
DIANA PATRICIA ROLDAN VALLEJOS

Firma del graduado
Roldán Vallejos Diana Patricia

PAUL ALEJANDRO ROSALES VIZCARRA
Firmado digitalmente por PAUL ALEJANDRO ROSALES VIZCARRA
Fecha: 2026.07.05 21:36:57 -05'00'

Firma del graduado
Rosales Vizcarra Paúl Alejandro

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
RAISA NATALIA VACA VILLAMAR

Firma del graduado
Vaca Villamara Raisa Natalia

Autorización de Derechos de Propiedad Intelectual

Nosotros, **Rosales Vizcarra Paúl Alejandro; Roldán Vallejos Diana Patricia; Faican Jiménez Evelyn Cristina; Paredes León Pamela Estefania; Vaca Villamara Raisa Natalia y; Moyano Espinoza Luis Enrique**, en calidad de autores del trabajo de investigación titulado "***Privacidad desde el diseño y por defecto: aplicación del uso de biometría en el escenario de una entidad del sector de la salud"***, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes del Código Orgánico de la Economía Social del Conocimiento, la Creatividad y la Innovación.

D. M. Quito, junio 2026.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
EVELYN CRISTINA FAICAN JIMENEZ

Firma del graduado
Faican Jiménez Evelyn Cristina

Firmado electrónicamente por:
Luis Enrique Moyano Espinoza

Firma del graduado
Moyano Espinoza Luis Enrique

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
PAMELA ESTEFANIA PAREDES LEON

Firma del graduado
Paredes León Pamela Estefania

Firmado electrónicamente por:
DIANA PATRICIA ROLDAN VALLEJOS

Firma del graduado
Roldán Vallejos Diana Patricia

PAUL ALEJANDRO ROSALES VIZCARRA

Firmado digitalmente por PAUL ALEJANDRO ROSALES VIZCARRA
Fecha: 2026.07.05 21:37:38 -05'00'

Firma del graduado
Rosales Vizcarra Paúl Alejandro

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
RAISA NATALIA VACA VILLAMAR

Firma del graduado
Vaca Villamara Raisa Natalia

Acuerdo de confidencialidad

La Biblioteca de la Universidad Internacional del Ecuador se compromete a:

1. No divulgar, utilizar ni revelar a otros la **información confidencial** obtenida en el presente trabajo, ya sea intencionalmente o por falta de cuidado en su manejo, en forma personal o bien a través de sus empleados.
2. Manejar la **información confidencial** de la misma manera en que se maneja la información propia de carácter confidencial, la cual bajo ninguna circunstancia podrá estar por debajo de los estándares aceptables de debida diligencia y prudencia.
3. Breve información de él porque su tesis es confidencial.

Jacqueline Guerrero
Coordinador Maestría en
Protección de Datos

Gabriela Fernández
Gestora Cultural

Aprobación de dirección y coordinación del programa

Nosotros, **Nombre del Director/a EIG y Jacqueline Guerrero Carrera, Coordinadora UIDE,** declaramos que los graduandos: **Faican Jiménez Evelin Cristina, Moyano Espinoza Luis Enrique, Paredes León Pamela Estefania, Rolán Vallejos Diana Patricia, Rosales Vizcarra Paúl Alejandro y Vaca Villamara Raisa Matalia** 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

Este trabajo está dedicado a Dios, por iluminar mi camino y darme la fuerza necesaria para perseverar ante cada desafío y alcanzar esta importante meta.

A mis padres, **Sandra Jiménez y Mario Faican**, quienes con su amor, esfuerzo y ejemplo han sido la base de cada uno de mis logros. Gracias por enseñarme a creer en mis capacidades, por impulsarme a superarme constantemente y por estar presentes en cada paso de mi vida. Este logro es el reflejo de los valores y principios que me han inculcado.

A mis hermanas, **Priscila Faican y Odalis Cárdenas**, por su cariño sincero, por compartir mis alegrías y desafíos, y por ser una fuente permanente de apoyo y motivación.

A **Paul Peralta**, por acompañarme con amor, paciencia y comprensión durante esta etapa. Gracias por ser un apoyo constante, por alentarme a continuar y por celebrar conmigo cada avance alcanzado.

Finalmente, me permito dedicar unas palabras a mí misma, **Evelyn Cristina Faican Jiménez**, porque detrás de este trabajo existen años de estudio, esfuerzo, sacrificio y perseverancia. La culminación de este camino en la Maestría en Protección de Datos Personales representa mucho más que la obtención de un título; simboliza el resultado de incontables horas de dedicación, el compromiso con la excelencia profesional y la satisfacción de haber superado cada reto con determinación y valentía.

Como Ingeniera Biomédica y Abogada, este logro constituye una nueva meta alcanzada en mi vida académica y profesional, reafirmando mi convicción de que los sueños se hacen realidad cuando se persiguen con disciplina, pasión y constancia. Hoy cierro una etapa llena de aprendizajes y crecimiento, llevando conmigo la gratitud hacia quienes me acompañaron en este recorrido y la certeza de que cada esfuerzo realizado ha valido la pena.

A todos ustedes, gracias por formar parte de mi historia, por creer en mí cuando más lo necesité y por acompañarme en la construcción de este sueño que hoy se hace realidad. Este trabajo es el reflejo del amor, el apoyo, la confianza y los valores que he recibido a lo largo de mi vida.

Con todo mi amor, gratitud y respeto.

Evelyn Cristina Faican Jiménez.

A mis padres Luis y Judith que están en el cielo, por ser el cimiento de mi vida y mi mayor ejemplo de constancia.

A mi esposa Alicia, por su paciencia infinita, su amor incondicional y por ser mi refugio en los días de mayor presión.

A mis hijos, para demostrarles que nunca es tarde para aprender y que los sueños se alcanzan con disciplina.

Luis Enrique Moyano Espinoza

Dedico este trabajo, en primer lugar, a Dios, por ser mi guía en cada paso de este camino, por darme fortaleza en los momentos difíciles y por permitirme alcanzar una meta tan importante en mi vida.

A mis padres, por su amor incondicional, sus enseñanzas, su esfuerzo y su apoyo constante. Gracias por ser el pilar fundamental de mi formación personal y profesional, por creer en mí y motivarme siempre a seguir adelante.

A mi esposo, por su amor, paciencia y comprensión durante este camino. Gracias por estar a mi lado, por apoyarme en los momentos de cansancio y dificultad, por animarme a no rendirme y por ser una fuente constante de motivación para culminar esta etapa tan importante de mi vida.

A mi familia, por acompañarme a lo largo de este proceso, por sus palabras de aliento, su cariño y su confianza en cada etapa de este logro.

Y finalmente, me la dedico a mí misma, por la constancia, el esfuerzo y la perseverancia demostrados durante este proceso, por no desistir ante los desafíos y por luchar con dedicación para alcanzar una meta más en mi vida profesional.

Pamela Estefania Paredes León

Este trabajo, como cada uno de mis logros, está dedicado a Dios y a mi familia, porque son quienes, con amor, fe y apoyo incondicional, han guiado cada una de mis decisiones y me han acercado a mi propósito de vida.

A ellos les debo la fortaleza para perseverar, la inspiración para seguir creciendo y la certeza de que cada meta alcanzada tiene un significado mayor cuando se comparte con quienes más amamos.

Roldán Vallejos Diana Patricia

"Darkest nights make the brightest stars;" "Feel the wxndz."

- ***Farid Galecio***

Concluir este trabajo de investigación y alcanzar un nuevo hito académico en mi vida me permite mirar hacia atrás y reconocer que nada de lo que he logrado habría sido posible sin el amor, la entrega y el apoyo incondicional de mis padres, el Ing. Henry Mangoni Rosales Mafla y la Dra. Georgia Rocío Vizcarra Vázcones. A ellos les debo mucho más que la oportunidad de acceder a una formación de cuarto nivel, les debo la confianza que han depositado en mí, las enseñanzas que han guiado cada una de mis decisiones y la convicción de que todo sueño puede convertirse en realidad cuando se cuenta con personas que creen en uno, incluso antes de que los demás puedan hacerlo.

A lo largo de mi vida, sobre todo en el ámbito profesional, nunca han existido ideas demasiado grandes, proyectos demasiado ambiciosos o metas demasiado lejanas para mis padres. Ante cada iniciativa, por más compleja, arriesgada o incluso descabellada que pudiera parecer, ellos siempre han estado presentes, brindándome su respaldo, su consejo y, sobre todo, su confianza inquebrantable. Han sido mi refugio en los momentos de incertidumbre, mi impulso en las etapas de mayor exigencia y el ejemplo permanente de esfuerzo, perseverancia y amor incondicional. Son las únicas personas que admiro profundamente con devoción y tenerlos a mi lado constituye, sin lugar a dudas, uno de los mayores privilegios y bendiciones de mi vida.

Las palabras resultan insuficientes para expresar la magnitud de mi gratitud y las acciones jamás serán capaces de compensar todo aquello que hacen por mí cada día. Sé que me faltará la vida entera para agradecerles plenamente cada sacrificio, cada desvelo, cada consejo y cada oportunidad que me han brindado con absoluta generosidad. Este logro también les pertenece, porque en cada página de esta investigación se encuentra el reflejo de los valores, principios y enseñanzas que me han transmitido. Con el más profundo amor, admiración y respeto, les dedico estas líneas a quienes considero, sin la menor duda, los mejores padres del mundo.

Paúl Alejandro Rosales Vizcarra

Dedico este trabajo a todas las personas que han creído en mí y me han acompañado en este camino. De manera especial, lo dedico a mi hija, quien representa mi mayor motivación y la razón por la que cada

esfuerzo vale la pena. Que este logro sea un ejemplo de que la perseverancia, la disciplina y la pasión por aprender permiten alcanzar las metas más importantes.

Finalmente, me dedico este logro a mí misma, por la constancia, el sacrificio y la determinación demostrados a lo largo de este proceso, recordando que cada desafío superado ha contribuido a mi crecimiento y a la construcción de nuevos sueños y oportunidades.

Raisa Natalia Vaca Villamara

AGRADECIMIENTOS

Expreso mi más profundo agradecimiento a todas las personas que hicieron posible la culminación de esta etapa académica y profesional.

Agradezco a Dios por concederme salud, sabiduría y fortaleza para afrontar los retos que surgieron a lo largo de este proceso de formación y por permitirme alcanzar esta meta con satisfacción y orgullo.

Mi sincero reconocimiento a la institución, autoridades, docentes y tutores de la Maestría en Protección de Datos Personales, por su dedicación, profesionalismo y compromiso con la formación de sus estudiantes. Sus enseñanzas, orientación y experiencia contribuyeron significativamente a mi crecimiento académico y al desarrollo de este trabajo de investigación.

A mis compañeros de maestría, gracias por compartir conocimientos, experiencias y momentos de aprendizaje que enriquecieron esta trayectoria. El compañerismo, el intercambio de ideas y el apoyo mutuo hicieron de este camino una experiencia más valiosa y enriquecedora.

A mi familia y seres queridos, gracias por comprender las exigencias de este proceso, por su respaldo incondicional y por motivarme a continuar incluso en los momentos de mayor dificultad.

Finalmente, agradezco a todas aquellas personas que, de manera directa o indirecta, aportaron con su apoyo, orientación y confianza para que este objetivo pudiera concretarse. Cada contribución fue importante para alcanzar este logro que hoy culmina una etapa de crecimiento personal, académico y profesional.

Con gratitud y aprecio:

Evelyn Cristina Faican Jiménez

A la UIDE y cuerpo docente:

Por brindarme las herramientas académicas necesarias para crecer profesionalmente.

A Sandrita: Por su guía experta, su paciencia y su rigor científico durante todo este proceso de investigación.

A mi grupo de maestría: Por los debates compartidos, las noches de desvelo y el apoyo mutuo.

A Dios: Por darme la salud y la fortaleza mental para culminar con éxito este peldaño académico.

Luis Enrique Moyano Espinoza

Expreso mi más profundo agradecimiento a Dios, por brindarme sabiduría, fortaleza y constancia a lo largo de este camino, y por permitirme culminar una etapa tan importante en mi vida académica y profesional.

A mis padres y a mi familia, por su amor, apoyo incondicional, paciencia y confianza en cada momento. Gracias por ser mi motivación constante, por acompañarme en los momentos de esfuerzo y por impulsarme siempre a seguir adelante.

A mi esposo, por su amor, comprensión y apoyo permanente durante este proceso. Gracias por estar a mi lado, por alentarme en los momentos de dificultad y por ser parte fundamental de este logro.

A mis docentes, por compartir sus conocimientos, experiencias y enseñanzas, las cuales han contribuido de manera significativa a mi formación profesional y al desarrollo de este trabajo de investigación.

Finalmente, agradezco a todas las personas que, de una u otra manera, formaron parte de este camino y contribuyeron con su apoyo, consejos y motivación para la culminación de esta meta.

Pamela Estefania Paredes León

Agradezco a la Universidad, a su cuerpo docente y a los valiosos profesionales que acompañaron este proceso, por sus enseñanzas, guía e inspiración para continuar mi formación académica y profesional.

Diana Patricia Roldán Vallejos

"La verdadera fuerza está en la disciplina y en construir una rutina inquebrantable de poder elegir cada día el progreso sobre la comodidad".

- *Ana Lucía Leones Lucas*

La culminación del presente trabajo representa el resultado de un esfuerzo colectivo marcado por el compromiso, la dedicación y la convicción compartida de construir conocimiento desde la reflexión crítica y el trabajo en equipo. Expreso, por consiguiente, mi más profundo agradecimiento a mis compañeros de grupo, con quienes tuve el privilegio de recorrer este proceso de investigación, intercambiando ideas, afrontando desafíos y alcanzando cada objetivo con responsabilidad, respeto y entusiasmo. La experiencia compartida deja, además de un producto académico, valiosas enseñanzas y la satisfacción de haber crecido juntos en el ámbito profesional y humano.

De igual manera, manifiesto mi sincero reconocimiento a los docentes de la presente maestría que, con su experiencia, exigencia académica y permanente acompañamiento, enriquecieron significativamente nuestro aprendizaje y nos impulsaron a desarrollar una visión más profunda y rigurosa de la protección de datos personales. Extiendo de igual forma, mi gratitud a la Universidad Internacional del Ecuador por constituirse en

un espacio de excelencia académica que promueve el pensamiento crítico, el intercambio de conocimientos y la formación integral de profesionales comprometidos con la investigación, la ética y la transformación de la sociedad.

Paúl Alejandro Rosales Vizcarra

A Dios, por guiar cada uno de mis pasos, darme fortaleza en los momentos de dificultad y permitirme culminar esta importante etapa de crecimiento personal y profesional.

A mi familia, por su amor incondicional, comprensión y apoyo constante durante este proceso. Gracias por ser mi inspiración diaria y por impulsarme a seguir adelante incluso en los momentos más desafiantes.

A mis docentes y compañeros de maestría, por compartir sus conocimientos, experiencias y enseñanzas, contribuyendo significativamente a mi formación académica y humana.

Raisa Natalia Vaca Villamara

RESUMEN

La presente investigación determina que la implementación de sistemas de inteligencia artificial para el tratamiento de datos personales sensibles y biométricos en el ámbito sanitario constituye un escenario de elevado riesgo, debido a su impacto directo en derechos fundamentales como la privacidad, la igualdad, la no discriminación y la protección de la salud. Si bien estas herramientas tecnológicas pueden favorecer la eficiencia en la gestión de la información clínica y servir como apoyo en la toma de decisiones médicas, presentan limitaciones importantes relacionadas con la falta de transparencia en sus procesos, la dependencia de la calidad de los datos y la posibilidad de generar errores o resultados sesgados.

De igual forma, el análisis normativo evidencia que la Ley Orgánica de Protección de Datos Personales exige la aplicación estricta de principios y garantías reforzadas, junto con la implementación de medidas técnicas, organizativas y jurídicas idóneas. Sin embargo, la ausencia de controles adecuados incrementa la probabilidad de riesgos como accesos no autorizados, pérdida o alteración de información clínica y la emisión de decisiones automatizadas incorrectas.

Asimismo, se establece que la supervisión humana es indispensable en el ámbito sanitario, mientras que los mecanismos de evaluación de impacto, auditoría y monitoreo permanente constituyen instrumentos clave para la gestión de los riesgos asociados a estas tecnologías. De igual manera, la calidad, integridad y representatividad de los datos influyen de manera directa en la confiabilidad de los resultados, pudiendo ocasionar situaciones de discriminación si no se gestionan adecuadamente.

Finalmente, se concluye que, en las condiciones actuales analizadas, la implementación de sistemas de inteligencia artificial para el tratamiento de datos biométricos y de salud en el Hospital Oncológico Vida Nueva **no resulta jurídicamente viable**, debido a la insuficiencia de garantías que permitan asegurar la protección integral de los derechos de los titulares.

Palabras clave: Inteligencia Artificial, Protección de Datos Personales, Datos Biométricos, Datos de Salud, Evaluación de Impacto en la Protección de Datos Personales (EIPD)

ABSTRACT

This research determines that the implementation of artificial intelligence systems for the processing of sensitive personal data and biometric data in the healthcare sector constitutes a high-risk scenario due to its direct impact on fundamental rights such as privacy, equality, non-discrimination, and health protection. Although these technological tools may improve the efficiency of clinical information management and support medical decision-making processes, they present significant limitations related to the lack of transparency in their operation, dependence on data quality, and the possibility of generating errors or biased outcomes.

The legal analysis conducted reveals that the Ecuadorian Organic Law on Personal Data Protection (Ley Orgánica de Protección de Datos Personales – LOPDP) requires the strict application of data protection principles, enhanced safeguards, and the implementation of appropriate technical, organizational, and legal measures. However, the absence of adequate controls increases the likelihood of risks such as unauthorized access, loss or alteration of clinical information, and inaccurate automated decision-making.

Furthermore, the study establishes that human oversight is essential in healthcare environments, while data protection impact assessments, audits, and continuous monitoring constitute key mechanisms for managing the risks associated with artificial intelligence technologies. Likewise, the quality, integrity, and representativeness of the data directly influence the reliability of the results and may lead to discriminatory effects if not properly managed.

Finally, the research concludes that, under the conditions analyzed, the implementation of artificial intelligence systems for the processing of biometric and health data at the Hospital Oncológico Vida Nueva is not legally viable, due to the insufficiency of safeguards required to ensure the comprehensive protection of data subjects' fundamental rights.

Keywords: Artificial Intelligence, Personal Data Protection, Biometric Data, Health Data, Data Protection Impact Assessment (DPIA)

TABLA DE CONTENIDOS

CAPITULO I

1. INTRODUCCIÓN

La transformación digital ha modificado profundamente la forma en que las organizaciones recopilan procesa y utilizan información personal. En este contexto, el desarrollo de tecnologías basadas en inteligencia artificial (IA) y sistemas biométricos ha generado nuevas oportunidades para optimizar procesos de identificación, autenticación y acceso a servicios, particularmente en sectores que manejan grandes volúmenes de información sensible, como es el sector de la salud. Sin embargo, estos avances tecnológicos también plantean importantes desafíos jurídicos y éticos relacionados con la protección de datos personales, la privacidad, la seguridad de la información y el respeto de los derechos fundamentales de los titulares.

El desarrollo de tecnologías biométricas plantea una particular complejidad jurídica porque utiliza rasgos físicos, fisiológicos o conductuales que permiten identificar o autenticar de manera unívoca a una persona. A diferencia de otros mecanismos de seguridad, como contraseñas, credenciales o tokens, los datos biométricos poseen una conexión directa con la identidad corporal del titular y presentan un carácter difícilmente sustituible en caso de una vulneración. Esta característica incrementa significativamente el nivel de riesgo del tratamiento, especialmente cuando la biometría se vincula con información clínica, diagnósticos, antecedentes médicos, resultados de laboratorio, tratamientos y demás datos propios de la relación sanitaria.

En el ámbito sanitario frente a lo antes expuesto, la utilización de sistemas biométricos para el acceso a historias clínicas electrónicas, la identificación de pacientes y profesionales de la salud, así como la gestión de servicios médicos, supone el tratamiento simultáneo de

datos biométricos y datos relativos a la salud, categorías que reciben una protección reforzada dentro del ordenamiento jurídico ecuatoriano. La especial sensibilidad de esta información, sumada al carácter irreversible de los datos biométricos y a los riesgos asociados al uso de sistemas de IA, exige un análisis riguroso que permita determinar si tales tratamientos resultan compatibles con los principios de licitud, necesidad, proporcionalidad, minimización, transparencia, seguridad y responsabilidad proactiva previstos en la normativa de protección de datos personales.

La promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP) y la posterior emisión de su Reglamento General consolidaron en Ecuador un régimen jurídico orientado a garantizar el control de las personas sobre su información personal. No obstante, la aplicación práctica de estas disposiciones frente a tecnologías emergentes continúa generando importantes interrogantes, especialmente cuando se trata de tratamientos de alto riesgo que involucran decisiones automatizadas, sistemas biométricos e IA. En consecuencia, las organizaciones se enfrentan al desafío de equilibrar los beneficios derivados de la innovación tecnológica con la obligación de proteger los derechos fundamentales de las personas.

La presente investigación toma como punto de partida el caso de “BioTrust”, organización integradora que provee servicios biométricos a entidades públicas y privadas mediante sistemas de captura, plantillas biométricas, motores de IA, detección de vida, antifraude y mecanismos de verificación. Dentro de este escenario, el estudio se delimita al “Hospital Oncológico Vida Nueva”, entidad sanitaria ficticia ubicada en el contexto ecuatoriano, que analiza la posibilidad de implementar un reconocimiento facial como mecanismo de autenticación para el acceso a historias clínicas electrónicas y otros recursos institucionales. A partir de este escenario, se examinan los requisitos normativos aplicables,

los riesgos asociados al tratamiento de datos biométricos y de salud, las obligaciones de gobernanza exigidas a los responsables del tratamiento y la pertinencia de aplicar mecanismos preventivos como la Evaluación de Impacto en la Protección de Datos Personales (EIPD).

La precitada problemática adquiere mayor intensidad cuando el tratamiento biométrico se combina con sistemas de IA. Estas herramientas pueden aportar valor en determinados contextos sanitarios, particularmente cuando permiten mejorar diagnósticos, apoyar decisiones clínicas o identificar patrones complejos que no podrían obtenerse mediante métodos tradicionales. No obstante, también pueden generar riesgos asociados a la opacidad algorítmica, sesgos, errores de identificación, decisiones automatizadas y pérdida de control efectivo sobre la información personal. Por consiguiente, su incorporación en entornos hospitalarios exige un análisis reforzado de necesidad, proporcionalidad, minimización, transparencia, seguridad, supervisión humana y responsabilidad proactiva.

El objetivo principal de la presente investigación consiste, por lo tanto, en determinar la viabilidad jurídica y la conveniencia del uso de sistemas biométricos en el sector de la salud, específicamente en el Hospital Oncológico Vida Nueva, a la luz del marco constitucional ecuatoriano, la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la normativa emitida por la Superintendencia de Protección de Datos Personales y los estándares internacionales aplicables. Para ello, se analizan las bases de legitimación del tratamiento, la naturaleza jurídica de los datos biométricos, los riesgos derivados de la IA, los posibles impactos sobre los derechos fundamentales y las medidas de mitigación que podrían implementarse bajo el enfoque de privacidad desde el diseño y por defecto.

Finalmente, este trabajo busca aportar criterios jurídicos y prácticos que permitan a las organizaciones adoptar decisiones informadas respecto del uso de tecnologías biométricas e IA en entornos de alto riesgo. De esta manera, la investigación pretende demostrar que la protección de datos personales no constituye un obstáculo para la innovación tecnológica, sino una condición esencial para su desarrollo responsable, sostenible y respetuoso de los derechos fundamentales de las personas.

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.

Una entidad del sector de la salud, como un hospital quiere acceso a historias clínicas mediante el uso de rostros: la finalidad (seguridad y trazabilidad) es legítima, pero la pregunta es si la biometría es necesaria o si existen alternativas menos intrusivas. La historia clínica implica datos altamente sensibles; por eso, un error de autenticación (falso positivo) o una filtración tendría consecuencias clínicas y reputacionales severas.

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 se delimita epistemológicamente en el campo del derecho a la protección de datos personales aplicado a tecnologías biométricas e inteligencia artificial (IA) en el sector de la salud, específicamente. "La legislación sobre protección de datos personales en el ámbito sa-nitario aún no está completamente desarrollada, lo que genera incertidumbre sobre cómo manejar los datos sensibles cuando se emplean tecnologías basadas en IA" (Marcos Lalama y otros, 2025, p. 4). No se analizará a continuación, por consiguiente, la biometría como una herramienta aislada de autenticación, ni la IA como una innovación neutral, sino como tratamientos de alto riesgo que pueden incidir sobre datos de salud, datos biométricos, historias clínicas, inferencias automatizadas y decisiones con impacto en derechos fundamentales. Esta delimitación responde al caso *BioTrust*, en el que se advierte que el desafío no es únicamente técnico, sino correspondiente a protección de datos personales, gobernanza de terceros y control del riesgos.

La delimitación espacial por su parte se circunscribe exclusivamente en el denominado "Hospital Oncológico Vida Nueva" como organización hospitalaria que trata datos sensibles en procesos clínicos, administrativos y tecnológicos, como una entidad sanitaria ficticia dentro del territorio ecuatoriano, y no al sector de la salud en abstracto. Esta precisión permite identificar tratamientos concretos, tales como acceso a historias clínicas, diagnósticos asistido por IA, telemedicina, gestión de consultas, transmisión de datos

clínicos, recetas electrónicas, seguimiento remoto de pacientes y almacenamiento de grabaciones sensibles.

La delimitación temporal finalmente, se ubica en el marco ecuatoriano vigente en materia de protección de datos personales, el cual comprende el rango de 2021, al mes de mayo de 2026 específicamente, con especial énfasis en la emisión de la Ley Orgánica de Protección de Datos Personales (en adelante, LOPDP), debidamente expedida el veintiséis (26) de mayo de 2021; su Reglamento General, emitido el trece (13) de noviembre de 2023; las resoluciones emitidas por la respectiva Autoridad de protección de Datos Personales, la Superintendencia de protección de Datos Personales (SPDP), específicamente aquellas que tratan los siguientes temas: Gestión de Riesgos y Evaluación de Impacto, Tratamientos de Datos Personales a Gran Escala, el Reglamento del Delegado de Protección de Datos Personales (DPD) y; Transferencias y Uso de Sistemas de IA para la Garantía del Derecho a la Protección de Datos Personales. Este período resulta relevante debido a la consolidación del régimen ecuatoriano de protección de datos personales aplicable al tratamiento de datos biométricos y tecnologías emergentes.

En definitiva, el problema queda delimitado como una pregunta de viabilidad jurídica condicionada. La presente investigación no pretende, por consiguiente, afirmar que toda IA empleada y ejecutada en el sector de la salud sea inadmisible, ni que toda biometría sea ilegítima, sino determinar bajo qué condiciones el tratamiento puede superar los estándares de necesidad, proporcionalidad, minimización, seguridad, explicabilidad, supervisión humana y responsabilidad proactiva y demostrada.

2.2. Justificación

La presente investigación en primer lugar se justifica jurídicamente porque el tratamiento de datos biométricos y de salud, dentro de un hospital, compromete categorías especialmente

protegidas y exige un estándar reforzado de cumplimiento. En este contexto, el estudio permite examinar la aplicación de principios como la responsabilidad proactiva y demostrada, proporcionalidad, minimización, privacidad desde el diseño y evaluación de impacto, contribuyendo a determinar bajo qué condiciones el uso de tecnologías biométricas e IA puede resultar jurídicamente viable dentro del ordenamiento ecuatoriano. No obstante, frente a lo expuesto cabe mencionar que, “Aunque la LOPDP cubre aspectos fundamentales de la protección de datos, no proporciona directrices claras sobre el tratamiento de datos en sistemas automatizados impulsados por IA” (Michelle Iñiguez y Luis Maldonado, 2025, p. 30).

La justificación social en segundo lugar se encuentra en la necesidad de proteger la intimidad, dignidad, igualdad y autonomía de pacientes oncológicos o personas que acuden a servicios de salud en condiciones de especial vulnerabilidad. Por consiguiente, “Se impone la misión de aprender a usar algo novedoso y que aún no se domina, para abordar una subjetividad o un conjunto de subjetividades que no se manifiestan como transparentes desde el comienzo” (Susana Otero y otros, 2025, p. 142). En el presente caso hospitalario, una filtración o un acceso indebido no afectaría únicamente un dato aislado, sino información clínica que puede revelar diagnósticos, tratamientos, antecedentes y condiciones personales sensibles. Inclusive, se ha advertido que “la IA aplicada a la salud puede generar beneficios significativos en términos de eficiencia y precisión diagnóstica, pero también puede producir efectos adversos cuando no se encuentra adecuadamente regulada” (Diana Sanabria, 2025, p. 9) particularmente en lo relativo a sesgos algorítmicos y desigualdad en el acceso a servicios médicos.

La justificación tecnológica por otro lado se sostiene en que la transformación digital del sector salud es una realidad institucional, pero su avance requiere seguridad, interoperabilidad, gobernanza de datos y capacidades organizacionales suficientes. La

Organización Mundial de la Salud, frente a lo expuesto ha señalado que la IA puede mejorar la calidad de la atención médica, siempre que su implementación se realice bajo principios de seguridad, transparencia y supervisión humana (2021). Este planteamiento refuerza la idea de que la tecnología no es problemática en sí misma, sino en la forma en que se integra dentro de estructuras institucionales que garanticen su control efectivo.

La justificación política e institucional por su parte, radica en que el cumplimiento normativo puede convertirse en un factor de confianza pública y sostenibilidad organizacional. Por consiguiente, la presente investigación no se limita a describir normas, sino a generar valor desde la perspectiva jurídica correspondiente a la materia tratada, incorporando análisis de riesgos, impacto en el negocio, madurez institucional, próximos pasos y recomendaciones que permitan viabilizar el proyecto. La Política Nacional de Transformación Digital del Sector Salud, debidamente emitida por el Ministerio de Salud Pública en el año 2024, reconoce la necesidad de incorporar tecnologías digitales para mejorar la calidad y el acceso a los servicios, pero también advierte que estos procesos deben desarrollarse bajo estándares de seguridad, interoperabilidad y protección de datos personales. En consecuencia, el estudio contribuye a evaluar si las instituciones cuentan con la capacidad normativa y organizacional necesaria para implementar inteligencia artificial sin comprometer derechos fundamentales, lo que resulta clave para la formulación de políticas públicas sostenibles.

Finalmente, desde una perspectiva económica, la investigación permitirá comprender que la implementación de tecnologías biométricas y de IA no únicamente implica beneficios potenciales, sino también costos asociados a cumplimiento normativo, gestión de riesgos y seguridad de la información. Una implementación deficiente puede generar costos regulatorios, sanciones, pérdida reputacional, interrupción de servicios y afectación a la confianza de pacientes. En consecuencia, invertir en una evaluación de impacto, gobernanza, capacitación, controles de acceso, auditorías y respuestas ante incidentes

resulta menos gravoso que enfrentar una vulneración de datos biométricos o clínicos sin la capacidad institucional de obtener respuesta eficiente. Por ello, la justificación del presente estudio radica también en la necesidad de demostrar que la protección de datos personales no constituye un obstáculo para la innovación, sino una condición indispensable para su sostenibilidad.

2.3. Problemas jurídicos

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

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

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

2.4. Objetivos

2.4.1 Objetivo general

Determinar la viabilidad jurídica y la conveniencia del uso de sistemas de biometría en la organización Hospital Oncológico Vida Nueva, a la luz de la normativa y principios de protección de datos personales, a fin de formular una conclusión jurídica fundamentada

sobre la viabilidad, no viabilidad o viabilidad condicionada y elaborar recomendaciones conforme al principio de privacidad desde el diseño y por defecto, incluso para el supuesto de que la organización decida avanzar pese a un resultado negativo de la EIPD.

2.4.2 Objetivos específicos

1. Evaluar el marco normativo aplicable al tratamiento de datos biométricos mediante sistemas de biometría, identificando las bases jurídicas que podrían legitimar su uso por parte de la organización Hospital Oncológico Vida Nueva, considerando tanto la legislación general de protección de datos como la normativa sectorial correspondiente.

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

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

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

3. FUNDAMENTOS TEÓRICOS

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

La privacidad es considerada un derecho fundamental inherente a toda persona, estrechamente vinculado con la dignidad humana, la libertad individual y el libre desarrollo de la personalidad (Organización de las Naciones Unidas, 1948). Este derecho permite a cada individuo mantener control sobre su información personal, decidir quién puede acceder a ella y limitar injerencias arbitrarias tanto por parte de particulares como de entidades públicas. En este sentido, la privacidad no solo protege la vida íntima de las personas, sino que también garantiza su autonomía dentro de una sociedad cada vez más digitalizada (Constitución de la República del Ecuador, 2008).

Con el crecimiento acelerado de las tecnologías de la información y la comunicación, el concepto tradicional de privacidad evolucionó hacia la protección de datos personales. Esta nueva dimensión responde a la necesidad de regular el tratamiento de información que identifica o hace identificable a una persona natural, estableciendo principios y obligaciones orientados a garantizar que los datos sean tratados de manera lícita, transparente, segura y proporcional (Organización para la Cooperación y el Desarrollo Económicos, 2013). La digitalización de procesos, el comercio electrónico, el uso de redes sociales y la automatización de servicios han incrementado significativamente la exposición de información personal, haciendo indispensable la creación de mecanismos de control y protección (Abad Arévalo y otros., 2023).

A nivel internacional, la protección de datos personales ha adquirido especial relevancia mediante la creación de normativas específicas. Uno de los principales referentes es el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, vigente desde

2018, el cual estableció estándares rigurosos relacionados con consentimiento informado, responsabilidad proactiva, gestión de incidentes de seguridad y ejercicio de derechos de los titulares (Unión Europea, 2016). Su influencia ha trascendido el ámbito europeo, convirtiéndose en un modelo normativo para múltiples jurisdicciones alrededor del mundo.

En América Latina, diversos países han desarrollado legislaciones específicas en materia de protección de datos, inspiradas principalmente en estándares europeos pero adaptadas a sus realidades jurídicas y sociales. Países como Argentina, Brasil, Colombia y México cuentan con marcos regulatorios consolidados y autoridades encargadas de supervisar el cumplimiento de obligaciones relacionadas con el tratamiento de datos personales (Lara Santana, 2023). Este avance regional responde al incremento del intercambio digital de información y a la necesidad de brindar mayores garantías a los ciudadanos frente al uso masivo de datos.

En el Ecuador, el desarrollo normativo sobre protección de datos personales se consolidó de manera más reciente respecto a otros países de la región. No obstante, la Constitución de la República de 2008 ya reconocía derechos vinculados a la intimidad, privacidad y control de información personal (Constitución de la República del Ecuador, 2008). Posteriormente, con la promulgación de la LOPDP en el año 2021, se estableció un marco jurídico integral que regula el tratamiento de datos en instituciones públicas y privadas, incorporando principios como legalidad, transparencia, finalidad, minimización, exactitud, confidencialidad e integridad (Ley Orgánica de Protección de Datos Personales, 2021).

Además, esta normativa reconoce derechos fundamentales para los titulares de datos, entre ellos acceso, rectificación, actualización, eliminación, oposición, portabilidad y suspensión del tratamiento. La incorporación de estos derechos busca fortalecer el control de las

personas sobre su información y promover una cultura organizacional basada en responsabilidad y cumplimiento normativo (Apolo y López, 2024). En sectores sensibles como salud, banca, telecomunicaciones y educación, la aplicación de estas disposiciones resulta especialmente relevante debido al manejo de grandes volúmenes de información confidencial.

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

En Ecuador, la protección de datos personales constituye un desafío emergente, considerando que durante varios años el tratamiento de información personal se desarrolló sin contar con una regulación específica y completa. Si bien la promulgación de la LOPDP representó un avance importante dentro del marco jurídico nacional, su aplicación efectiva todavía enfrenta dificultades vinculadas al nivel de preparación institucional, conocimiento técnico y cultura organizacional (Ley Orgánica de Protección de Datos Personales, 2021; Lara Santana, 2023).

Uno de los principales obstáculos identificados es el escaso conocimiento sobre la relevancia de la privacidad y el manejo adecuado de datos personales. En muchas instituciones públicas y privadas aún se percibe esta materia como un requisito exclusivamente legal o documental, limitándose al cumplimiento formal mediante elaboración de políticas, sin una implementación real dentro de sus procesos operativos. De igual forma, gran parte de la población desconoce los derechos que la normativa reconoce respecto a su información personal, lo cual limita la capacidad de exigir protección y control sobre sus datos (Apolo y López, 2024).

Otro aspecto crítico radica en las limitaciones técnicas, económicas y operativas que presentan muchas organizaciones para adecuarse a las exigencias normativas. La

implementación de un sistema efectivo de protección de datos requiere inversiones en tecnología, controles de seguridad, organización documental, clasificación de información, capacitación constante del personal y establecimiento de procedimientos para gestionar incidentes de seguridad. Sin embargo, numerosas instituciones, especialmente pequeñas y medianas, carecen de recursos financieros y talento especializado para cumplir adecuadamente estas obligaciones (Abad Arévalo y otros, 2023).

El avance de la digitalización en sectores estratégicos también incrementa significativamente los riesgos asociados al tratamiento de información personal. Áreas como salud, banca, educación y telecomunicaciones gestionan grandes volúmenes de datos sensibles, cuya exposición o uso inadecuado podría afectar gravemente los derechos de las personas. En particular, el sector salud enfrenta retos importantes debido al manejo de historias clínicas, diagnósticos médicos, resultados de laboratorio y datos biométricos, información que requiere niveles reforzados de confidencialidad y seguridad (Ley Orgánica de Protección de Datos Personales, 2021).

A esto se suma el uso creciente de servicios tercerizados, almacenamiento en la nube y plataformas tecnológicas externas, lo que genera desafíos adicionales en relación con el control y supervisión del tratamiento de datos. En varios casos, las organizaciones comparten información con proveedores externos sin contar con contratos adecuados, cláusulas de confidencialidad o mecanismos de monitoreo suficientes, incrementando riesgos legales, reputacionales y operativos (Organización para la Cooperación y el Desarrollo Económicos, 2013).

De igual manera, resulta necesario fortalecer una cultura institucional orientada al cumplimiento y gobernanza de datos. La protección de datos personales no debe concebirse únicamente como una obligación normativa, sino como una práctica estratégica vinculada a

la confianza organizacional, reputación institucional y responsabilidad corporativa. Para ello, es indispensable incorporar políticas internas, evaluaciones periódicas de riesgos, auditorías y programas de sensibilización dirigidos al personal (Lara Santana, 2023; Abad Arévalo y otros, 2023).

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

La evolución tecnológica ha transformado significativamente el sector de la salud, permitiendo perfeccionar diagnósticos, automatizar procesos clínicos y mejorar la atención médica mediante el uso de herramientas basadas en inteligencia artificial (IA). Actualmente, hospitales, clínicas, laboratorios entre otros utilizan sistemas inteligentes capaces de analizar grandes volúmenes de información médica, identificar patrones y apoyar en la toma de decisiones clínicas. Sin embargo, este avance tecnológico también genera importantes desafíos en materia de protección de datos personales, especialmente debido a la sensibilidad de la información relacionada con la salud de las personas (Russell & Norvig, 2021).

Los datos de la salud constituyen una categoría especial de datos personales debido a que contienen información sensible sobre el estado físico y mental de las personas, historias clínicas, diagnósticos, tratamientos, resultados de laboratorio, información genética y biométrica son datos altamente sensibles cuyo tratamiento indebido puede afectar derechos fundamentales como la privacidad, la dignidad y la no discriminación. En consecuencia, el uso de IA en el sector de la salud exige niveles reforzados de protección jurídica y técnica (Solove, 2021).

En el contexto ecuatoriano, la LOPDP reconoce a los datos relativos a la salud como datos sensibles y establece obligaciones específicas para su tratamiento. Entre los principios aplicables destacan la licitud, finalidad, proporcionalidad, confidencialidad y minimización de datos. Estos principios cobran especial relevancia en sistemas de IA utilizados en hospitales y plataformas digitales de salud, donde frecuentemente se procesan grandes cantidades de información para entrenar algoritmos predictivos y modelos de aprendizaje automático (Tene & Polonetsky, 2013).

La inteligencia artificial en el sector de la salud ofrece importantes beneficios. Por ejemplo, puede facilitar diagnósticos tempranos mediante análisis de imágenes médicas, detectar patrones epidemiológicos, optimizar la asignación de recursos hospitalarios y personalizar tratamientos conforme a las características de cada paciente. Asimismo, herramientas de IA pueden contribuir al desarrollo de medicina predictiva y preventiva, incrementando la eficiencia de los sistemas de salud (Topol, 2019).

No obstante, el uso de IA en el sector de la salud también plantea riesgos significativos. Uno de los principales problemas es la toma de decisiones automatizadas basadas en algoritmos que podrían generar sesgos o discriminación. Si los sistemas son entrenados con bases de datos incompletas o no representativas, podrían producir diagnósticos erróneos o tratamientos diferenciados que afecten negativamente a ciertos grupos poblacionales. Esto resulta particularmente delicado cuando las decisiones médicas impactan directamente en la vida y salud de los pacientes (Mittelstadt et al., 2016).

Adicionalmente, existe el riesgo de accesos no autorizados, filtraciones o uso indebido de información médica. Las bases de datos sanitarias son objetivos frecuentes de ciberataques debido al alto valor económico y estratégico de la información clínica. Por ello, las instituciones de salud deben implementar medidas técnicas y organizativas robustas, tales

como cifrado, controles de acceso, anonimización, seudonimización, auditorías periódicas y protocolos de seguridad de la información (Cavoukian, 2011).

Desde una perspectiva normativa, tanto la LOPDP como el Reglamento General de Protección de Datos exigen transparencia respecto al tratamiento automatizado de datos y reconocen derechos relacionados con decisiones automatizadas y elaboración de perfiles. En el sector de la salud, esto implica que los pacientes deben ser informados sobre el uso de sistemas de IA, las finalidades del tratamiento, los riesgos asociados y los mecanismos para ejercer sus derechos de acceso, rectificación, oposición y eliminación de datos (Voigt & Von dem Bussche, 2017).

Asimismo, el principio de "privacidad desde el diseño y por defecto" (*privacy by design and by default*) adquiere especial importancia en el desarrollo de tecnologías en el ámbito de la salud. Las aplicaciones médicas y plataformas de telemedicina deben incorporar mecanismos de protección de datos desde las primeras etapas de diseño, garantizando que únicamente se recolecta la información estrictamente necesaria y que exista supervisión humana sobre las decisiones automatizadas (Cavoukian, 2011).

A nivel internacional, organismos como la *World Health Organization* y el *National Institute of Standards and Technology* (NIST) han promovido lineamientos éticos y técnicos para el uso responsable de IA en el sector de la salud, enfatizando la necesidad de garantizar transparencia, seguridad, equidad y protección de los derechos humanos en el desarrollo de estas tecnologías (NIST, 2023).

La inteligencia artificial representa una herramienta con enorme potencial para transformar positivamente el sector de la salud; sin embargo, su implementación debe realizarse bajo estrictos estándares de protección de datos personales y ética digital. La innovación tecnológica no puede desvincularse de la obligación de proteger la privacidad y dignidad de

los pacientes. Por ello, el desafío actual consiste en equilibrar los beneficios de la IA con mecanismos efectivos de gobernanza, seguridad y responsabilidad que permitan un uso confiable y humano de las tecnologías sanitarias.

3.4. Biometría: aproximación conceptual y jurídica

3.4.1. Sistemas biométricos y datos biométricos

La incorporación de tecnologías biométricas en el sector de la salud ha transformado significativamente la forma en que se identifican pacientes, profesionales de la salud y usuarios de servicios médicos. Los hospitales, clínicas y plataformas de telemedicina utilizan cada vez con mayor frecuencia sistemas biométricos para controlar accesos, autenticar identidades, proteger historias clínicas electrónicas y optimizar procesos asistenciales. No obstante, debido a la naturaleza sensible de los datos biométricos, su tratamiento implica importantes desafíos jurídicos, éticos y de protección de datos personales.

La biometría puede definirse como el conjunto de técnicas y procedimientos tecnológicos destinados a identificar o verificar la identidad de una persona mediante características físicas, fisiológicas o conductuales únicas. Estos sistemas funcionan mediante la captura, procesamiento y comparación de patrones biométricos que permiten individualizar a una persona con altos niveles de precisión (Jain, Ross, & Prabhakar, 2004).

Los datos biométricos constituyen información personal obtenida a partir de un tratamiento técnico específico relacionado con características físicas, fisiológicas o conductuales de una persona natural, que permiten o confirman su identificación única. En el ámbito sanitario, estos datos pueden utilizarse para acceder a expedientes clínicos, autenticar

personal médico, controlar el ingreso a áreas restringidas o validar la identidad de pacientes en servicios digitales de salud.

Entre las principales características de los datos biométricos destacan su unicidad, permanencia, universalidad y capacidad de identificación. La unicidad implica que cada individuo posee rasgos biométricos diferenciables; la permanencia se refiere a que dichos rasgos suelen mantenerse relativamente estables en el tiempo; la universalidad supone que prácticamente todas las personas poseen características biométricas medibles; y la capacidad identificativa permite distinguir a un individuo dentro de una base de datos (Mordini & Tzovaras, 2012).

Existen diversos tipos de biometría aplicados en el sector de la salud. Los sistemas biométricos fisiológicos utilizan características corporales como huellas dactilares, reconocimiento facial, iris, retina, geometría de la mano o ADN. Por otro lado, los sistemas biométricos conductuales analizan patrones de comportamiento como la voz, firma electrónica, ritmo de escritura o dinámica de tecleo. Actualmente, el reconocimiento facial y la autenticación mediante huella digital son de los mecanismos más utilizados en instituciones sanitarias y plataformas de historia clínica electrónica.

Una de las principales particularidades jurídicas de los datos biométricos es su irrevocabilidad y permanencia. A diferencia de contraseñas o credenciales tradicionales, los datos biométricos no pueden modificarse fácilmente si son comprometidos. Una filtración de huellas dactilares, patrones faciales o datos de iris puede generar consecuencias permanentes para el titular, debido a que estas características acompañan al individuo durante gran parte de su vida. Esta situación incrementa significativamente los riesgos

asociados a robo de identidad, vigilancia masiva y uso indebido de información sensible (Cavoukian, 2011).

En el ámbito de la salud, estos riesgos adquieren una dimensión aún más delicada, debido a que los sistemas biométricos suelen vincularse directamente con datos médicos y clínicos. Una vulneración de seguridad podría no solo exponer información identificativa, sino también diagnósticos, tratamientos, historial médico o datos genéticos de los pacientes. Esto puede afectar derechos fundamentales como privacidad, confidencialidad médica, dignidad y no discriminación.

Desde una perspectiva jurídica, los datos biométricos son considerados categorías especiales o sensibles de datos personales. En Ecuador, la LOPDP establece que el tratamiento de datos sensibles requiere mayores garantías de protección y, en muchos casos, consentimiento explícito del titular. Asimismo, el Reglamento General de Protección de Datos reconoce a los datos biométricos como datos especialmente protegidos cuando son tratados para identificar de manera unívoca a una persona natural.

Entre los principales riesgos jurídicos específicos de la biometría en salud destacan:

1. **Riesgo de vulneración a la privacidad:** La recopilación masiva de datos biométricos puede permitir monitoreo constante y seguimiento indebido de pacientes o personal médico.
2. **Riesgo de discriminación y exclusión:** Algoritmos biométricos pueden presentar sesgos que afecten el reconocimiento adecuado de determinados grupos poblacionales, generando errores de identificación o acceso desigual a servicios sanitarios.

3. **Riesgo de uso secundario incompatible:** Los datos biométricos recolectados con fines médicos podrían utilizarse posteriormente para finalidades distintas, como vigilancia laboral o comercial, vulnerando el principio de finalidad.
4. **Riesgo de filtración irreversible:** A diferencia de una contraseña, una huella dactilar o patrón facial comprometido no puede ser reemplazado fácilmente, generando afectaciones permanentes al titular.
5. **Riesgo de decisiones automatizadas:** Sistemas biométricos integrados con inteligencia artificial podrían generar decisiones automatizadas erróneas respecto a autenticación, acceso a tratamientos o validación de identidad de pacientes.

Frente a estos riesgos, las instituciones sanitarias deben implementar medidas reforzadas de seguridad y gobernanza. Entre ellas destacan el cifrado de datos biométricos, anonimización, controles estrictos de acceso, almacenamiento descentralizado, auditorías periódicas, evaluaciones de impacto en protección de datos (EIPD) y políticas de privacidad transparentes. Asimismo, resulta indispensable aplicar el principio de privacidad desde el diseño (*privacy by design*), garantizando que la protección de datos se incorpore desde el desarrollo inicial de las tecnologías biométricas.

Los sistemas biométricos representan una herramienta eficiente para fortalecer la seguridad y optimizar procesos en el sector de la salud; sin embargo, su utilización implica elevados riesgos jurídicos y éticos debido a la sensibilidad, permanencia e irrevocabilidad de los datos biométricos. Por ello, el tratamiento de esta información debe realizarse bajo estrictos estándares de protección de datos personales, seguridad de la información y respeto a los derechos fundamentales de los pacientes y usuarios del sistema sanitario.

3.4.2. Tratamiento de datos biométricos

El tratamiento de datos biométricos constituye una de las actividades más sensibles dentro del régimen de protección de datos personales, debido a que implica información directamente vinculada con la identidad física y única de una persona natural. A diferencia de otros datos personales, los datos biométricos presentan características de permanencia, irreversibilidad y singularidad, lo que implica que una vulneración puede generar consecuencias permanentes e irreparables para el titular. Por esta razón, tanto la normativa internacional como la LOPDP los reconocen como categorías especiales de datos sujetas a un régimen reforzado de protección (Ley Orgánica de Protección de Datos Personales, 2021; Unión Europea, 2016).

En términos generales, el tratamiento de datos biométricos comprende cualquier operación realizada sobre este tipo de información, incluyendo su recopilación, almacenamiento, registro, organización, consulta, utilización, transferencia, supresión o cualquier otra forma de procesamiento, ya sea automatizado o manual. Actualmente, estas operaciones se ejecutan mediante tecnologías como reconocimiento facial, huellas dactilares, escaneo de iris, reconocimiento de voz o análisis conductual, frecuentemente integradas con sistemas de inteligencia artificial (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2013).

No obstante, el uso de tecnología avanzada no garantiza por sí mismo su legitimidad jurídica. El tratamiento de datos biométricos solo es válido cuando se sustenta en una base jurídica habilitante y cuando respeta los principios de legalidad, finalidad, proporcionalidad, minimización de datos, seguridad y confidencialidad (Ley Orgánica de Protección de Datos Personales, 2021).

La LOPDP establece que todo tratamiento de datos personales debe contar con una base de legitimación válida. En el caso de datos sensibles como los biométricos, este requisito adquiere un nivel de exigencia reforzado debido al alto riesgo que su tratamiento representa para los derechos fundamentales del titular (Asamblea Nacional del Ecuador, 2021).

a) Consentimiento explícito del titular

El consentimiento constituye una de las principales bases de legitimación. En el caso de datos biométricos, debe ser libre, previo, específico, informado, inequívoco y explícito (Ley Orgánica de Protección de Datos Personales, 2021).

El titular debe conocer claramente qué datos serán tratados, con qué finalidad, durante cuánto tiempo, quién tendrá acceso, cuáles son los riesgos y cuáles son sus derechos.

Sin embargo, este consentimiento presenta limitaciones cuando existe una relación de poder desigual entre el titular y el responsable del tratamiento, como ocurre en ámbitos laborales, educativos, sanitarios o de servicios públicos, donde la negativa puede generar consecuencias negativas (Apolo y López, 2024).

Asimismo, la complejidad de los sistemas biométricos y de inteligencia artificial puede dificultar la comprensión del tratamiento, afectando la transparencia y el entendimiento del uso de los datos (OCDE, 2013).

Por ello, el consentimiento no debe interpretarse como una autorización ilimitada, sino que debe complementarse con los principios de necesidad y proporcionalidad (Reglamento General de Protección de Datos, 2016).

b) Cumplimiento de obligaciones legales

El tratamiento también puede ser legítimo cuando es necesario para cumplir obligaciones legales establecidas en el ordenamiento jurídico. En ciertos casos, la normativa puede autorizar el uso de sistemas biométricos para fines de identificación, seguridad o prestación de servicios públicos (Ley Orgánica de Protección de Datos Personales, 2021).

c) Protección de intereses vitales

El tratamiento de datos biométricos puede justificarse cuando sea indispensable para proteger intereses vitales del titular o de otra persona natural, especialmente en situaciones de emergencia médica o riesgo grave para la vida o integridad física (Reglamento General de Protección de Datos, 2016).

d) Interés público y prestación de servicios

También puede legitimarse el tratamiento cuando exista un interés público debidamente fundamentado o cuando sea necesario para la prestación de servicios, siempre que exista habilitación normativa expresa y garantías adecuadas de protección (Ley Orgánica de Protección de Datos Personales, 2021).

Consentimiento en sistemas biométricos

El consentimiento adquiere especial relevancia en sistemas biométricos debido a que implican mecanismos de identificación permanente o autenticación automatizada. Sin embargo, también representa una de las bases más problemáticas desde el punto de vista jurídico y ético.

Uno de los principales problemas radica en determinar si el consentimiento puede considerarse verdaderamente libre cuando el acceso a servicios depende obligatoriamente del uso de biometría. En estos casos, la ausencia de alternativas reales puede desnaturalizar el consentimiento. Además, los datos biométricos son irrevocables, lo que incrementa

significativamente los riesgos asociados a filtraciones o usos indebidos. Por ello, el consentimiento debe analizarse bajo estándares reforzados de transparencia, necesidad y minimización. El responsable del tratamiento debe demostrar que no existen alternativas menos invasivas, que el tratamiento es estrictamente necesario, que existen medidas de seguridad adecuadas y que el titular puede ejercer efectivamente sus derechos (Reglamento General de Protección de Datos, 2016).

3.5. Privacidad desde el diseño y por defecto

La privacidad desde el diseño y por defecto constituye uno de los pilares fundamentales del moderno sistema de protección de datos personales y adquiere especial relevancia en tratamientos de alto riesgo, como aquellos que involucran datos biométricos y sistemas de inteligencia artificial en el sector salud. Este enfoque implica que la protección de datos no debe incorporarse únicamente como una medida reactiva posterior a la implementación tecnológica, sino como un elemento estructural presente desde las fases iniciales de diseño, desarrollo, adquisición, configuración y operación de los sistemas que realizan tratamiento de datos personales. En consecuencia, las organizaciones deben prever anticipadamente los riesgos que podrían afectar los derechos y libertades de los titulares, integrando mecanismos preventivos de protección antes de que el tratamiento sea ejecutado.

En el ordenamiento jurídico ecuatoriano, este principio encuentra sustento en la LOPDP y en su Reglamento General, los cuales incorporan la obligación de aplicar medidas técnicas y organizativas apropiadas para garantizar que el tratamiento se realice conforme a los principios de licitud, minimización, proporcionalidad, seguridad y responsabilidad proactiva. De manera complementaria, la Superintendencia de Protección de Datos Personales ha reforzado este enfoque mediante resoluciones relacionadas con gestión de riesgos, evaluación de impacto y tratamiento de datos mediante sistemas de inteligencia artificial,

exigiendo que los responsables implementen mecanismos preventivos que permitan identificar, evaluar y mitigar riesgos desde el diseño del tratamiento y durante todo su ciclo de vida.

Desde una perspectiva comparada, el Reglamento General de Protección de Datos de la Unión Europea (RGPD), particularmente en su artículo 25, desarrolla expresamente el principio de "protección de datos desde el diseño y por defecto" ("*data protection by design and by default*"), estableciendo que el responsable deberá aplicar medidas técnicas y organizativas apropiadas destinadas a aplicar eficazmente los principios de protección de datos e integrar las garantías necesarias en el tratamiento. La Agencia Española de Protección de Datos (AEPD), por su parte, ha sostenido que este principio no constituye únicamente una obligación técnica, sino una obligación de gobernanza y cumplimiento continuo (AEPD, 2025), especialmente en tratamientos biométricos, inteligencia artificial y decisiones automatizadas, donde los riesgos para los derechos fundamentales pueden ser elevados incluso antes de que el sistema entre en funcionamiento.

En el tratamiento de datos biométricos mediante inteligencia artificial, la privacidad desde el diseño exige adoptar un enfoque preventivo y restrictivo respecto de la recolección y utilización de datos sensibles. Esto implica que el responsable del tratamiento debe justificar previamente la necesidad y proporcionalidad del uso de biometría frente a alternativas menos intrusivas, evitando implementar sistemas automatizados únicamente por razones de eficiencia operativa o conveniencia tecnológica. En el ámbito sanitario, esta exigencia adquiere una dimensión reforzada, debido a que la historia clínica y los datos biométricos contienen información especialmente sensible cuya exposición, alteración o uso indebido puede generar consecuencias irreversibles sobre la privacidad, integridad y dignidad de las personas.

Bajo este enfoque, las medidas técnicas aplicables deben orientarse a reducir el riesgo desde la arquitectura misma del sistema. Entre ellas destacan la seudonimización y anonimización de datos cuando sea posible, el cifrado en tránsito y en reposo, la segmentación y segregación de accesos, el uso de autenticación multifactor, la trazabilidad de operaciones mediante registros de auditoría, la limitación de privilegios por roles y la minimización del almacenamiento de biometría cruda, priorizando el uso de plantillas biométricas irreversibles. Asimismo, en sistemas de inteligencia artificial resulta indispensable implementar mecanismos de validación y supervisión humana, controles de explicabilidad, auditorías periódicas del modelo, pruebas de sesgo algorítmico y monitoreo continuo del rendimiento.

Desde el punto de vista organizativo, la privacidad desde el diseño exige la incorporación de mecanismos internos de gobernanza y cumplimiento que permitan garantizar la protección efectiva de los datos personales durante todo el ciclo de vida del tratamiento. Esto comprende la realización previa de Evaluaciones de Impacto en la Protección de Datos (EIPD), la participación temprana del Delegado de Protección de Datos (DPD), la definición de políticas internas de seguridad, protocolos de gestión de incidentes, controles sobre encargados del tratamiento y procesos de capacitación continua para el personal que interviene en el tratamiento de datos biométricos e inteligencia artificial. La adopción de estas medidas no solo responde a una obligación normativa, sino que constituye una manifestación concreta del principio de responsabilidad proactiva previsto en la LOPDP.

En este sentido, la privacidad desde el diseño y por defecto debe entenderse como un mecanismo de prevención jurídica y técnica frente a tratamientos potencialmente invasivos o desproporcionados. Su aplicación resulta especialmente relevante en sistemas biométricos con inteligencia artificial, debido a que los riesgos no se limitan únicamente a

brechas de seguridad o accesos no autorizados, sino que incluyen decisiones automatizadas opacas, discriminación algorítmica, reutilización indebida de datos, perfilamiento y pérdida de control sobre información sensible. Por ello, el cumplimiento normativo no puede reducirse a la simple obtención del consentimiento del titular, sino que exige demostrar que el sistema fue diseñado bajo criterios de necesidad, proporcionalidad, minimización y seguridad desde su origen.

CAPITULO II

1.Evaluación normativa

La protección de datos personales en Ecuador, parte de la creación de nuestro legislador, como un derecho constitucional de tipo fundamental. El artículo 66, numeral 19 de la Constitución frente a lo expuesto, reconoce el derecho de las personas a decidir sobre su información personal y exige autorización del titular o mandato legal para su recolección, archivo, procesamiento, distribución o difusión. Este reconocimiento constitucional fue desarrollado posteriormente por la LOPDP de forma más profunda y extensiva.

La LOPDP constituye el eje principal del régimen jurídico ecuatoriano en esta materia, mientras que el Reglamento General, expedido mediante Decreto Ejecutivo No. 904, desarrolla los preceptos y procedimientos necesarios para su aplicación. Dicho Reglamento establece que sus disposiciones aplican a personas naturales y jurídicas, públicas o privadas, nacionales o extranjeras, cuando realicen tratamientos de datos personales en el marco de actividades como responsables o encargados.

A este marco se suma la normativa emitida por la Superintendencia de Protección de Datos Personales, que actualmente cuenta con resoluciones, guías, modelos, circulares,

consultas absueltas, procedimientos administrativos y el Sistema Nacional de Registro de Datos Personales. Esta producción normativa resulta relevante porque concreta obligaciones prácticas para responsables y encargados, especialmente en materia de gestión de riesgos, evaluación de impacto, cláusulas contractuales, transferencias de datos, delegado de protección de datos, seudonimización, anonimización, bloqueo, eliminación, interés legítimo, tratamiento a gran escala e inteligencia artificial.

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

El tratamiento de datos personales en el Ecuador no puede entenderse como una simple recolección de información. Debe responder a una estructura jurídica previa, documentada y verificable. En primer lugar, la organización debe identificar quién actúa como responsable del tratamiento, quién actúa como encargado, quiénes son los destinatarios de la información y cuál es la relación de cada actor con el titular de los datos. La propia Superintendencia define al responsable como quien decide sobre la finalidad y el tratamiento, y al titular como la persona natural cuyos datos son objeto de tratamiento.

En segundo lugar, cada tratamiento debe contar con una finalidad determinada, explícita y legítima. Esto significa que la entidad debe explicar para qué recopila los datos, por qué los necesita, durante cuánto tiempo los conservará y bajo qué base de legitimación los tratará. La SPDP reconoce como bases aplicables el cumplimiento de obligaciones legales, el interés público, el ejercicio de poderes públicos y, cuando corresponda, el consentimiento del titular, de acuerdo con los supuestos de licitud previstos en la LOPDP.

En tercer lugar, debe cumplirse el principio de información y transparencia. El titular debe conocer, antes o al momento de la recolección, la identidad del responsable, las finalidades del tratamiento, las categorías de datos utilizadas, los posibles destinatarios, el tiempo de

conservación, los derechos que puede ejercer y los canales disponibles para hacerlo. Este deber no se satisface con una cláusula genérica, sino con una política o aviso de privacidad claro, accesible y coherente con el tratamiento real.

También se requiere una base documentada para el consentimiento cuando esta sea la legitimación utilizada. Dicho consentimiento debe ser previo, informado y otorgado mediante una acción afirmativa clara. No obstante, el consentimiento no es la única base posible; por ello, la evaluación normativa debe revisar caso por caso si el tratamiento se sustenta en una obligación legal, una relación contractual, el interés público, el interés legítimo u otra causa admitida por la normativa aplicable. La SPDP incluso ha emitido normativa específica sobre el interés legítimo como base de legitimación.

Otro requisito formal consiste en implementar medidas de seguridad técnicas, jurídicas y organizativas acordes con la naturaleza del dato, el volumen de información, el contexto del tratamiento y los riesgos para los derechos de los titulares. Estas medidas deben estar respaldadas por políticas de acceso, controles de privilegios, mecanismos de borrado seguro, gestión de riesgos y evaluaciones de impacto cuando el tratamiento pueda generar riesgos relevantes.

Cuando intervengan terceros, proveedores o encargados del tratamiento, la relación debe estar regulada contractualmente. Esto exige incorporar cláusulas de protección de datos que definan instrucciones, confidencialidad, finalidad, medidas de seguridad, subencargados, conservación, devolución o eliminación de datos, atención de derechos y responsabilidades frente a incidentes. La SPDP emitió una resolución específica que establece la obligación de incorporar cláusulas de protección de datos personales en contratos celebrados dentro del territorio ecuatoriano.

La organización también debe evaluar si corresponde designar un Delegado de Protección de Datos Personales. Esta figura cumple un rol de supervisión, asesoría y punto de contacto con la autoridad de control y con los titulares. La SPDP ha emitido normativa específica sobre el Delegado de Protección de Datos, lo que refuerza la necesidad de documentar su designación, funciones, independencia y canales de comunicación cuando resulte aplicable.

Finalmente, los tratamientos deben considerar reglas sobre conservación, bloqueo, eliminación, anonimización, seudonimización y transferencias nacionales o internacionales. La información no puede conservarse indefinidamente; debe mantenerse únicamente durante el tiempo necesario para cumplir la finalidad o atender responsabilidades legales. La propia SPDP señala que, cumplido ese período, los datos deben eliminarse, anonimizarse o bloquearse conforme a mecanismos definidos.

2.La necesidad de un inventario de datos

El inventario de datos personales es una herramienta indispensable para demostrar cumplimiento normativo. Su importancia radica en que permite conocer qué datos trata la organización, de quiénes son, para qué se utilizan, dónde se almacenan, quién accede a ellos, con quién se comparten, durante cuánto tiempo se conservan y qué riesgos genera su tratamiento. Sin este levantamiento, la protección de datos queda reducida a una declaración formal, sin evidencia suficiente para sostener decisiones jurídicas, técnicas u organizativas.

Desde una perspectiva normativa, el inventario permite aplicar de forma ordenada los principios de licitud, finalidad, minimización, proporcionalidad, calidad, conservación, seguridad y responsabilidad proactiva. Además, facilita identificar los tratamientos que

requieren consentimiento, aquellos que se sustentan en una obligación legal, los que involucran datos sensibles, los que implican transferencias internacionales o los que pueden requerir evaluación de impacto. La SPDP mantiene dentro de sus servicios el Sistema Nacional de Registro de Datos Personales, lo que confirma la importancia de contar con información organizada y trazable sobre las actividades de tratamiento.

En términos prácticos, el inventario debe contener, al menos, la identificación del proceso, la finalidad del tratamiento, la base de legitimación, las categorías de titulares, las categorías de datos personales, los sistemas o archivos utilizados, los responsables internos, los encargados o proveedores involucrados, las transferencias o comunicaciones realizadas, el plazo de conservación, las medidas de seguridad aplicables y el nivel de riesgo asociado. Esta información permite que la organización responda de forma objetiva ante auditorías, solicitudes de titulares, requerimientos de la autoridad de control o incidentes de seguridad.

La necesidad del inventario también se justifica porque ningún programa de protección de datos puede gestionarse adecuadamente si la entidad desconoce sus propios flujos de información. Por ejemplo, no sería posible atender correctamente un derecho de acceso o eliminación si no se sabe en qué sistemas se encuentra la información del titular. Tampoco sería viable valorar una vulneración de seguridad sin conocer qué datos fueron afectados, cuántos titulares podrían estar involucrados, qué terceros tuvieron acceso o qué medidas de mitigación corresponden.

Por ello, el inventario no debe considerarse un documento aislado, sino la base operativa del sistema de cumplimiento en protección de datos personales. A partir de él se construyen la matriz de riesgos, las evaluaciones de impacto, las cláusulas contractuales, los avisos de privacidad, los procedimientos de atención de derechos, los controles de seguridad y las políticas de conservación y eliminación. En consecuencia, su actualización periódica

permite que la organización no solo cumpla formalmente la normativa, sino que pueda demostrar de manera verificable cómo protege los datos personales bajo su responsabilidad.

3.Gobernanza de la protección de datos personales

3.1 Políticas, instrucciones de trabajo y flujogramas

El presente apartado tiene como finalidad establecer las políticas, instrucciones de trabajo y flujogramas aplicables al sector de la salud, específicamente al Hospital Oncológico Vida Nueva, como herramientas esenciales para garantizar la correcta ejecución de los procesos asistenciales, administrativos y operativos dentro de las instituciones sanitarias. Estos instrumentos permiten estandarizar procedimientos, fortalecer la calidad en la prestación de los servicios de salud y asegurar el cumplimiento de la normativa vigente y de los principios de seguridad del paciente.

Las políticas definen lineamientos y criterios de actuación orientados a la protección de la salud y los derechos de los pacientes; las instrucciones de trabajo describen de manera detallada la forma adecuada de ejecutar actividades clínicas y administrativas; y los flujogramas facilitan la representación gráfica de los procesos, permitiendo identificar responsabilidades, tiempos de respuesta y puntos de control. En conjunto, estos mecanismos contribuyen a optimizar la atención sanitaria, reducir riesgos, mejorar la eficiencia institucional y promover una gestión basada en la calidad, la seguridad y la mejora continua. A continuación, procederemos a redactar los avisos de privacidad interno como externo del Hospital Oncológico Vida Nueva, así como las instrucciones de trabajo y los flujogramas:

***REF**: Documento disponible en el Anexo No. 1.*

En lo referente al plan de capacitación se ha establecido como objetivo general fortalecer las capacidades institucionales del personal del Hospital en materia de protección de datos personales, confidencialidad de la información sanitaria y uso responsable de tecnologías biométricas e inteligencia artificial, mediante la implementación de un programa estructurado de capacitación y comunicación que garantice el cumplimiento normativo y la gestión adecuada de riesgos.

Adicionalmente, el presente plan tiene como finalidad garantizar la implementación efectiva de la Política Institucional de Protección de Datos Personales del Hospital, mediante el desarrollo sistemático de capacidades institucionales, la estandarización de conocimientos en el tratamiento de datos personales y la consolidación de una cultura organizacional basada en la confidencialidad, seguridad y responsabilidad proactiva:

***REF**: Documento disponible en el Anexo No. 2.*

En lo referente a los flujogramas se propone el siguiente diagrama de flujo:

***REF**: Documento disponible en el Anexo No. 3.*

3.2 Matriz RACI

La matriz RACI constituye una herramienta de gestión que permite definir y clarificar los roles y responsabilidades de cada participante dentro de un proceso o actividad institucional. Su aplicación en el sector de la salud resulta fundamental para garantizar una adecuada coordinación entre las diferentes áreas y profesionales involucrados, promoviendo una ejecución eficiente, organizada y alineada con los objetivos de calidad y seguridad del paciente.

A través de esta matriz se identifican los responsables de ejecutar las actividades, quienes aprueban o supervisan los procesos, las personas que deben ser consultadas y aquellas que deben mantenerse informadas, fortaleciendo así la comunicación, la trazabilidad y el control interno dentro de la organización sanitaria.

Gestión de Datos Personales

Matriz de Asignación de Responsabilidades - RACI y cronograma de implementación

Fecha de elaboración:	24/03/2026	**Versión:**	1.0	**Código:**	PRIV-RACI-2026-001
Proyecto:	Programa de Gobernanza de Privacidad y Protección de Datos Personales				
Alcance:	Gobernanza, inventario, cumplimiento, controles, atención de derechos, incidentes, capacitación, auditoría y cierre.				

Total actividades	18	**No iniciadas**	16	**En ejecución**	2	**Terminadas**	0	**Avance global**	2%

R: NO INICIADA | **A: EN EJECUCIÓN** | **V: TERMINADO**

Actividad			Seguimiento		Roles				Fechas comprometidas			Control	
No	**Fase**	**Detalle**	**Estado**	**% avance**	**Responsable (R)**	**Aprobador (A)**	**Consultado (C)**	**Informado (I)**	**Inicio**	**Fin**	**Duración (días)**	**Entregable**	**Observaciones**
1	Inicio	Kick-off del programa, definición de alcance, objetivos, entregables, patrocinio y plan de trabajo.	A: EN EJECUCIÓN	25%	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	DPO	TI, Seguridad de la Información, Áreas de Negocio	Usuarios Clave	24/03/2026	25/03/2026	2	Acta de inicio y plan de trabajo aprobados	Requiere disponibilidad de las áreas para confirmar alcance, criticidad y patrocinio.
2	Inventario	Identificación de procesos que tratan datos personales y nombramiento de responsables por cada proceso de negocio.	A: EN EJECUCIÓN	10%	Áreas de Negocio	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	DPO, TI	Seguridad de la Información, Usuarios Clave	24/03/2026	31/03/2026	8	Mapa de tratamientos por proceso y dueño funcional	Insumo base para inventario, evaluación de riesgos y actualización documental.
3	Inventario	Levantamiento del inventario de bases de datos, aplicaciones, repositorios, integraciones y flujos de información.	R: NO INICIADA	0%	TI	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	Áreas de Negocio, Seguridad de la Información	DPO, Usuarios Clave	26/03/2026	02/04/2026	8	Inventario técnico y diagrama de flujo de datos	Debe incluir origen, destino, almacenamiento, acceso, respaldo y transferencias.
4	Clasificación	Clasificación de datos personales, identificación de categorías especiales/sensibles y criticidad por tratamiento.	R: NO INICIADA	0%	DPO	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	Áreas de Negocio, Seguridad de la Información, TI	Usuarios Clave	01/04/2026	03/04/2026	3	Matriz de clasificación y criticidad	Aplicar criterios de confidencialidad, impacto y minimización de datos.
5	Cumplimiento	Definición de finalidades, bases de legitimación, plazo de conservación y revisión de necesidad/proporcionalidad.	R: NO INICIADA	0%	DPO	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	Áreas de Negocio	TI, Seguridad de la Información, Usuarios Clave	06/04/2026	10/04/2026	5	Matriz de bases legales, finalidades y conservación	Alinear con obligaciones regulatorias, contractuales y operativas.
6	Terceros	Identificación de encargados, terceros, proveedores y transferencias nacionales/internacionales vinculadas a los tratamientos.	R: NO INICIADA	0%	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	DPO	Áreas de Negocio, TI, Seguridad de la Información	Usuarios Clave	08/04/2026	14/04/2026	7	Registro de encargados y transferencias	Validar contratos, anexos de privacidad y medidas mínimas exigibles a terceros.
7	Documentación	Revisión y actualización de avisos de privacidad, consentimientos, cláusulas contractuales y formatos de recolección.	R: NO INICIADA	0%	DPO	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	Áreas de Negocio, Usuarios Clave	TI, Seguridad de la Información	13/04/2026	17/04/2026	5	Paquete documental actualizado	Considerar canales físicos, digitales, web, formularios y grabaciones.
8	Brechas	Evaluación de brechas entre situación actual y marco objetivo de privacidad y protección de datos.	R: NO INICIADA	0%	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	DPO	TI, Seguridad de la Información, Áreas de Negocio	Usuarios Clave	15/04/2026	21/04/2026	7	Informe de hallazgos y plan de acción	Priorizar por criticidad, exposición, probabilidad e impacto.
9	Riesgos	Evaluación de riesgos y DPIA/PIA para tratamientos críticos o de alto impacto.	R: NO INICIADA	0%	DPO	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	Seguridad de la Información, TI, Áreas de Negocio	Usuarios Clave	20/04/2026	24/04/2026	5	Evaluación de impacto y plan de tratamiento	Documentar riesgos residuales, controles existentes y responsables de mitigación.
10	Políticas	Definición o actualización de política de privacidad y procedimientos de gestión de datos personales.	R: NO INICIADA	0%	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	DPO	TI, Seguridad de la Información, Áreas de Negocio	Usuarios Clave	27/04/2026	30/04/2026	4	Política y procedimientos aprobados	Incluir lineamientos sobre recolección, uso, intercambio, conservación y destrucción.
11	Retención	Diseño de matriz de retención, archivo, bloqueo y eliminación segura de datos personales.	R: NO INICIADA	0%	DPO	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	TI, Áreas de Negocio, Seguridad de la Información	Usuarios Clave	29/04/2026	05/05/2026	7	Matriz de retención y disposición segura	Definir evidencias, responsables y medios de destrucción o anonimización.
12	Controles TI	Implementación de controles técnicos: accesos, perfiles, cifrado, respaldo, segregación y trazabilidad.	R: NO INICIADA	0%	TI	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	Seguridad de la Información, DPO	Áreas de Negocio, Usuarios Clave	04/05/2026	13/05/2026	10	Controles TI implementados y evidenciados	Aplicar principio de mínimo privilegio y monitoreo de accesos a información personal.
13	Seguridad	Implementación de controles organizacionales y de seguridad: DLP, hardening, monitoreo y gestión de vulnerabilidades.	R: NO INICIADA	0%	Seguridad de la Información	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	TI, DPO	Áreas de Negocio, Usuarios Clave	06/05/2026	15/05/2026	10	Plan de controles de seguridad desplegado	Asegurar cobertura sobre endpoints, correo, repositorios y accesos remotos.
14	Derechos	Diseño y validación del procedimiento para atención de derechos de titulares y solicitudes regulatorias.	R: NO INICIADA	0%	DPO	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	Áreas de Negocio, TI, Seguridad de la Información	Usuarios Clave	11/05/2026	15/05/2026	5	Procedimiento, SLA y formatos de atención	Definir canal, responsable, tiempos de respuesta, trazabilidad y evidencias.
15	Incidentes	Definición del procedimiento de gestión y notificación de incidentes o brechas de datos personales.	R: NO INICIADA	0%	Seguridad de la Información	DPO	TI, Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	Áreas de Negocio, Usuarios Clave	13/05/2026	19/05/2026	7	Runbook de incidentes y matriz de escalamiento	Contemplar detección, contención, análisis, notificación y cierre.
16	Capacitación	Ejecución de campaña de capacitación y concienciación para usuarios y líderes de proceso.	R: NO INICIADA	0%	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	DPO	Áreas de Negocio, Seguridad de la Información	TI, Usuarios Clave	18/05/2026	22/05/2026	5	Registro de capacitación y evaluación	Incluir inducción, refuerzo y evaluación mínima de comprensión.
17	Auditoría	Prueba de cumplimiento, revisión de evidencias y auditoría interna del esquema de protección de datos.	R: NO INICIADA	0%	DPO	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	TI, Seguridad de la Información, Áreas de Negocio	Usuarios Clave	25/05/2026	28/05/2026	4	Informe de auditoría interna	Levantar hallazgos, acciones correctivas y responsables con fecha compromiso.
18	Cierre	Cierre del proyecto, validación ejecutiva, KPI de cumplimiento y traspaso a operación continua.	R: NO INICIADA	0%	Gerente del Programa de Gobernanza de Privacidad y Protección de Datos Personales	DPO	TI, Seguridad de la Información, Áreas de Negocio	Usuarios Clave	29/05/2026	02/06/2026	5	Acta de cierre, KPI y hoja de ruta continua	Formalizar gobierno operativo, frecuencia de revisión y plan de mejora continua.

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

El derecho a la información constituye uno de los pilares fundamentales del sistema de protección de datos personales, debido a que garantiza que los titulares conozcan de manera clara, previa y transparente cómo serán tratados sus datos personales, quién será responsable del tratamiento, cuáles son las finalidades perseguidas y qué derechos pueden ejercer frente al tratamiento de su información. Este derecho se encuentra estrechamente vinculado con los principios de transparencia, lealtad y responsabilidad proactiva previstos en la LOPDP, así como con estándares internacionales de protección de datos como el Reglamento General de Protección de Datos de la Unión Europea (Reglamento General de Protección de Datos, 2016).

En el caso del Hospital Oncológico Vida Nueva, el cumplimiento del derecho a la información adquiere especial relevancia debido a la implementación de sistemas biométricos e inteligencia artificial destinados a procesos de autenticación, acceso a historias clínicas electrónicas, validación de identidad de pacientes y prestación de servicios de telemedicina. Estas actividades implican el tratamiento de datos sensibles relacionados tanto con la salud como con características biométricas de los pacientes, lo cual incrementa significativamente el nivel de riesgo para los derechos y libertades de los titulares.

En este contexto, el Hospital Oncológico Vida Nueva no solo debe contar con bases jurídicas válidas que legitimen el tratamiento de datos biométricos, sino también garantizar mecanismos efectivos de transparencia que permitan a los pacientes, colaboradores y usuarios comprender de manera suficiente cómo serán utilizados sus datos personales, cuáles son los riesgos asociados al tratamiento y qué medidas de seguridad serán implementadas para proteger la información tratada.

La LOPDP establece que toda persona tiene derecho a recibir información respecto de la existencia del tratamiento de sus datos personales, las finalidades específicas del tratamiento, la base jurídica aplicable, el plazo de conservación, las transferencias nacionales o internacionales previstas, la identificación del responsable del tratamiento y los mecanismos disponibles para ejercer derechos como acceso, rectificación, eliminación, oposición, portabilidad o suspensión del tratamiento (Ley Orgánica de Protección de Datos Personales, 2021). En consecuencia, el Hospital Oncológico Vida Nueva debe garantizar que esta información sea proporcionada de manera previa al inicio del tratamiento y mediante mecanismos claros, accesibles y comprensibles para los titulares.

Los avisos de privacidad constituyen uno de los principales mecanismos mediante los cuales el Hospital Oncológico Vida Nueva puede materializar el cumplimiento del derecho a la información. Estos documentos permiten comunicar a los titulares las condiciones bajo las cuales serán tratados sus datos personales y deben caracterizarse por utilizar lenguaje claro, sencillo y fácilmente entendible, evitando cláusulas ambiguas o excesivamente técnicas que dificulten la comprensión del tratamiento biométrico y del uso de inteligencia artificial dentro de la institución.

Debido a la sensibilidad de los tratamientos realizados, los avisos de privacidad implementados por el Hospital Oncológico Vida Nueva deben incorporar información reforzada relacionada con:

- La identificación del responsable del tratamiento;
- Las finalidades específicas del uso de biometría e inteligencia artificial;
- La base jurídica que legitima el tratamiento;
- Las categorías de datos personales y biométricos tratados;

- La existencia de decisiones automatizadas;
- Posibles transferencias nacionales o internacionales de información;
- El plazo de conservación de los datos;
- Las medidas generales de seguridad implementadas;
- Los mecanismos para ejercer derechos ARCO;
- La información de contacto del Delegado de Protección de Datos (DPD).

Asimismo, el principio de transparencia exige que la información proporcionada por el Hospital Oncológico Vida Nueva no se limite únicamente a la entrega formal de documentos o consentimientos, sino que resulte efectivamente comprensible para los pacientes y usuarios. Esto adquiere especial importancia en sistemas de inteligencia artificial, debido a que los titulares generalmente desconocen el funcionamiento de los algoritmos utilizados para reconocimiento facial, autenticación biométrica o detección automatizada de patrones clínicos. Por ello, la institución debe procurar niveles adecuados de explicabilidad, supervisión humana y comunicación transparente respecto al funcionamiento general de estas tecnologías y sus posibles implicaciones sobre los derechos de los pacientes (Mittelstadt et al., 2016).

De igual manera, el deber de información dentro del Hospital Oncológico Vida Nueva no debe limitarse únicamente al momento inicial de recolección de datos. La transparencia debe mantenerse durante todo el ciclo de vida del tratamiento, lo que implica informar a los titulares sobre cambios relevantes en las finalidades del tratamiento, incorporación de nuevas tecnologías biométricas, modificaciones en las medidas de seguridad o transferencias adicionales de datos personales. Este enfoque responde al principio de responsabilidad proactiva previsto en la normativa ecuatoriana de protección de datos

personales y exige que la institución pueda demostrar continuamente el cumplimiento de sus obligaciones legales.

El incumplimiento del derecho a la información podría generar importantes consecuencias jurídicas, reputacionales y operativas para el Hospital Oncológico Vida Nueva. La ausencia de avisos de privacidad adecuados, la utilización de consentimientos ambiguos o la falta de transparencia respecto del uso de biometría e inteligencia artificial podrían configurar tratamientos ilícitos o desproporcionados, vulnerando principios esenciales de la LOPDP. Además, debido a que los datos biométricos son irrevocables y altamente sensibles, una deficiente gestión de la información podría afectar directamente derechos fundamentales como la privacidad, la intimidad, la dignidad y la autodeterminación informativa de los pacientes.

A nivel institucional, la falta de transparencia también podría afectar la confianza de pacientes, médicos y colaboradores respecto al uso de tecnologías digitales dentro del Hospital Oncológico Vida Nueva. La percepción de vigilancia excesiva, monitoreo constante o utilización opaca de inteligencia artificial puede generar rechazo institucional, afectaciones reputacionales y conflictos legales relacionados con vulneración de derechos fundamentales.

Desde la perspectiva de privacidad desde el diseño y por defecto, el Hospital Oncológico Vida Nueva debe incorporar los avisos de privacidad y mecanismos de transparencia como parte integral de su arquitectura de cumplimiento normativo. Esto implica diseñar mecanismos de información accesibles desde el inicio del tratamiento, utilizar modelos de consentimiento granular, implementar políticas internas claras y garantizar procesos continuos de actualización y comunicación frente a cambios tecnológicos o nuevas finalidades del tratamiento. Asimismo, la institución debe integrar evaluaciones de impacto,

controles de transparencia y supervisión humana efectiva como parte de su modelo de gobernanza de datos personales y gestión de riesgos.

3.4 Cláusulas contractuales entre los agentes de tratamiento de datos personales

Las cláusulas contractuales entre los agentes de tratamiento de datos personales constituyen mecanismos jurídicos fundamentales para garantizar que el tratamiento de información personal se realice conforme a principios de legalidad, seguridad, confidencialidad y responsabilidad proactiva. En el caso del Hospital Oncológico Vida Nueva, la implementación de sistemas biométricos e inteligencia artificial implica la participación de diversos actores, como proveedores tecnológicos, plataformas de almacenamiento, empresas de soporte y encargados del tratamiento, quienes pueden acceder a datos sensibles relacionados con la salud y biometría de los pacientes.

a. Cláusula de objeto del tratamiento

- El encargado del tratamiento realizará actividades de almacenamiento, autenticación biométrica y soporte tecnológico respecto de los datos personales tratados por el Hospital Oncológico Vida Nueva.

b. Cláusula de finalidad

- Los datos personales únicamente podrán ser utilizados para procesos de autenticación biométrica, acceso seguro a historias clínicas electrónicas y prestación de servicios de telemedicina.

c. Cláusula de confidencialidad

- El encargado del tratamiento se obliga a mantener absoluta confidencialidad respecto de los datos personales y datos sensibles a los que tenga acceso.

d. **Cláusula de seguridad de la información**

- Debe incluir: cifrado; control de accesos; autenticación multifactor; registros de auditoría; respaldo de información; monitoreo de incidentes; segmentación de accesos.

e. **Cláusula de tratamiento de datos sensibles**

- El encargado reconoce que los datos biométricos y de salud constituyen categorías especiales de datos personales y se obliga a implementar medidas reforzadas de protección.

f. **Cláusula de prohibición de uso no autorizado**

- Queda prohibido utilizar los datos personales para fines comerciales, publicitarios o distintos a los establecidos contractualmente.

g. **Cláusula de subcontratación**

- El encargado no podrá subcontratar operaciones de tratamiento sin autorización previa y escrita del Hospital Oncológico Vida Nueva.

h. **Cláusula de notificación de incidentes de seguridad**

- Debe incluir: tiempo máximo de notificación; tipo de incidente; medidas correctivas; plan de contención.

i. **Cláusula de transferencias internacionales**

- Las transferencias internacionales de datos personales únicamente podrán realizarse cuando existan garantías adecuadas de protección de datos.

j. **Cláusula de derechos ARCO**

Obliga al encargado a colaborar con solicitudes de titulares, debe incluir: acceso; rectificación; eliminación; oposición y portabilidad.

k. Cláusula de conservación y eliminación de datos

Determina cuánto tiempo se conservarán los datos y cómo serán eliminados.

l. Cláusula de auditoría y supervisión

Permite al hospital verificar cumplimiento; El Hospital Oncológico Vida Nueva podrá realizar auditorías periódicas respecto del cumplimiento de obligaciones de protección de datos personales.

m. Cláusula de responsabilidad e indemnización

Define consecuencias por incumplimientos, debe incluir: responsabilidad por filtraciones; daños reputacionales; sanciones administrativas; incumplimiento de medidas de seguridad.

n. Cláusula de cumplimiento normativo

El encargado garantiza el cumplimiento de la LOPDP, su Reglamento General y demás normativa aplicable.

o. Cláusula sobre inteligencia artificial y biometría

- El proveedor de sistemas biométricos e inteligencia artificial deberá implementar mecanismos de supervisión humana y controles orientados a mitigar sesgos algorítmicos y errores de identificación.

p. Cláusula de privacidad desde el diseño y por defecto

- Obliga a incorporar protección de datos desde la arquitectura tecnológica; El encargado implementará medidas de privacidad desde el diseño y por defecto en todos los sistemas utilizados para el tratamiento de datos biométricos.”

q. Cláusula de trazabilidad y registro de actividades

- Permite mantener evidencia del tratamiento, debe incluir: logs; accesos; modificaciones y consultas.

r. Cláusula de terminación contractual

- Regula obligaciones posteriores a la finalización del contrato; La terminación del contrato no extingue las obligaciones de confidencialidad y protección de datos personales.

CAPITULO III

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

La biometría permite identificar o autenticar a una persona a partir de rasgos físicos o conductuales, mientras que la IA incrementa esa capacidad mediante análisis automatizado de grandes volúmenes de datos, reconocimiento de patrones, inferencias predictivas y apoyo a decisiones. En materia de salud, esta convergencia puede tener utilidad en supuestos clínicamente justificados, como diagnósticos por imagen asistidos, análisis histopatológicos digitales, modelos predictivos supervisados y apoyo a decisiones médicas. Sin embargo, no todo uso tecnológico útil es jurídicamente admisible.

En efecto, la normativa exige la implementación de medidas técnicas, pero también organizativas o administrativas (políticas internas, controles de acceso, gestión de incidentes), jurídicas (cláusulas de confidencialidad, contratos con encargados, bases de legitimación) y físicas (protección de infraestructuras, control de ingreso a archivos o servidores). Esta visión holística es especialmente crítica cuando se integran sistemas de IA con biometría en salud, dado el riesgo reforzado sobre derechos fundamentales.

El estado del arte en Ecuador respecto a la compatibilidad entre la biometría e IA en el sector de la salud exige una construcción que trascienda el marco legal positivo vigente y se articule desde un enfoque integral normativo, doctrinal y técnico. En el plano normativo, la LOPDP y su Reglamento constituyen la base por defecto en materia de protección de datos personales dentro de Ecuador, pero deben complementarse específicamente frente a lo que establece la Resolución No. SPDPSPD-2026-0009-R, emitida por la SPDP, para la materia específica, que introduce obligaciones específicas para sistemas de IA, así como con el apoyo de estándares internacionales que posteriormente puedan ser incorporados vía bloque de constitucionalidad a Ecuador, como el Convenio 108+, la Recomendación de la UNESCO sobre Ética de la Inteligencia Artificial y las directrices de la OMS en materia de IA relativas al sector de la salud, que imponen principios de proporcionalidad, supervisión humana, no discriminación, transparencia y rendición de cuentas.

Desde una perspectiva doctrinal, por ende, la convergencia entre biometría e IA en entornos hospitalarios ha sido conceptualizada como un tratamiento de alto riesgo, en el que la legitimidad no depende únicamente de la finalidad, sino de la estricta necesidad y de la capacidad del sistema de respetar la autonomía del paciente, evitar sesgos y garantizar decisiones explicables. En el plano técnico, el estándar ideal no se agota en la funcionalidad del sistema, sino que exige modelos auditables, entrenamiento con datos representativos,

control de sesgos, trazabilidad de decisiones, seguridad integral y mecanismos efectivos de intervención humana. Bajo este enfoque, la implementación de IA en el sector de la salud resulta jurídicamente admisible únicamente en aplicaciones clínicamente justificadas, como el diagnóstico por imagen asistido o sistemas de apoyo a decisiones médicas, quedando excluidos, por falta de proporcionalidad, usos como el reconocimiento facial generalizado para acceso o identificación, en tanto no superan el test de necesidad frente a alternativas menos intrusivas.

Sin embargo, el marco ecuatoriano todavía no cuenta con una ley orgánica específica de IA. Por ello, el estándar ideal debe complementarse con instrumentos de política pública y estándares internacionales. En el ámbito interno, la Estrategia para el Fomento del Desarrollo y Uso Ético y Responsable de la IA en Ecuador, emitida por el MINTEL, mediante Acuerdo Ministerial No. MINTEL-MINTEL-2025-0030, incorpora lineamientos de gobernanza, adopción segura y uso ético de IA, en concordancia con estándares internacionales como la referida Recomendación de la UNESCO.

Desde una dimensión ética, por ende, el estándar mínimo aplicable al uso de IA en salud debe partir de una premisa central, la tecnología únicamente es legítima si permanece subordinada a la dignidad humana, a la autonomía del paciente y a la protección efectiva de sus derechos. Por ello, la gobernanza ética de estos sistemas no puede reducirse a una declaración de buenas prácticas, sino que debe traducirse en exigencias concretas de supervisión humana significativa, transparencia comprensible, explicabilidad de los resultados, responsabilidad identificable, prevención de sesgos, robustez técnica, seguridad desde el diseño y rendición de cuentas. En consecuencia, el marco ideal ecuatoriano debe asumir que la ética no opera como un complemento externo de la regulación, sino como un

criterio de validez material para determinar si un sistema de IA puede ser admitido, limitado o descartado en función de su impacto sobre derechos fundamentales.

En este contexto, la IA en el ámbito sanitario únicamente puede considerarse jurídicamente admisible cuando aporta un valor añadido real e irreemplazable frente a métodos tradicionales, lo cual se evidencia en aplicaciones como el diagnóstico por imagen asistido, el análisis histopatológico digital, los modelos predictivos clínicos y la robótica médica, en las que la capacidad de procesamiento y detección de patrones supera la intervención humana ordinaria. Sin embargo, esta utilidad no exonera el cumplimiento del test de proporcionalidad, que exige demostrar que el tratamiento es necesario y que no existen alternativas menos intrusivas, lo que excluye usos como la identificación generalizada mediante biometría. En cuanto a la legitimación del tratamiento, si bien el consentimiento explícito constituye una base habilitante, su aplicación en salud es limitada debido a la relación asimétrica entre paciente e institución y a su inviabilidad operativa en múltiples escenarios, por lo que deben privilegiarse otras bases como el cumplimiento de obligaciones en el ámbito sanitario, y la protección de intereses vitales, especialmente en contextos de diagnóstico, tratamiento y gestión sanitaria.

En definitiva, el análisis evidencia que la integración de sistemas biométricos con IA en el sector de la salud constituye un tratamiento de alto riesgo, no únicamente por el carácter sensible de los datos involucrados, sino por su naturaleza irreversible y por la posibilidad de generar decisiones automatizadas con impacto directo en derechos fundamentales. En este contexto, la implementación generalizada de biometría con IA en hospitales no resulta jurídicamente viable, pues no solo carece de una base de legitimación adecuada en términos estructurales, sino que además no garantiza de manera suficiente el control humano efectivo, la explicabilidad de las decisiones, ni la prevención de sesgos, elementos que

constituyen condiciones mínimas para su compatibilidad con el régimen de protección de datos personales.

Si bien el ordenamiento jurídico ecuatoriano ha desarrollado un marco relevante, este resulta aún insuficiente frente a los desafíos específicos que plantea la IA en entornos sanitarios. En consecuencia, la construcción de un estándar jurídico adecuado exige necesariamente la incorporación de criterios doctrinales y técnicos provenientes del ámbito internacional, particularmente aquellos que imponen supervisión humana significativa, explicabilidad, auditoría algorítmica y control de sesgos, como condiciones indispensables para la protección efectiva de los derechos del paciente. Bajo esta lectura, y en coherencia con los parámetros constitucionales y los estándares internacionales aplicables, la implementación de sistemas biométricos con IA en el sector de la salud, en los términos planteados, no puede considerarse jurídicamente viable en el estado actual del derecho ecuatoriano, en la medida en que tampoco satisface los estándares éticos mínimos que exigen que toda aplicación tecnológica en salud se encuentre efectivamente subordinada a la dignidad humana, la autonomía del paciente y la protección integral de sus derechos.

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

El presente análisis se desarrolla sobre el caso hipotético del Hospital Vida Nueva, institución privada prestadora de servicios de salud que incorpora herramientas de inteligencia artificial en sus procesos clínicos, administrativos y de telemedicina. La organización opera mediante una infraestructura digital integrada conformada por historias clínicas electrónicas, plataformas de atención médica virtual, sistemas automatizados de

apoyo al diagnóstico y herramientas predictivas para priorización de pacientes y gestión hospitalaria.

Dentro de sus operaciones, la institución realiza tratamientos de datos personales sensibles, incluyendo datos de salud, biométricos, genéticos y conductuales, los cuales son procesados mediante sistemas de IA para finalidades relacionadas con diagnóstico asistido, clasificación de riesgo clínico, seguimiento remoto de pacientes, automatización de procesos hospitalarios y análisis predictivo en atención médica.

En virtud de lo anterior, el análisis de riesgos se delimita específicamente a los tratamientos efectuados por dicha organización y a los riesgos derivados del uso de inteligencia artificial aplicada directamente en los procesos de tratamiento de datos personales de pacientes, personal médico y usuarios de servicios digitales de salud.

En este contexto, el presente análisis de riesgos se orienta a identificar, clasificar y valorar los riesgos que puedan afectar los derechos fundamentales de los titulares de datos personales, especialmente en escenarios donde intervienen sistemas automatizados o modelos de inteligencia artificial aplicados al tratamiento de datos de salud. Su finalidad principal es determinar las medidas técnicas, organizativas y jurídicas necesarias para reducir los niveles de riesgo, establecer controles de seguridad adecuados y estructurar un plan de acción y respuesta ante incidentes. Únicamente en aquellos casos en los que, pese a la implementación de controles, subsistan riesgos altos o críticos para los derechos y libertades de los titulares, corresponderá la realización de una Evaluación de Impacto en la Protección de Datos Personales (EIPD), conforme a la LOPDP y su Reglamento.

El precitado análisis, por ende, se fundamenta en los principios y disposiciones previstos en la LOPDP, en particular aquellos relacionados con la licitud del tratamiento, la finalidad, la proporcionalidad, la seguridad y la responsabilidad proactiva. De igual forma, se consideran

las garantías reconocidas en la Constitución de la República del Ecuador, tales como el derecho a la protección de datos personales, la intimidad, la igualdad y el acceso a servicios de salud adecuados. Asimismo, se incorporan estándares internacionales en materia de protección de datos y gobernanza de sistemas de IA, en cuanto resultan aplicables al contexto analizado.

Desde una perspectiva metodológica, el referido análisis de riesgos se construye a partir de la identificación de activos críticos dentro de una organización del sector de la salud, respecto de los cuales se analizan amenazas, vulnerabilidades y posibles impactos. Los riesgos han sido organizados en dimensiones específicas: (i) privacidad y protección de datos personales, (ii) seguridad de la información, (iii) discriminación y (iv) sesgos algorítmicos, lo que permite un análisis integral de los efectos que el uso de IA puede generar sobre los derechos de los titulares.

Cada riesgo ha sido definido con precisión, codificado de manera sistemática y valorado en función de su probabilidad de ocurrencia y su impacto sobre los derechos fundamentales, lo que permite determinar su nivel de criticidad. En consecuencia, el presente análisis de riesgos constituye una herramienta de decisión previa para determinar si el tratamiento con IA en el ámbito hospitalario puede continuar bajo condiciones reforzadas o si, por el contrario, determinados riesgos impiden o condicionan su implementación. Su finalidad es permitir una lectura razonada de la matriz, identificar los riesgos altos o críticos, justificar las medidas de mitigación necesarias y establecer la base para la futura EIPD y el plan de respuesta ante incidentes, por consiguiente.

Matriz de Valoración de Riesgo

Proyecto	VALORACIÓN DE RIESGO EN EL SECTOR DE LA SALUD
ID	LOPDP-00011
Fecha de inicio	25 DE ABRIL DE 2026
Fecha de fin	28 DE ABRIL DE 2026

Activo	Amenazas	Descripción	Dimensión Afectada	Vulnerabilidad	Probabilidad	Impacto	Riesgo Inherente	Tipo de Control	Controles	Riesgo Residual
1. RESGUARDO DE LA INFORMACIÓN DE LA HISTORIA CLINICA	HACKEOS Y FUGA DE DATOS	**Riesgo P-01:** Acceso no autorizado a datos personales sensibles de salud, sin base jurídica suficiente, lo que puede vulnerar el derecho a la protección de datos personales y el principio de licitud,	Confidencialidad	Acceso sin autenticación robusta, gestión deficiente de permisos, exposición de datos sensibles e insuficiente segmentación de accesos	Muy Probable	**Crítico**	**Crítico**	Preventivo	Anonimización, cifrado de datos, control de acceso y gestión de credenciales	Medio
Información personal del paciente: Datos identificativos y de contacto	Acceso no autorizado y fuga de información personal	**Riesgo P-03:** Exposición o divulgación no autorizada de datos identificativos y de contacto del paciente por fallas de acceso o manejo inadecuado de información.	Confidencialidad	Falta de anonimización y controles de acceso	Muy Probable	**Crítico**	**Crítico**	Preventivo	Anonimización, control de accesos, minimización de datos	Medio
Registro de información clínica del paciente (antecedentes)	Alteración o modificación no autorizada de antecedentes clínicos	**Riesgo P-04:** Modificación indebida o inconsistente de información clínica que afecte la integridad del historial médico.	Integridad	Falta de validación de datos	Muy Probable	**Crítico**	**Crítico**	Preventivo	Validación de datos, auditorías, trazabilidad	Medio

Gestión administrativa del paciente: programación y control de citas médicas, facturación, procesamiento de pagos y administración de información contractual.	Errores en gestión administrativa y acceso indebido	**Riesgo A-02**: Errores o accesos no autorizados en procesos administrativos del paciente, incluyendo citas, facturación y documentación contractual.	Integridad	Deficiencias en autorización y validación de procesos administrativos	Muy Probable	**Crítico**	**Crítico**	Preventivo	Gestión de accesos basada en roles	Medio
Sistema interno del hospital: Plataforma One-book	Hackeo / fuga de datos	**Riesgo S-01:** Vulneración de sistemas clínicos por fallas de seguridad, afectando datos sensibles	Confidencialidad	Vulnerabilidades del sistema, mala configuración	**Inminente**	**Crítico**	**Crítico**	Preventivo	Cifrado, firewall, monitoreo, gestión de accesos	Medio
Uso y almacenamiento de información clínica en dispositivos personales (laptops, tabletas y equipos móviles) del personal médico y administrativo.	Uso no autorizado de dispositivos personales / fuga de información	**Riesgo S-04:** Almacenamiento o traslado de información clínica en dispositivos personales sin controles institucionales adecuados.	Confidencialidad	Falta de políticas de seguridad	Muy Probable	**Crítico**	**Crítico**	Preventivo	Políticas de uso de dispositivos, gestión de dispositivos autorizados y capacitación	Medio
Procesamiento, registro y almacenamiento de resultados clínicos en equipos de laboratorio.	Alteración o corrupción de resultados clínicos	**Riesgo S-10:** Modificación, pérdida o registro incorrecto de resultados clínicos antes de su integración al sistema institucional.	Integridad	Falta de controles y validación	**Inminente**	**Crítico**	**Crítico**	Preventivo	Validación de resultados, auditorías, control de calidad	Medio
Cierre de la atención médica y generación del informe de alta del paciente.	Fuga o uso indebido de información	**Riesgo P-05**: Exposición de datos en reportes finales, vulnerando la intimidad del paciente .	Confidencialidad	Falta de control en generación de informes	Muy Probable	**Crítico**	**Crítico**	Preventivo	Control de acceso, revisión médica, cifrado de documentos	Medio

2. SERVICIOS DE ATENCIÓN MÉDICA VIRTUAL (TELEMEDICINA)	Intercepción de comunicaciones, hackeos, fuga de datos, acceso no autorizado y fallos del sistema	**Riesgo S-02:** Acceso no autorizado a comunicaciones médicas, vulnerando el derecho a la intimidad.	Confidencialidad	Plataformas no seguras, credenciales débiles, falta de cifrado y uso de dispositivos personales sin control	Muy Probable	**Crítico**	**Crítico**	Preventivo	Cifrado de extremo a extremo, autenticación multifactor, control de accesos, auditoría de IA, políticas de seguridad, backups y redundancia	Medio
Consulta médica virtual (videollamadas. Atencion remota)	Intercepción de comunicaciones	**Riesgo S-03:** Acceso indebido a consultas virtuales.	Confidencialidad	Plataformas no seguras	Muy Probable	**Crítico**	**Crítico**	Preventivo	Cifrado de extremo a extremo,	Medio
Transmisión de datos clínicos en línea	Fuga de datos	**Riesgo S-06:** Exposición durante transmisión de información clínica.	Confidencialidad	Falta de cifrado	Muy Probable	**Crítico**	**Crítico**	Preventivo	Cifrado de datos, VPN	Medio
Acceso remoto a historia clínica	Acceso no autorizado	**Riesgo S-07**: Ingreso no autorizado a sistemas clínicos.	Confidencialidad	Credenciales débiles	Muy Probable	**Crítico**	**Crítico**	Preventivo	MFA, control de accesos	Medio
Generación de recetas electrónicas y ordenes de exámenes	Manipulación o falsificación de documentos	**Riesgo S-08:** Falsificación de documentos médicos digitales.	Integridad	Falta de firma digital	**Inminente**	**Crítico**	**Crítico**	Preventivo	Firma electrónica, validación documental y trazabilidad	Medio
Uso de dispositivos personales en telemedicina	Uso no autorizado de aplicaciones y dispositivos personales	**Riesgo S-09:** Fuga de datos por uso de apps no autorizadas.	Confidencialidad	Falta de políticas de seguridad	Muy Probable	**Crítico**	**Crítico**	Preventivo	Restricción de apps, capacitación	Medio
Registro de consultas virtuales	Manipulación de registros clínicos	**Riesgo A-03:** Alteración, pérdida o registro incorrecto de consultas virtuales que comprometa la integridad y trazabilidad de la información clínica.	Integridad	Falta de control de registros	Muy Probable	**Crítico**	**Crítico**	Preventivo	Cifrado de extremo a extremo, autenticación multifactor, control de accesos, políticas de seguridad, backups y redundancia	Medio

Almacenamiento de grabaciones de consultas	Restricción de aplicaciones autorizadas, gestión de dispositivos y capacitación	**Riesgo P-04:** Exposición de grabaciones sensibles.	Confidencialidad	Almacenamiento inseguro	**Inminente**	**Crítico**	**Crítico**	Preventivo	Cifrado, control de accesos	Medio
Seguimiento remoto de pacientes	Fallo del sistema	**Riesgo S-10:** Interrupción del servicio médico.	Disponibilidad	Dependencia tecnológica	**Inminente**	**Crítico**	**Crítico**	Preventivo	Backups, redundancia, continuidad	Medio
Suplantación de identidad	Suplantación de identidad (paciente o profesional de salud)	**Riesgo S-05:** Acceso fraudulento mediante credenciales robadas, vulnerando la seguridad del tratamiento y el derecho a la protección de datos	Confidencialidad	Credenciales débiles, ausencia de autenticación multifactor, falta de validación de identidad en tiempo real, inexistencia de mecanismos biométricos o firma electrónica.	Muy Probable	**Crítico**	**Crítico**	Preventivo	Autenticación multifactor (MFA), verificación biométrica, firma electrónica avanzada, validación de identidad en tiempo real, monitoreo de accesos sospechosos, gestión segura de credenciales.	Medio

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

Impacto a las dimensiones afectas	
5	Crítico
3	Moderado
2	Menor
1	Irrelevante

Riesgo	
4	Alto
3	Medio
2	Bajo
1	Muy Bajo

Probabilidad \ Impacto	Crítico	Severo	Moderado	Menor	Irrelevante
Inminente	Crítico	Crítico	Alto	Medio	Bajo
Muy Probable	Crítico	Alto	Alto	Medio	Bajo
Probable	Alto	Alto	Medio	Bajo	Irrelevante
Poco Probable	Medio	Medio	Bajo	Bajo	Irrelevante
Improbable	Bajo	Bajo	Irrelevante	Irrelevante	Irrelevante

La presente matriz de análisis y valoración de riesgos fue elaborada con el propósito de identificar, evaluar y gestionar los riesgos asociados al tratamiento de datos personales y al uso de tecnologías digitales e inteligencia artificial (IA) en los procesos de atención médica, tanto presencial, como virtual. Su desarrollo responde a la necesidad de proteger activos críticos, tales como la historia clínica, la información de los pacientes, las plataformas hospitalarias y los sistemas de telemedicina, considerando que implican un tratamiento de datos sensibles, cuya afectación puede generar consecuencias jurídicas, operativas y asistenciales.

En este contexto, la precitada matriz estructura un análisis integral que vincula amenazas, vulnerabilidades y dimensiones afectadas tales como la confidencialidad, integridad y disponibilidad, permitiendo determinar el nivel de riesgo y establecer, por consiguiente, controles adecuados. Se identifican amenazas como accesos no autorizados, fuga de datos, manipulación de información clínica y riesgos emergentes derivados de la inteligencia artificial, como el sesgo algorítmico y la falta de explicabilidad. Este análisis no únicamente permite identificar riesgos, sino también comprender su origen y sus posibles efectos sobre los derechos fundamentales de los titulares. El referido enfoque se fundamenta en el principio de responsabilidad proactiva y en la protección de datos desde el diseño previstos en la LOPDP y su Reglamento.

Asimismo, la valoración de los riesgos se sustenta en un *rationale* o razonamiento técnico-jurídico, que garantiza la explicabilidad del análisis. Esto implica que cada nivel asignado, pudiendo ser estos la probabilidad y el impacto, responde a criterios objetivos como el volumen y sensibilidad de los datos, la frecuencia del tratamiento, el uso de inteligencia artificial, la intervención de terceros y la madurez de los controles. De igual forma, se justifica el tipo de control aplicado y las medidas de mitigación, asegurando que la matriz sea

coherente, verificable y alineada con las exigencias normativas. En este sentido, la matriz se convierte en un instrumento auditable y jurídicamente sostenible.

La probabilidad ha sido valorada como “muy probable” o “inminente” debido al tratamiento masivo de datos, la interconexión de sistemas y el uso de inteligencia artificial, que introduce riesgos estructurales como la automatización y la opacidad de los modelos. Por su parte, el impacto se considera “alto” o “crítico” al tratarse de datos de salud, cuya vulneración puede afectar derechos fundamentales. Esto implica que el riesgo no es eventual, sino inherente al propio tratamiento de datos. En consecuencia, la combinación de ambas variables da lugar a niveles de riesgo predominantemente críticos, propios de un entorno de alto riesgo, aunque mitigables mediante controles adecuados.

Finalmente, y en coherencia con el estado del arte, el uso de inteligencia artificial en el sector salud debe evaluarse bajo criterios de necesidad y proporcionalidad. Su implementación únicamente será viable si se justifica su uso, se descartan alternativas menos intrusivas, se realiza una Evaluación de Impacto en la Protección de Datos (EIPD) y se garantiza supervisión humana efectiva; de lo contrario, podría resultar incompatible con la LOPDP en materia de datos sensibles, sobre la base del presente tratamiento en específico. Por lo tanto, la adopción de estas tecnologías debe responder a un equilibrio entre innovación y protección de derechos fundamentales.

Del análisis efectuado se evidencia que los principales riesgos no derivan únicamente de incidentes tradicionales de seguridad de la información, sino también del uso de sistemas de inteligencia artificial integrados directamente en los tratamientos de datos personales de salud. En particular, se identifican riesgos asociados a decisiones automatizadas, perfilamiento, sesgos algorítmicos, falta de explicabilidad y dependencia de modelos

predictivos, lo que confirma la necesidad de implementar mecanismos de supervisión humana significativa, gobernanza algorítmica y controles reforzados de protección de datos desde el diseño.

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

Considerando los altos riesgos asociados al tratamiento de datos biométricos y sistemas de inteligencia artificial en el sector salud, resulta indispensable contar con mecanismos internos que permitan gestionar adecuadamente incidentes de seguridad y brechas de datos personales. En este contexto, el presente apartado desarrolla un **Plan de Respuesta ante Incidentes de Seguridad** orientado a establecer procedimientos de detección, contención, notificación, mitigación y documentación de vulneraciones de seguridad, conforme a la LOPDP, su Reglamento General y los principios de responsabilidad proactiva y gestión de riesgos aplicables al tratamiento de datos personales sensibles:

***REF**: Documento disponible en el Anexo No. 4.*

CAPITULO IV

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

1.1. Identificación del conflicto jurídico concreto

El caso concreto plantea un conflicto jurídico entre el derecho fundamental a la protección de datos personales y el derecho a la intimidad de los pacientes, frente al interés institucional del

Hospital Oncológico Vida Nueva de implementar sistemas biométricos con inteligencia artificial para fortalecer la seguridad hospitalaria, restringir accesos no autorizados y optimizar la gestión clínica.

La tensión con el derecho a la salud surge porque el Hospital Oncológico Vida Nueva tiene la obligación de garantizar la continuidad, calidad y seguridad de la atención sanitaria, así como la confidencialidad de las historias clínicas y demás información médica de los pacientes. Desde esta perspectiva, la implementación de mecanismos de autenticación robusta busca prevenir accesos no autorizados, errores en la identificación de usuarios y posibles incidentes que podrían comprometer la prestación de servicios de salud. Por tanto, la medida persigue la protección de bienes jurídicos vinculados al derecho a la salud, particularmente la seguridad del paciente y la adecuada gestión de información clínica. Sin embargo, la consecución de dichos fines debe armonizarse con el respeto al derecho a la protección de datos personales y a la intimidad, evitando restricciones desproporcionadas o innecesarias.

1.2. Identificación y delimitación de los derechos involucrados

Se identifican como derechos directamente afectados el derecho a la protección de datos personales, la intimidad y la autodeterminación informativa, debido a que el hospital realiza tratamientos de datos biométricos y datos relativos a la salud mediante sistemas tecnológicos de autenticación y control hospitalario. La afectación adquiere especial relevancia por tratarse de información altamente sensible y confidencial, cuyo uso indebido o exposición podría generar consecuencias permanentes sobre la privacidad y dignidad de los titulares. Por otra parte, el interés contrapuesto corresponde a la seguridad hospitalaria, la confidencialidad de las historias clínicas y el derecho a la salud, en tanto el hospital busca garantizar un acceso seguro y eficiente a información médica crítica, prevenir suplantaciones y

fortalecer los controles de acceso institucionales. Los titulares afectados son principalmente pacientes oncológicos, personal médico y trabajadores administrativos, destacándose los pacientes como un grupo en situación de especial vulnerabilidad debido a su condición médica y a la sensibilidad de la información tratada.

1.3. Determinación de la intensidad de la afectación

La afectación al derecho a la protección de datos personales puede calificarse como alta debido a la concurrencia de varios factores. En primer lugar, el tratamiento involucra datos biométricos, considerados categorías especiales de datos por su capacidad de identificar de manera unívoca a una persona y por su carácter permanente e irreversible. En segundo lugar, dichos datos se encuentran vinculados a información relativa a la salud de pacientes oncológicos, cuya protección exige un estándar reforzado de tutela conforme a la Ley Orgánica de Protección de Datos Personales y a los instrumentos internacionales de derechos humanos. Finalmente, la utilización de sistemas de inteligencia artificial incrementa los riesgos de errores de identificación, opacidad algorítmica y limitaciones para el ejercicio efectivo de los derechos de los titulares, circunstancias que elevan significativamente la intensidad de la injerencia sobre el derecho fundamental analizado.

1.4. Aplicación del test de proporcionalidad

En cuanto al juicio de idoneidad, el sistema biométrico resulta apto para fortalecer la seguridad hospitalaria, restringir accesos indebidos y garantizar la trazabilidad sobre historias clínicas y plataformas institucionales. La biometría permite autenticar usuarios mediante identificadores únicos y reducir riesgos de suplantación dentro de un entorno sanitario en el que la protección de la información clínica constituye una finalidad constitucionalmente legítima.

Respecto del juicio de necesidad, corresponde analizar si la utilización de biometría constituye la medida menos restrictiva para alcanzar el objetivo perseguido. En este contexto, resulta necesario valorar la eficacia comparativa de mecanismos alternativos, tales como la autenticación multifactor, los tokens de seguridad, las credenciales institucionales con doble verificación y los sistemas reforzados de auditoría. La existencia de estas alternativas plantea la necesidad de justificar por qué el tratamiento biométrico sería indispensable para alcanzar el mismo nivel de protección de la información clínica y de seguridad institucional. En consecuencia, la evaluación debe centrarse en determinar si la biometría aporta una ventaja sustancial que no pueda obtenerse mediante mecanismos menos intrusivos para los derechos de los titulares.

En cuanto a la proporcionalidad en sentido estricto, corresponde valorar si los beneficios derivados del fortalecimiento de la seguridad hospitalaria compensan la intensidad de la afectación producida sobre el derecho a la protección de datos personales y la intimidad. Si bien la biometría puede incrementar los niveles de seguridad y reducir riesgos de acceso indebido, también implica un tratamiento intensivo de categorías especiales de datos, cuyos efectos potenciales pueden extenderse de manera permanente sobre los titulares en caso de vulneración o uso indebido.

1.5. Conclusión ponderativa

En consecuencia, la legitimidad constitucional de la medida dependerá de que el Hospital Oncológico Vida Nueva pueda demostrar que el uso de biometría resulta estrictamente necesario para alcanzar los fines perseguidos y que no existen alternativas menos intrusivas con eficacia equivalente. Asimismo, deberá implementar garantías reforzadas de protección de datos, tales como minimización, cifrado, limitación de acceso, supervisión humana efectiva y la realización previa de una Evaluación de Impacto en la Protección de Datos. Solo

bajo estas condiciones podría considerarse constitucionalmente admisible la restricción al derecho a la protección de datos personales y al derecho a la intimidad.

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

2.1. Descripción sintética del tratamiento

La Evaluación de Impacto en la Protección de Datos Personales (EIPD) es necesaria en el Hospital Oncológico Vida Nueva debido a que el tratamiento proyectado involucra datos biométricos, datos de salud, sistemas de inteligencia artificial y acceso a historias clínicas dentro de un entorno sanitario de alta sensibilidad. El sistema utiliza reconocimiento facial como mecanismo de autenticación para fortalecer la seguridad, trazabilidad y protección de la información clínica de pacientes, personal sanitario y personal administrativo.

2.2. Justificación de la obligatoriedad de la EIPD

La obligatoriedad de la EIPD se refuerza por el uso de datos biométricos, cuya naturaleza irreversible implica riesgos superiores a los de otros mecanismos de identificación, justamente porque la biometría es difícil de revocar si se compromete. Además, el tratamiento se realiza a escala institucional, involucrando múltiples titulares y procesos asistenciales críticos, lo que incrementa el impacto potencial ante accesos indebidos, filtraciones o usos no autorizados de la información. Por ello, resulta indispensable evaluar previamente los riesgos y la eficacia de medidas como cifrado, seudonimización, autenticación multifactor, limitación de accesos y procedimientos de respuesta ante incidentes.

Por consiguiente, la EIPD se justifica por la concurrencia de múltiples factores de alto riesgo que pueden afectar los derechos a la protección de datos, la intimidad y la salud. Su finalidad

es determinar si el tratamiento cumple con los principios de necesidad, proporcionalidad, minimización, seguridad, supervisión humana y privacidad desde el diseño, así como verificar si las medidas implementadas permiten reducir los riesgos a niveles aceptables.

2.3. Identificación de riesgos relevantes

La identificación de riesgos en el Hospital Oncológico Vida Nueva permitió evidenciar que los principales riesgos asociados al uso de sistemas de inteligencia artificial se relacionan con accesos no autorizados a historias clínicas, exposición de información sensible, alteración de registros médicos y decisiones automatizadas sustentadas en modelos algorítmicos potencialmente sesgados. En este contexto, los riesgos pueden agruparse de la siguiente manera, riesgos para los derechos y libertades dentro del cual existe la posibilidad de acceso no autorizado, filtración o uso indebido de datos personales y clínicos, lo que podría afectar los derechos a la privacidad y a la protección de datos personales, considerando la naturaleza sensible de la información tratada; riesgos tecnológicos, los sistemas de IA pueden generar errores debido a datos incompletos, fallos técnicos o limitaciones algorítmicas. Estas situaciones podrían afectar el derecho a la protección de la salud y a la integridad física al influir en decisiones médicas incorrectas; riesgos organizacionales la dependencia excesiva de la tecnología, la falta de supervisión profesional o la insuficiente capacitación del personal pueden derivar en decisiones inadecuadas y comprometer la calidad y seguridad de la atención sanitaria, y riesgos de sesgo y discriminación, la utilización de conjuntos de datos no representativos puede generar resultados menos precisos para determinados grupos poblacionales, afectando los derechos a la igualdad y a la no discriminación.

Estos riesgos adquieren especial relevancia debido a que el tratamiento involucra datos que permiten identificar directamente a los pacientes y revelar información íntima relacionada con su estado de salud y características biométricas.

2.4. Medidas de mitigación previstas o propuestas

Para mitigarlos, se plantean medidas técnicas, organizativas y jurídicas. Entre las primeras destacan el cifrado, la autenticación multifactor, los controles de acceso, la anonimización y las auditorías de seguridad. A nivel organizativo, se propone la capacitación continua del personal, la definición de responsabilidades y la supervisión humana de las decisiones clínicas relevantes. Finalmente, las medidas jurídicas contemplan el cumplimiento de la normativa de protección de datos, la obtención del consentimiento cuando corresponda y la realización de evaluaciones de impacto.

En consecuencia, se concluye que el uso del sistema de inteligencia artificial analizado no resulta jurídicamente viable en su estado actual. Aunque ofrece beneficios para el diagnóstico y la gestión clínica, persisten riesgos relevantes relacionados con la protección de datos, la transparencia de las decisiones automatizadas, los errores algorítmicos y los posibles sesgos discriminatorios. Si bien las medidas de mitigación reducen estos riesgos, no garantizan plenamente la protección efectiva de los derechos fundamentales de los pacientes, por lo que se requiere fortalecer los mecanismos de supervisión, auditoría, transparencia y control humano antes de considerar su implementación.

2.5. Evaluación del riesgo residual

A pesar de las medidas de mitigación implementadas, persiste un riesgo residual elevado para los derechos y libertades de los titulares debido a la naturaleza especialmente sensible

de los datos tratados y al uso de sistemas de inteligencia artificial en procesos relacionados con la atención médica. En particular, subsisten riesgos asociados a accesos no autorizados, filtraciones de información, alteración de registros clínicos y posibles errores o sesgos en las recomendaciones automatizadas, los cuales podrían afectar los derechos a la privacidad, protección de datos personales, igualdad, no discriminación, salud e integridad de los pacientes.

Desde una perspectiva jurídica, el riesgo residual no puede considerarse plenamente aceptable en el estado actual del tratamiento. No obstante, podría resultar tolerable de forma condicionada si se demuestra la necesidad del tratamiento, la inexistencia de alternativas menos intrusivas y la implementación de controles reforzados, incluyendo supervisión humana efectiva, auditorías periódicas, gestión de sesgos, trazabilidad de las decisiones y mecanismos claros de responsabilidad. En consecuencia, la continuidad del tratamiento debe estar sujeta a la adopción y verificación previa de medidas adicionales que garanticen una protección adecuada de los derechos fundamentales de los titulares.

2.6. Conclusión de la DPIA

La presente EIPD permite concluir que el tratamiento analizado no resulta jurídicamente viable en los términos propuestos. Si bien la finalidad perseguida como fortalecer la seguridad hospitalaria, optimizar el control de acceso y mejorar la gestión clínica es legítima y constitucionalmente relevante, el tratamiento implica una afectación intensa a los derechos a la protección de datos personales, la intimidad y la autodeterminación informativa, debido al uso conjunto de datos biométricos, datos de salud e inteligencia artificial. Del análisis de riesgos, la ponderación de derechos y el test de proporcionalidad realizado se desprende que la medida supera el juicio de idoneidad, pero no supera de manera suficiente el juicio de necesidad, al existir alternativas menos intrusivas que

permitirían alcanzar niveles razonables de seguridad sin recurrir al tratamiento masivo y permanente de categorías especiales de datos.

Adicionalmente, aun cuando se implementen medidas de mitigación técnicas, organizativas y jurídicas, subsiste un riesgo residual elevado derivado de la naturaleza irreversible de los datos biométricos, la opacidad inherente a los sistemas de IA y las posibles consecuencias sobre los derechos fundamentales de los pacientes, quienes constituyen un grupo especialmente vulnerable. En consecuencia, el tratamiento presenta una incompatibilidad estructural con los principios de necesidad, minimización y proporcionalidad exigidos por la LOPDP y por los estándares desarrollados en materia de protección de datos personales que forman parte del bloque de constitucionalidad ecuatoriano. Por ello, desde una perspectiva jurídica y constitucional, la implementación del sistema biométrico con IA en el contexto analizado no puede considerarse una medida legítima ni proporcional, debiendo optarse por mecanismos alternativos menos lesivos que permitan alcanzar la misma finalidad con una menor afectación a los derechos de los titulares.

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

3.1.Viabilidad Jurídica

Luego del análisis del proyecto, del marco normativo aplicable y de la evaluación de riesgos realizada, se concluye que la implementación del sistema biométrico propuesto para el Hospital Oncológico Vida Nueva no es jurídicamente viable en las condiciones actuales. Si bien la finalidad de fortalecer la seguridad institucional y controlar el acceso a las historias clínicas electrónicas es legítima, el tratamiento involucra datos biométricos y datos de salud,

categorías especiales de datos personales que requieren una protección reforzada conforme a la normativa ecuatoriana.

La evaluación evidenció riesgos elevados para los derechos y libertades de los titulares, especialmente en relación con la privacidad, la confidencialidad de la información sanitaria y la protección de datos personales. Debido al carácter sensible, permanente e irreversible de los datos biométricos, y al mantenimiento de un riesgo residual significativo que no supera adecuadamente los principios de necesidad, proporcionalidad y minimización, se recomienda abstenerse de implementar el sistema y optar por mecanismos de autenticación menos invasivos y más compatibles con la legislación vigente.

3.2. Fundamentos de la decisión

La presente decisión se fundamenta en el análisis del marco constitucional ecuatoriano, la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento y los resultados de la Evaluación de Impacto en la Protección de Datos Personales (EIPD) realizada para la implementación de un sistema de autenticación biométrica con inteligencia artificial en el Hospital Oncológico Vida Nueva. Si bien la finalidad perseguida de proteger la seguridad de las historias clínicas electrónicas y evitar accesos no autorizados, es legítima, el tratamiento propuesto involucra categorías especiales de datos personales, como datos biométricos y datos de salud, lo que exige un nivel reforzado de protección y una evaluación estricta de necesidad y proporcionalidad.

3.3. Recomendaciones jurídicas y organizacionales

Con base en el análisis normativo, la ponderación de derechos y los resultados de la Evaluación de Impacto en Protección de Datos Personales, cualquier decisión sobre la implementación de un sistema biométrico debe ajustarse a los principios de licitud,

transparencia, finalidad, minimización, proporcionalidad, seguridad y responsabilidad proactiva. En caso de considerarse viable su implementación, el Hospital deberá establecer controles reforzados, incluyendo una base jurídica clara, información previa a los titulares, limitación estricta de la finalidad, restricciones al uso secundario de los datos, períodos de conservación definidos, medidas de seguridad adecuadas y auditorías periódicas con participación del Delegado de Protección de Datos y las áreas competentes.

Si la viabilidad fuera condicionada, el tratamiento deberá limitarse exclusivamente a los casos estrictamente necesarios, restringiéndose a áreas críticas y finalidades vinculadas con la seguridad de acceso a historias clínicas, garantizando además alternativas no biométricas que eviten efectos discriminatorios. No obstante, para el Hospital Oncológico Vida Nueva, al haberse determinado la no viabilidad jurídica del sistema biométrico, se recomienda abstenerse de su implementación y optar por mecanismos de autenticación menos invasivos, seguros y compatibles con la normativa ecuatoriana de protección de datos personales.

3.4. Conclusiones

En definitiva, la evaluación integral del tratamiento permite concluir que la implementación de sistemas biométricos con IA para el acceso y gestión de historias clínicas en el Hospital Oncológico Vida Nueva presenta una incompatibilidad sustancial con los estándares reforzados de protección exigibles para el tratamiento de datos biométricos y datos de salud. La intensidad de la afectación potencial sobre los derechos a la protección de datos personales, intimidad, autodeterminación informativa e igualdad, sumada a la existencia de alternativas menos intrusivas capaces de satisfacer la finalidad de seguridad perseguida, impide considerar jurídicamente admisible la medida en las condiciones analizadas. En consecuencia, cualquier eventual replanteamiento del proyecto requerirá una reformulación

integral de su alcance, arquitectura y mecanismos de control, acompañada de una nueva evaluación que permita verificar si las condiciones que fundamentan la presente decisión han sido efectivamente superadas.

CAPITULO V

1. CONCLUSIONES GENERALES

La presente investigación permitió concluir que la implementación de un sistema de autenticación biométrica basado en inteligencia artificial para el acceso a historias clínicas y otros sistemas del Hospital Oncológico Vida Nueva constituye un tratamiento de datos personales de alto riesgo, debido a que involucra simultáneamente datos biométricos y datos relativos a la salud, categorías especialmente protegidas por la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales y los estándares internacionales de protección de datos. En consecuencia, la viabilidad jurídica de este tratamiento no puede presumirse de manera automática, sino que se encuentra condicionada al cumplimiento estricto de los principios de licitud, necesidad, proporcionalidad, minimización, seguridad, transparencia y responsabilidad proactiva y demostrada.

Respecto del primer problema jurídico planteado, se determinó que el uso de biometría en el Hospital Oncológico Vida Nueva es jurídicamente viable únicamente de manera condicionada. La investigación evidenció que la finalidad perseguida por la organización (fortalecer la seguridad, la trazabilidad y el control de acceso a información clínica sensible) es legítima; sin embargo, la legitimidad de la finalidad no resulta suficiente para justificar por sí sola el tratamiento de datos biométricos. La organización debe demostrar que la biometría constituye una medida necesaria frente a alternativas menos intrusivas y que su

implementación incorpora garantías técnicas, jurídicas y organizativas reforzadas que permitan proteger adecuadamente los derechos y libertades de los titulares.

En relación con el segundo problema jurídico, se concluyó que el uso de biometría en el ámbito sanitario no resulta recomendable de forma irrestricta, debido a la sensibilidad e irreversibilidad de los datos biométricos y a los riesgos derivados de errores de autenticación, accesos indebidos, filtraciones de información, sesgos algorítmicos y decisiones automatizadas. No obstante, cuando existan necesidades de seguridad especialmente justificadas y no se disponga de mecanismos alternativos igualmente eficaces y menos invasivos, su utilización podría considerarse admisible siempre que se adopten medidas robustas de privacidad desde el diseño y por defecto, supervisión humana efectiva, auditorías periódicas, mecanismos de explicabilidad y controles permanentes de seguridad de la información.

Finalmente, respecto del tercer problema jurídico, la Evaluación de Impacto en la Protección de Datos Personales realizada permitió identificar, analizar y valorar los riesgos asociados al tratamiento proyectado, concluyendo que estos pueden reducirse significativamente mediante la implementación de medidas de mitigación adecuadas. Sin embargo, la existencia de riesgos residuales inherentes a la naturaleza de la biometría y de la inteligencia artificial impide considerar el tratamiento como completamente exento de riesgos. Por tal motivo, la EIPD no justifica una implementación incondicional, sino una viabilidad condicionada al mantenimiento permanente de controles técnicos, organizativos y jurídicos que garanticen la protección efectiva de los derechos fundamentales de los pacientes.

En definitiva, la investigación demuestra que la inteligencia artificial y los sistemas biométricos pueden aportar beneficios relevantes al sector de la salud, pero su implementación debe desarrollarse bajo un modelo de gobernanza basado en la protección

de datos personales, la gestión de riesgos y el respeto a la dignidad humana. La innovación tecnológica no constituye un fin en sí mismo, sino una herramienta que únicamente resulta legítima cuando se encuentra subordinada a la protección efectiva de los derechos fundamentales de las personas.

1.2. CONCLUSIONES ESPECÍFICAS

1. La utilización de sistemas de inteligencia artificial para el tratamiento de datos biométricos y relativos a la salud representa una actividad de alto riesgo, debido a la naturaleza especialmente sensible de la información involucrada y a la posibilidad de afectar derechos fundamentales como la privacidad, la igualdad, la no discriminación, la dignidad y la protección de la salud.
2. Aunque la inteligencia artificial puede contribuir a optimizar la gestión de la información clínica y apoyar la toma de decisiones médicas, sus resultados no deben considerarse infalibles, ni sustituir el criterio de los profesionales de la salud. La falta de transparencia de determinados modelos, los errores algorítmicos y la utilización de datos incompletos o poco representativos pueden producir diagnósticos, clasificaciones o recomendaciones incorrectas.
3. El tratamiento de esta información exige el cumplimiento reforzado de los principios establecidos en la Ley Orgánica de Protección de Datos Personales, particularmente los de juridicidad, transparencia, finalidad, minimización, proporcionalidad, exactitud, seguridad, confidencialidad y responsabilidad proactiva. El cumplimiento formal de la normativa no resulta suficiente si no se acompaña de medidas técnicas, organizativas y jurídicas efectivas.
4. La calidad, integridad, actualización y representatividad de los datos utilizados para entrenar y operar los sistemas de inteligencia artificial son elementos determinantes

para garantizar resultados confiables. La utilización de bases de datos sesgadas o insuficientes puede reproducir patrones discriminatorios y afectar con mayor intensidad a determinados pacientes o grupos vulnerables.

5. La supervisión humana constituye una garantía indispensable en el ámbito sanitario. Toda decisión que pueda producir efectos jurídicos, médicos o significativos sobre los pacientes debe permitir la intervención de personal competente, la revisión de los resultados, la corrección de errores y la impugnación de las decisiones automatizadas.
6. Antes de implementar el sistema, el Hospital Oncológico Vida Nueva deberá realizar una Evaluación de Impacto en Protección de Datos Personales que permita identificar los riesgos, valorar su probabilidad y gravedad, determinar las medidas de mitigación y comprobar si el riesgo residual resulta jurídicamente aceptable. Esta evaluación deberá complementarse con auditorías periódicas, controles de seguridad, monitoreo continuo y mecanismos de trazabilidad.
7. En las condiciones actualmente analizadas, la implementación del sistema no resulta jurídicamente viable, debido a que no se han acreditado garantías suficientes para prevenir accesos no autorizados, pérdida o alteración de información clínica, decisiones automatizadas erróneas, discriminación algorítmica o afectaciones a los derechos de los titulares.
8. La inviabilidad identificada no debe interpretarse como una prohibición definitiva del uso de inteligencia artificial en el Hospital. El proyecto podría ser reconsiderado cuando se establezca una base de legitimación adecuada, se delimiten claramente las finalidades del tratamiento, se adopten medidas de privacidad desde el diseño y por defecto, se garantice la intervención humana y se demuestre que los riesgos han sido reducidos a un nivel aceptable.

En consecuencia, cualquier futura implementación deberá estar precedida por un modelo integral de gobernanza de datos e inteligencia artificial, orientado no solo al cumplimiento normativo, sino también a garantizar que la tecnología sea segura, transparente, explicable, proporcional y respetuosa de los derechos de los pacientes.

Bibliografía (Normas APA) (Biblioteca Virtual de UIDE)

Cavoukian, A. (2011). *Privacy by Design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.

Campillo, P. (2019). *El derecho de protección de datos personales y la industria de la salud digital*. Universidad Carlos III de Madrid. https://e-archivo.uc3m.es/entities/publication/189238d8-d15e-4c72-a3f0-e006d5cf8530

Deben eliminarse la referencia de **Lorena, P. C. (2019)** porque corresponde a la misma obra y constituye un duplicado.

Diana, M. (2025). *Inteligencia artificial en la gestión de servicios de salud: desafíos éticos, beneficios y oportunidades* [Trabajo de titulación, Pontificia Universidad Católica del Ecuador]. Repositorio Institucional PUCE. https://repositorio.puce.edu.ec/items/35cdc1bb-0aa3-4a54-97c4-05ef93d38cbf

International Organization for Standardization. (2017). *ISO/IEC 29134:2017. Information technology—Security techniques—Guidelines for privacy impact assessment*. ISO.

Iñiguez Pineda, M. J., & Maldonado Ruiz, L. M. (2025). Protección de datos personales frente al desarrollo de inteligencia artificial en Ecuador: Análisis y propuestas legislativas. *Visionario Digital, 9*(2), 24–48. https://doi.org/10.33262/visionariodigital.v9i2.3366

Lalama-Flores, M. A., Lalama-Gavilánez, M. S., López-Barrionuevo, C. G., & Reyes-Pérez, M. A. (2025). Perspectiva de los profesionales de la salud ante la adopción de inteligencia artificial en la medicina. *Revista Metropolitana de Ciencias Aplicadas, 8*(2), 66–73. https://doi.org/10.62452/rn2d5e60

Michelini, D., Berón, S., & Bridarolli, I. (2025). Ética e inteligencia artificial generativa (IAG) en la investigación educativa superior y en la salud mental. En S. Otero, M. E. Crowe, A. Sartuqui, & A. Altman (Eds.), *Actas de las Jornadas ICALA 2025* (pp. 127-140). Ediciones del ICALA. https://www.icala.org.ar/publicaciones/Libros-EdICALA/ACTAS-Jornadas%20ICALA%202025.pdf

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2), 1–21. https://doi.org/10.1177/2053951716679679

Naranjo, L. (2022). *Protección de datos personales en Ecuador: Comentarios a la Ley Orgánica de Protección de Datos Personales*. Corporación de Estudios y Publicaciones.

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. U.S. Department of Commerce.

Piñar Mañas, J. L. (2016). *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*. Reus.

Remolina Angarita, N. (2020). *Tratamiento de datos personales: Aproximación internacional y latinoamericana*. Universidad de los Andes.

Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.

Velasco San Pedro, L. A. (2019). *Protección de datos personales y derechos fundamentales en la sociedad digital*. Tirant lo Blanch.

World Health Organization. (2021). *Ethics and governance of artificial intelligence for health: WHO guidance*. World Health Organization. https://www.who.int/publications/i/item/9789240029200

Normativa Nacionales

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

Ecuador. Presidencia de la República. (2023).

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

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

Resoluciones, lineamientos y directrices para la aplicación de la Ley Orgánica de Protección de Datos Personales. Superintendencia de Protección de Datos Personales. Superintendencia de Protección de Datos Personales. (2024).

Normativa Internacional

Agencia Española de Protección de Datos. (2021). *Guía de evaluaciones de impacto relativas a la protección de datos (EIPD)*. Agencia Española de Protección de Datos.

Agencia Española de Protección de Datos. (2025). *¿Qué es la protección de datos desde el diseño y por defecto?* https://www.aepd.es/preguntas-frecuentes/2-tus-obligaciones-como-responsable-del-tratamiento/9-analisis-de-riesgos/FAQ-0224-que-es-la-proteccion-de-datos-desde-el-diseno-y-por-defecto

European Data Protection Board. (2023). *Guidelines on data protection impact assessment (DPIA) and high-risk processing*. European Data Protection Board.

International Organization for Standardization. (2022). *ISO/IEC 27701:2019. Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines*. ISO.

Ministerio de Salud Pública del Ecuador. (2024). *Política Nacional de Transformación Digital del Sector Salud*. https://www.salud.gob.ec/wp-content/uploads/2025/07/polltica_nacional_de_transformaciOn_digital_del_sector_salud_14nov2024___.pdf

Organización de los Estados Americanos. (2021). *Principios actualizados sobre la privacidad y la protección de datos personales*. Organización de los Estados Americanos.

Organización Mundial de la Salud. (2024). *Inteligencia artificial para la salud*. https://www.who.int/publications/m/item/artificial-intelligence-for-health

Organization for Economic Co-operation and Development. (2013). *OECD guidelines governing the protection of privacy and transborder flows of personal data*. OECD Publishing.

Red Iberoamericana de Protección de Datos. (2017). *Estándares de protección de datos personales para los Estados iberoamericanos*. https://www.redipd.org

ANEXOS

ANEXO NO. 1 – AVISOS DE PRIVACIDAD (INTERNO & EXTERNO)

AVISO DE PRIVACIDAD (INTERNO):

El Hospital Oncológico Vida Nueva, en cumplimiento con lo dispuesto en la LOPDP, su Reglamento, Resoluciones de la Superintendencia de Protección de Datos Personales, y demás normativa aplicable en la materia (en conjunto, "Normativa de Protección de Datos Personales"), implementa la siguiente Política General de Protección de Datos (la "Política"), con la finalidad de establecer los lineamientos y principios bajo los cuales realizará el tratamiento de datos personales en el desarrollo de sus actividades.

1. ¿Quién es el responsable del tratamiento de mis datos personales?: Conforme a lo establecido en la LOPDP, El Hospital es la responsable del tratamiento de los datos personales objeto de este instrumento y pone a disposición de sus colaboradores el presente Aviso, con el objeto de garantizar su derecho a la protección de éstos contenida en nuestros archivos/bases de datos personales.

Adicionalmente le informamos:

- Nuestra denominación social: Hospital Oncológico Vida Nueva
- Nuestra dirección: Av. Paraíso y Agustín Landívar Cuenca-Ecuador.
- El canal de contacto de nuestro Delegado de protección de datos personales: dpd@hospitalvidanueva.med.ec
- Teléfono: 074096567, ext. 2507 – 1720.

El Hospital ha designado un Delegado de Protección de Datos Personales (“DPD”), quien, de forma independiente, vela por el correcto cumplimiento de la Normativa de Protección de Datos Personales, además de ser el punto de contacto de la compañía con la Autoridad de Protección de Datos Personales. Los datos de contacto del DPD de El Hospital son los siguientes:

- Nombre: Juan Martin Pérez Solano
- Dirección: Avenida del Paraíso y Agustín Landivar
- Correo electrónico: dpd@hospitalvidanueva.med.ec
- Número de teléfono: 074096567 ext. 2507 – 1720.

2. Alcance: El presente Aviso Interno de Protección de Datos Personales aplica al tratamiento de los datos personales proporcionados por los colaboradores de El Hospital, así como de aquellos que se recolecten en el marco de la relación laboral, en la medida en que sean necesarios para la gestión, desarrollo y cumplimiento de las obligaciones derivadas de dicha relación.

3. Base Legal: El tratamiento de los datos personales de los colaboradores de El Hospital se realiza conforme a lo dispuesto en la LOPDP y se fundamenta en: (i) la necesidad del tratamiento para la ejecución de la relación laboral y el cumplimiento de obligaciones contractuales y precontractuales; (ii) el cumplimiento de obligaciones legales y regulatorias a cargo del empleador; (iii) la satisfacción de intereses legítimos del Hospital, siempre que no prevalezcan los derechos y libertades fundamentales del titular; y (iv) el consentimiento del titular, en los casos en que la ley así lo exija.

4. Definiciones: Para efectos del presente Aviso Interno de Protección de Datos Personales, se entenderá por:

- Datos personales: Información que identifica o hace identificable a una persona natural, directa o indirectamente.
- Datos sensibles: Datos personales que, por su naturaleza, requieren una protección especial, tales como aquellos relativos a la salud, datos biométricos, origen étnico, entre otros.
- Titular: Persona natural a quien corresponden los datos personales; para efectos del presente aviso, los colaboradores de El Hospital.
- Responsable del tratamiento: Persona natural o jurídica que decide sobre la finalidad y tratamiento de los datos personales; en este caso, El Hospital.
- Encargado del tratamiento: Persona natural o jurídica que trata datos personales por cuenta del responsable.
- Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- Consentimiento: Manifestación de la voluntad libre, específica, informada e inequívoca del titular para el tratamiento de sus datos personales.
- Anonimización: Proceso mediante el cual los datos personales dejan de ser atribuibles a un titular identificado o identificable.
- Base legal: Fundamento jurídico que legitima el tratamiento de datos personales.
- Transferencia de datos: Comunicación de datos personales a un tercero dentro o

fuera del territorio ecuatoriano.

- Medidas de seguridad: Conjunto de acciones técnicas, organizativas y administrativas destinadas a proteger los datos personales.

5. Finalidades del Tratamiento: El Hospital tratará los datos personales de sus colaboradores para las siguientes finalidades:

- La gestión integral de la relación laboral, desde la etapa precontractual hasta su terminación.
- El cumplimiento de obligaciones legales y regulatorias aplicables al empleador. o La administración de procesos internos, incluyendo nómina, talento humano, evaluación de desempeño y capacitación.
- La implementación de medidas de seguridad física y lógica, incluyendo control de accesos y, de ser el caso, sistemas biométricos.
- La gestión de la salud ocupacional y prevención de riesgos laborales.
- La atención de requerimientos de autoridades competentes.

6. ¿Cómo recogen mis datos?: Los datos personales de los colaboradores del Hospital son recabados principalmente de forma directa del titular, mediante la entrega de información en formularios, documentos, plataformas institucionales o sistemas informáticos, tanto en la etapa precontractual como durante la ejecución de la relación laboral.

Adicionalmente, podrán obtenerse de forma indirecta a través de terceros autorizados o fuentes públicas y privadas, siempre que exista una base legal que legitime dicho tratamiento, conforme a la LOPDP.

7. ¿Qué datos personales están siendo tratados?: En virtud de la relación entre el Colaborador y El Hospital. El Hospital tratará los siguientes datos:

a. Datos Personales no sensibles:

- Datos identificativos (como, por ejemplo: número de cédula, nombres, apellidos, entre otros).
- Datos de contacto (como, por ejemplo: correo electrónico, dirección del domicilio, celular, entre otros).
- Datos de características personales (como, por ejemplo: estado civil, número de cargas familiares, edad, sexo, entre otros).
- Datos de circunstancias sociales (como, por ejemplo: características de alojamiento, vivienda, situación familiar, propiedades, posesiones, aficiones y estilos de vida, entre otros).
- Datos financieros (como, por ejemplo, estado de la cuenta bancarias y saldos promedio, declaraciones del IVA, impuesto a la renta, entre otros).
- Académicos o profesionales (como, por ejemplo: formación educativa, titulaciones, historial del estudiante, experiencia profesional).

b. Datos Personales Sensibles:

- Datos Biométricos (como, por ejemplo: huella dactilar, reconocimiento facial, entre otros).
- Características personales o fisiológicas (como, por ejemplo: peso, estatura, entre otros).

- Datos de salud (como, por ejemplo: enfermedades o discapacidades, entre otros).
- Origen étnico o racial (como, por ejemplo: nacionalidad, entre otros).
- Antecedentes penales, procesos judiciales o investigaciones previas. También podrán tratarse datos de geolocalización, dirección IP, navegación a través herramientas tecnológicas de la entidad o aplicativos móviles, así como grabaciones o imágenes.

La normativa sobre tratamiento de datos clasifica como “categorías especiales” a ciertos datos sensibles, entre los cuales se incluye, la información sobre su estado de salud, biométricos, entre otros. El Hospital no recopilará ni utilizará este tipo de datos, a menos que exista una obligación legal de hacerlo o sean necesarios para el cumplimiento de la relación contractual existente. Respecto de los datos de salud, la obtención y el tratamiento del dato se realizará conforme a los requisitos establecidos en la normativa vigente, para lo cual consiente explícitamente su tratamiento.

Para ello, El Hospital ha implementado acciones, medidas y previsiones especiales, tendientes a salvaguardar el derecho a la protección de datos personales.

8. ¿Cómo y por qué están siendo tratados mis datos personales?: El Hospital tratara distintos tipos de datos personales para las finalidades indicadas en esta sección. Los datos personales se utilizarán:

a. Sobre la base de la ejecución de nuestras obligaciones contractuales, para:

- Desarrollar, mantener, cumplir y controlar el cumplimiento de sus funciones, y dar cumplimiento a las obligaciones y funciones del departamento de Recursos Humanos

relativas a las actividades de formación y capacitación, control de asistencia, gestión de nóminas y beneficios sociales.

- Pago de nómina.
- Identificación.
- Resguardo de información de prestaciones de trabajadores.
- Gestión de seguros para la atención de enfermedades o accidentes, seguros de vida, así como todos aquellos seguros y/o servicios relacionados a esto con motivo de la relación laboral, incluida la seguridad social obligatoria.
- Emisión y gestión de beneficios, recompensas y premios. o Administración de personal para el ingreso y salida de los trabajadores (cartas de renuncia, liquidación laboral, información de entrevistas de salida), así como cambios en la relación laboral (promociones, transferencias).
- Evaluaciones del desempeño y reportes de competencias, clima laboral (cumpleaños, trabajadores destacados, comunicación formal de quejas y sugerencias de los trabajadores).
- Hacer consultas, investigaciones y revisiones en relación con sus quejas o reclamaciones. o Ponernos en contacto con usted al correo electrónico que usted nos haya proporcionado y/o el de uso interno de la empresa en relación con las finalidades mencionadas con en esta política.
- Gestión de procesos de comunicación interna y externa sobre servicios ofertados por El Hospital y programas internos como, por ejemplo, campañas de clima laboral, prevención de riesgos, entre otros.
- Para la gestión de cumplimiento interno: lo que puede involucrar la realización de

investigaciones, entrevistas, obtención de pruebas relacionadas con el cumplimiento de las normas internas de trabajo que formen parte de El Hospital.

- Elaboración de procesos de educación continua.

b. Sobre la base del consentimiento libre, informado, inequívoco y específico, para:

- Envío de comunicaciones comerciales por cualquier canal, incluido por vía electrónica. Así, El Hospital tratará sus Datos Personales para realizar el envío de comunicaciones comerciales, relacionadas con servicios financieros, seguros, servicios socio sanitarios y/o de salud o bienestar por cualquier vía, incluyendo vía electrónica sobre ofertas personalizadas que respondan a sus intereses.
- Uso de los datos de sus familiares (pareja e hijos) en caso de que tengamos que repartir utilidades, actualizar datos, gestionar concursos y demás actividades relacionadas a su relación laboral
- Gestión de riesgos: En esta situación generamos un perfil con sus datos personales para: cesiones de datos a nuestros proveedores dentro del marco del cumplimiento de las obligaciones y actividades que se desprenden del contrato de trabajo; cambios en lugar y modalidad de trabajo y reclutamiento y selección de personal.

c. Sobre la base del cumplimiento de una norma u obligación legal, para:

- Cumplimiento de obligaciones y deberes en materia de prevención de riesgos laborales y salud ocupacional, prevención de lavado de activos, financiamiento del terrorismo y otros delitos.
- Cumplimiento de obligaciones que le correspondan a El Hospital por mandato legal. El Hospital podrá tratar sus datos personales para cumplir con determinadas

obligaciones, incluyendo, pero sin limitarse, al cumplimiento de lo establecido en la normativa relativa a: lavado de activos, protección de datos de carácter personal, salud y seguridad ocupacional, laboral, entre otras.

d. Sobre la base de interés legítimo, para:

- Control de acceso a las instalaciones, con el objetivo de garantizar el acceso del personal a las instalaciones de la institución, lo que implica el uso de herramientas de reconocimiento facial.
- Seguridad dentro de las instalaciones, con el objetivo de precautelar la seguridad del personal y los bienes de la compañía y del grupo empresarial, lo que implica el uso de herramientas de videovigilancia

9. Plazo de Conservación: Sus datos personales serán conservados durante la duración de la relación laboral y hasta por el tiempo que lo requieran las leyes aplicables vigentes, incluso de manera indefinida, en cuyo caso la información permanecerá bloqueada y será accedida y tratada únicamente para el cumplimiento de obligaciones legales o cumplimiento de disposición de autoridad competente.

El trabajador deberá entregar información verídica y actualizada. El incumplimiento de esta obligación acarreará las consecuencias aplicables conforme al Código de Trabajo, la LOPDP y demás leyes o reglamentos vigentes sobre el tema.

10. Almacenamiento de los datos: Los datos personales de los colaboradores de El Hospital serán almacenados en repositorios físicos y electrónicos bajo condiciones de seguridad adecuadas, conforme a los principios de confidencialidad, integridad, disponibilidad y minimización establecidos en la LOPDP.

El Hospital adoptará medidas técnicas, organizativas y administrativas apropiadas para prevenir el acceso, uso, modificación o divulgación no autorizada de los datos. Asimismo, el acceso a la información estará restringido al personal debidamente autorizado, en función de sus competencias y necesidades operativas.

11. Terceros con quienes compartimos sus datos y justificaciones: Para el cumplimiento de las obligaciones legales y laborales, sin que sus datos sean cedidos para otras finalidades distintas a las ya establecidas, estos pueden ser comunicados a terceros, tales como:

- Entidades e instituciones de la administración pública, en razón de sus competencias (Ministerio de Trabajo, Instituto Ecuatoriano de Seguridad Social, Servicio de Rentas Internas, Unidad de Análisis Financiero y Económico, Superintendencia de Compañías, Valores y Seguros, Jueces y Tribunales, fiscalía general del Estado, Policía Nacional, entre otras).
- Auditores externos en cumplimiento de obligaciones contractuales y legales aplicables a la institución.
- Servicios de salud ocupacional y prevención de riesgos laborales.
- Proveedores que asisten a la gestión de las actividades de cumplimiento/*compliance* como: proveedores de software de herramientas de cumplimiento, entre otros.
- Aquellas entidades o clientes que exijan o ante las cuales sea necesario identificar a los trabajadores (aseguradoras, formación, capacitación, mensajería, así como aquellas entidades o clientes que requieran datos identificativos y laborales del personal para llevar a cabo el servicio contratado y que acrediten la relación con la empresa).

El Hospital puede realizar transferencias internacionales de datos, mismas que se realizarán conforme a lo establecido en la LOPDP y las garantías definidas en esta.

Los datos personales también serán procesados por nuestros proveedores de servicios que actúan en nuestro nombre. Con fines de eficiencia del servicio, algunos de estos destinatarios pueden encontrarse en territorios fuera del país donde se recopilaron sus datos personales, que pueden no ofrecer un nivel de protección de datos comparable al del país donde se recopilaron sus datos. Según lo requerido por la ley aplicable de protección de datos, transferiremos sus datos con garantías adecuadas y según los mecanismos específicos requeridos por la Ley Orgánica de Protección de Datos. Entre estos proveedores se podrá facilitar información a:

- Proveedores de almacenamiento en la nube.
- Proveedores de software, plataformas y aplicaciones.
- Proveedores de análisis de datos.
- Proveedores de investigación, incluidos los que implementan estudios o proyectos de investigación en colaboración con Las Compañías o en su nombre.
- Proveedores que ayudan a Las Compañías a mejorar la seguridad de sus aplicaciones.
- Consultores y otros proveedores de servicios profesionales.

El Hospital podría requerir compartir su información de otra manera que no sea la descrita en esta política, si es así, se lo notificaremos previamente y obtendremos de usted previamente la aceptación expresa correspondiente.

12. ¿Qué derechos tengo sobre mis datos y cómo puedo ejercerlos?: En base a la legislación de protección de datos personales usted tiene derecho a:

a) Que le proporcionemos más detalles sobre el uso que hacemos de sus datos.

b) Que le proporcionemos una copia de los datos personales que nos ha proporcionado en los lineamientos de la LOPDP.

c) Que actualicemos cualquier dato que haya modificado o que haya cambiado y rectifiquemos cualquier inexactitud en los datos personales que tratamos en los lineamientos de la LOPDP.

d) Que eliminemos cualquier dato personal que ya no tengamos un fundamento legal para utilizar.

e) Cuando el tratamiento se base en el consentimiento, pueda retirar su consentimiento para que dejemos de realizar ese tratamiento concreto.

f) Oponerse a cualquier tratamiento basado en el interés legítimo cuando: i) No se afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública, de interés público o cuyo tratamiento está ordenado por la ley; ii) El tratamiento de datos personales tenga por objeto la mercadotecnia directa, en cuyo caso el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles y los datos personales dejarán de ser tratados para dichos fines; iii) Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo, previsto en la LOPDP, y se justifique en una situación concreta personal del titular, siempre que una ley no disponga lo contrario, A menos que nuestras razones para llevar a cabo dicho tratamiento superen cualquier

perjuicio a sus derechos de protección de datos.

g) Suspender el tratamiento de sus datos, en las siguientes situaciones: i) Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos; ii) El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; iii) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; y, iv) Cuando el interesado se haya opuesto al tratamiento en virtud de lo que indica la LOPDP, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

h) La portabilidad de sus datos en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables en los lineamientos de la LOPDP.

i) No ser sujeto de decisiones total o parcialmente automatizadas, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o que atenten contra sus derechos y libertades fundamentales.

El ejercicio de estos derechos está sujeto a ciertas excepciones, en algunos casos establecidas en la LOPDP, para salvaguardar el interés público (p. ej., prevenir o detectar un acto ilícito) y los intereses de la institución. Si ejerce alguno de estos derechos, se verificará la legitimidad de la solicitud y recibirá una respuesta en el plazo de hasta quince (15) días.

Si no está satisfecho con el uso que se hace de su información personal o de la respuesta que ha recibido al ejercer sus derechos, tiene derecho a presentar una queja ante la

Autoridad de Protección de Datos Personales, a través de los canales que esta habilite para el efecto.

Asimismo, podrás solicitar la revocación del consentimiento otorgado para el tratamiento de sus datos, cuando la base legal de su tratamiento sea el consentimiento.

Para cualquier requerimiento relativo al tratamiento de datos, el titular deberá enviar una comunicación especificando el derecho que quisiera ejercer al correo electrónico dpd@hospitalvidanueva.med.ec o presentar una solicitud en el departamento de talento humano en las instalaciones del Hospital ubicadas en Av. Paraiso, Cuenca.

13. ¿Cómo protegen mis datos personales?: El Hospital reconoce y garantiza a sus colaboradores el ejercicio de los derechos previstos en la LOPDP, incluyendo el acceso, rectificación, actualización, eliminación, oposición y portabilidad de sus datos personales. Para ello, la institución ha habilitado mecanismos y canales internos que permiten la atención oportuna de las solicitudes presentadas por los titulares, dentro de los plazos establecidos por la ley.

Adicionalmente, El Hospital implementa medidas de seguridad técnicas, administrativas y organizativas orientadas a salvaguardar los datos personales contra accesos no autorizados, pérdida, alteración o divulgación indebida.

14. Datos de contacto: del Responsable del tratamiento y Delegado de Protección de Datos Personales

El Hospital Oncológico Vida Nueva en su calidad de responsable del tratamiento de datos personales, pone a disposición de los titulares los siguientes canales de contacto:

- Domicilio: Avenida del Paraíso y Agustín Landívar, Cuenca – Ecuador
- Teléfono: 074096567 ext. 2507 – 1720
- Correo electrónico: dpd@hospitalvidanueva.med.ec

El Hospital ha designado un Delegado de Protección de Datos Personales, quien actúa de forma independiente como punto de contacto para consultas, solicitudes o reclamos relacionados con el tratamiento de datos personales.

- Nombre: Juan Martin Pérez Solano
- Dirección: Avenida del Paraíso y Agustín Landívar, Cuenca – Ecuador
- Correo electrónico: dpd@hospitalvidanueva.med.ec
- Teléfono: 074096567 ext. 2507 – 1720

15. Uso de Imagen: Los trabajadores autorizan al Hospital, para que, de forma directa o por medio de terceros, registre y fije en medios sonoros, fotográficos y/o audiovisuales aspectos de su imagen, como la representación gráfica de su cara, cuerpo, silueta o cualquier otro tipo de forma o aspecto, que lo identifique bajo cualquier medio conocido o por conocer, así como su voz, buen nombre, acreditación, fama, reconocimiento y demás características asociadas.

Los trabajadores declaran que conocen y aceptan que no percibirán ninguna remuneración adicional por el uso de su imagen, ya que la sola celebración de un contrato de trabajo con El Hospital los hace elegibles para participar de los procesos descritos en el párrafo anterior, de manera que se entenderá que cualquier derecho relacionado con el uso de la imagen de

los trabajadores se encuentra satisfecho por el pago de la remuneración pactada en su respectivo contrato de trabajo.

Los trabajadores autorizan a El Hospital, para que, incluso luego de concluida la relación laboral, difundan las imágenes fotográficas y/o audiovisuales tomadas o grabadas y en las que aparezca su imagen, a través de las redes sociales corporativas oficiales, tales como Instagram, YouTube y Facebook, entre otras. Los trabajadores declaran que conocen y aceptan que pueden existir publicaciones que salgan de la administración y control de El Hospital y sus relacionadas por las cuales no les hará responsables.

16. ¿Cuándo se actualiza este aviso?: El presente Aviso Interno de Protección de Datos Personales podrá ser actualizado cuando se produzcan cambios en la normativa aplicable, en los procesos internos de El Hospital o en las finalidades del tratamiento de datos. Cualquier modificación será comunicada oportunamente a los colaboradores a través de los canales institucionales.

Última actualización: 24 de marzo de 2026.

17. Legislación Aplicable y Resolución de Conflictos: El presente Aviso Interno de Protección de Datos Personales se regula por lo establecido en la LOPDP, su normativa secundaria de desarrollo, lineamientos y resoluciones emitidas por la autoridad de control, así como por cualquier otra disposición legal aplicable en materia de protección de datos personales en la República del Ecuador.

AVISO DE PRIVACIDAD (EXTERNO):

1. Identificación del responsable del tratamiento: El Hospital Oncológico Vida Nueva, es una institución de derecho privado sin fines de lucro, con domicilio en la ciudad de Cuenca,

República del Ecuador, actúa en calidad de responsable del tratamiento de datos personales en los términos establecidos en la LOPDP.

En tal calidad, el Hospital Oncológico Vida Nueva determina las finalidades, medios y condiciones del tratamiento de los datos personales de los titulares, garantizando su tratamiento conforme a principios de licitud, lealtad, transparencia, finalidad, proporcionalidad y responsabilidad proactiva, así como el pleno respeto de los derechos fundamentales de los titulares.

2. Alcance: La presente Política de Privacidad es aplicable a todos los usuarios que accedan y utilicen este sitio web. Mediante su uso, el titular de los datos personales declara haber leído y aceptado las condiciones aquí establecidas.

El tratamiento de los datos personales se realizará conforme a la normativa vigente en la República del Ecuador, en particular la LOPDP, garantizando el respeto de los principios de licitud, finalidad, proporcionalidad y transparencia en todas las actividades de tratamiento.

3. Definiciones: Para efectos de la presente Política de Privacidad, se entenderá por:

- Privacidad: Derecho fundamental que permite a las personas ejercer control sobre quién, cuándo y cómo se procesa su información personal.
- Protección de datos personales: Conjunto de normas, principios y procedimientos destinados a garantizar el tratamiento adecuado, seguro y legítimo de los datos personales.
- Dato personal: Toda información que identifica o hace identificable a una persona natural, ya sea de manera directa o indirecta, incluyendo datos de identificación, contacto o comportamiento.

- Datos personales sensibles: Aquellos datos que, por su naturaleza, requieren un nivel de protección reforzado, tales como los que revelan origen racial o étnico, convicciones religiosas, opiniones políticas, afiliación sindical, así como datos relativos a la salud, vida sexual, datos genéticos o biométricos.
- Tratamiento de datos personales: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, tales como la recolección, registro, organización, almacenamiento, uso, consulta, transferencia, difusión, conservación o eliminación.
- Anonimización: Proceso mediante el cual los datos personales son transformados de forma irreversible, impidiendo la identificación directa o indirecta del titular.
- Cookies: Archivos o dispositivos de almacenamiento que permiten recordar información sobre la actividad del usuario en un sitio web, con el fin de facilitar la navegación y mejorar la experiencia del usuario.
- Base de legitimación (base jurídica): Fundamento legal que autoriza el tratamiento de datos personales, tales como el consentimiento del titular, el cumplimiento de obligaciones legales, la ejecución de una relación contractual, la protección de intereses vitales, el interés público o el interés legítimo del responsable, conforme a la LOPDP.

4. Partes que intervienen en el tratamiento de datos personales

- Titular: Persona natural a quien corresponden los datos personales objeto de tratamiento.
- Responsable del tratamiento: Persona natural o jurídica que decide sobre la finalidad, contenido y uso del tratamiento de datos personales.

- Encargado del tratamiento: Persona natural o jurídica que trata datos personales por cuenta del responsable.
- Delegado de Protección de Datos Personales (DPD): Persona designada por el responsable para supervisar el cumplimiento de la normativa de protección de datos, asesorar a la organización y actuar como punto de contacto con los titulares y la autoridad de control.
- Autoridad de control: Entidad encargada de supervisar el cumplimiento de la normativa de protección de datos personales en el Ecuador, actualmente la Superintendencia de Protección de Datos Personales.

5. Datos personales tratados y finalidades del tratamiento

5.1 Categorías de datos personales tratados: El Hospital podrá recolectar y tratar las siguientes categorías de datos personales:

a) Datos identificativos

- Nombres y apellidos
- Número de cédula o documento de identidad –
- Fecha de nacimiento

b) Datos de contacto

- Dirección domiciliaria
- Correo electrónico
- Número telefónico

c) Datos administrativos y financieros

- Información de seguros médicos
- Datos de facturación
- Información de pagos

d)Datos sensibles

- Historia clínica
- Diagnósticos médicos
- Resultados de exámenes
- Tratamientos médicos
- Información genética (cuando aplique)

e) Datos de navegación y tecnológicos: Cuando el titular accede al sitio web o plataformas digitales del Hospital, se podrán recolectar:

- Dirección IP
- Tipo y modelo de dispositivo
- Sistema operativo
- Navegador utilizado
- Fecha y hora de acceso
- Proveedor de conexión

- Información de navegación dentro del sitio

f) Datos para registro en plataformas digitales: En caso de que el titular se registre en sistemas, aplicaciones o servicios digitales del Hospital:

- Datos identificativos
- Datos de contacto
- Datos de salud (cuando sea necesario para la atención médica)

g) Datos para comunicaciones: En caso de suscripción voluntaria:

- Nombre completo
- Correo electrónico

5.2 Uso de cookies y tecnologías similares: El sitio web del Hospital podrá utilizar cookies y tecnologías similares con la finalidad de:

- Facilitar la navegación del usuario
- Recordar preferencias
- Mejorar la experiencia de uso
- Optimizar los servicios digitales

En caso de que el usuario registre información en formularios o comentarios, podrá optar por almacenar sus datos en cookies para evitar su ingreso reiterado. Estas cookies podrán tener una duración determinada conforme a su finalidad.

El usuario podrá configurar su navegador para rechazar o eliminar cookies, sin perjuicio de que ello pueda afectar el funcionamiento del sitio web.

5.3 Tratamiento de datos personales y finalidades: El Hospital podrá recolectar, registrar, organizar, almacenar, consultar, utilizar, transferir y, en general, realizar cualquier tipo de tratamiento sobre los datos personales de los titulares, en el marco de la prestación de sus servicios de salud y de conformidad con la normativa vigente.

El tratamiento de los datos personales se realizará con la finalidad de garantizar la adecuada prestación de servicios médicos, incluyendo la atención integral de los pacientes, el diagnóstico, tratamiento y seguimiento de enfermedades, así como la gestión y administración de las historias clínicas.

Asimismo, los datos serán tratados para la gestión operativa y administrativa de los servicios institucionales, lo que comprende el agendamiento de citas, procesos de admisión hospitalaria, facturación, cobros y gestión de seguros de salud.

De igual forma, los datos personales podrán ser tratados para el cumplimiento de obligaciones legales y regulatorias aplicables al sector sanitario, incluyendo la atención de requerimientos de autoridades competentes, la realización de auditorías médicas o administrativas, la defensa de los intereses institucionales en procesos administrativos o judiciales, así como la atención de solicitudes, peticiones, quejas o requerimientos presentados por los titulares o ante los órganos de control competentes.

En el entorno digital, el tratamiento de datos personales permitirá el acceso y uso del sitio web y plataformas institucionales, la personalización de la experiencia del usuario, la mejora de los servicios ofrecidos y la garantía de la seguridad de los sistemas de información. En

este sentido, el acceso al sitio web, en general, no requiere registro previo; sin embargo, determinados servicios podrán requerir la provisión de datos personales, por lo que, en caso de que el titular decida no proporcionarlos, es posible que no pueda acceder a ciertas funcionalidades o que el Hospital no pueda atender adecuadamente sus requerimientos.

Finalmente, previa autorización del titular cuando corresponda, los datos podrán ser tratados para el envío de información relacionada con servicios, campañas o actividades institucionales.

En los casos en que se traten datos personales de niños, niñas y adolescentes, el Hospital garantizará que dicho tratamiento se realice en atención al interés superior del menor, adoptando las medidas necesarias para la protección de sus derechos y, cuando corresponda, contando con la autorización de sus representantes legales.

6. Base legal del tratamiento: El tratamiento de datos personales por parte del Hospital se fundamenta en las bases de legitimación previstas en la LOPDP, en función de la naturaleza de los servicios prestados.

En este sentido, el tratamiento se sustenta principalmente en la ejecución de la relación médico–paciente, en el cumplimiento de obligaciones legales aplicables al sector sanitario y, cuando corresponda, en la protección de intereses vitales del titular o de terceros.

Sin perjuicio de lo anterior, mediante la aceptación del presente Aviso de Privacidad, el titular otorga su consentimiento libre, específico, informado e inequívoco para el tratamiento de sus datos personales en aquellos casos en los que dicho consentimiento sea requerido, especialmente en lo relacionado con el uso del sitio web, plataformas digitales y el envío de comunicaciones institucionales.

El titular podrá revocar su consentimiento en cualquier momento, sin que ello afecte la licitud del tratamiento realizado con anterioridad.

7. Tiempo de conservación: El Hospital conservará los datos personales durante el tiempo estrictamente necesario para cumplir con las finalidades descritas en la presente Política de Privacidad, en particular para la adecuada prestación de los servicios de salud, la gestión de las historias clínicas y la atención integral de los pacientes. Adicionalmente, los datos podrán ser conservados durante los plazos establecidos en la normativa aplicable al sector sanitario, así como por el tiempo necesario para el cumplimiento de obligaciones legales y regulatorias, la atención de requerimientos de autoridades competentes y la defensa de los derechos e intereses institucionales en procesos administrativos o judiciales.

El período de conservación podrá variar en función de la naturaleza de los datos personales y de las finalidades del tratamiento. Una vez cumplidos dichos plazos, los datos serán eliminados, anonimizados o bloqueados, según corresponda. El Hospital implementa medidas técnicas, organizativas y administrativas adecuadas para garantizar la seguridad de los datos personales durante todo su ciclo de vida, evitando su pérdida, uso indebido, acceso no autorizado o tratamiento ilícito.

8. Almacenamiento de datos: Los datos personales tratados por el Hospital podrán ser almacenados en servidores propios o en infraestructuras tecnológicas de terceros, ubicados en el Ecuador o en otros países, siempre garantizando que dichos entornos cuenten con medidas de seguridad adecuadas para la protección de la información.

En caso de que los datos sean almacenados o tratados fuera del territorio ecuatoriano, el Hospital adoptará las medidas necesarias para asegurar un nivel adecuado de protección, conforme a la normativa vigente en materia de protección de datos personales.

Asimismo, el Hospital implementa medidas técnicas, organizativas y administrativas destinadas a proteger los datos personales contra pérdida, uso indebido, acceso no autorizado, alteración o divulgación.

El tratamiento de los datos personales se realizará conforme a las bases de legitimación previstas en la normativa aplicable, incluyendo, cuando corresponda, el consentimiento del titular.

9. ¿Con quién se comparten los datos personales?: Para la adecuada prestación de los servicios de salud y el cumplimiento de las finalidades descritas en la presente Política de Privacidad, el Hospital podrá compartir los datos personales de los titulares con terceros, únicamente cuando resulte necesario y conforme a la normativa vigente en materia de protección de datos personales. En este sentido, los datos podrán ser compartidos con aliados estratégicos en el marco de relaciones institucionales o contractuales que resulten necesarias para la ejecución de los servicios ofrecidos por el Hospital.

Asimismo, los datos podrán ser comunicados a proveedores y prestadores de servicios, tales como compañías de seguros de salud, instituciones médicas, laboratorios clínicos y administrativos o tecnológicos. De igual forma, los datos personales podrán ser compartidos con organismos o autoridades públicas competentes, en cumplimiento de obligaciones legales o en atención a requerimientos judiciales, administrativos o regulatorios debidamente fundamentados.

En todos los casos, el Hospital garantizará que la comunicación de datos personales se realice bajo condiciones de confidencialidad y seguridad, limitándose a la información estrictamente necesaria para el cumplimiento de las finalidades correspondientes. Cuando

sea posible y apropiado, se adoptarán medidas como la anonimización o seudonimización de los datos personales, con el fin de reducir los riesgos asociados a su tratamiento.

10. Transferencia de datos: El Hospital podrá transferir y almacenar datos personales en infraestructuras ubicadas fuera del territorio ecuatoriano, en jurisdicciones cuyas normativas de protección de datos puedan diferir de las aplicables en el Ecuador; no obstante, en todos los casos, la institución adoptará las medidas necesarias para garantizar un nivel adecuado de protección, seguridad y confidencialidad de los datos personales, conforme a la normativa vigente y a lo establecido en la presente Política de Privacidad.

11. Derechos de los titulares: el Hospital garantiza a los titulares de datos personales el ejercicio de sus derechos, de conformidad con la normativa vigente en materia de protección de datos personales.

En este sentido, el titular podrá ejercer los derechos de acceso, mediante el cual podrá conocer y obtener información sobre el tratamiento de sus datos personales; rectificación y actualización, cuando los datos sean inexactos, incompletos o desactualizados; eliminación, cuando los datos no sean necesarios para las finalidades para las cuales fueron recolectados o cuando se haya retirado el consentimiento, salvo las excepciones legales aplicables; oposición, cuando existan motivos legítimos relacionados con su situación particular; y limitación del tratamiento, en los casos previstos en la normativa vigente.

Asimismo, el titular tiene derecho a no ser objeto de decisiones basadas únicamente en tratamientos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos o le afecten significativamente.

El ejercicio de estos derechos podrá realizarse conforme a los mecanismos establecidos por el Hospital, sin perjuicio de las limitaciones previstas en la ley, especialmente en el ámbito de la prestación de servicios de salud y el cumplimiento de obligaciones legales

12. Responsabilidad sobre la exactitud de los datos personales: El titular de los datos personales es responsable de la veracidad, exactitud, vigencia y autenticidad de la información proporcionada a el Hospital, comprometiéndose a mantenerla debidamente actualizada.

En este sentido, el titular se obliga a proporcionar información completa, correcta y actualizada al momento de su registro, admisión o utilización de los servicios, a fin de garantizar una adecuada prestación de los servicios de salud y la correcta gestión de la información.

el Hospital Oncológico Vina Nueva no será responsable por la inexactitud o falta de actualización de los datos personales proporcionados por el titular, cuando dicha situación no sea imputable a la institución.

Sin perjuicio de lo anterior, el Hospital podrá suspender o limitar el acceso a determinados servicios cuando los datos proporcionados resulten falsos, incompletos o inexactos, en la medida en que ello afecte la adecuada prestación de los servicios o el cumplimiento de obligaciones legales.

13. Datos de contacto del responsable del tratamiento: El Hospital Oncológico Vida Nueva en su calidad de responsable del tratamiento de datos personales, pone a disposición de los titulares los siguientes canales de contacto:

- Domicilio: Avenida del Paraíso y Agustín Landívar, Cuenca – Ecuador

- Teléfono: 074096567 ext. 2507 – 1720
- Correo electrónico: dpd@hospitalvidanueva.med.ec.

14. Datos de contacto del Delegado de Protección de Datos Personales (DPD): El Hospital Oncológico Vida Nueva ha designado un Delegado de Protección de Datos Personales, quien actúa de forma independiente como punto de contacto para consultas, solicitudes o reclamos relacionados con el tratamiento de datos personales.

- Nombre: Juan Martin Pérez Solano
- Dirección: Avenida del Paraíso y Agustín Landívar, Cuenca – Ecuador
- Correo electrónico: dpd@hospitalvidanueva.med.ec.
- Teléfono: 074096567 ext. 2507 – 1720

15. Derecho a la portabilidad de los datos personales: El titular de los datos personales tendrá derecho a recibir los datos personales que haya proporcionado a el Hospital , en un formato estructurado, de uso común y lectura mecánica, así como a transmitirlos a otro responsable del tratamiento cuando sea técnicamente posible.

El ejercicio de este derecho procederá siempre que no afecte derechos de terceros, se respete la confidencialidad de la información y se cumplan las condiciones establecidas en la normativa vigente, especialmente en el ámbito del tratamiento de datos de salud.

16. Modificación de la Política de Privacidad: El Hospital se reserva el derecho de modificar, actualizar o sustituir la presente Política de Privacidad en cualquier momento, con el fin de adaptarla a cambios normativos, criterios de la autoridad de control o mejoras en sus procesos internos. Cualquier modificación será publicada a través de los canales oficiales

de la institución. En todo caso, el tratamiento de los datos personales se regirá por la versión de la Política de Privacidad vigente al momento de su recopilación.

ANEXO NO. 2 – PLAN DE CAPACITACIÓN & COMUNICACIÓN

PLAN DE CAPACITACIÓN:

El presente plan como alcance es de APLICACIÓN OBLIGATORIA para todos los actores que intervienen en el tratamiento de datos personales dentro del Hospital, incluyendo:

- Personal médico y asistencial
- Área de Trabajo Social
- Área de Estadística
- Personal administrativo
- Área de Tecnologías de la Información
- Seguridad de la Información
- Directivos y responsables de procesos
- Encargados y subencargados de tratamiento (proveedores tecnológicos como BioTrust)

El referido plan comprende acciones de formación, sensibilización, actualización normativa, comunicación interna y evaluación periódica, orientadas a garantizar la efectiva implementación de la Política Institucional de Protección de Datos Personales y de las medidas de seguridad vinculadas al tratamiento de datos de salud, datos biométricos y

demás categorías de información gestionadas por la organización. Respecto a la estructura de capacitación se establece:

a) Programa de inducción obligatoria: Todo el personal deberá recibir capacitación al inicio de su relación laboral. Contenido mínimo a cumplir:

- Principios de protección de datos personales
- Tratamiento de datos sensibles (salud y biometría)
- Confidencialidad de la historia clínica
- Uso correcto de sistemas institucionales
- Responsabilidad individual en el tratamiento de datos

b) Capacitación especializada por área

Área de Trabajo Social

- Manejo de datos socioeconómicos y familiares
- Confidencialidad reforzada en casos vulnerables
- Gestión de expedientes sociales
- Transferencia de información a terceros (derivaciones)

Área Médica

- Acceso legítimo a historia clínica
- Registro y trazabilidad

- Uso de autenticación biométrica
- Minimización en la consulta de datos

Área de Estadística

- Tratamiento de datos agregados y anonimización
- Prevención de re-identificación
- Uso de datos con fines secundarios

TI y Seguridad de la Información

- Control de accesos (IAM)
- Cifrado de datos
- Gestión de incidentes
- Evaluaciones de impacto (EIPD)
- Seguridad en sistemas biométricos

c) Capacitación en tecnologías críticas (biometría e IA)

- Funcionamiento del reconocimiento biométrico
- Riesgos de suplantación y errores (falsos positivos/negativos)
- Sesgos algorítmicos
- Principio de proporcionalidad en el uso de IA
- Alternativas no biométricas (*fallback*)

El plan de capacitación del Hospital se estructura bajo un enfoque diferenciado por niveles de responsabilidad y exposición al riesgo, reconociendo que no todos los actores institucionales enfrentan las mismas obligaciones, ni riesgos en el tratamiento de datos personales. En este sentido, la formación se organiza en tres niveles interdependientes: inducción obligatoria, capacitación especializada por áreas y capacitación en tecnologías críticas.

El programa de inducción obligatoria constituye el punto de partida del sistema de cumplimiento institucional, garantizando que todo el personal, desde el inicio de su relación laboral, comprenda los principios rectores de la protección de datos personales, la naturaleza sensible de la información de salud y las responsabilidades individuales derivadas del acceso a sistemas institucionales. Este componente no se limita a una exposición normativa, sino que busca generar conciencia sobre el impacto real que una mala gestión de la información puede tener en los derechos de los pacientes y en la responsabilidad institucional.

Por su parte, la capacitación especializada por áreas responde a un criterio de riesgo operativo, reconociendo que unidades como Trabajo Social, Estadística, áreas médicas y Tecnologías de la Información manejan distintos tipos de datos y enfrentan escenarios diferenciados de exposición. En consecuencia, los contenidos son adaptados a las funciones específicas de cada área, profundizando en aspectos como la confidencialidad reforzada en contextos de vulnerabilidad, la anonimización de datos, la trazabilidad de accesos y la gestión de incidentes de seguridad.

Finalmente, la capacitación en tecnologías críticas, particularmente en biometría e inteligencia artificial, introduce un componente de alta especialización, orientado a

garantizar que el personal comprenda no solo el funcionamiento técnico de estas herramientas, sino también sus implicaciones jurídicas, éticas y operativas. Este componente resulta fundamental en el contexto del Hospital, donde el uso de tecnologías biométricas para el acceso a historias clínicas incrementa significativamente el nivel de riesgo regulatorio.

1.2. Modalidades de capacitación

- Sesiones presenciales para personal crítico
- Plataformas virtuales institucionales
- Cápsulas formativas (*microlearning*)
- Simulaciones de incidentes de seguridad
- Talleres prácticos por área

Las modalidades de capacitación adoptadas por el Hospital responden a un criterio de eficiencia, accesibilidad y aplicabilidad práctica, combinando mecanismos tradicionales con herramientas digitales que permiten una mayor cobertura institucional.

Las sesiones presenciales se reservan para personal crítico o áreas de alto riesgo, donde resulta necesario profundizar en aspectos técnicos o realizar análisis de casos complejos. Estas sesiones permiten una interacción directa, resolución de dudas y aplicación práctica del conocimiento en escenarios reales.

Las plataformas virtuales institucionales facilitan la capacitación masiva del personal, garantizando acceso continuo a contenidos actualizados y permitiendo la estandarización del conocimiento en toda la organización. Este mecanismo se complementa con cápsulas

formativas o bajo el denominado "*microlearning*", diseñadas para reforzar conceptos clave de manera ágil y periódica.

Adicionalmente, se incorporan simulaciones de incidentes de seguridad, que permiten evaluar la capacidad de respuesta del personal ante situaciones reales de vulneración de datos personales, así como talleres prácticos por área, orientados a la aplicación directa de políticas y procedimientos en el entorno laboral.

Este enfoque multimodal no solo mejora la retención del conocimiento, sino que permite integrar la capacitación dentro de la dinámica operativa del hospital, evitando que sea percibida como una obligación aislada.

PLAN DE COMUNICACIÓN:

2. Objetivo del plan de comunicación El plan de comunicación del Hospital tiene como finalidad garantizar la difusión continua, estructurada y segmentada de las políticas, lineamientos y buenas prácticas en materia de protección de datos personales, asegurando su comprensión y aplicación efectiva por parte del personal en el desarrollo de sus funciones.

A diferencia del plan de capacitación, que responde a un proceso formativo estructurado, el plan de comunicación actúa como un mecanismo permanente de refuerzo institucional, orientado a reducir errores operativos, fortalecer la cultura organizacional en privacidad y asegurar la actualización constante frente a cambios normativos o tecnológicos.

3. Estrategia y canales de comunicación

El presente plan de comunicación del Hospital se estructura bajo un enfoque multicanal, dinámico y basado en riesgo, que articula la comunicación institucional, operativa y reactiva como mecanismos complementarios dentro del modelo de gobernanza de datos personales. Este enfoque reconoce que la efectividad de la protección de datos no depende únicamente de la existencia de políticas y procedimientos, sino de la capacidad institucional de difundirlos, interiorizarlos y aplicarlos de manera consistente en todos los niveles organizacionales.

Desde esta perspectiva, la comunicación institucional cumple una función estructural dentro del sistema de cumplimiento, al garantizar la difusión formal, íntegra y oportuna de las políticas de protección de datos personales, protocolos internos, lineamientos de seguridad de la información y disposiciones normativas aplicables. Esta comunicación se canaliza a través de medios oficiales como la intranet corporativa, correos institucionales y repositorios documentales, asegurando la trazabilidad de la información difundida y la disponibilidad permanente de los documentos normativos para todo el personal. Su finalidad no se limita a informar, sino a establecer un marco común de actuación que permita alinear a toda la organización bajo criterios homogéneos de cumplimiento.

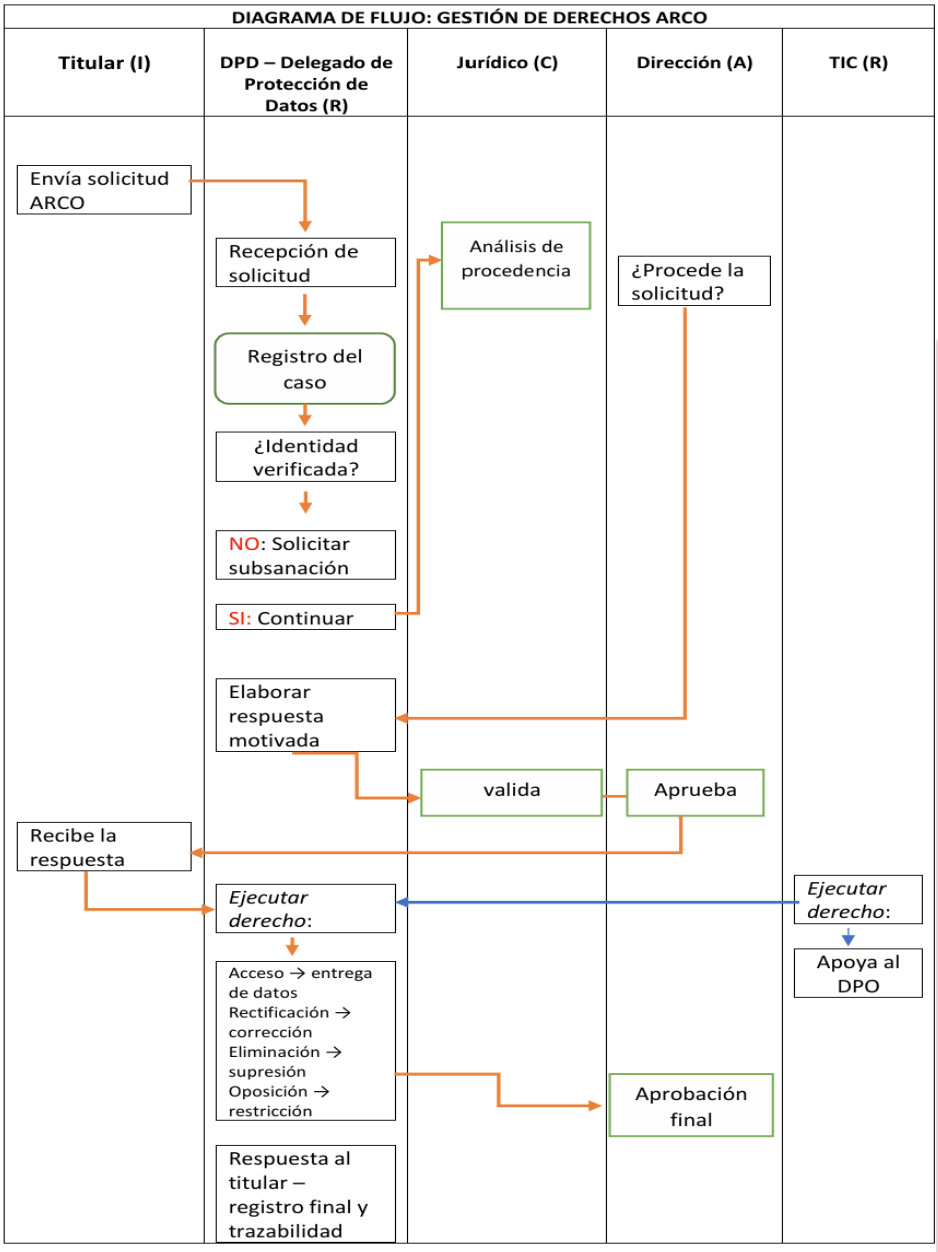
Por su parte, la comunicación operativa se orienta a traducir los lineamientos institucionales en prácticas concretas dentro de la operación diaria del hospital. En este nivel, la estrategia se enfoca en reforzar conductas seguras y prevenir errores humanos mediante recordatorios periódicos, señalética en áreas críticas, mensajes integrados en sistemas institucionales y comunicaciones breves de carácter práctico. Estas acciones se dirigen especialmente a actividades de alto riesgo, como el acceso a historias clínicas, el uso de credenciales institucionales, la gestión de datos biométricos y el tratamiento de información sensible en áreas como Trabajo Social y Estadística. La comunicación operativa cumple así una función

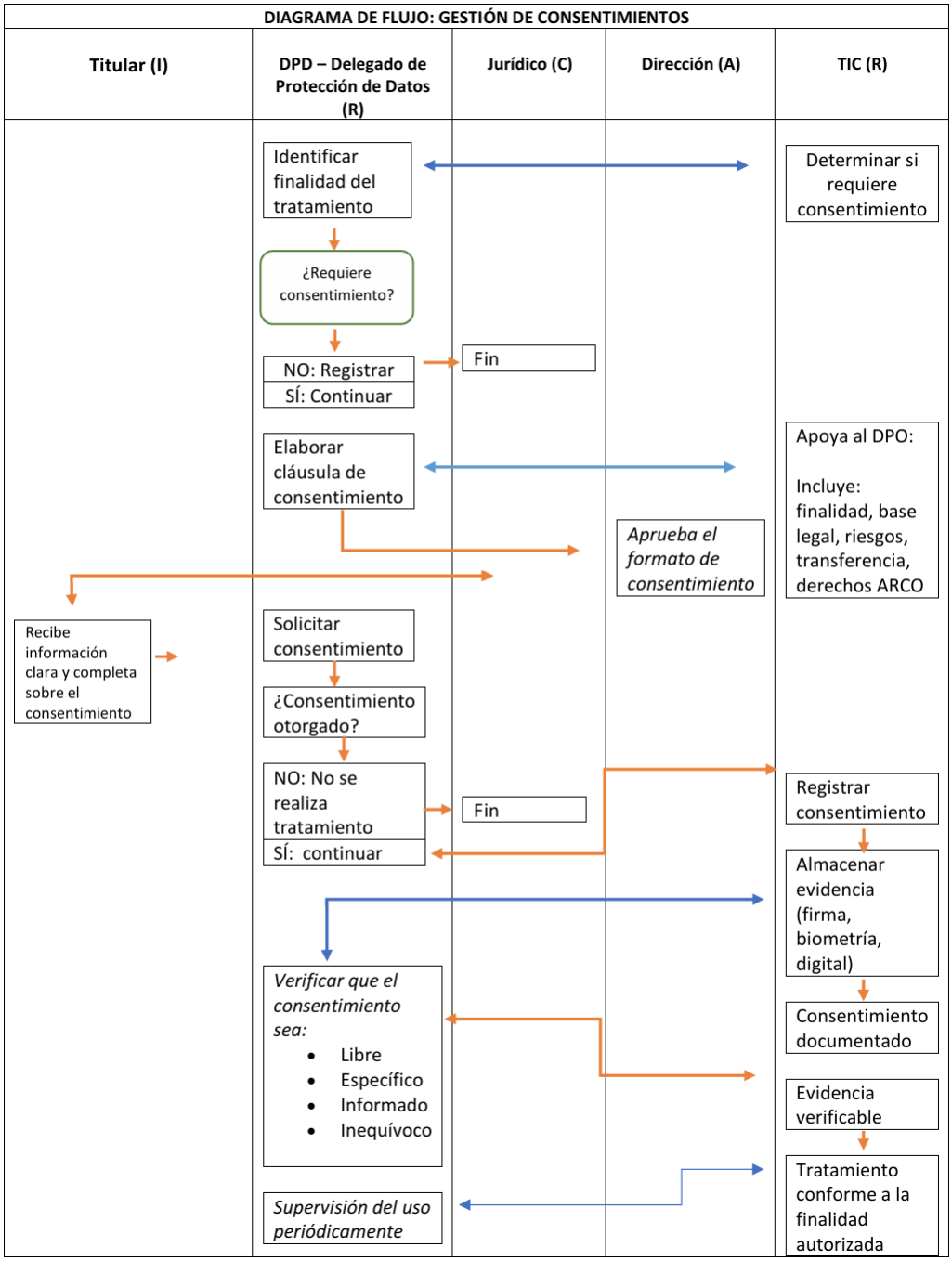
preventiva, reduciendo la probabilidad de incidentes derivados de omisiones, desconocimiento o uso inadecuado de los sistemas. En complemento, la comunicación reactiva constituye un mecanismo de respuesta inmediata frente a incidentes de seguridad, eventos de riesgo o modificaciones relevantes en el marco normativo o tecnológico. Este tipo de comunicación se activa bajo criterios de oportunidad, proporcionalidad y claridad, con el objetivo de informar al personal sobre la naturaleza del riesgo identificado, las medidas correctivas adoptadas y los ajustes necesarios en los procedimientos internos. Su adecuada implementación permite contener incidentes, evitar su repetición y fortalecer la capacidad institucional de respuesta frente a escenarios adversos.

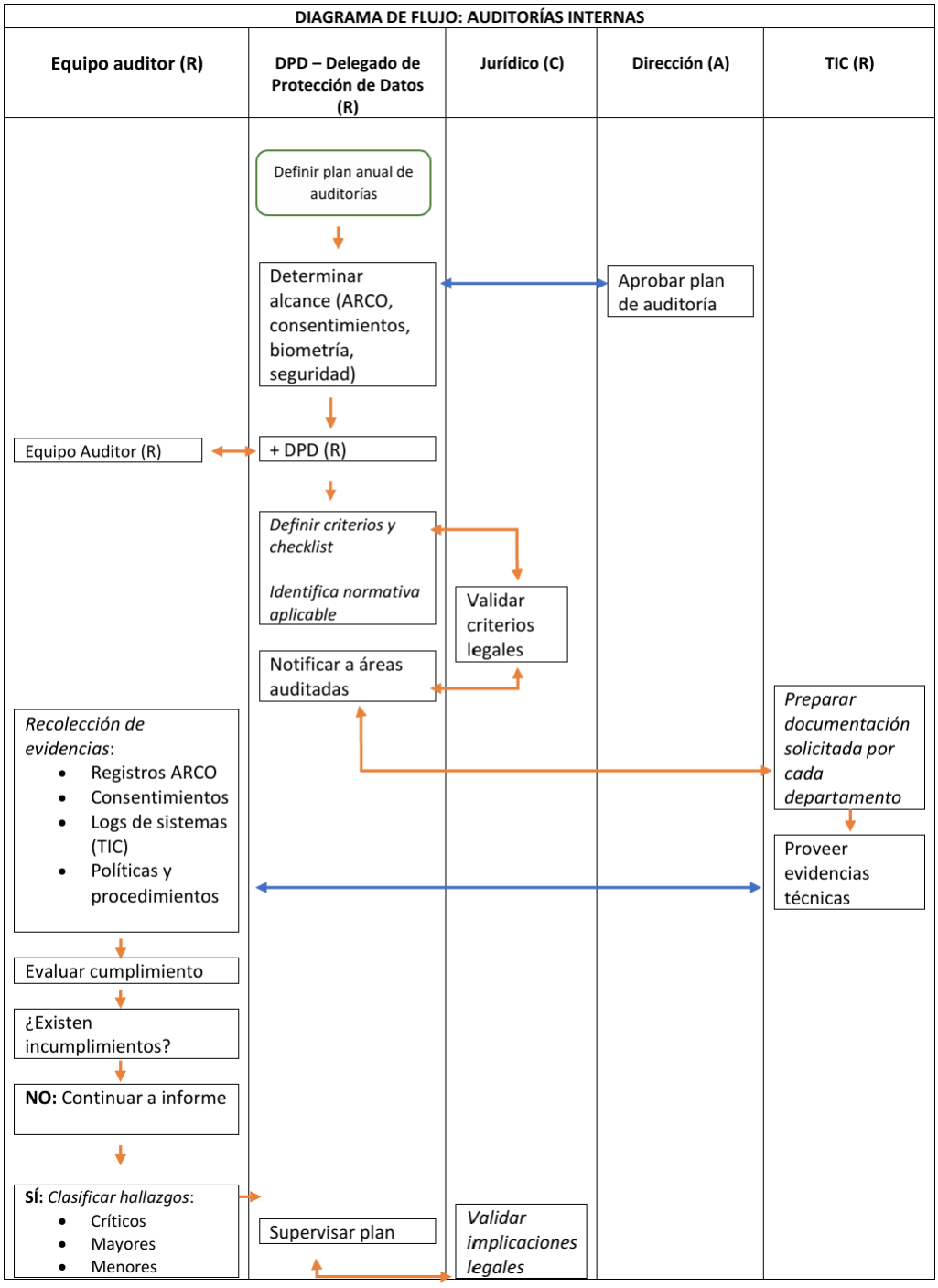
Adicionalmente, el plan incorpora un enfoque de segmentación estratégica de la comunicación, reconociendo que los distintos perfiles organizacionales requieren niveles diferenciados de información. En este sentido, los contenidos comunicacionales se adaptan en función del rol, nivel de responsabilidad y grado de exposición al tratamiento de datos personales, de modo que el personal médico, administrativo, técnico y directivo reciba información pertinente, comprensible y aplicable a su contexto operativo. Este criterio de segmentación evita la sobrecarga informativa y mejora la efectividad del mensaje.

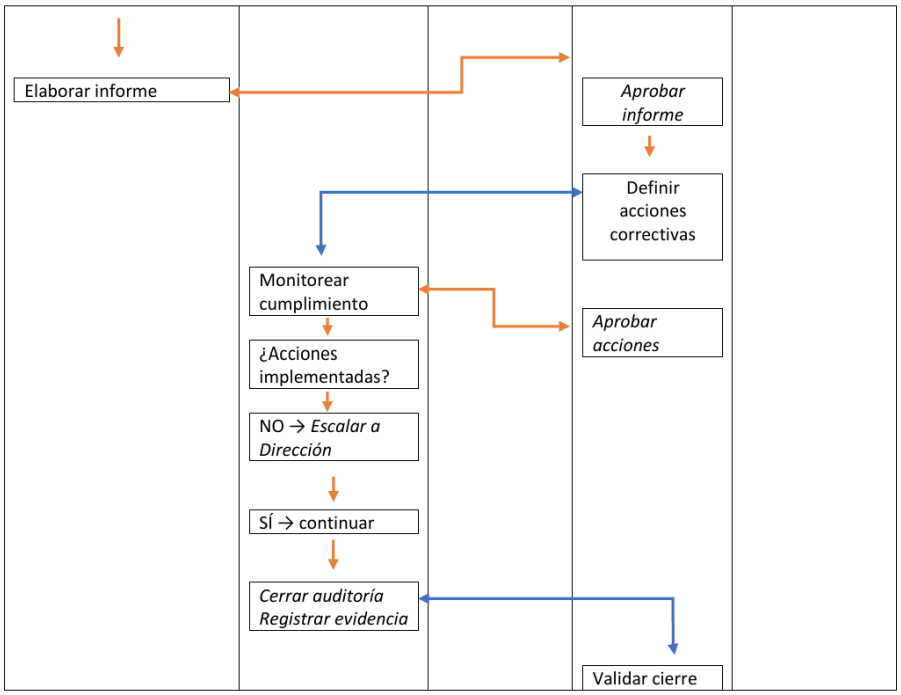
Finalmente, la estrategia de comunicación se concibe como un proceso continuo de refuerzo cultural, orientado a consolidar una cultura institucional de privacidad y protección de datos personales. En este marco, la comunicación no se limita a la transmisión de información, sino que actúa como un instrumento de gestión del comportamiento organizacional, promoviendo la responsabilidad individual, la conciencia del riesgo y el compromiso institucional con la confidencialidad y la seguridad de la información.

ANEXO NO. 3 – FLUJOGRAMAS DE PROCESOS: GESTIÓN DE DERECHOS ARCO, GESTIÓN DE CONSENTIMIENTOS & AUDITORÍAS INTERNAS.









ANEXO NO. 4 PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN QUE INVOLUCREN DATOS PERSONALES

1. ANTECEDENTES

El Hospital Oncológico Vida Nueva reconoce que el tratamiento de datos personales sensibles, en especial datos de salud y biométricos mediante sistemas de IA, implica un alto riesgo para los derechos de los titulares. En este contexto, la gestión de incidentes de seguridad es esencial, debido a que cualquier vulneración puede afectar la confidencialidad, integridad y disponibilidad de la información, así como derechos fundamentales. Por consiguiente, resulta imprescindible contar con un instrumento interno que establezca lineamientos claros, cuyo eje central sea el protocolo de reporte de brechas de seguridad

conforme a la LOPDP y su Reglamento General, garantizando una respuesta oportuna, documentada y jurídicamente adecuada.

2. OBJETIVO

Establecer el procedimiento interno que debe seguir el Hospital Oncológico Vida Nueva ante la ocurrencia de incidentes de seguridad que afecten datos biométricos tratados mediante sistemas de inteligencia artificial, a través de la implementación de un protocolo estructurado de detección, notificación, gestión y documentación de brechas de seguridad, conforme a la LOPDP, su Reglamento General y la Resolución No. SPDP-SPD-2026-0009-R emitida por la Superintendencia de Protección de Datos Personales, que establece lineamientos específicos para el tratamiento de datos personales mediante sistemas de inteligencia artificial, con la finalidad de garantizar el cumplimiento de las obligaciones legales, minimizar los riesgos derivados del tratamiento y proteger de manera efectiva los derechos de los titulares de los datos personales.

3. TERMINOLOGÍA

Para efectos del presente Plan de Respuesta ante Incidentes de Seguridad, se adoptan las siguientes definiciones:

Incidente de seguridad biométrica con IA: Evento que afecta o puede afectar la seguridad de datos biométricos y sistemas automatizados que los procesan. En el ámbito de la salud, comprende riesgos sobre información de pacientes, personal sanitario, accesos e historias clínicas electrónicas.

Datos personales: Información que identifica o hace identificable a pacientes, profesionales de salud, personal administrativo o terceros vinculados a la institución.

Datos sensibles: Datos cuyo tratamiento indebido puede dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales

Brecha o vulneración de seguridad: Violación que ocasiona pérdida, alteración, divulgación o acceso no autorizado a datos personales tratados por la institución.

Datos biométricos: Datos obtenidos de características físicas, fisiológicas o conductuales utilizados para identificación o autenticación de pacientes y personal.

Inteligencia artificial (IA): Sistemas tecnológicos que procesan datos y generan resultados o decisiones automatizadas aplicadas a procesos clínicos, administrativos o de la seguridad.

DPD: Delegado de Protección de Datos Personales, encargado de supervisar el cumplimiento normativo institucional.

Riesgo residual: Nivel de riesgo que permanece luego de aplicar controles y medidas de mitigación.

4. MARCO NORMATIVO APLICABLE

4.1. Normativa nacional

Constitución de la República del Ecuador (2008): Art. 66, numeral 19: Reconoce el derecho a la protección de datos personales y exige autorización del titular o mandato legal para su tratamiento; **Art. 66 numeral 20:** Garantiza el derecho a la intimidad personal y familiar.

Ley Orgánica de Protección de Datos Personales - LOPDP (2021) Art. 43: Establece la obligación de notificar vulneraciones de seguridad a la autoridad competente dentro de plazos determinados, así como la obligación del encargado de informar al responsable del

tratamiento; **Art. 46:** Establece la obligación de notificar al titular cuando la vulneración implique riesgo para sus derechos y libertades.

Reglamento General de la LOPDP (2023): Arts. 25 al 28: Desarrollan la finalidad, contenido y procedimiento de la notificación de vulneraciones de seguridad, incluyendo el reporte a la autoridad, la información mínima requerida, la obligación del encargado de informar al responsable y la comunicación al titular en lenguaje claro.

Resolución SPDP-SPD-2026-0009-R: Establece lineamientos para el tratamiento de datos personales mediante sistemas de IA.

Resolución SPDP-SPD-2026-0012-R: Regula lineamientos de gestión de riesgos y evaluación de impacto en protección de datos personales.

Código Orgánico Integral Penal - COIP (2014): Art. 229: Sanciona la revelación ilegal de bases de datos; **Art. 232:** Tipifica ataques a la integridad de sistemas informáticos.

4.2. Estándares internacionales de referencia

Reglamento General de Protección de Datos - RGPD (2016): Art. 32: Seguridad del tratamiento y medidas técnicas y organizativas; **Art. 33:** Notificación de violaciones de seguridad a la autoridad de control; **Art. 34:** Comunicación de brechas al titular cuando exista alto riesgo.

ISO/IEC 27035 (2023): Establece directrices para identificación, análisis, respuesta y mejora continua frente a incidentes de seguridad.

ISO/IEC 27001 (2023) Define requisitos para implementar un Sistema de Gestión de Seguridad de la Información basado en riesgos.

5. ALCANCE

El presente Plan de Respuesta ante Incidentes de Seguridad aplica al Hospital Oncológico Vida Nueva, a todo tratamiento de datos personales y sensibles (salud y biométricos), incluidos aquellos procesados mediante IA. Su cumplimiento es obligatorio para personal y terceros involucrados, y comprende sistemas, plataformas, dispositivos y entornos físicos y digitales, así como todas las fases de gestión de incidentes: detección, análisis, contención, notificación, remediación y cierre, conforme a la LOPDP y su Reglamento.

Se considerarán incidentes, entre otros, los siguientes:

- **Acceso no autorizado a bases de datos biométricas:** ingreso, consulta, extracción o manipulación indebida de información biométrica por accesos internos o externos no autorizados.
- **Filtración, pérdida o alteración de datos biométricos:** exposición, eliminación, corrupción o modificación accidental o ilícita de registros biométricos o datos asociados.
- **Fallas en sistemas de IA:** errores técnicos, sesgos algorítmicos o decisiones automatizadas incorrectas que afecten procesos clínicos, autenticación o clasificación de riesgos.

6. POLÍTICA (Fases del protocolo de respuesta)

6.1. Fase 1 (Detección e identificación del incidente): Una vez que cualquier miembro de la organización detecte o tenga sospecha fundada de la existencia de un incidente de seguridad relacionado con sistemas biométricos basados en IA, deberá comunicarlo de forma inmediata al DPD a través del canal interno habilitado para tal efecto (dpd@hospitalvidanueva.med.ec). Recibida la notificación, el DPD, en coordinación con el área de TI, deberá en un plazo máximo de seis (06) horas identificar la naturaleza del

incidente, determinando su tipo (acceso no autorizado, pérdida, alteración, filtración, etc.), alcance y sistemas comprometidos, registrar la fecha y hora de detección del incidente, así como la fecha y hora en que fue conocido por el responsable del tratamiento, clasificar preliminarmente la gravedad del incidente (crítica, alta, media o baja), considerando el tipo de datos personales involucrados, en especial si se trata de datos sensibles como biométricos, activar formalmente el equipo de respuesta a incidentes, el mismo que estará conformado por el DPD, junto con las áreas de TI, Jurídica y Alta Dirección.

6.2. Fase 2 (Contención y análisis): Una vez identificado el incidente, el equipo de respuesta deberá ejecutar de manera inmediata las acciones de contención y análisis, bajo la dirección del DPD. Se deberá aislar los sistemas, aplicaciones o redes comprometidas con el fin de evitar la propagación del incidente y mitigar sus efectos; preservar las evidencias digitales conforme a estándares de informática forense, garantizando la integridad, autenticidad y trazabilidad de la información recolectada; y analizar el incidente para determinar las categorías de datos personales afectados (identificativos, sensibles, biométricos, etc.), el número aproximado de titulares afectados, así como las posibles consecuencias y riesgos para los derechos y libertades de los titulares. Asimismo, durante esta fase deberá determinarse si el incidente constituye o no una vulneración de seguridad de datos personales conforme a la LOPDP y su Reglamento General, considerando si existió acceso no autorizado, pérdida, alteración, divulgación o destrucción de información. El resultado de este análisis permitirá definir las medidas de mitigación aplicables y establecer los pasos posteriores a seguir, incluyendo la necesidad de notificación a la autoridad de control y/o a los titulares de los datos. Durante esta fase, la participación del DPD es obligatoria, debiendo levantarse un acta de incidente que documente de forma detallada los hechos conocidos, acciones ejecutadas y decisiones adoptadas.

6.3. Fase 3 (Notificación a la autoridad de control)

Una vez determinada la existencia de una vulneración de seguridad de datos personales, la organización deberá evaluar si es probable que dicha vulneración constituya un riesgo para los derechos y libertades de las personas naturales, conforme al artículo 24 del Reglamento General a la LOPDP. En caso afirmativo, deberá notificarse a la Superintendencia de Protección de Datos Personales tan pronto como sea posible y, como máximo, dentro del **término de cinco (05) días** desde que se tuvo constancia del incidente, de conformidad con el artículo 43 de la LOPDP. Asimismo, deberá realizarse la notificación correspondiente a la ARCOTEL conforme a la normativa sectorial aplicable. La notificación deberá incluir, al menos, la naturaleza de la vulneración, los titulares o grupos afectados, las categorías y volumen de datos comprometidos, los sistemas involucrados, la causa presunta del incidente, las posibles consecuencias y las medidas adoptadas o previstas para su mitigación. En caso de no contar inicialmente con toda la información requerida, podrá remitirse una notificación preliminar y complementarla posteriormente. Por otro lado, cuando el incidente sea detectado por un encargado del tratamiento, este deberá comunicarlo al responsable tan pronto como sea posible y, como máximo, dentro del **término de dos (02) días**. Todo el proceso deberá documentarse adecuadamente como evidencia del cumplimiento del principio de responsabilidad proactiva y trazabilidad en la gestión del incidente.

6.4. Fase 4 (Notificación a los titulares)

La notificación a los titulares procederá cuando la vulneración de seguridad pueda generar un riesgo para sus derechos y libertades fundamentales. En estos casos, el responsable deberá comunicar el incidente sin dilación indebida y dentro del **término de tres (03) días** contados desde que tuvo conocimiento de la existencia del riesgo derivado de la vulneración. La referida comunicación deberá ser individual, directa, oportuna y redactada en lenguaje claro, sencillo y comprensible. Deberá informar la naturaleza del incidente, las categorías de

datos comprometidos, las posibles consecuencias, las medidas adoptadas por la organización, las recomendaciones para que el titular pueda protegerse, los canales de contacto del DPD o área responsable, y los derechos que puede ejercer. No será necesaria la notificación directa cuando existan medidas técnicas u organizativas efectivas que eliminen o reduzcan el riesgo, cuando se hayan adoptado acciones que impidan su materialización, o cuando la comunicación individual implique un esfuerzo desproporcionado. En este último caso, deberá realizarse una comunicación pública por un medio idóneo. Estas excepciones deberán justificarse y documentarse.

6.5. Fase 5 (Remediación y cierre)

Implementar medidas correctivas: Adoptar acciones para eliminar la causa raíz del incidente y evitar su repetición, corrigiendo vulnerabilidades técnicas, accesos o configuraciones. En sistemas de IA, evaluar fallas del modelo, datos o configuración.

Revisar y actualizar medidas de seguridad: Evaluar y fortalecer controles técnicos y organizativos como cifrado, accesos y auditorías. Ajustar protocolos y capacitar al personal ante debilidades detectadas.

Documentar el incidente (LOPDP): Registrar el incidente de forma completa, incluyendo naturaleza, datos afectados, consecuencias, medidas y notificaciones. Este registro evidencia el cumplimiento del principio de responsabilidad proactiva y demostrada (Art. 10, literal k de la LOPDP).

Evaluar impacto en el riesgo residual: Analizar si el incidente modifica el riesgo residual previamente identificado. De ser necesario, actualizar la matriz de riesgos y redefinir medidas de mitigación.

Determinar necesidad de reDPIA: Evaluar si el incidente requiere una nueva Evaluación de Impacto en Protección de Datos. Aplica cuando existan nuevos riesgos o cambios significativos en el tratamiento.

7. ROLES Y RESPONSABILIDADES

La estructura organizacional para el plan de respuesta ante incidentes de seguridad está compuesta por:

Rol	Responsabilidad en el plan
Delegado de Protección de Datos (DPD)	Coordina el protocolo, notifica a la autoridad y a los titulares, documenta el incidente.
Área de Tecnología (TI / Sistemas)	Detecta, contiene y analiza técnicamente el incidente. Preserva evidencias.
Área Jurídica	Evalúa implicaciones legales, asesora sobre plazos y contenido de notificaciones
Alta Dirección	Aprueba decisiones críticas, asume responsabilidad institucional del incidente.
Personal en general	Detecta y reporta internamente cualquier incidente o sospecha al DPP.

8. FLUJOGRAMA DEL PROTOCOLO DE NOTIFICACIÓN

***REF**: Documento disponible en el Anexo No. 1, adjunto al presente plan.*

9. REGISTRO DE INCIDENTES Y DOCUMENTACIÓN

De conformidad con la LOPDP, el registro interno de incidentes deberá contener la siguiente información:

- Fecha y hora de detección y de conocimiento del incidente, para el cómputo de plazos legales.
- Naturaleza del incidente y categorías de datos afectados, indicando si se trata de datos sensibles (salud, biométricos, etc.).
- Consecuencias reales y potenciales, evaluando el impacto en los derechos de los titulares.
- Medidas adoptadas, incluyendo acciones de contención, remediación y mitigación (técnicas, organizativas y jurídicas).
- Notificaciones realizadas, tanto a la autoridad de control como a los titulares, con detalle de fechas y medios utilizados.

Decisión sobre la necesidad de una reDPIA, en caso de nuevos riesgos o cambios en el nivel de riesgo.

ANEXO NO. 5 CORRESPONDIENTE AL PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN - FLUJOGRAMA DEL PROTOCOLO DE NOTIFICACIÓN

FLUJOGRAMA DEL PROTOCOLO DE NOTIFICACIÓN

Incidentes de seguridad sobre datos biométricos, datos de salud y sistemas de inteligencia artificial

Objetivo	Responsable institucional	Áreas involucradas
Gestionar, contener, documentar y notificar vulneraciones que afecten datos personales de alta sensibilidad.	Responsable del tratamiento, con asesoría y supervisión del DPD. El DPD no decide fines ni ejecuta medidas técnicas.	DPD, Tecnología, Jurídico, Alta Dirección, personal operativo y proveedores autorizados, según corresponda.