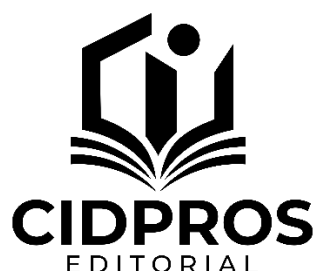


Protección ^{de} datos personales y privacidad en la sociedad digital

Sofía Verónica Murillo Vásquez, Jhonatan
Alberto Cifuentes Carreño, David Israel
Báez Herrera, Adriana Carolina Calderón
Muñoz & Galo Fernando Almeida
Casanova

Protección de datos personales y privacidad en la sociedad digital

Sofía Verónica Murillo Vásquez, Jhonatan Alberto
Cifuentes Carreño, David Israel Báez Herrera, Adriana
Carolina Calderón Muñoz & Galo Fernando Almeida
Casanova





Datos bibliográficos

ISBN	978-9907-848-08-3
Título del libro	Protección de datos personales y privacidad en la sociedad digital
Autores	Sofía Verónica Murillo Vásquez Jhonatan Alberto Cifuentes Carreño David Israel Báez Herrera Adriana Carolina Calderón Muñoz Galo Fernando Almeida Casanova
Editorial	CIDPROS EDITORIAL
Materia	340 - Derecho
Público objetivo	Profesional / académico
Año	2026
Número de edición	1
Tamaño	3.56Mb
Soporte	Libro digital descargable
Formato	PDF (.pdf)
Idioma	Español
DOI	https://doi.org/10.70577/7me6nd31

Hecho en Ecuador / Made in Ecuador

MSc. Sofía Verónica Murillo Vásquez

Notaría Octava de Guayaquil – Ministerio de Educación

sveronica1@hotmail.es

<https://orcid.org/0009-0002-3869-8320>

Durán, Guayas, Ecuador

Semblanza

Sofía Verónica Murillo Vásquez nació en Guayaquil, Ecuador, el 17 de mayo de 1982. Es abogada, educadora, docente universitaria, asesora legal y mediadora, con una trayectoria profesional caracterizada por la integración del Derecho y la educación como espacios de servicio, formación y transformación social.

Desde el año 2004 se desempeña como docente del Ministerio de Educación del Ecuador, institución en la que ha desarrollado una trayectoria de más de dos décadas dedicada a la enseñanza y a la formación de nuevas generaciones. Su experiencia educativa se ha fortalecido con estudios de cuarto nivel en Derecho, Educación y Ciencias de la Educación, contando con tres títulos de maestría: Derecho con mención en Derecho Constitucional; Educación con mención en Pedagogía; y Ciencias de la Educación con mención en Diseño y Evaluación del Plan de Estudios. Es, además, Abogada y Licenciada en Ciencias de la Educación, y ha complementado su formación con estudios especializados en contratación pública, didáctica, inclusión educativa y tecnologías aplicadas a la educación.



Su trayectoria académica y profesional se extiende también al ámbito universitario. Actualmente ejerce la docencia universitaria en la Universidad Bolivariana del Ecuador, tanto en programas de pregrado como de posgrado, donde participa en procesos de planificación académica, rediseño curricular, evaluación por competencias y formación profesional.

En el ámbito jurídico, cuenta con más de una década de experiencia vinculada a la asesoría legal y al Derecho Notarial, desempeñándose como asesora legal en la Notaría Octava del cantón Guayaquil. Su ejercicio profesional comprende áreas del Derecho Notarial, Registral, Civil, Mercantil y de Familia, experiencia que le ha permitido relacionar la formación jurídica con la práctica profesional y con las necesidades concretas de la sociedad.

A esta trayectoria se suma su formación como Mediadora, Negociadora y Conciliadora certificada por el Consejo de la Judicatura, incorporando a su ejercicio profesional herramientas para el diálogo, la negociación, la prevención y solución de conflictos, desde una perspectiva orientada al entendimiento y a la construcción de acuerdos.

Su concepción de la educación se fundamenta en la inclusión, la innovación y el reconocimiento de la diversidad. Su experiencia en Diseño Universal para el Aprendizaje, metodologías activas, competencias digitales y evaluación por competencias refleja una

permanente búsqueda de nuevas formas de enseñar y aprender, colocando a la persona y a su desarrollo integral en el centro del proceso educativo.

A lo largo de su carrera, ha construido un perfil interdisciplinario en el que convergen educación, Derecho, mediación y tecnología, convencida de que el conocimiento adquiere verdadero sentido cuando se transforma en una herramienta para comprender la realidad, resolver problemas y contribuir al bienestar colectivo.

Su trayectoria representa el compromiso de una profesional que ha encontrado en la educación y el Derecho dos caminos complementarios para servir a la sociedad. Desde la docencia, la práctica jurídica y la mediación, Sofía Verónica Murillo Vásquez continúa aportando a la formación de profesionales con pensamiento crítico, criterio jurídico, sensibilidad humana, capacidad de diálogo y responsabilidad social.

Mgtr. Jhonatan Alberto Cifuentes Carreño

Docente del Ministerio de Educación

jcifuca@gmail.com

<https://orcid.org/0009-0003-8581-6999>

Durán, Guayas, Ecuador

Semblanza

Jhonatan Alberto Cifuentes Carreño es docente, profesional de las artes y especialista en tecnología e innovación educativa, cuya trayectoria se caracteriza por la integración de la educación, la creatividad, la comunicación y las nuevas tecnologías como herramientas para el desarrollo humano y la construcción de aprendizajes significativos. Es Licenciado en Arte, con especialización en Música, Danza, Teatro y Pintura, por la Universidad de Guayaquil, y posee una Maestría en Tecnología e Innovación Educativa por la Universidad Tecnológica ECOTEC. Actualmente se encuentra finalizando una Maestría en Lengua y Literatura, formación que amplía su perspectiva profesional hacia los ámbitos de la comunicación, el lenguaje, la lectura, la escritura y la construcción del conocimiento.



Desde el año 2019 se desempeña como docente del Ministerio de Educación del Ecuador, desarrollando una trayectoria orientada a la formación integral de sus estudiantes. Su experiencia educativa se ha fortalecido mediante procesos de capacitación en innovación, creatividad, metodologías activas, inclusión educativa, derechos humanos, emprendimiento y formación artística, así como en estrategias pedagógicas vinculadas con las nuevas demandas de la educación contemporánea.

Su preparación en Tecnología e Innovación Educativa le ha permitido acercarse a los procesos de transformación digital desde una perspectiva pedagógica, comprendiendo el papel que cumplen las herramientas tecnológicas en la enseñanza y en las nuevas formas de comunicación, interacción y acceso a la información.

De manera complementaria, desarrolla una importante labor como docente de personas adultas mayores en el Centro de Atención al Adulto Mayor (CAAM), programa gestionado por el Instituto Ecuatoriano de Seguridad Social (IESS) del Ecuador. Esta experiencia le ha permitido participar en procesos de acompañamiento y formación dirigidos a este grupo de la población, promoviendo espacios de aprendizaje, participación, creatividad y desarrollo personal.

Su trabajo con adultos mayores adquiere especial relevancia frente a los cambios que ha generado la incorporación de las tecnologías digitales en la vida cotidiana. Desde esta experiencia, reconoce la importancia de facilitar procesos de aprendizaje que permitan a las personas desenvolverse con mayor autonomía y confianza en los entornos digitales, al mismo tiempo que desarrollan una actitud consciente frente al uso de la información y las nuevas formas de comunicación.

Su formación artística constituye otro componente esencial de su trayectoria. Como profesional de la música, danza, teatro y pintura, entiende el arte como un medio para estimular la creatividad, la sensibilidad, la expresión y el pensamiento crítico. Esta visión se articula con su experiencia docente y con su formación tecnológica, generando una perspectiva interdisciplinaria en la que convergen arte, educación, comunicación e innovación.

La combinación de su formación en tecnología, su preparación en Lengua y Literatura y su experiencia educativa le permite abordar los desafíos de la sociedad contemporánea desde una mirada integral, en la que el desarrollo tecnológico debe estar acompañado de educación, pensamiento crítico, responsabilidad y conciencia sobre el manejo de la información.

A lo largo de su trayectoria, Jhonatan Alberto Cifuentes Carreño ha consolidado un perfil profesional orientado al aprendizaje permanente y a la innovación, convencido de que la educación debe responder a las transformaciones sociales y tecnológicas sin perder de vista su dimensión humana. Su experiencia refleja el compromiso de un educador que encuentra en la tecnología, el arte y la comunicación oportunidades para generar aprendizajes, fortalecer capacidades y contribuir a una sociedad más consciente, inclusiva y responsable.

MSc. David Israel Báez Herrera

Investigador Independiente

dbmasternet@gmail.com

<https://orcid.org/0009-0009-2487-7214>

Quito, Pichincha, Ecuador

Semblanza

David Israel Báez Herrera es un investigador y profesional ecuatoriano residente en Quito, especializado en tecnologías de la información, transformación digital, gestión de proyectos e innovación educativa. Cuenta con un Bachelor of Arts (BA) en Redes y Sistemas Operativos, una maestría en Telecomunicaciones y una maestría en Innovación Educativa.

Actualmente cursa un Doctorado en Dirección de Proyectos, en el que desarrolla una investigación orientada al fortalecimiento de los procesos de evaluación interna y acreditación de las instituciones de educación superior mediante un modelo apoyado en una plataforma digital para la gestión, validación y análisis de evidencias. Posee más de diez certificaciones internacionales y acreditaciones de formación especializada en tecnologías, metodologías y estándares promovidos por organizaciones reconocidas como Cisco, Amazon Web Services (AWS), Red Hat, WatchGuard, Microsoft y Hewlett Packard (HP), además de formación en gestión de proyectos bajo el enfoque PMP y en sistemas de gestión basados en normas ISO.

Su preparación comprende áreas como redes, ciberseguridad, telecomunicaciones, computación en la nube, desarrollo de software, bases de datos, infraestructura tecnológica, sistemas operativos y dirección de proyectos. También cuenta con formación y certificaciones relacionadas con los sistemas de gestión de la calidad ISO 9001 y de seguridad de la información ISO/IEC 27001, así como una certificación como Delegado de Protección de Datos, conocimientos que le han permitido intervenir en iniciativas de calidad, seguridad digital, privacidad, protección de datos personales y cumplimiento normativo. Su perfil académico se complementa con más de 150 cursos de formación continua, cuatro diplomados vinculados con programación, investigación científica e inteligencia artificial y la participación en seminarios internacionales relacionados con sus áreas de especialización.

A lo largo de más de quince años de trayectoria, ha asesorado y acompañado a organizaciones públicas y privadas de los sectores educativo, financiero, bancario, inmobiliario, de la construcción y del desarrollo tecnológico en proyectos de infraestructura, redes, telecomunicaciones, seguridad informática y transformación digital. En el ámbito de la educación superior, ha liderado y participado en la implementación de soluciones de software a medida para la gestión académica, administrativa y contable, contribuyendo a la automatización de actividades, la integración de información, la generación de indicadores y el fortalecimiento de la toma de decisiones institucionales. Su experiencia también comprende



el diseño instruccional de contenidos y entornos virtuales de aprendizaje, la administración de plataformas educativas, el desarrollo de sistemas de información, la mejora y optimización de procesos y la implementación, mantenimiento y evaluación de sistemas de gestión de la calidad. Su ejercicio profesional se caracteriza por integrar la tecnología, la educación, la investigación y la gestión organizacional desde una perspectiva interdisciplinaria orientada a la innovación, la mejora continua, la seguridad de la información y el cumplimiento normativo.

Mantiene un firme compromiso con la ética profesional, la actualización permanente y la generación de soluciones tecnológicas que contribuyan a elevar la calidad educativa, fortalecer la eficiencia de las organizaciones y producir un impacto positivo y sostenible en la sociedad.

Abg. Adriana Carolina Calderón Muñoz

Investigador Independiente

ab.carolinacalderonm@gmail.com

<https://orcid.org/0009-0005-8229-8908>

Playas, Guayas, Ecuador

Semblanza

Carolina Calderón Muñoz es una jurista ecuatoriana, con más de 10 años de experiencia en el ámbito público y privado, desde muy temprana edad fortaleció su sensibilidad social y conciencia ambiental, que pudo desarrollar utilizando al Derecho como una herramienta al servicio de su país, desarrollándose en múltiples instituciones como Consejo Nacional de la Judicatura, Universidad de Guayaquil, Federación Nacional de Cooperativas Pesqueras, Cooperativas de transportes y otras.

Cuenta con una sólida formación académica: es abogada, magister en relaciones internacionales con mención en cooperación Internacional, Magister en Derecho Constitucional, Doctora Honoris Causa como reconocimiento a su trayectoria Social, Experta en Derechos Humanos con enfoque en Género, diplomada en Políticas Públicas, actualmente se desempeña como abogada litigante, y conferencista internacional en Derecho Ambiental y sustentabilidad, en diversas Universidades de Latinoamérica demostrando así su compromiso con la Academia y el medio ambiente siguiendo los lineamientos de los Objetivos del desarrollo sostenible.

Convencida de que solo una comunidad instruida, puede hacer cambios significativos, escribe artículos que contribuyan a investigadores y al desarrollo de futuros profesionales.



MSc. Galo Fernando Almeida Casanova

Universidad Politécnica Estatal del Carchi

galo.almeida@upec.edu.ec

<https://orcid.org/0009-0000-3388-6264>

Tulcán, Carchi, Ecuador

Semblanza

Galo Almeida es ingeniero en finanzas por la Universidad Central del Ecuador y posee un magíster en administración de empresas con mención en innovación socioproductiva sostenible, otorgado por la Universidad Tecnológica Indoamérica (Ecuador). Actualmente avanza en su Doctorado en Administración de Empresas en la Universidad Central de Querétaro, México.

Además, cuenta con una formación complementaria orientada a la gestión y al desarrollo organizacional, entre la que destacan un Diplomado en Gerencia de Organizaciones Solidarias (Universidad Santo Tomás, Colombia), un Diplomado en Emprendimiento e Innovación (Fundación Perea, Colombia), un Diplomado en Gerencia de Microfinanzas y Gestión del Cambio (Universidad Metropolitana de Honduras) y una Certificación en Gestión Integral de Riesgos Financieros (Risk Management Consulting).

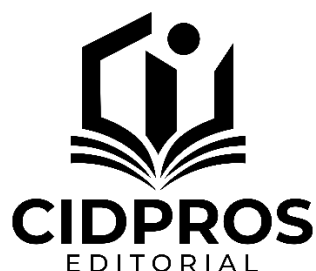
Con más de 15 años de experiencia en los sectores público y privado, su trayectoria ensemble se distingue por una clara orientación tanto académica como práctica. En el ámbito docente, ha impartido clases en la Universidad Politécnica Estatal del Carchi y en el Instituto Superior Tecnológico de Técnicas Empresariales y del Conocimiento, abarcando áreas contables y administrativas.

En su labor profesional, se ha desempeñado como consultor en la Administración Integral de Riesgos dentro del sector financiero de la Economía Popular y Solidaria. También fue Experto en Riesgo Financiero en el Instituto Ecuatoriano de Seguridad Social y Subgerente Administrativo Financiero en la Cooperativa de Ahorro y Crédito Pablo Muñoz Vega.

Su experiencia incluye funciones como Director Nacional de Investigación y Capacitación (en funciones) y Especialista de Investigación y Capacitación en la Superintendencia de Economía Popular y Solidaria. En el ámbito de la banca pública, ha trabajado como Analista de Riesgo de Crédito y Control Metodológico, así como Oficial de Crédito en el Banco Nacional de Fomento y BanEcuador. Además, formó parte del Banco del Pacífico, desempeñando roles como cajero, supervisor de cajas y asesor de atención al cliente.

Su perfil se caracteriza por una sólida formación académica y una amplia experiencia en gestión financiera, docencia, investigación, capacitación y administración integral de riesgos, con un énfasis especial en el fortalecimiento institucional y el desarrollo del sector financiero popular y solidario.





El contenido y las ideas expuestas en esta obra se encuentran protegidos por la normativa vigente en materia de propiedad intelectual y constituyen derechos exclusivos de su(s) autor(es).

Derechos de Autor © 2026

Este documento se publica bajo los términos y condiciones de la licencia:



Creative Commons Reconocimiento – No Comercial – Compartir Igual 4.0 Internacional (CC BY-NC-SA 4.0)

Usted es libre de compartir y adaptar el material, siempre que otorgue el crédito correspondiente, no lo utilice con fines comerciales y distribuya sus contribuciones bajo la misma licencia.

Para ver una copia de esta licencia, visite: <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>

Sinopsis

La protección de datos personales y la privacidad constituyen dimensiones esenciales para garantizar los derechos individuales en una sociedad caracterizada por la circulación permanente de información digital. Esta obra analiza los fundamentos jurídicos de la privacidad, las categorías de datos protegidos y los principios que deben orientar su tratamiento, considerando la relación entre intimidad, autodeterminación informativa y control sobre la información personal. Asimismo, examina las etapas del tratamiento de datos en entornos digitales, los procesos de recolección, almacenamiento, transferencia, elaboración de perfiles y utilización de sistemas automatizados e inteligencia artificial. El libro aborda también el consentimiento, la transparencia y los principales derechos reconocidos a los titulares, así como las obligaciones de responsables y encargados del tratamiento. Se estudian las vulneraciones de seguridad, filtraciones, daños, infracciones, sanciones y mecanismos de reparación disponibles frente a afectaciones de la privacidad. Finalmente, se desarrollan los sistemas de cumplimiento normativo, las políticas internas, la protección de datos desde el diseño y por defecto, las evaluaciones de impacto, las medidas de seguridad, la auditoría y los mecanismos institucionales y jurídicos de tutela. La obra ofrece una visión integral orientada a comprender los desafíos jurídicos y organizativos de la protección de datos en el entorno digital contemporáneo.

Palabras clave: protección de datos personales; privacidad; tratamiento de datos; derechos digitales; cumplimiento normativo.

Synopsis

Personal data protection and privacy are essential dimensions for safeguarding individual rights in a society characterized by the constant circulation of digital information. This book examines the legal foundations of privacy, the categories of protected data, and the principles that should guide data processing, considering the relationship between intimacy, informational self-determination, and control over personal information. It also analyzes the stages of data processing in digital environments, including collection, storage, transfer, profiling, and the use of automated systems and artificial intelligence. The book also addresses consent, transparency, and the main rights recognized to data subjects, as well as the obligations of data controllers and processors. Security breaches, data leaks, resulting damages, infringements, sanctions, and available mechanisms for redress are examined. Finally, the book develops compliance systems, internal policies, data protection by design and by default, impact assessments, security measures, auditing, and institutional and legal mechanisms for effective privacy protection. The work provides a comprehensive perspective aimed at understanding the legal and organizational challenges involved in protecting personal data within contemporary digital environments.

Keywords: personal data protection; privacy; data processing; digital rights; regulatory compliance.

Índice de Contenido

Sinopsis	12
Synopsis	14
Introducción	17
Capítulo 1 Privacidad y protección jurídica de los datos personales	20
1.1 Concepto y evolución del derecho a la privacidad	21
1.2 Datos personales y categorías de información protegida	24
1.3 Principios jurídicos de la protección de datos personales	28
1.4 Privacidad, intimidad y autodeterminación informativa	31
1.5 Sujetos que intervienen en la protección de datos personales	34
1.6 Riesgos jurídicos derivados del uso indebido de datos personales	38
1.7 Protección de datos personales como garantía de los derechos individuales	41
Capítulo 2 Tratamiento de datos personales en entornos digitales	45
2.1 Concepto y etapas del tratamiento de datos personales	46
2.2 Recolección de datos mediante plataformas y servicios digitales	49
2.3 Almacenamiento, conservación y eliminación de datos personales	52
2.4 Elaboración de perfiles y análisis automatizado de información personal	55
2.5 Tratamiento de datos mediante inteligencia artificial y sistemas algorítmicos	59
2.6 Transferencia y comunicación de datos personales a terceros	63
2.7 Tratamiento de datos personales en redes sociales y aplicaciones digitales	66
2.8 Riesgos asociados al tratamiento masivo y automatizado de datos	70
Capítulo 3 Consentimiento, transparencia y derechos de los titulares	73
3.1 Consentimiento como fundamento para el tratamiento de datos personales	74
3.2 Requisitos para la validez del consentimiento	77
3.3 Información previa y deber de transparencia frente al titular	81
3.4 Derecho de acceso a los datos personales	83
3.5 Rectificación y actualización de información personal	86
3.6 Supresión, eliminación y derecho al olvido	91

3.7	Oposición y limitación del tratamiento de datos personales	93
3.8	Portabilidad de datos y decisiones automatizadas.....	96
Capítulo 4 Responsabilidad jurídica por vulneraciones de datos personales		100
4.1	Vulneraciones de seguridad y exposición de datos personales	101
4.2	Responsabilidad de responsables y encargados del tratamiento	104
4.3	Responsabilidad por acceso, uso o divulgación no autorizada de datos	107
4.4	Incidentes de seguridad, filtraciones y deber de notificación	110
4.5	Daños derivados de las vulneraciones de datos personales.....	113
4.6	Infracciones y sanciones en materia de protección de datos.....	116
4.7	Reparación y mecanismos de reclamación frente a vulneraciones de privacidad...	120
Capítulo 5 Cumplimiento normativo y tutela de la privacidad.....		123
5.1	Sistemas de cumplimiento en materia de protección de datos personales	124
5.2	Políticas internas y procedimientos para la gestión de información personal.....	127
5.3	Protección de datos desde el diseño y por defecto	131
5.4	Evaluación de riesgos e impacto en la privacidad.....	134
5.5	Medidas técnicas y organizativas para la seguridad de los datos.....	137
5.6	Supervisión, auditoría y control del cumplimiento normativo.....	140
5.7	Mecanismos institucionales y jurídicos para la tutela efectiva de la privacidad.....	144
Conclusión		148
Bibliografía		151

Introducción

La expansión de los entornos digitales ha transformado profundamente la forma en que las personas producen, comunican y almacenan información sobre sí mismas. Actividades cotidianas como realizar compras, utilizar redes sociales, acceder a servicios públicos, recibir atención sanitaria o interactuar con plataformas digitales generan cantidades crecientes de datos personales. Esta realidad ha convertido la privacidad en una cuestión central para el ejercicio de derechos en la sociedad contemporánea. La protección de información personal ya no puede limitarse a impedir intromisiones directas en la vida privada, sino que exige establecer condiciones jurídicas y organizativas para controlar su recopilación, utilización, conservación, circulación y eliminación.

Los datos personales poseen un valor creciente para instituciones públicas, empresas y proveedores tecnológicos porque permiten identificar usuarios, gestionar servicios, analizar comportamientos y automatizar decisiones. Sin embargo, esta capacidad también incrementa las posibilidades de utilización excesiva, acceso no autorizado, elaboración de perfiles, vigilancia, discriminación o pérdida de control sobre la información. La misma tecnología que facilita procesos administrativos y comerciales puede ampliar los riesgos para la privacidad cuando las operaciones realizadas sobre los datos no están claramente delimitadas. Por esta razón, el tratamiento de información personal requiere reglas que permitan aprovechar sus beneficios sin convertir la innovación tecnológica en una justificación para debilitar las garantías individuales.

La protección jurídica de los datos parte del reconocimiento de que la persona debe conservar facultades sobre información que permite identificarla o describir aspectos de su vida. Esta perspectiva relaciona privacidad, intimidad y autodeterminación informativa, pero reconoce que cada concepto protege dimensiones particulares. La privacidad establece límites frente a injerencias injustificadas, mientras la protección de datos desarrolla derechos y obligaciones específicos sobre el uso de información personal. En el ordenamiento ecuatoriano, esta construcción se sostiene en garantías constitucionales, instrumentos internacionales y una legislación especializada que establece principios, responsabilidades, derechos de los titulares y mecanismos destinados a controlar las actividades de tratamiento.

Uno de los desafíos fundamentales se encuentra en la complejidad que ha adquirido el ciclo de vida de los datos. La información puede recopilarse directamente del titular, obtenerse mediante dispositivos y aplicaciones, almacenarse en infraestructuras externas, combinarse con

otras bases y utilizarse para producir inferencias que inicialmente no estaban disponibles. En estas condiciones, conocer quién controla los datos y con qué finalidad puede resultar difícil para las personas. El tratamiento digital requiere, por tanto, analizar todas sus etapas y no únicamente el momento de la recolección. Finalidad, minimización, conservación, seguridad y transparencia deben mantenerse durante toda la existencia de la información.

El consentimiento ocupa un lugar relevante dentro de esta estructura, aunque no representa una autorización ilimitada para cualquier tratamiento posterior. Su validez depende de que exista libertad, información suficiente y una manifestación vinculada con finalidades determinadas. De igual manera, la transparencia constituye una condición necesaria para que el titular pueda comprender qué ocurre con sus datos y ejercer los derechos reconocidos por el ordenamiento jurídico. Acceso, rectificación, actualización, eliminación, oposición, limitación, portabilidad y garantías frente a determinadas decisiones automatizadas permiten intervenir sobre la información y evitar que la persona permanezca en una posición completamente pasiva frente a organizaciones con amplias capacidades tecnológicas.

La seguridad representa otra dimensión indispensable porque incluso un tratamiento inicialmente legítimo puede convertirse en fuente de afectaciones cuando los datos son expuestos, alterados, destruidos o consultados por personas no autorizadas. Las vulneraciones pueden originarse en ataques informáticos, errores humanos, deficiencias organizativas, configuraciones inadecuadas o fallas de proveedores externos. Sus consecuencias pueden alcanzar dimensiones económicas, reputacionales, personales y jurídicas. Por ello, la responsabilidad de responsables y encargados no comienza después de una filtración, sino desde la planificación del tratamiento, mediante la identificación de riesgos, implementación de controles y establecimiento de mecanismos capaces de detectar y responder oportunamente frente a incidentes.

Cuando ocurre una vulneración, la protección jurídica exige determinar responsabilidades y ofrecer respuestas adecuadas a las personas afectadas. La notificación de incidentes, las medidas correctivas, los procedimientos de reclamación y los mecanismos de reparación forman parte de esta respuesta. Las infracciones y sanciones cumplen además una función preventiva al establecer consecuencias frente al incumplimiento de obligaciones relacionadas con seguridad, transparencia, ejercicio de derechos o utilización legítima de la información. Sin embargo, la tutela efectiva no puede reducirse a la imposición de multas, pues también debe permitir detener tratamientos indebidos, corregir información, reducir consecuencias y ofrecer vías administrativas o jurisdiccionales para restablecer los derechos vulnerados.

El cumplimiento normativo adquiere, en este contexto, una dimensión organizativa que supera la simple existencia de documentos jurídicos. Las instituciones necesitan desarrollar sistemas internos capaces de convertir las disposiciones legales en procedimientos verificables. Esto requiere definir responsabilidades, establecer políticas de tratamiento, capacitar al personal, supervisar proveedores, documentar decisiones y evaluar periódicamente la eficacia de las medidas adoptadas. La protección desde el diseño y por defecto refuerza esta orientación preventiva al exigir que la privacidad sea considerada desde la planificación de sistemas y servicios. De esta manera, el cumplimiento deja de funcionar como respuesta posterior y comienza a integrarse en la propia estructura de las operaciones.

La evaluación de riesgos, las medidas técnicas y organizativas, las auditorías y los mecanismos de supervisión permiten mantener ese cumplimiento frente a cambios tecnológicos y organizacionales. Ningún sistema permanece adecuado indefinidamente, porque nuevas herramientas, proveedores, finalidades o modalidades de procesamiento pueden modificar las amenazas existentes. La gestión de privacidad requiere entonces revisión continua, trazabilidad y capacidad de corrección. Esta perspectiva resulta especialmente relevante ante tecnologías automatizadas e inteligencia artificial, cuya capacidad para procesar grandes cantidades de información puede generar decisiones o inferencias difíciles de comprender. La innovación debe acompañarse de criterios de proporcionalidad, transparencia y responsabilidad capaces de preservar los derechos de las personas.

Esta obra aborda progresivamente estas cuestiones mediante cinco dimensiones articuladas: los fundamentos jurídicos de la privacidad y la protección de datos, las condiciones del tratamiento en entornos digitales, el consentimiento y los derechos de los titulares, la responsabilidad frente a vulneraciones y los mecanismos de cumplimiento y tutela. El propósito es ofrecer una comprensión integrada de la protección de datos personales en una sociedad donde la información circula de forma permanente entre individuos, instituciones y tecnologías. La tutela de la privacidad requiere finalmente equilibrar aprovechamiento legítimo de información, innovación digital y respeto efectivo por la autonomía y los derechos individuales.



Capítulo 1

Privacidad y protección jurídica de los datos personales

Sofía Verónica Murillo Vásquez

1.1 Concepto y evolución del derecho a la privacidad

El derecho a la privacidad protege un ámbito de la vida personal frente a injerencias que carecen de justificación jurídica. Su contenido comprende la posibilidad de preservar información, decisiones, relaciones y aspectos de la esfera individual que no deben quedar sometidos a observación, utilización o difusión indiscriminada. Con el desarrollo de las tecnologías digitales, esta protección dejó de referirse únicamente a espacios físicos o comunicaciones privadas y comenzó a abarcar el tratamiento sistemático de información personal. Esta transformación explica que la privacidad se relacione actualmente con el control que cada persona puede ejercer sobre sus datos y sobre los usos posteriores de esa información (Zambrano Rendón et al., 2023).

La formulación jurídica de la privacidad antecede a los actuales sistemas de protección de datos personales. En el plano internacional, la Declaración Universal de Derechos Humanos (1948), en su artículo 12, establece que ninguna persona debe ser objeto de injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, y reconoce su derecho a la protección legal frente a esas actuaciones. Esta disposición consolidó la privacidad dentro del lenguaje internacional de los derechos humanos y permitió que su protección dejara de depender exclusivamente de normas internas. Su contenido constituye un antecedente relevante para comprender la posterior ampliación del derecho hacia los problemas asociados con la información personal y su circulación.

El reconocimiento internacional se fortaleció posteriormente con instrumentos jurídicos vinculantes. El Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 17, prohíbe las injerencias arbitrarias o ilegales en la vida privada, la familia, el domicilio y la correspondencia, así como los ataques ilegales a la honra y reputación. En el sistema interamericano, la Convención Americana sobre Derechos Humanos (1969), en su artículo 11, protege la honra, la dignidad y la vida privada frente a injerencias arbitrarias o abusivas. Estas disposiciones muestran que la privacidad pasó a configurarse como una garantía exigible frente a actuaciones estatales y particulares capaces de afectar injustificadamente la esfera personal.

La evolución tecnológica modificó de manera sustancial las condiciones en las que ese derecho debía ser protegido. La digitalización facilitó la recopilación, almacenamiento, reproducción y circulación de cantidades crecientes de información vinculada con personas identificadas o identificables. Como resultado, una afectación de la privacidad puede producirse sin necesidad de ingresar físicamente en un espacio reservado. El acceso, cruce, conservación o divulgación

de información también puede incidir en la esfera individual. En este contexto, la protección de datos personales adquiere una dimensión propia, orientada a establecer límites sobre las operaciones realizadas con información personal y a reconocer facultades efectivas a sus titulares (Ojeda Bello & Cutié Mustelier, 2021).

En Ecuador, esta evolución encuentra un reconocimiento constitucional expreso. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, se garantiza el derecho a la protección de datos de carácter personal, que comprende el acceso y la decisión sobre dicha información, además de su correspondiente protección. La misma disposición establece que la recolección, archivo, procesamiento, distribución o difusión requieren autorización del titular o mandato de la ley. La Constitución distingue así una dimensión específica relacionada con los datos personales y atribuye al individuo capacidad jurídica de decisión sobre información vinculada con su persona, más allá de la protección general de la intimidad.

Esta construcción jurídica permite diferenciar, aunque estén relacionadas, la privacidad y la protección de datos personales. La primera comprende una esfera más amplia vinculada con la vida privada de la persona, mientras que la segunda establece garantías aplicables específicamente a la información personal y a las operaciones efectuadas sobre ella. En Ecuador, la discusión adquirió mayor relevancia a medida que aumentaron las posibilidades tecnológicas de obtener y utilizar información en ámbitos administrativos, comerciales, sanitarios y digitales. La necesidad de fortalecer la tutela institucional de este derecho ha sido identificada, además, como una cuestión vinculada con políticas públicas y garantías constitucionales (Ordóñez Pineda et al., 2022).

La aprobación de la Ley Orgánica de Protección de Datos Personales profundizó esta evolución desde un reconocimiento constitucional hacia un régimen jurídico especializado. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 1, establece como objeto garantizar el ejercicio del derecho a la protección de datos personales mediante la regulación de principios, derechos, obligaciones y mecanismos de tutela. Su artículo 2 extiende su ámbito material al tratamiento de datos personales contenidos en cualquier soporte, sean automatizados o no, así como a sus usos posteriores. Esta regulación evidencia que la privacidad informacional requiere reglas aplicables durante todo el tratamiento y no únicamente frente a la divulgación final de información.

La ampliación del derecho también responde a la sensibilidad que ciertos datos adquieren según su naturaleza y contexto de utilización. Los datos relacionados con salud muestran con especial claridad este problema, pues su almacenamiento electrónico facilita la gestión de servicios, pero simultáneamente incrementa las posibilidades de acceso, uso y circulación. El estudio de historias clínicas electrónicas en Ecuador evidencia que la incorporación de tecnologías de información exige mecanismos jurídicos capaces de preservar los derechos del titular durante el tratamiento de información sanitaria (Martínez-Jara & Pérez-Ycaza, 2022). Por ello, la evolución de la privacidad debe entenderse también como respuesta a formas cada vez más complejas de producción y utilización de datos personales.

La protección jurídica de la privacidad tampoco puede analizarse únicamente desde relaciones entre el individuo y el Estado. Los entornos digitales incorporan empresas, plataformas, instituciones sanitarias y otros actores privados que recopilan o administran información personal. Esta pluralidad modifica las fuentes de riesgo y exige que las garantías operen frente a distintas formas de poder informacional. La experiencia derivada de aplicaciones utilizadas durante la emergencia sanitaria mostró que la colaboración público-privada puede generar problemas regulatorios respecto de las condiciones y finalidades del tratamiento, especialmente cuando intervienen datos relativos a la salud (Ordell Font, 2022). La privacidad contemporánea requiere, por tanto, obligaciones aplicables a quienes participan efectivamente en el tratamiento.

Junto con el reconocimiento sustantivo del derecho, el ordenamiento ecuatoriano contempla mecanismos destinados a hacerlo exigible. De acuerdo con la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), en su artículo 49, la acción de hábeas data permite acceder a documentos, datos genéticos, bancos o archivos de datos personales y conocer su uso, finalidad, origen, destino y tiempo de vigencia. La misma disposición permite solicitar actualización, rectificación, eliminación o anulación en los casos previstos por la ley. Esta garantía muestra una evolución relevante: la protección ya no consiste únicamente en impedir intromisiones, sino también en proporcionar instrumentos para intervenir sobre información previamente recopilada.

En el contexto ecuatoriano actual, el derecho a la privacidad debe entenderse como una construcción jurídica que combina protección frente a injerencias, capacidad de decisión sobre información personal y mecanismos de tutela frente a tratamientos que puedan afectar otros derechos. La legislación especializada responde al crecimiento de prácticas digitales en las que los datos adquieren valor para entidades públicas y privadas. El análisis de la normativa

ecuatoriana muestra que la protección de datos se ha incorporado al ámbito de los derechos digitales y exige condiciones jurídicas para su ejercicio efectivo (Moran Barreto, 2023). En consecuencia, su evolución refleja el tránsito desde la reserva de la vida privada hacia un control jurídico más amplio sobre la información personal.

1.2 Datos personales y categorías de información protegida

Los datos personales comprenden información vinculada con una persona natural identificada o identificable y constituyen el objeto central del régimen jurídico de protección de datos. Su importancia no depende únicamente del formato en el que se encuentren, pues pueden presentarse como información escrita, numérica, gráfica, fotográfica, sonora o almacenada digitalmente. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, define el dato personal a partir de su relación con una persona natural y de la posibilidad de identificarla directa o indirectamente. Esta amplitud permite aplicar la protección jurídica a información producida en contextos administrativos, comerciales, sanitarios y tecnológicos (Zambrano Rendón et al., 2023).

La identificación de una persona no depende exclusivamente de datos evidentes como nombres, apellidos o números de identificación. Una combinación de elementos vinculados con ubicación, actividad, características físicas, preferencias o relaciones puede permitir reconocer a una persona incluso cuando su nombre no aparece expresamente. Esta circunstancia adquiere especial importancia en los entornos digitales, donde diferentes fragmentos de información pueden relacionarse entre sí. La protección jurídica debe considerar, por tanto, tanto los datos que identifican directamente como aquellos que permiten una identificación indirecta mediante asociación o análisis. Esta concepción amplia evita restringir la tutela únicamente a registros tradicionalmente considerados identificativos (Ojeda Bello & Cutié Mustelier, 2021).

La Constitución ecuatoriana reconoce esta información como objeto de un derecho específico. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, las personas tienen derecho a la protección de sus datos de carácter personal, incluido el acceso y la decisión sobre ellos. La disposición establece además que su recolección, archivo, procesamiento, distribución o difusión requieren autorización del titular o mandato legal. Esta garantía constitucional permite comprender que la protección se extiende a distintas operaciones realizadas sobre la información y no solamente a su divulgación. El dato personal queda así vinculado jurídicamente con la capacidad de decisión de su titular.

No todos los datos personales presentan el mismo nivel de riesgo cuando son utilizados indebidamente. La legislación ecuatoriana reconoce categorías que requieren una protección reforzada debido a la posibilidad de producir discriminación, afectaciones a la intimidad u otras consecuencias sobre derechos fundamentales. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 25, constituyen categorías especiales los datos sensibles, los datos de niñas, niños y adolescentes, los datos de salud y los datos de personas con discapacidad y de sus sustitutos relacionados con la discapacidad. Esta clasificación permite ajustar las garantías jurídicas a la naturaleza y potencial impacto de la información tratada.

Dentro de estas categorías, los datos sensibles reciben una consideración específica por las consecuencias que puede producir su utilización. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, incluye dentro de esta noción información relativa a etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos y datos genéticos, además de aquella cuyo tratamiento indebido pueda generar discriminación o afectar derechos y libertades fundamentales. La protección reforzada responde al efecto que la exposición, clasificación o utilización de estas características puede tener sobre la persona afectada.

Los datos relativos a la salud requieren particular atención porque pueden revelar condiciones físicas o mentales, diagnósticos, tratamientos, antecedentes clínicos y otra información producida durante la atención sanitaria. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, los define como datos relacionados con la salud física o mental de una persona, incluida la prestación de servicios sanitarios que revelen información sobre su estado. Su tratamiento mediante historias clínicas electrónicas incrementa las posibilidades de disponibilidad e intercambio, pero también exige controles capaces de prevenir accesos o usos incompatibles con su finalidad original (Martínez-Jara & Pérez-Ycaza, 2022).

El carácter especialmente protegido de determinados datos también modifica las condiciones jurídicas para su tratamiento. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 26, el tratamiento de datos sensibles se encuentra prohibido como regla general, salvo que concurra alguna de las circunstancias expresamente previstas, entre ellas el consentimiento explícito del titular para fines claramente determinados. La norma contempla además supuestos relacionados con obligaciones laborales, protección de intereses vitales, datos manifiestamente públicos, orden judicial, investigación y tratamiento de

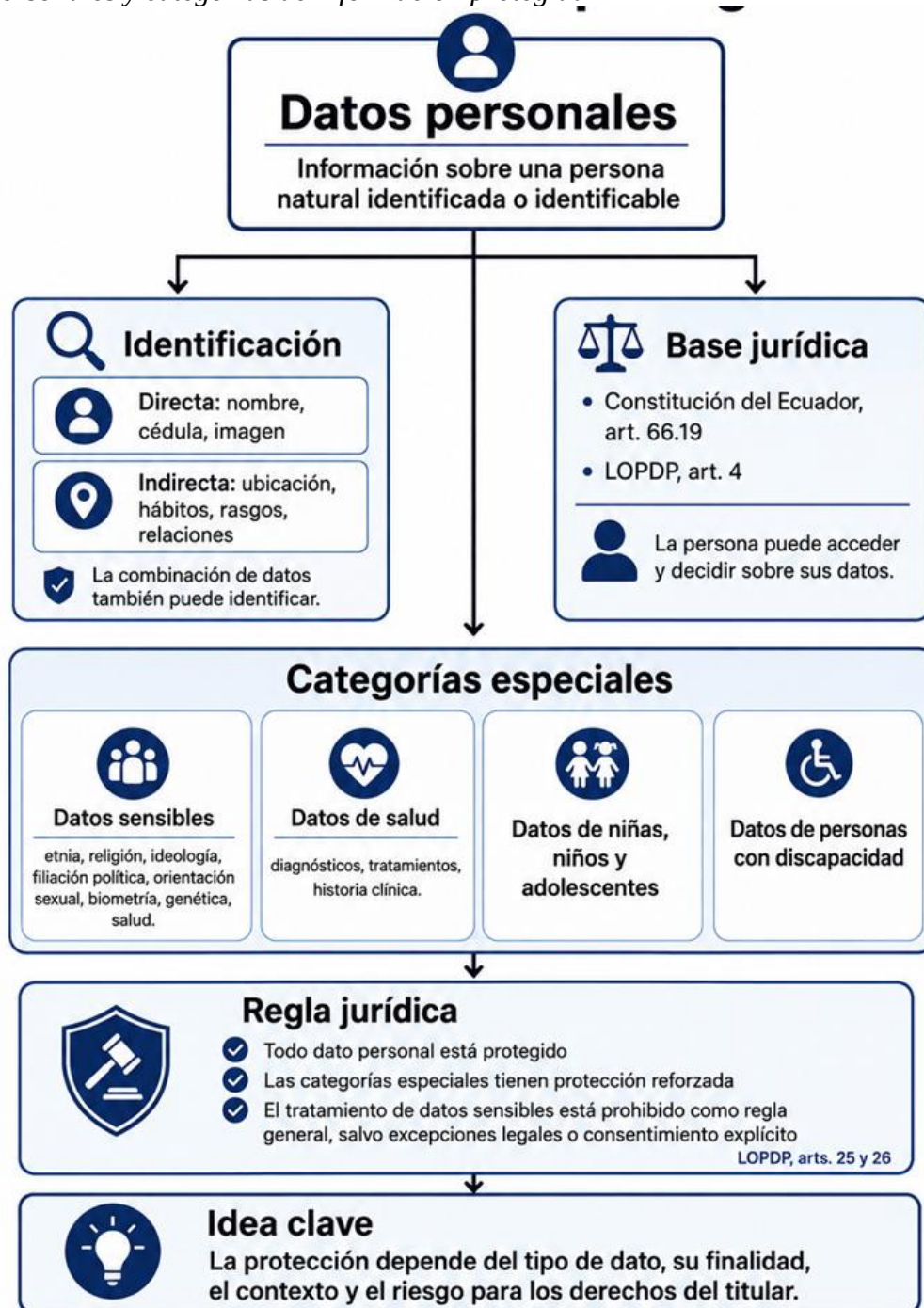
información sanitaria. Esta regulación evidencia que la sensibilidad del dato exige mayores condiciones de legitimidad que las aplicables al tratamiento ordinario de información personal.

La información correspondiente a niñas, niños y adolescentes forma igualmente parte de las categorías especiales reconocidas por la legislación ecuatoriana. Su inclusión en el artículo 25 de la Ley Orgánica de Protección de Datos Personales (2021) responde a la necesidad de considerar las condiciones particulares en las que las personas menores de edad ejercen sus derechos y participan en entornos digitales. Plataformas educativas, servicios electrónicos, redes sociales y aplicaciones pueden recopilar información sobre identidad, comportamiento, ubicación o preferencias. La protección de estos datos requiere considerar que las consecuencias de una exposición o utilización inadecuada pueden mantenerse durante períodos prolongados y afectar diferentes dimensiones de su desarrollo personal (Ordóñez Pineda et al., 2022).

La clasificación jurídica de los datos personales adquiere especial relevancia cuando intervienen instituciones públicas y privadas simultáneamente. La información puede originarse en una relación sanitaria, educativa, laboral o administrativa y posteriormente circular mediante plataformas tecnológicas operadas por otros sujetos. En esos escenarios, determinar qué información se encuentra protegida y cuál es su categoría permite establecer las condiciones aplicables a su tratamiento. El análisis desarrollado durante la expansión de servicios digitales asociados con la emergencia sanitaria evidenció problemas derivados del tratamiento de información personal y especialmente de datos de salud dentro de relaciones público-privadas (Ordelin Font, 2022). La naturaleza del dato condiciona, por ello, las garantías que deben acompañar su utilización.

La existencia de categorías especiales no significa que los demás datos personales carezcan de protección. La tutela jurídica se aplica a toda información que permita identificar o hacer identificable a una persona, mientras que determinadas categorías reciben garantías adicionales por el riesgo que presentan. Esta diferencia resulta importante para evitar una interpretación limitada según la cual solamente los datos sensibles requieren medidas de protección. Incluso información aparentemente ordinaria puede adquirir relevancia cuando se combina, conserva durante largos períodos o se utiliza para finalidades distintas de aquellas que justificaron inicialmente su recopilación. El marco ecuatoriano ha avanzado hacia una comprensión amplia de esta protección como parte de los derechos digitales de las personas (Moran Barreto, 2023).

Figura 1
Datos personales y categorías de información protegida



Nota. El esquema organiza las principales formas de identificación y las categorías que requieren distintos niveles de protección jurídica según la naturaleza y el riesgo asociado a los datos personales.

La clasificación de los datos cumple, en consecuencia, una función jurídica práctica: permite determinar el grado de protección requerido, las condiciones para el tratamiento y los riesgos que deben ser considerados antes de utilizar información personal. En Ecuador, la diferenciación entre datos personales generales y categorías especiales establece una estructura que responde tanto a la naturaleza de la información como a las consecuencias posibles de su

tratamiento. La protección no depende únicamente del contenido aislado de un dato, sino también del contexto, la finalidad y la capacidad de producir efectos sobre su titular. Esta perspectiva resulta necesaria para aplicar de manera efectiva las garantías constitucionales y legales de protección de datos personales.

1.3 Principios jurídicos de la protección de datos personales

Los principios jurídicos de protección de datos establecen los criterios que deben observarse durante la obtención, utilización, almacenamiento, comunicación y eliminación de información personal. Su función consiste en limitar el tratamiento y orientar la conducta de quienes deciden sobre los datos o realizan operaciones por cuenta de terceros. En Ecuador, estos principios desarrollan el derecho reconocido constitucionalmente y permiten evaluar si una determinada actividad resulta compatible con las garantías del titular. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, la recolección, archivo, procesamiento, distribución o difusión de datos personales requiere autorización del titular o mandato legal.

La regulación específica se encuentra en el artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021), que establece los principios de juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización, proporcionalidad, confidencialidad, calidad y exactitud, conservación, seguridad, responsabilidad proactiva y demostrada y aplicación favorable al titular. Estos principios no constituyen requisitos aislados, sino condiciones que deben observarse durante el tratamiento de información personal. Su aplicación permite valorar tanto la legitimidad inicial de la recopilación como las decisiones posteriores relativas al uso y conservación de los datos. La literatura ecuatoriana destaca su importancia para establecer límites concretos frente al tratamiento de información personal (Zambrano Rendón et al., 2023).

El principio de juridicidad exige que el tratamiento se realice conforme con la Constitución, los instrumentos internacionales, la legislación especializada, su reglamento y las demás normas aplicables. La lealtad, por su parte, impide recurrir a medios o finalidades ilícitas o desleales, mientras que la transparencia requiere que las personas comprendan de manera accesible cómo se utilizan sus datos. Estos criterios reducen la asimetría informativa existente entre el titular y las organizaciones que realizan el tratamiento. El artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021) incorpora expresamente estos principios y vincula la transparencia con comunicaciones comprensibles para el titular.

La finalidad, pertinencia, minimización y proporcionalidad delimitan qué datos pueden recopilarse y hasta dónde puede extenderse su utilización. Una organización no debería reunir información simplemente porque dispone de capacidad tecnológica para hacerlo; debe existir una finalidad determinada que justifique el tratamiento y una relación razonable entre esa finalidad y la cantidad de información utilizada. Estas exigencias adquieren especial relevancia en entornos digitales donde la acumulación de datos puede producirse de manera continua. La aplicación de principios jurídicos permite controlar prácticas que amplían posteriormente los usos originalmente previstos y protege a las personas frente a tratamientos excesivos o incompatibles con las condiciones iniciales (Ordóñez Pineda et al., 2022).

La calidad, exactitud y conservación introducen obligaciones vinculadas con el contenido de los datos y con el período durante el cual permanecen disponibles. Información incorrecta, desactualizada o conservada innecesariamente puede producir consecuencias perjudiciales cuando se utiliza para adoptar decisiones sobre una persona. Por ello, el artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021) exige que los datos sean exactos y estén actualizados cuando resulte necesario, además de limitar su conservación al tiempo indispensable para cumplir las finalidades del tratamiento. Estas reglas evidencian que la protección jurídica continúa durante toda la existencia de la información y no concluye después de obtenerla.

Tabla 1
Principios jurídicos aplicables al tratamiento de datos personales

Principio	Contenido esencial	Aplicación en el tratamiento
Juridicidad	Exige conformidad con el ordenamiento jurídico aplicable.	Impide tratamientos contrarios a las normas que protegen los datos personales.
Lealtad	Prohíbe medios y finalidades ilícitas o desleales.	Exige una actuación legítima frente al titular.
Transparencia	Requiere información accesible, comprensible y clara.	Permite conocer cómo y para qué se utilizan los datos.
Finalidad	Vincula el tratamiento con propósitos determinados.	Limita usos posteriores incompatibles con la finalidad establecida.
Pertinencia y minimización	Restringe el tratamiento a los datos necesarios.	Evita recopilar información excesiva respecto de la finalidad.
Proporcionalidad	Exige correspondencia entre tratamiento y finalidad.	Limita operaciones que resulten excesivas para el objetivo perseguido.
Confidencialidad	Impone reserva sobre la información personal.	Reduce accesos, comunicaciones y divulgaciones no autorizadas.

Principio	Contenido esencial	Aplicación en el tratamiento
Calidad y exactitud	Requiere información correcta y actualizada cuando sea necesario.	Disminuye decisiones sustentadas en datos erróneos o desactualizados.
Conservación	Limita el almacenamiento al período necesario.	Evita mantener indefinidamente información sin justificación.
Seguridad	Exige medidas adecuadas frente a riesgos y vulnerabilidades.	Protege los datos frente a pérdida, alteración, acceso o divulgación indebida.
Responsabilidad proactiva y demostrada	Obliga a adoptar y acreditar medidas de cumplimiento.	Traslada al responsable la necesidad de demostrar una gestión adecuada.
Aplicación favorable al titular	Prioriza la interpretación que favorezca los derechos del titular.	Orienta la resolución de dudas en materia de protección de datos.

Nota. La tabla organiza el alcance práctico de los principios previstos para orientar y limitar las distintas operaciones realizadas sobre datos personales.

La confidencialidad y la seguridad responden directamente a los riesgos derivados del acceso o utilización indebida de información. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, los responsables y encargados deben preservar la confidencialidad y aplicar medidas de seguridad adecuadas frente a riesgos, amenazas y vulnerabilidades. La seguridad no puede reducirse a la instalación de herramientas informáticas, porque también requiere procedimientos organizativos y controles sobre las personas autorizadas para acceder a la información. Esta necesidad resulta especialmente evidente respecto de datos sanitarios, cuya exposición puede afectar de forma directa la esfera privada del titular (Martínez-Jara & Pérez-Ycaza, 2022).

La responsabilidad proactiva y demostrada modifica la forma de entender el cumplimiento de las obligaciones de protección de datos. No resulta suficiente reaccionar después de una vulneración; quienes realizan el tratamiento deben adoptar medidas previamente y encontrarse en condiciones de acreditar que han actuado conforme con la normativa. Esta perspectiva relaciona los principios jurídicos con procedimientos internos de gestión, evaluación de riesgos y documentación de decisiones. En contextos donde participan instituciones públicas y empresas privadas, la definición de responsabilidades adquiere particular importancia porque pueden intervenir varios actores en diferentes etapas del tratamiento. Estas relaciones plantean dificultades adicionales para delimitar obligaciones y garantizar la protección efectiva de los titulares (Ordellin Font, 2022).

Los principios también funcionan como criterios para interpretar las reglas específicas sobre protección de datos. Una operación puede cumplir formalmente determinados requisitos y, sin embargo, generar problemas si utiliza cantidades excesivas de información, mantiene datos durante períodos injustificados o impide al titular comprender el tratamiento realizado. La legislación ecuatoriana incorpora, además, el principio de aplicación favorable al titular dentro del artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021). Este criterio refuerza la posición jurídica de la persona cuando existan dudas sobre el alcance de los derechos y obligaciones aplicables. La protección de datos se configura así mediante estándares que orientan decisiones concretas y no únicamente mediante prohibiciones generales.

La aplicación conjunta de estos principios permite examinar el tratamiento desde su diseño hasta la eliminación de los datos. Una práctica legítima requiere fundamento jurídico, finalidad determinada, información suficiente al titular, uso proporcional, calidad de los registros, conservación limitada, confidencialidad y seguridad. El incumplimiento de uno de estos componentes puede comprometer la protección incluso cuando los demás se hayan observado formalmente. En el contexto ecuatoriano, la incorporación de estos principios ha contribuido a precisar las obligaciones vinculadas con los derechos digitales y a establecer parámetros para controlar la utilización de información personal (Moran Barreto, 2023). Su importancia reside en condicionar jurídicamente cada decisión adoptada sobre los datos personales.

1.4 Privacidad, intimidad y autodeterminación informativa

La privacidad, la intimidad y la autodeterminación informativa son conceptos relacionados, pero no equivalentes. La privacidad comprende el ámbito de la vida personal que una persona puede mantener alejado de injerencias injustificadas; la intimidad se refiere con mayor precisión a aspectos especialmente reservados de la vida individual y familiar; y la autodeterminación informativa alude a la capacidad de decidir sobre el uso de los propios datos. En los entornos digitales, estas dimensiones convergen porque gran parte de la vida privada se expresa mediante información susceptible de recopilación, almacenamiento y análisis. Esta relación ha reforzado la necesidad de proteger jurídicamente el control individual sobre los datos personales (Zambrano Rendón et al., 2023).

La protección de la intimidad tiene reconocimiento expreso en el ordenamiento constitucional ecuatoriano. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 66, numeral 20, se reconoce y garantiza el derecho a la intimidad personal y familiar. Esta disposición protege un espacio reservado frente a intromisiones que puedan afectar aspectos

personales que no deben ser expuestos sin justificación. Su alcance se complementa con el numeral 19 del mismo artículo, que reconoce específicamente el derecho a la protección de datos de carácter personal. La coexistencia de ambas garantías permite distinguir la intimidad como esfera protegida y los datos personales como objeto de control jurídico específico.

La autodeterminación informativa amplía la protección tradicional de la intimidad porque no se limita a impedir que terceros conozcan información reservada. Su contenido supone que la persona pueda conocer qué datos se recopilan, decidir sobre determinados usos y ejercer derechos frente a quienes realizan el tratamiento. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, el derecho a la protección de datos comprende el acceso y la decisión sobre información de carácter personal. Esta facultad de decisión constituye uno de los fundamentos jurídicos de la autodeterminación informativa y conecta la autonomía individual con el control sobre la circulación de datos en sistemas públicos y privados.

La transformación digital ha modificado la forma en que estas garantías pueden resultar afectadas. Una persona puede mantener reservados determinados aspectos de su vida y, al mismo tiempo, quedar expuesta a inferencias elaboradas a partir de datos aparentemente dispersos. Información sobre ubicación, hábitos, relaciones, búsquedas o consumo puede combinarse para reconstruir características personales que el titular nunca comunicó de manera directa. Esta posibilidad muestra que la protección contemporánea no puede limitarse a impedir la divulgación de secretos. También debe considerar la capacidad tecnológica de generar conocimiento nuevo a partir de información previamente disponible, lo que introduce riesgos adicionales para la autonomía individual (Ojeda Bello & Cutié Mustelier, 2021).

La Ley Orgánica de Protección de Datos Personales desarrolla esta dimensión mediante un conjunto de derechos que permiten al titular intervenir en el tratamiento de su información. La Ley Orgánica de Protección de Datos Personales (2021), en sus artículos 12 al 22, regula derechos relacionados con información, acceso, rectificación, actualización, eliminación, oposición, portabilidad y decisiones basadas en tratamientos automatizados, entre otros. Estos mecanismos convierten la autodeterminación informativa en facultades jurídicas concretas y permiten que la persona no quede reducida a una posición pasiva frente al tratamiento. La protección de datos se vincula así con la posibilidad efectiva de conocer, cuestionar y modificar determinadas operaciones realizadas sobre información personal.

La intimidad adquiere una relevancia especial cuando el tratamiento involucra información relacionada con salud, sexualidad, identidad, características biométricas u otros aspectos sensibles. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, reconoce como datos sensibles diversas categorías cuya utilización indebida puede originar discriminación o afectar derechos y libertades fundamentales. Esta clasificación muestra que la afectación de la privacidad no depende únicamente de que una información sea secreta. También importa la capacidad que tenga un dato para revelar dimensiones profundas de la identidad o para producir consecuencias desfavorables cuando es utilizado fuera de su contexto legítimo (Martínez-Jara & Pérez-Ycaza, 2022).

La relación entre privacidad y autodeterminación informativa también se manifiesta en la necesidad de establecer límites a la recopilación de datos. El titular difícilmente puede ejercer control sobre su información si desconoce qué datos se obtienen, con qué finalidad se utilizan o durante cuánto tiempo se conservarán. Por ello, la transparencia y la finalidad constituyen condiciones necesarias para que la capacidad de decisión tenga contenido real. La experiencia ecuatoriana demuestra que la protección de datos requiere combinar reconocimiento constitucional, regulación especializada y actuación institucional, especialmente cuando existen tratamientos vinculados con servicios públicos, tecnologías digitales o situaciones extraordinarias que incrementan la recopilación de información (Ordóñez Pineda et al., 2022).

El ordenamiento ecuatoriano incorpora además una garantía jurisdiccional directamente relacionada con la autodeterminación informativa. De acuerdo con la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), en su artículo 49, la acción de hábeas data permite conocer la existencia de datos personales, acceder a ellos y obtener información sobre su uso, finalidad, origen, destino y tiempo de vigencia. La norma también contempla la posibilidad de solicitar actualización, rectificación, eliminación o anulación cuando corresponda. Esta garantía convierte el control sobre la información personal en una facultad exigible frente a quienes administran archivos o bases de datos y refuerza la tutela de la vida privada.

La privacidad también puede verse comprometida por relaciones entre instituciones públicas y actores privados que comparten, almacenan o procesan información. En estos escenarios, la persona puede perder claridad sobre quién controla sus datos y qué decisiones se adoptan respecto de ellos. El análisis de tratamientos realizados durante la pandemia mostró que la cooperación entre entidades públicas y privadas puede crear tensiones relacionadas con finalidades, acceso y circulación de información sensible (Ordellin Font, 2022). Desde la

perspectiva de la autodeterminación informativa, esta complejidad exige identificar responsabilidades y garantizar que la intervención de múltiples actores no reduzca la capacidad del titular para conocer y ejercer sus derechos.

La privacidad y la intimidad tampoco desaparecen cuando una persona utiliza servicios digitales voluntariamente. La participación en redes sociales, aplicaciones, plataformas educativas o servicios comerciales puede implicar la entrega de información, pero esa conducta no supone una autorización ilimitada para cualquier uso posterior. La protección jurídica exige considerar la finalidad del tratamiento, la información proporcionada al titular y los límites establecidos por la normativa. El desarrollo de los derechos digitales en Ecuador ha reforzado la idea de que la utilización de tecnologías debe mantenerse compatible con las garantías constitucionales y con el control de las personas sobre su información (Moran Barreto, 2023).

La relación entre privacidad, intimidad y autodeterminación informativa permite comprender por qué la protección de datos personales constituye una garantía autónoma y, al mismo tiempo, conectada con otros derechos. La intimidad protege ámbitos especialmente reservados; la privacidad establece límites frente a injerencias injustificadas; y la autodeterminación informativa proporciona facultades para intervenir sobre el tratamiento de información personal. En el entorno digital, estas dimensiones se complementan porque una afectación puede originarse tanto por la exposición directa de información como por su recopilación, combinación o utilización posterior. El derecho contemporáneo debe preservar, por ello, la capacidad efectiva de la persona para mantener control jurídico sobre los datos que la representan.

1.5 Sujetos que intervienen en la protección de datos personales

La protección de datos personales se articula mediante un conjunto de sujetos con funciones diferenciadas dentro del tratamiento. No todos intervienen con el mismo grado de decisión ni asumen las mismas obligaciones. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 5, identifica como integrantes del sistema al titular, responsable del tratamiento, encargado del tratamiento, destinatario, Autoridad de Protección de Datos Personales y delegado de protección de datos. Esta clasificación permite determinar quién ejerce derechos, quién decide sobre el tratamiento, quién actúa por cuenta de otro sujeto y quién supervisa el cumplimiento normativo.

El titular ocupa una posición central porque es la persona natural a quien corresponden los datos objeto de tratamiento. Su intervención no se limita a proporcionar información, ya que

conserva facultades jurídicas para conocer, controlar y cuestionar determinadas operaciones realizadas sobre sus datos. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, la persona tiene derecho al acceso y a la decisión sobre sus datos personales, además de su correspondiente protección. Esta posición jurídica exige que los demás sujetos respeten las condiciones de licitud, finalidad y transparencia aplicables al tratamiento y garanticen el ejercicio efectivo de los derechos reconocidos al titular.

El responsable del tratamiento constituye el sujeto que determina la finalidad y las condiciones esenciales bajo las cuales serán utilizados los datos personales. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, define al responsable como la persona natural o jurídica, pública o privada, autoridad pública u otro organismo que, individual o conjuntamente, decide sobre la finalidad y el tratamiento. Esta capacidad decisoria permite diferenciarlo del encargado y explica la relevancia de las obligaciones que recaen sobre él. La actuación de responsables públicos y privados puede presentar distintos niveles de complejidad, particularmente cuando una misma operación involucra varias instituciones o servicios tecnológicos (Ordellin Font, 2022).

El encargado del tratamiento actúa en una posición distinta porque realiza operaciones sobre datos por cuenta del responsable. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, lo define como la persona natural o jurídica, pública o privada, autoridad pública u organismo que trata datos personales a nombre y por cuenta de un responsable. Esta diferencia resulta importante en servicios de almacenamiento, procesamiento, soporte tecnológico o gestión externalizada de información. Aunque el encargado no determina autónomamente la finalidad principal, su intervención puede afectar directamente la seguridad y confidencialidad de los datos, razón por la cual también está sometido a obligaciones específicas dentro del sistema de protección.

El destinatario, el delegado de protección de datos y la autoridad de control completan la estructura institucional. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, define al destinatario como la persona natural o jurídica a quien se comunican datos personales. En ese mismo artículo, el delegado de protección de datos aparece como la persona encargada de informar y asesorar sobre obligaciones legales, supervisar el cumplimiento y cooperar con la autoridad competente. La Autoridad de Protección de Datos Personales, por su parte, ejerce una función pública independiente de supervisión y tutela. Esta diversidad de actores exige una delimitación clara de competencias y responsabilidades (Ordóñez Pineda et al., 2022).

Tabla 2*Sujetos que participan en el sistema de protección de datos personales*

Sujeto	Función principal	Relación con el tratamiento
Titular	Ejerce derechos sobre sus datos personales.	Es la persona natural a quien corresponde la información tratada.
Responsable del tratamiento	Decide la finalidad y las condiciones esenciales del tratamiento.	Determina para qué y cómo se utilizan los datos.
Encargado del tratamiento	Ejecuta operaciones por cuenta del responsable.	Trata datos siguiendo las condiciones establecidas por el responsable.
Destinatario	Recibe datos personales mediante una comunicación o transferencia.	Accede a información que le ha sido comunicada legítimamente.
Delegado de protección de datos	Informa, asesora y supervisa el cumplimiento normativo.	Actúa como punto de contacto y apoyo especializado dentro de la organización.
Autoridad de Protección de Datos Personales	Supervisa la aplicación de la normativa y tutela los derechos.	Ejerce funciones de control dentro del sistema de protección de datos.

Nota. La tabla diferencia a los sujetos según su capacidad de decisión, ejecución, recepción, supervisión o ejercicio de derechos dentro del tratamiento de datos personales.

La distinción entre responsable y encargado resulta especialmente relevante porque evita atribuir obligaciones de manera indistinta a todos los participantes. Quien determina la finalidad del tratamiento conserva una posición decisoria que no desaparece por contratar a un tercero para ejecutar operaciones técnicas. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, responsables y encargados deben aplicar medidas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas para garantizar y demostrar el cumplimiento normativo. La norma también exige implementar políticas de protección de datos acordes con las características del tratamiento, lo que vincula las responsabilidades de ambos sujetos con una gestión preventiva y documentada.

La participación de destinatarios y terceros introduce una dimensión adicional, porque la información puede salir del ámbito operativo inicial y quedar disponible para otros actores. En estos casos, la determinación de responsabilidades depende de la forma en que se realiza la comunicación, de las finalidades aplicables y de la posición jurídica de quien recibe los datos. Los entornos públicos y privados pueden generar cadenas complejas de tratamiento, especialmente cuando intervienen proveedores tecnológicos, instituciones sanitarias o plataformas externas. La protección efectiva exige conocer qué sujeto controla cada operación

y con qué fundamento accede a la información, pues la multiplicidad de participantes puede incrementar los riesgos de uso indebido (Martínez-Jara & Pérez-Ycaza, 2022).

Figura 2

Sujetos que intervienen en la protección de datos personales



Nota. El esquema representa las funciones diferenciadas de los principales sujetos que participan en el tratamiento, desde el ejercicio de derechos y la toma de decisiones hasta la ejecución, recepción y supervisión de las operaciones con datos personales.

El delegado de protección de datos cumple una función interna de asesoramiento y supervisión que contribuye a vincular la gestión cotidiana con las obligaciones jurídicas. Su tarea no sustituye al responsable ni al encargado, sino que facilita el cumplimiento, identifica posibles deficiencias y mantiene comunicación con la autoridad competente. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, el delegado debe informar sobre las obligaciones aplicables, velar o supervisar su cumplimiento y cooperar con la Autoridad de Protección de Datos Personales. Esta función adquiere importancia en organizaciones que realizan tratamientos complejos, continuos o vinculados con categorías especiales de información.

La identificación precisa de los sujetos permite asignar derechos y obligaciones según la intervención real de cada participante. En tratamientos simples, esta delimitación puede resultar relativamente directa; sin embargo, los servicios digitales, la externalización y la cooperación entre instituciones pueden crear relaciones donde varios actores intervienen simultáneamente. La protección jurídica exige analizar quién decide, quién ejecuta, quién recibe y quién

supervisa cada operación. Esta delimitación evita que la distribución contractual de tareas termine debilitando la posición del titular. La literatura sobre protección de datos en Ecuador advierte precisamente que la efectividad del derecho depende de instituciones y mecanismos capaces de controlar actuaciones públicas y privadas relacionadas con información personal (Moran Barreto, 2023).

1.6 Riesgos jurídicos derivados del uso indebido de datos personales

El uso indebido de datos personales puede producir afectaciones jurídicas incluso cuando la información haya sido obtenida inicialmente de manera legítima. El riesgo aparece cuando los datos se utilizan para finalidades distintas de las informadas, se conservan sin necesidad, se comunican a terceros sin fundamento o quedan expuestos por medidas de seguridad insuficientes. En Ecuador, la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige que el tratamiento respete principios de finalidad, minimización, confidencialidad, seguridad y responsabilidad proactiva. La vulneración de estos principios puede comprometer derechos del titular y generar responsabilidades para quienes intervienen en el tratamiento (Zambrano Rendón et al., 2023).

Uno de los riesgos más evidentes corresponde al acceso no autorizado a información personal. La exposición puede producirse mediante filtraciones, uso indebido de credenciales, fallos de seguridad o actuaciones deliberadas de personas con acceso a sistemas y bases de datos. El riesgo aumenta cuando la información afectada corresponde a datos sensibles o permite reconstruir aspectos relevantes de la vida privada. De acuerdo con el COIP (2014), en su artículo 178, acceder, interceptar, examinar, retener, grabar, reproducir, difundir o publicar determinados datos personales sin consentimiento o autorización legal puede constituir violación a la intimidad. La norma incorpora así consecuencias penales frente a determinadas formas de intromisión ilegítima.

La divulgación ilícita constituye otro riesgo porque puede ampliar de manera irreversible el número de personas que acceden a la información. Una base de datos puede contener antecedentes personales, financieros, laborales, sanitarios o identificativos cuya revelación afecte la privacidad y facilite otros usos perjudiciales. El COIP (2014), en su artículo 229, tipifica la revelación ilegal de información registrada en ficheros, archivos, bases de datos o medios semejantes cuando la conducta vulnera voluntariamente el secreto, la intimidad y la privacidad. Esta respuesta penal muestra que la protección de datos trasciende el ámbito

administrativo cuando determinadas conductas lesionan bienes jurídicos especialmente protegidos.

Los datos relacionados con la salud evidencian con particular claridad las consecuencias del uso indebido. Una historia clínica puede contener diagnósticos, tratamientos, antecedentes y otra información cuyo acceso fuera del contexto asistencial afecta directamente la intimidad. La digitalización facilita la disponibilidad de estos registros, pero también incrementa los puntos desde los cuales pueden producirse accesos no autorizados, transferencias indebidas o exposiciones accidentales. El tratamiento de historias clínicas electrónicas exige, por ello, controles jurídicos y técnicos adecuados a la sensibilidad de la información y a las consecuencias que una vulneración podría producir sobre el titular (Martínez-Jara & Pérez-Ycaza, 2022).

El riesgo jurídico también surge cuando las organizaciones no identifican adecuadamente las responsabilidades de quienes intervienen en el tratamiento. La existencia de proveedores tecnológicos, operadores externos, instituciones públicas y entidades privadas puede dificultar la determinación de quién debía adoptar medidas preventivas o controlar determinados accesos. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, obliga a responsables y encargados a aplicar herramientas administrativas, técnicas, físicas, organizativas y jurídicas, así como procesos de evaluación y gestión de riesgos. La norma exige además adoptar medidas destinadas a prevenir, reducir, mitigar y controlar vulneraciones identificadas, lo que configura una obligación preventiva y no únicamente reactiva (Ordelin Font, 2022).

Tabla 3

Riesgos jurídicos asociados al uso indebido de datos personales

Riesgo	Manifestación	Posible afectación jurídica
Acceso no autorizado	Consulta o utilización de información sin habilitación legítima.	Vulneración de privacidad, intimidad y confidencialidad.
Divulgación indebida	Comunicación o publicación de datos sin fundamento jurídico.	Exposición del titular y posible responsabilidad administrativa, civil o penal.
Uso incompatible	Utilización para finalidades distintas de las justificadas inicialmente.	Incumplimiento de los principios de finalidad y lealtad.
Conservación excesiva	Mantenimiento de información durante períodos innecesarios.	Incremento injustificado de la exposición y del riesgo de vulneración.

Riesgo	Manifestación	Posible afectación jurídica
Tratamiento de datos sensibles	Uso inadecuado de información sobre salud, identidad u otras categorías especiales.	Discriminación, afectación de derechos y mayor gravedad del daño.
Transferencia indebida	Entrega o acceso de terceros sin base jurídica suficiente.	Pérdida de control sobre la información y ampliación de responsabilidades.
Fallas de seguridad	Pérdida, alteración, destrucción o exposición de datos.	Vulneración de obligaciones de seguridad y deberes de protección.
Perfilado indebido	Elaboración de inferencias o clasificaciones sin condiciones legítimas.	Afectación de autonomía, privacidad y ejercicio de otros derechos.

Nota. La tabla sintetiza conductas y situaciones que pueden convertir el tratamiento de información personal en una fuente de afectación jurídica para el titular.

Los riesgos no se limitan a la pérdida material de información. El uso combinado de diferentes bases de datos puede revelar características que originalmente no estaban disponibles de forma explícita. Cuando se cruzan registros sobre salud, ubicación, consumo, relaciones o actividades digitales, pueden construirse perfiles capaces de influir en decisiones relacionadas con acceso a servicios, oportunidades o condiciones contractuales. Esta forma de tratamiento incrementa la posibilidad de discriminación y pérdida de autonomía informativa. La protección jurídica debe considerar, por tanto, no solo el dato aislado, sino también las consecuencias derivadas de su agregación, interpretación y reutilización en contextos distintos de aquellos en que fue obtenido (Ojeda Bello & Cutié Mustelier, 2021).

Las relaciones entre instituciones públicas y privadas pueden ampliar estos riesgos cuando la información circula entre múltiples participantes. Una persona puede entregar datos a una entidad para una finalidad concreta y desconocer posteriormente qué proveedores intervienen, dónde se almacenan los registros o qué usos secundarios se realizan. Las experiencias relacionadas con tratamientos de información durante situaciones de emergencia muestran que la expansión de mecanismos tecnológicos puede generar tensiones entre objetivos institucionales y garantías individuales, especialmente cuando se procesan datos sensibles (Ordóñez Pineda et al., 2022). La existencia de una finalidad legítima no elimina la obligación de controlar accesos, limitar usos y mantener condiciones adecuadas de protección durante todo el tratamiento.

La normativa ecuatoriana exige que la gestión de riesgos sea permanente. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, dispone que responsables y encargados deben aplicar metodologías de análisis y gestión de riesgos y adoptar medidas

destinadas a prevenir, impedir, reducir, mitigar y controlar amenazas y vulneraciones. Esta obligación resulta coherente con el principio de seguridad previsto en el artículo 10 de la misma ley, según el cual las medidas deben atender a la naturaleza de los datos, al contexto y a los riesgos existentes. El cumplimiento exige, por ello, revisar periódicamente las condiciones del tratamiento y no limitar la seguridad a una evaluación inicial.

El uso indebido de datos personales puede afectar simultáneamente privacidad, intimidad, reputación, igualdad y capacidad de decisión. Su gravedad depende de la naturaleza de la información, la amplitud de la exposición, los sujetos que acceden a ella y las consecuencias posteriores para el titular. El desarrollo de una legislación especializada en Ecuador responde precisamente a la necesidad de establecer límites frente a prácticas digitales capaces de producir afectaciones que no siempre encajan en formas tradicionales de intromisión en la vida privada (Moran Barreto, 2023). La prevención jurídica exige combinar principios, responsabilidades, medidas de seguridad y mecanismos de tutela capaces de responder tanto a conductas deliberadas como a fallas organizativas.

1.7 Protección de datos personales como garantía de los derechos individuales

La protección de datos personales constituye una garantía vinculada con el ejercicio de otros derechos individuales porque la información permite identificar, describir y, en determinados contextos, evaluar a una persona. Cuando los datos son tratados sin límites adecuados, pueden afectarse la privacidad, la intimidad, la igualdad, la reputación o la autonomía. Por esta razón, el derecho no se limita a impedir accesos indebidos, sino que establece condiciones para recopilar, utilizar, conservar y comunicar información personal. En el ámbito ecuatoriano, esta relación entre datos y derechos individuales se ha fortalecido mediante normas específicas que reconocen facultades de control a los titulares (Zambrano Rendón et al., 2023).

La Constitución ecuatoriana establece el fundamento principal de esta garantía. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, se reconoce el derecho a la protección de datos de carácter personal, que comprende el acceso y la decisión sobre información y datos de esta naturaleza, así como su correspondiente protección. La misma disposición condiciona la recolección, archivo, procesamiento, distribución o difusión a la autorización del titular o al mandato de la ley. Esta formulación vincula directamente la protección de datos con la capacidad individual de decidir sobre información que permite representar, identificar o caracterizar a una persona dentro de diferentes relaciones sociales.

La garantía de los datos personales se conecta también con el derecho a la intimidad. La Constitución de la República del Ecuador (2008), en su artículo 66, numeral 20, reconoce expresamente el derecho a la intimidad personal y familiar. La relación entre ambas disposiciones permite comprender que la tutela de datos no constituye un mecanismo exclusivamente técnico, porque protege aspectos de la vida individual susceptibles de quedar expuestos mediante registros, bases de datos o sistemas digitales. La protección jurídica resulta especialmente importante cuando los datos revelan características personales cuya divulgación o utilización puede modificar la forma en que la persona es observada, clasificada o tratada por instituciones públicas y privadas (Ojeda Bello & Cutié Mustelier, 2021).

Esta protección también cuenta con fundamento internacional. La Declaración Universal de Derechos Humanos (1948), en su artículo 12, establece que ninguna persona debe sufrir injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia y reconoce su derecho a la protección de la ley frente a tales actuaciones. El Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 17, incorpora una garantía semejante frente a injerencias arbitrarias o ilegales. Aunque estos instrumentos fueron formulados antes de la actual expansión digital, sus disposiciones proporcionan una base jurídica para proteger a las personas frente a formas contemporáneas de intervención sobre información relacionada con su vida privada.

En el ámbito interamericano, la protección de la privacidad se vincula igualmente con la dignidad individual. La Convención Americana sobre Derechos Humanos (1969), en su artículo 11, reconoce el derecho al respeto de la honra y dignidad y prohíbe las injerencias arbitrarias o abusivas en la vida privada, la familia, el domicilio y la correspondencia. En los entornos digitales, una afectación de estas garantías puede originarse mediante recopilaciones desproporcionadas, divulgaciones no autorizadas o reutilizaciones de información para finalidades distintas. La protección de datos funciona entonces como una garantía instrumental que permite trasladar principios generales de privacidad a situaciones concretas de tratamiento, almacenamiento y circulación de información personal.

La legislación especializada ecuatoriana desarrolla esta función protectora. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 1, la norma tiene como objeto garantizar el ejercicio del derecho a la protección de datos personales mediante la regulación de principios, derechos, obligaciones y mecanismos de tutela. Esta disposición muestra que la garantía no depende únicamente de prohibiciones, sino también de una estructura que distribuye responsabilidades y reconoce facultades al titular. Los mecanismos

de protección resultan especialmente relevantes en contextos donde instituciones y plataformas disponen de capacidades tecnológicas superiores a las del individuo para recopilar, relacionar y analizar información (Ordóñez Pineda et al., 2022).

Los derechos reconocidos al titular permiten convertir la protección de datos en una garantía ejercitable. La Ley Orgánica de Protección de Datos Personales (2021), en sus artículos 12 al 22, regula facultades relacionadas con información, acceso, rectificación, actualización, eliminación, oposición, portabilidad y decisiones basadas en tratamientos automatizados. Estas herramientas permiten que la persona intervenga cuando sus datos son utilizados de manera incorrecta, desactualizada o incompatible con sus derechos. Su importancia radica en que proporcionan respuestas diferenciadas según el tipo de afectación. De este modo, la tutela no se reduce a reclamar después de una vulneración, sino que permite actuar durante distintas etapas del tratamiento de información personal.

La garantía adquiere mayor intensidad cuando se utilizan categorías especiales de datos. Información relacionada con salud, identidad, orientación sexual, datos biométricos o antecedentes personales puede generar consecuencias especialmente graves si se utiliza fuera de los límites establecidos. La Ley Orgánica de Protección de Datos Personales (2021), en sus artículos 25 y 26, establece una protección particular para determinadas categorías y restringe el tratamiento de datos sensibles salvo en los supuestos jurídicamente permitidos. Esta diferenciación responde a la capacidad de ciertos datos para afectar simultáneamente intimidad, igualdad y dignidad. El tratamiento de historias clínicas electrónicas muestra con claridad la necesidad de preservar estas garantías durante todo el ciclo de utilización de la información (Martínez-Jara & Pérez-Ycaza, 2022).

La tutela de los derechos individuales requiere también mecanismos jurisdiccionales. De acuerdo con la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), en su artículo 49, la acción de hábeas data permite acceder a documentos y archivos de datos personales, conocer su uso, finalidad, origen, destino y tiempo de vigencia, y solicitar su actualización, rectificación, eliminación o anulación cuando proceda. Esta garantía ofrece una vía para reaccionar frente a tratamientos que afectan derechos y permite someter el manejo de información personal a control jurídico. Su existencia confirma que la protección de datos implica facultades exigibles y no únicamente expectativas de comportamiento dirigidas a quienes administran bases de información.

La protección de datos individuales adquiere especial importancia cuando intervienen múltiples actores en un mismo tratamiento. Instituciones públicas, empresas, proveedores tecnológicos y plataformas pueden acceder sucesivamente a la información, lo que dificulta identificar quién controla cada operación. Estas relaciones incrementan el riesgo de pérdida de trazabilidad y de utilización para finalidades diferentes de las inicialmente previstas. El análisis de experiencias vinculadas con tratamientos de información en situaciones de emergencia evidencia que la intervención conjunta de actores públicos y privados puede generar tensiones respecto de privacidad, finalidad y control de datos sensibles (Ordelin Font, 2022). La garantía efectiva exige, por ello, responsabilidades claras y mecanismos que permitan al titular identificar a los sujetos involucrados.

La protección de datos personales cumple finalmente una función preventiva frente a decisiones y prácticas que pueden condicionar el ejercicio de otros derechos. Información incorrecta, incompleta o utilizada fuera de contexto puede influir en procedimientos administrativos, servicios, relaciones laborales, acceso a prestaciones o evaluaciones automatizadas. Por ello, preservar la calidad, finalidad, seguridad y confidencialidad de los datos contribuye a evitar afectaciones que trascienden la esfera estrictamente informativa. En Ecuador, la consolidación de este derecho refleja una transición hacia mecanismos más específicos de tutela frente a los riesgos asociados con la digitalización y el tratamiento sistemático de información personal (Moran Barreto, 2023).



Capítulo 2

Tratamiento de datos personales en entornos digitales

Jhonatan Alberto Cifuentes Carreño

2.1 Concepto y etapas del tratamiento de datos personales

El tratamiento de datos personales comprende cualquier operación realizada sobre información vinculada con una persona natural identificada o identificable. No se limita a la recopilación inicial, sino que abarca acciones posteriores como organización, almacenamiento, consulta, modificación, transferencia, conservación y eliminación. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, define el tratamiento como cualquier operación o conjunto de operaciones realizadas sobre datos personales, mediante procedimientos automatizados o no automatizados. Esta amplitud resulta esencial en los entornos digitales, donde una misma información puede atravesar varias fases y ser utilizada por diferentes sistemas o actores durante su ciclo de vida.

El tratamiento comienza normalmente con la obtención o recolección de datos. Esta etapa puede producirse de manera directa, cuando el titular proporciona información a una institución o plataforma, o indirecta, cuando los datos se generan mediante navegación, uso de dispositivos, registros automáticos o interacción con servicios digitales. La legalidad de esta fase depende de que exista una base que justifique la obtención y de que la persona conozca, cuando corresponda, las condiciones esenciales del tratamiento. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige observar principios de juridicidad, transparencia, finalidad, minimización y proporcionalidad desde el inicio de cualquier operación sobre datos.

Después de la recopilación, los datos suelen pasar por procesos de organización y clasificación que permiten incorporarlos a bases estructuradas. Esta etapa puede incluir depuración, asociación, etiquetado, segmentación o integración con otros registros. En entornos digitales, estas operaciones facilitan el análisis posterior, pero también incrementan la capacidad de obtener información adicional a partir de datos aparentemente dispersos. La analítica contemporánea permite identificar patrones, inferir características o anticipar comportamientos a partir de grandes volúmenes de información, lo que modifica el alcance tradicional del tratamiento. Por esta razón, la protección debe considerar no solo los datos originales, sino también las inferencias que pueden generarse posteriormente (Mühlhoff, 2021).

El almacenamiento constituye otra etapa fundamental porque determina durante cuánto tiempo y bajo qué condiciones permanece disponible la información. Los datos pueden conservarse en servidores institucionales, servicios en la nube, dispositivos locales o infraestructuras operadas por terceros. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10,

establece el principio de conservación, según el cual los datos no deben mantenerse durante un período superior al necesario para cumplir las finalidades que justificaron su tratamiento. Este límite evita que la acumulación indefinida de información amplíe de manera injustificada los riesgos de acceso, filtración, reutilización o combinación con otros conjuntos de datos.

La conservación prolongada de información plantea riesgos específicos cuando se realiza a gran escala. La retención masiva puede permitir reconstruir hábitos, desplazamientos, comunicaciones o relaciones durante períodos extensos y convertir registros inicialmente fragmentarios en perfiles detallados. El análisis jurídico de sistemas de retención de datos ha mostrado que la duración, amplitud y generalización del almacenamiento pueden generar tensiones importantes con la privacidad y con los límites que deben regir la vigilancia de personas y grupos (Mitsilegas et al., 2023). Por ello, la etapa de conservación debe vincularse con criterios de necesidad, proporcionalidad y finalidad, evitando que el almacenamiento se convierta en una práctica automática sin revisión periódica.

Otra etapa corresponde al uso o consulta de los datos para ejecutar la finalidad declarada. En esta fase, la información puede utilizarse para prestar un servicio, verificar identidad, gestionar una relación contractual, realizar análisis o adoptar decisiones. El riesgo jurídico aparece cuando el uso se amplía hacia propósitos incompatibles con aquellos que justificaron inicialmente la recopilación. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, incorpora el principio de finalidad y exige que los datos se recojan para propósitos determinados, explícitos y legítimos. Esta exigencia limita la reutilización indiscriminada y obliga a vincular cada operación con una justificación concreta.

El tratamiento puede incluir también comunicación, transferencia o acceso por parte de terceros. En los ecosistemas digitales, un mismo dato puede circular entre proveedores de servicios, plataformas, empresas vinculadas y operadores tecnológicos sin que el titular perciba con claridad cada movimiento. Estas operaciones modifican el control efectivo sobre la información y exigen definir qué sujeto recibe los datos, con qué finalidad y bajo qué condiciones. Los modelos de intercambio seguro muestran que la transferencia no debe entenderse únicamente como movimiento físico de información, sino también como acceso compartido, procesamiento conjunto o utilización coordinada entre diferentes participantes (Agahari et al., 2022).

La modificación y actualización forman parte del ciclo de tratamiento porque la información puede cambiar con el tiempo. Datos desactualizados o incorrectos pueden generar decisiones

erróneas, afectar servicios o producir clasificaciones inadecuadas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, establece el principio de calidad y exactitud, que obliga a mantener información correcta y actualizada cuando resulte necesario para la finalidad perseguida. Esta etapa muestra que el tratamiento no es un proceso estático. Las organizaciones deben revisar periódicamente los registros, corregir inconsistencias y garantizar que la información utilizada conserve relación con la realidad de la persona a la que se refiere.

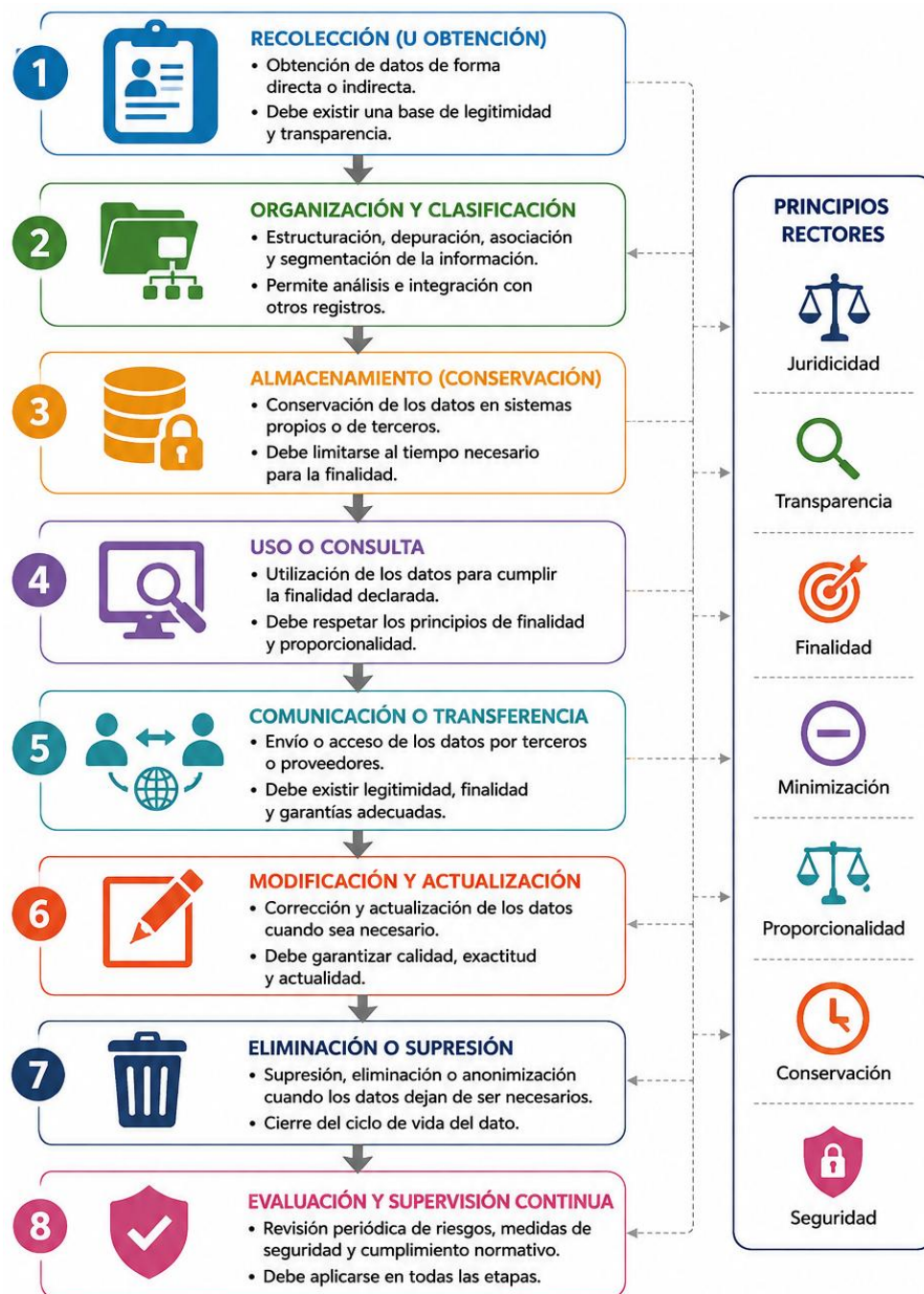
La etapa final del tratamiento debería incluir la supresión, eliminación o anonimización cuando los datos dejan de ser necesarios. El cierre del ciclo es tan importante como la recolección inicial, porque conservar información sin finalidad legítima prolonga innecesariamente los riesgos. En la práctica digital, la eliminación puede resultar compleja cuando existen copias de respaldo, sistemas distribuidos, servicios externos o bases replicadas. Por ello, la gestión del ciclo de vida requiere procedimientos capaces de identificar dónde se encuentran los datos y cómo deben retirarse. La aplicación de principios de minimización y conservación permite evitar que la información permanezca disponible de manera indefinida sin una razón jurídica suficiente.

Las distintas etapas del tratamiento pueden ejecutarse de forma automatizada mediante sistemas que recopilan, clasifican, almacenan y analizan información sin intervención humana constante. Esta automatización permite procesar grandes cantidades de datos con rapidez, pero también dificulta identificar cómo se producen determinadas inferencias o decisiones. Los estudios sobre ataques de privacidad en aprendizaje automático muestran que incluso los modelos ya entrenados pueden revelar información sensible sobre los datos utilizados durante su desarrollo, lo que amplía los riesgos más allá de las bases de datos tradicionales (Rigaki & Garcia, 2023). El tratamiento automatizado exige, por ello, controles que acompañen todo el ciclo tecnológico y no únicamente la fase de recopilación.

La comprensión del tratamiento como un proceso compuesto por etapas permite asignar obligaciones específicas en cada momento y evaluar los riesgos antes de que se materialicen. Recolección, organización, almacenamiento, uso, comunicación, actualización y eliminación forman parte de una misma secuencia jurídica y técnica. En entornos digitales, estas fases pueden superponerse y ejecutarse simultáneamente mediante aplicaciones, plataformas y sistemas automatizados. Los modelos de evaluación de privacidad aplicados a servicios digitales muestran que el cumplimiento depende de observar de manera integrada qué datos se

recopilan, cómo se utilizan y qué riesgos genera su procesamiento durante todo el ciclo (Kim et al., 2023).

Figura 3
Ciclo del tratamiento de datos personales



Nota. El esquema organiza las principales etapas que atraviesa la información personal y muestra los principios jurídicos que deben mantenerse durante todo el ciclo de tratamiento para reducir riesgos y preservar los derechos del titular.

2.2 Recolección de datos mediante plataformas y servicios digitales

La recolección de datos mediante plataformas y servicios digitales constituye una de las primeras operaciones del tratamiento y puede producirse de forma directa o indirecta. El usuario proporciona datos directamente cuando completa formularios, crea cuentas, realiza compras o solicita servicios; de manera indirecta, las plataformas pueden registrar identificadores, ubicación, actividad de navegación o características técnicas del dispositivo. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige que la persona pueda conocer que sus datos están siendo recogidos y tratados, conforme con los principios de lealtad y transparencia. Estas exigencias resultan especialmente relevantes cuando la recopilación ocurre de manera automatizada.

La recopilación digital no debe interpretarse como una autorización general para utilizar cualquier información disponible. El principio de finalidad previsto en el artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021) exige que los propósitos del tratamiento sean determinados, explícitos, legítimos y comunicados al titular. La misma disposición establece que los datos no deben utilizarse posteriormente para fines distintos de aquellos para los que fueron recopilados, salvo que exista una base jurídica que habilite un nuevo tratamiento. Este límite es particularmente importante en plataformas que combinan información procedente de múltiples interacciones para personalizar servicios, elaborar perfiles o desarrollar actividades comerciales posteriores.

La cantidad de información obtenida también debe guardar relación con la finalidad declarada. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, los principios de pertinencia y minimización exigen limitar la recopilación a los datos estrictamente necesarios, mientras que la proporcionalidad impide tratamientos excesivos respecto del propósito perseguido. Estas reglas son relevantes frente a aplicaciones que solicitan permisos o información que exceden lo indispensable para prestar su servicio. Los análisis de privacidad aplicados a aplicaciones móviles muestran precisamente que la evaluación de riesgos debe considerar qué datos se recopilan, qué permisos se solicitan y cómo se relacionan esas prácticas con las funciones ofrecidas al usuario (Kim et al., 2023).

La información proporcionada al titular condiciona además la legitimidad de la recolección. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, la persona debe recibir información sobre los fines del tratamiento, su base jurídica, los tipos de operaciones realizadas, el tiempo de conservación, la existencia de bases de datos y el origen de la información cuando esta no haya sido obtenida directamente. Esta obligación busca que el usuario comprenda qué ocurrirá con sus datos antes de adoptar una decisión sobre su entrega.

La falta de información suficiente puede impedir que el titular evalúe adecuadamente las consecuencias del tratamiento digital.

Las plataformas sociales presentan dificultades adicionales porque la información disponible puede exceder aquello que el usuario pretendía comunicar. Fotografías, publicaciones, comentarios o interacciones pueden revelar indirectamente ubicación, relaciones, hábitos u otras características personales. La exposición de estos datos incidentales demuestra que la recopilación digital no depende exclusivamente de formularios o registros explícitos. También puede derivarse de la observación y análisis de contenido generado por los propios usuarios, incluso cuando estos no anticiparon determinados usos posteriores. En consecuencia, la accesibilidad técnica de la información no elimina la necesidad de valorar su contexto, finalidad y posible afectación a la privacidad (Kutschera, 2023).

Tabla 4

Formas de recolección de datos en plataformas y servicios digitales

Forma de recolección	Ejemplos habituales	Riesgo principal para la privacidad
Proporcionada directamente	Formularios, registros, compras, solicitudes de servicio.	Recopilación excesiva respecto de la finalidad.
Generada por la actividad	Historial de navegación, búsquedas, clics e interacciones.	Seguimiento continuo del comportamiento.
Datos técnicos	Dirección IP, identificadores, dispositivo, sistema operativo.	Identificación o rastreo del usuario.
Datos de ubicación	GPS, redes inalámbricas o registros de conexión.	Reconstrucción de desplazamientos y rutinas.
Permisos de aplicaciones	Cámara, micrófono, contactos, almacenamiento.	Acceso a información no necesaria para el servicio.
Información en redes sociales	Publicaciones, fotografías, reacciones y relaciones.	Obtención de datos incidentales o inferidos.
Datos inferidos	Preferencias, intereses, características o segmentos.	Creación de perfiles que el titular no proporcionó directamente.

Nota. La tabla distingue las principales vías mediante las cuales los servicios digitales obtienen información y los riesgos que pueden surgir cuando la recopilación supera lo necesario o resulta poco transparente.

La recolección automatizada permite acumular información de forma continua y con una intensidad difícil de percibir por el usuario. Registros aparentemente triviales pueden adquirir un significado diferente cuando se combinan durante períodos prolongados. La información conductual puede utilizarse para inferir características personales, intereses o probabilidades que nunca fueron declaradas explícitamente. Este fenómeno amplía el concepto de riesgo porque el problema ya no consiste únicamente en qué datos entrega la persona, sino en qué información puede deducirse a partir de ellos. El análisis de la privacidad predictiva muestra

que los sistemas analíticos pueden generar conocimiento personal nuevo mediante correlaciones y modelos construidos sobre grandes conjuntos de datos (Mühlhoff, 2021).

La recolección mediante servicios digitales requiere además distinguir entre datos necesarios para ejecutar una función y datos obtenidos para finalidades adicionales. Una aplicación puede necesitar determinados identificadores para prestar el servicio principal, pero utilizar simultáneamente otra información para publicidad, análisis conductual o personalización. Desde la perspectiva jurídica, estas finalidades deben evaluarse por separado cuando no exista una conexión suficiente entre ellas. El artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021) exige que la finalidad sea determinada y que la recopilación se limite a lo necesario, por lo que la conveniencia empresarial de disponer de más información no constituye por sí sola una justificación jurídica suficiente.

La transparencia debe mantenerse incluso cuando la información no procede directamente del titular. El artículo 12 de la Ley Orgánica de Protección de Datos Personales (2021) contempla expresamente que la persona sea informada sobre el origen de sus datos cuando estos hayan sido obtenidos por otra vía. Esta previsión resulta importante en ecosistemas donde empresas reciben información de proveedores, socios comerciales, plataformas publicitarias o registros disponibles para determinados fines. El usuario puede desconocer que una organización posee datos sobre él si nunca mantuvo una relación directa con esa entidad. La trazabilidad de la fuente constituye, por tanto, una condición necesaria para ejercer posteriormente derechos sobre la información recopilada.

La recolección digital debe evaluarse como una operación jurídica desde el momento en que comienza y no únicamente cuando ocurre una filtración o utilización perjudicial. Las plataformas disponen de capacidades técnicas que permiten captar, combinar y analizar información a gran escala, lo que incrementa la necesidad de establecer límites previos. Estudios sobre aplicaciones digitales muestran que la evaluación del cumplimiento y del riesgo debe incorporar indicadores relacionados con recopilación, permisos, prácticas de privacidad y posibles usos posteriores (Kim et al., 2023). A su vez, la información incidental disponible en redes sociales evidencia que incluso datos aparentemente públicos pueden producir afectaciones cuando son extraídos de contexto y reutilizados para finalidades diferentes (Kutschera, 2023).

2.3 Almacenamiento, conservación y eliminación de datos personales

El almacenamiento constituye una fase del tratamiento en la que los datos personales permanecen disponibles para usos posteriores dentro de sistemas físicos o digitales. Puede realizarse en servidores propios, servicios en la nube, dispositivos institucionales, bases de datos distribuidas o infraestructuras operadas por terceros. La existencia de capacidad técnica para conservar grandes volúmenes de información no elimina la obligación de justificar su permanencia. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, incorpora el principio de conservación y exige que los datos se mantengan únicamente durante el tiempo necesario para cumplir las finalidades que justificaron su tratamiento.

La conservación debe guardar relación con una finalidad determinada y no convertirse en una práctica indefinida. Una organización puede necesitar mantener determinados registros por razones administrativas, contractuales o jurídicas, pero esa necesidad debe revisarse cuando cambian las condiciones del tratamiento. El artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021) establece que el período de conservación no debe exceder el tiempo necesario para alcanzar los fines declarados. Esta limitación reduce la exposición acumulativa de los titulares y obliga a establecer criterios internos para decidir cuándo un dato debe mantenerse, bloquearse, anonimizarse o eliminarse al dejar de cumplir una función legítima.

La retención prolongada puede transformar registros inicialmente limitados en conjuntos de información capaces de revelar hábitos, relaciones o trayectorias personales. Este efecto se incrementa cuando los datos pueden cruzarse con otras fuentes o conservarse durante períodos extensos. El análisis jurídico de los sistemas de retención masiva muestra que la duración y amplitud del almacenamiento influyen directamente en el nivel de afectación posible sobre la privacidad, especialmente cuando se acumulan metadatos o registros de comunicaciones (Mitsilegas et al., 2023). Por ello, el tiempo de conservación debe evaluarse conjuntamente con la naturaleza de los datos, la finalidad declarada y la posibilidad de utilización posterior.

El almacenamiento también exige garantizar confidencialidad, integridad y disponibilidad durante todo el período de conservación. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, establece el principio de seguridad y exige adoptar medidas adecuadas frente a riesgos, amenazas y vulnerabilidades. Esta obligación comprende la protección contra accesos no autorizados, alteraciones, pérdidas o divulgaciones indebidas. En servicios digitales, el riesgo puede aumentar cuando la información se replica en distintos sistemas o se aloja mediante proveedores externos. La gestión de privacidad en aplicaciones y servicios debe considerar, por tanto, no solo qué datos se recopilan, sino también dónde permanecen almacenados y durante cuánto tiempo (Kim et al., 2023).

La eliminación representa la fase en la que los datos dejan de estar disponibles cuando desaparece la finalidad que justificaba su conservación o cuando procede su supresión conforme con el ordenamiento jurídico. Este proceso puede resultar complejo en sistemas digitales porque la información puede encontrarse replicada en respaldos, registros históricos, servicios en la nube o sistemas asociados. La eliminación efectiva requiere identificar las ubicaciones donde permanecen copias y establecer procedimientos verificables para retirarlas. El principio de conservación previsto en el artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021) obliga a evitar que la disponibilidad técnica de almacenamiento se convierta en una justificación para conservar información innecesaria.

Tabla 5

Etapas y criterios para el almacenamiento, conservación y eliminación de datos personales

Etapas	Criterio jurídico principal	Riesgo asociado	Medida aplicable
Almacenamiento inicial	Finalidad y necesidad	Acumulación de información innecesaria	Definir qué datos deben conservarse
Organización de registros	Calidad y exactitud	Uso de datos desactualizados	Revisar y actualizar información
Conservación activa	Limitación temporal	Retención excesiva	Establecer plazos de conservación
Respaldo	Seguridad	Persistencia de copias no controladas	Gestionar copias y accesos
Almacenamiento externo	Confidencialidad y control	Dependencia de terceros	Definir responsabilidades contractuales
Revisión periódica	Responsabilidad proactiva	Permanencia sin finalidad vigente	Verificar necesidad de conservación
Eliminación	Supresión efectiva	Recuperación o reutilización posterior	Aplicar procedimientos verificables
Anonimización	Imposibilidad de identificación	Reidentificación mediante combinación	Evaluar el riesgo residual

Nota. La tabla organiza los criterios que deben aplicarse durante la permanencia y retiro de los datos para evitar una conservación injustificada o una eliminación incompleta.

La conservación de información en servicios externos introduce además problemas relacionados con control y distribución de responsabilidades. Cuando una organización utiliza infraestructura de terceros, los datos pueden encontrarse en sistemas que el responsable no administra directamente. Esta situación exige conocer qué operaciones realiza el proveedor, cómo protege la información y qué ocurre cuando finaliza la relación contractual. Los modelos de intercambio y procesamiento distribuido muestran que el control sobre los datos puede fragmentarse entre varios actores, lo que aumenta la necesidad de establecer condiciones claras

para acceso, conservación y eliminación (Agahari et al., 2022). La externalización tecnológica no elimina las obligaciones jurídicas vinculadas con la protección de información personal.

El almacenamiento prolongado también puede aumentar la posibilidad de usos secundarios no previstos inicialmente. Una base de datos creada para prestar un servicio puede adquirir posteriormente valor para análisis, segmentación, investigación o elaboración de perfiles. El hecho de que la información continúe disponible facilita estos usos, aunque la finalidad original haya desaparecido. El principio de finalidad del artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021) exige evitar que la permanencia de los datos permita tratamientos incompatibles con el propósito que justificó su recopilación. La conservación debe estar acompañada, por ello, de controles que impidan reutilizaciones oportunistas de información acumulada.

La eliminación debe contemplar también los sistemas automatizados que utilizan datos para desarrollar modelos o realizar análisis posteriores. Aunque se suprima un registro de una base operacional, determinada información puede haber sido incorporada a procesos de aprendizaje automático. Los estudios sobre ataques de privacidad muestran que algunos modelos pueden conservar patrones o permitir inferencias relacionadas con datos utilizados durante su entrenamiento, lo que introduce dificultades adicionales para garantizar una supresión completa (Rigaki & Garcia, 2023). Esta situación obliga a considerar que la eliminación en entornos digitales no siempre consiste únicamente en borrar un archivo, sino en evaluar si existen réplicas, derivados o modelos capaces de mantener información vinculada con el titular.

La gestión adecuada del almacenamiento exige integrar criterios de necesidad, seguridad, trazabilidad y revisión periódica durante todo el ciclo de vida de los datos. Conservar información durante más tiempo del requerido incrementa las posibilidades de acceso indebido, filtración, reutilización o combinación con otros registros. En sistemas digitales, este riesgo se amplifica por la facilidad para duplicar y distribuir información entre distintos entornos tecnológicos. La aplicación del principio de conservación obliga a justificar la permanencia del dato y a prever desde el inicio cómo será eliminado cuando deje de resultar necesario. La protección jurídica depende, por tanto, tanto de controlar la entrada de información como de gestionar adecuadamente su salida.

2.4 Elaboración de perfiles y análisis automatizado de información personal

La elaboración de perfiles consiste en utilizar datos personales para evaluar o predecir determinados aspectos relacionados con una persona. Estas operaciones pueden referirse a

preferencias, hábitos, comportamiento, rendimiento, ubicación, intereses, situación económica u otras características susceptibles de inferirse a partir de información previamente recopilada. En los entornos digitales, el perfilado suele desarrollarse mediante procedimientos automatizados que procesan grandes cantidades de datos y generan clasificaciones o probabilidades. La relevancia jurídica de estas prácticas radica en que pueden producir efectos sobre la persona sin que esta conozca con claridad cómo se construyó el perfil o qué variables fueron consideradas durante el análisis (Mühlhoff, 2021).

La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, reconoce la elaboración de perfiles como una forma de tratamiento automatizado destinada a evaluar determinados aspectos personales de una persona natural. Esta definición permite incluir dentro del ámbito jurídico actividades que no se limitan a almacenar o consultar información, sino que transforman los datos en valoraciones, predicciones o segmentaciones. La existencia de un perfil puede influir en la forma en que una persona recibe publicidad, accede a servicios o es evaluada por una organización. Por ello, el tratamiento automatizado debe respetar los principios generales de licitud, finalidad, proporcionalidad y transparencia aplicables a los datos personales.

La elaboración de perfiles puede basarse tanto en datos proporcionados directamente por el titular como en información generada durante su interacción con plataformas digitales. Registros de navegación, ubicación, búsquedas, compras, clics, tiempos de permanencia o actividad en redes sociales pueden convertirse en insumos para construir categorías de usuarios. El problema jurídico no se limita a la exactitud de los datos originales, porque los sistemas pueden producir inferencias que la persona nunca declaró de manera expresa. La privacidad predictiva muestra precisamente que grandes conjuntos de datos permiten estimar características sensibles o comportamientos futuros a partir de correlaciones estadísticas, ampliando considerablemente la capacidad de conocer y clasificar a las personas (Mühlhoff, 2021).

El análisis automatizado también puede operar sobre información aparentemente poco sensible y convertirla en conocimiento de mayor impacto. La combinación de horarios, ubicación, contactos, consumo o actividad en línea puede revelar rutinas, relaciones o preferencias que no serían evidentes al observar cada dato por separado. En este contexto, la minimización adquiere una función preventiva. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige que el tratamiento se limite a los datos pertinentes y necesarios para la finalidad declarada. Esta regla restringe la acumulación indiscriminada de información cuando

su utilización puede facilitar perfiles más detallados de los estrictamente necesarios para prestar un servicio.

La transparencia resulta especialmente relevante cuando el tratamiento automatizado genera inferencias difíciles de comprender para el titular. La persona necesita conocer no solo que sus datos están siendo utilizados, sino también qué finalidad persigue la operación y qué consecuencias puede producir. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, reconoce el derecho a recibir información sobre los fines del tratamiento, la base jurídica, los tipos de operaciones realizadas y otros elementos relevantes. En procedimientos automatizados, esta obligación debe interpretarse de manera que el titular pueda comprender suficientemente la existencia y alcance del análisis, evitando que el uso de sistemas complejos convierta el tratamiento en una práctica opaca.

Los perfiles pueden utilizarse para personalizar servicios, segmentar públicos o anticipar necesidades, pero también pueden introducir riesgos de discriminación o exclusión. Una clasificación automatizada puede generar consecuencias desfavorables si se construye a partir de datos incompletos, sesgados o poco representativos. Incluso cuando el algoritmo funciona conforme con sus parámetros técnicos, el resultado puede afectar derechos si atribuye características o riesgos a una persona de manera injustificada. Los estudios sobre privacidad y analítica muestran que el problema no se limita a la exposición de datos, sino también al poder de inferir información y tomar decisiones a partir de correlaciones que el titular no controla (Mühlhoff, 2021).

La exactitud de la información adquiere una importancia particular cuando los perfiles se utilizan para orientar decisiones. Un dato incorrecto puede producir una clasificación errónea que se reproduzca automáticamente en diferentes sistemas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, incorpora el principio de calidad y exactitud, que exige que los datos sean correctos y se mantengan actualizados cuando resulte necesario. Este principio debe aplicarse también a los procesos que generan inferencias, porque un perfil construido sobre información desactualizada puede producir efectos que no reflejan la situación real de la persona. La automatización no elimina la necesidad de revisar la calidad de los datos utilizados.

El perfilado puede intensificarse cuando las plataformas combinan información obtenida de diferentes fuentes. Los servicios digitales pueden integrar datos proporcionados por el usuario con registros técnicos, información procedente de terceros y datos inferidos durante la

interacción. Esta combinación incrementa la capacidad analítica y amplía el nivel de detalle de los perfiles. Los modelos de evaluación de privacidad aplicados a aplicaciones móviles muestran que las prácticas de recopilación y análisis deben examinarse de manera conjunta, porque el riesgo depende tanto de la cantidad de datos como de los usos posteriores que se realizan sobre ellos (Kim et al., 2023). El tratamiento debe evaluarse como un proceso acumulativo.

Las decisiones automatizadas representan una consecuencia posible del perfilado cuando el resultado del análisis se utiliza para determinar una respuesta sin intervención humana significativa. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce el derecho de las personas a no ser objeto de decisiones basadas única o parcialmente en valoraciones automatizadas que produzcan efectos jurídicos o afecten sus derechos y libertades fundamentales, salvo los supuestos previstos legalmente. Esta disposición introduce una garantía específica frente a sistemas capaces de transformar perfiles en decisiones relevantes para el titular y exige considerar la supervisión humana como elemento de protección frente a resultados potencialmente perjudiciales.

La seguridad también resulta esencial porque los sistemas de perfilado suelen concentrar grandes volúmenes de información y modelos capaces de revelar patrones sensibles. Los estudios sobre ataques de privacidad en aprendizaje automático muestran que determinados métodos pueden permitir inferir si una persona formó parte del conjunto de entrenamiento o recuperar información vinculada con los datos utilizados (Rigaki & Garcia, 2023). Esta posibilidad amplía el concepto tradicional de vulneración, pues el riesgo puede persistir incluso cuando la base original ya no es accesible. El diseño de sistemas automatizados debe incorporar medidas que reduzcan la exposición de los datos y limiten la capacidad de extraer información no prevista.

La elaboración de perfiles exige, en consecuencia, combinar límites jurídicos sobre la recopilación, transparencia sobre las finalidades, calidad de los datos y garantías frente a decisiones automatizadas. El problema no reside únicamente en que una organización conozca información sobre una persona, sino en que pueda transformar grandes volúmenes de datos en inferencias capaces de condicionar oportunidades o tratamientos posteriores. En los entornos digitales, donde el perfilado puede realizarse de manera continua y casi invisible, la protección efectiva requiere controlar tanto los datos de origen como los resultados derivados del análisis. Esta perspectiva permite preservar la autonomía del titular frente a procesos automatizados que afectan su esfera personal.

Figura 4

Elaboración de perfiles mediante el tratamiento automatizado de datos personales



Nota. El esquema sintetiza las etapas del perfilado y relaciona sus principales riesgos con las garantías jurídicas destinadas a preservar el control, la transparencia y la protección de los derechos del titular.

2.5 Tratamiento de datos mediante inteligencia artificial y sistemas algorítmicos

El tratamiento de datos mediante inteligencia artificial comprende operaciones en las que sistemas algorítmicos recopilan, organizan, relacionan o analizan información personal para producir resultados, clasificaciones, recomendaciones o predicciones. Estas tecnologías

pueden procesar volúmenes de datos muy superiores a los manejados mediante procedimientos tradicionales y detectar relaciones que no resultan evidentes para una persona. Desde la perspectiva jurídica, la utilización de inteligencia artificial no modifica la naturaleza protegida de los datos ni elimina las obligaciones asociadas a su tratamiento. Los riesgos aparecen cuando los modelos extraen inferencias nuevas, utilizan información para finalidades diferentes o dificultan que el titular comprenda cómo se obtiene un determinado resultado (Mühlhoff, 2021).

La aplicación de sistemas algorítmicos debe respetar los principios generales establecidos para cualquier tratamiento de información personal. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, las operaciones sobre datos deben observar, entre otros, los principios de juridicidad, lealtad, transparencia, finalidad, pertinencia, minimización, proporcionalidad, calidad, seguridad y responsabilidad proactiva. Estos criterios resultan especialmente relevantes para la inteligencia artificial porque la capacidad técnica de procesar grandes conjuntos de información podría favorecer recopilaciones excesivas. La disponibilidad de datos no constituye por sí misma una justificación jurídica para utilizarlos en el entrenamiento, funcionamiento o evaluación de modelos automatizados.

Los sistemas de inteligencia artificial pueden trabajar con datos proporcionados directamente por el titular, información obtenida de plataformas digitales o conjuntos de datos previamente recopilados para otras finalidades. Esta diversidad de fuentes exige determinar si el tratamiento mantiene compatibilidad con el propósito que justificó originalmente la obtención. El artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021) exige que los datos se recojan con fines determinados, explícitos y legítimos. Este principio limita la reutilización indiscriminada para entrenar algoritmos cuando la nueva finalidad carece de fundamento suficiente. La evaluación debe considerar tanto la procedencia de los datos como la finalidad concreta del sistema que los utilizará.

Una característica relevante de los sistemas algorítmicos es su capacidad para generar inferencias a partir de información previamente disponible. Un modelo puede estimar preferencias, conductas, riesgos o características personales sin que esos atributos hayan sido proporcionados expresamente. Esta capacidad amplía los riesgos tradicionales de privacidad porque el tratamiento no se limita a conservar información existente, sino que produce conocimiento nuevo sobre la persona. El concepto de privacidad predictiva permite analizar precisamente cómo la analítica de datos transforma registros conductuales en predicciones o

probabilidades aplicables a individuos y grupos, incluso cuando determinadas características sensibles no fueron reveladas directamente por los titulares (Mühlhoff, 2021).

La transparencia constituye una condición especialmente compleja en sistemas de inteligencia artificial. Algunos modelos utilizan procedimientos estadísticos cuya lógica resulta difícil de explicar mediante una descripción sencilla, pero esta dificultad técnica no elimina el deber de informar al titular. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, reconoce el derecho a recibir información sobre las finalidades, base jurídica, tipos de tratamiento y otros aspectos relevantes relacionados con los datos personales. Cuando intervienen sistemas automatizados, la información debe permitir comprender suficientemente que existe un tratamiento de esta naturaleza y cuáles pueden ser sus consecuencias para la persona afectada.

Los sistemas algorítmicos pueden intervenir además en decisiones que produzcan efectos concretos sobre los titulares. Una clasificación automatizada puede influir en la selección de contenidos, evaluación de riesgos, acceso a servicios o condiciones ofrecidas por una organización. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, el titular tiene derecho a no ser sometido a decisiones basadas única o parcialmente en valoraciones automatizadas que produzcan efectos jurídicos o afecten sus derechos y libertades fundamentales, salvo las excepciones previstas legalmente. Esta disposición establece un límite frente a decisiones relevantes adoptadas exclusivamente mediante procesamiento algorítmico.

La calidad de los datos constituye otro elemento decisivo porque los resultados de un algoritmo dependen de la información utilizada para desarrollarlo y aplicarlo. Datos incompletos, incorrectos o desactualizados pueden producir inferencias equivocadas y trasladar errores a decisiones posteriores. El principio de calidad y exactitud reconocido en el artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021) obliga a garantizar que la información resulte adecuada para las finalidades perseguidas. En sistemas automatizados, este deber debe extenderse al análisis de los conjuntos de datos y a la revisión de resultados, pues la automatización puede reproducir errores de manera sistemática y afectar simultáneamente a numerosos titulares.

La seguridad de la información adquiere una dimensión adicional cuando los datos son utilizados para entrenar modelos de aprendizaje automático. Algunas técnicas de ataque pueden intentar determinar si determinada información formó parte del conjunto de entrenamiento,

reconstruir atributos o extraer información sensible a partir del comportamiento del modelo. La literatura especializada ha identificado ataques de inferencia de membresía, reconstrucción y extracción como riesgos específicos de privacidad en aprendizaje automático (Rigaki & Garcia, 2023). Estos problemas evidencian que proteger únicamente la base de datos original puede resultar insuficiente, porque el propio modelo puede convertirse en una fuente indirecta de exposición de información utilizada durante su desarrollo.

La gestión de estos riesgos requiere adoptar medidas técnicas y organizativas desde las primeras fases del diseño del sistema. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, responsables y encargados deben implementar medidas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas para garantizar y demostrar el cumplimiento normativo. En proyectos de inteligencia artificial, esta obligación puede traducirse en controles de acceso, revisión de fuentes de datos, minimización, seudonimización, documentación de procesos y evaluación periódica de vulnerabilidades. La responsabilidad no comienza cuando se produce un incidente, sino desde la planificación de las operaciones que utilizarán información personal.

La evaluación del cumplimiento también debe considerar las aplicaciones y servicios digitales que incorporan inteligencia artificial como parte de sus funciones. Los modelos de análisis de privacidad muestran que es posible valorar sistemáticamente aspectos como permisos solicitados, volumen de información recopilada, finalidad del tratamiento y exposición a riesgos mediante indicadores estandarizados (Kim et al., 2023). Este enfoque resulta útil porque evita considerar el cumplimiento como una revisión exclusivamente documental. En sistemas automatizados, la protección exige observar cómo funciona realmente el tratamiento, qué datos utiliza, qué resultados genera y cuáles son las condiciones bajo las cuales esos resultados pueden afectar al titular.

El tratamiento mediante inteligencia artificial exige, en consecuencia, integrar principios jurídicos y controles técnicos durante todo el ciclo de vida del sistema. La legitimidad de los datos de entrada, la proporcionalidad de su uso, la transparencia, la seguridad y las garantías frente a decisiones automatizadas deben evaluarse de manera conjunta. La eficiencia o precisión de un modelo no sustituye estas exigencias, porque el tratamiento continúa sujeto a los derechos del titular. La protección jurídica debe acompañar tanto la fase de entrenamiento como la utilización posterior del sistema, especialmente cuando las inferencias producidas pueden modificar la forma en que una persona es evaluada, clasificada o tratada.

2.6 Transferencia y comunicación de datos personales a terceros

La transferencia y comunicación de datos personales a terceros constituye una fase especialmente sensible del tratamiento porque implica que la información sale del ámbito inicial en el que fue recopilada. Esta operación puede producirse entre empresas, instituciones públicas, proveedores tecnológicos, plataformas digitales o prestadores de servicios especializados. Desde la perspectiva jurídica, el hecho de que una organización posea legítimamente determinados datos no significa que pueda comunicarlos libremente a cualquier tercero. La transferencia debe contar con una base jurídica, responder a una finalidad legítima y respetar las condiciones bajo las cuales la información fue obtenida, evitando usos posteriores incompatibles con los derechos del titular.

La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, define la transferencia o comunicación como la manifestación, declaración, entrega, consulta, interconexión, cesión, transmisión, difusión o cualquier forma de revelación de datos personales realizada a una persona distinta del titular, responsable o encargado, según corresponda. Esta definición evidencia que la comunicación no se limita a entregar físicamente una base de datos. También puede producirse cuando un tercero obtiene acceso mediante sistemas interconectados, servicios en la nube, interfaces digitales o mecanismos de consulta remota. La amplitud del concepto obliga a analizar cualquier modalidad mediante la cual la información queda disponible para otro sujeto.

La intervención de terceros exige identificar con precisión quién recibe los datos y qué posición ocupa dentro del tratamiento. Un destinatario puede recibir información para desarrollar una finalidad propia o actuar dentro de una relación previamente definida con el responsable. Esta diferencia resulta jurídicamente relevante porque determina las obligaciones aplicables y el grado de autonomía del receptor. Los modelos de intercambio de datos muestran que el control sobre la información puede distribuirse entre varios participantes, especialmente cuando se utilizan tecnologías de procesamiento colaborativo. La protección debe considerar no solo la transferencia directa, sino también los mecanismos mediante los cuales distintos actores pueden acceder o producir resultados a partir de información compartida (Agahari et al., 2022).

La finalidad constituye uno de los principales límites para la comunicación de datos. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, los datos deben tratarse para fines determinados, explícitos y legítimos, y no pueden utilizarse posteriormente para propósitos incompatibles. Este principio resulta especialmente importante

cuando una organización pretende comunicar información a un tercero que utilizará los datos para actividades distintas de aquellas conocidas inicialmente por el titular. La existencia de una relación comercial entre organizaciones no constituye, por sí sola, una habilitación suficiente para ampliar el tratamiento. Cada comunicación debe mantener coherencia con la base jurídica y la finalidad correspondiente.

La transparencia también debe acompañar la transferencia de información. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, reconoce el derecho del titular a recibir información sobre destinatarios o categorías de destinatarios de sus datos, cuando corresponda. Esta obligación permite conocer si la información será compartida con terceros y bajo qué condiciones generales se producirá esa comunicación. En los servicios digitales, esta información resulta especialmente relevante porque muchos tratamientos dependen de proveedores externos de alojamiento, análisis, publicidad, autenticación o procesamiento. Sin transparencia suficiente, el titular puede desconocer cuántos sujetos participan realmente en el tratamiento de su información personal.

Las transferencias también deben respetar el principio de minimización. La comunicación a terceros no debería incluir más datos de los necesarios para alcanzar la finalidad legítima que justifica el intercambio. De acuerdo con el artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021), el tratamiento debe limitarse a información pertinente y estrictamente necesaria. Este criterio resulta aplicable tanto a transferencias puntuales como a accesos continuos mediante sistemas integrados. Cuando un tercero necesita únicamente determinados atributos para prestar un servicio, permitirle consultar bases completas puede ampliar innecesariamente el riesgo. La arquitectura del intercambio debe restringir el acceso según las funciones concretas de cada participante.

La seguridad constituye otro requisito esencial porque la transferencia introduce nuevos puntos de exposición. La información puede quedar comprometida durante su transmisión, recepción, almacenamiento o utilización posterior por el destinatario. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, exige a responsables y encargados adoptar medidas técnicas, administrativas, físicas, organizativas y jurídicas adecuadas para garantizar y demostrar el cumplimiento. En contextos de transferencia, estas medidas pueden incluir cifrado, autenticación, controles de acceso, registro de operaciones y acuerdos que delimiten responsabilidades. La protección debe mantenerse durante todo el recorrido de los datos y no únicamente mientras permanecen en la organización de origen.

Los entornos digitales han impulsado mecanismos de intercambio que buscan reducir la necesidad de transferir datos completos entre organizaciones. La computación multipartita segura permite que varios participantes obtengan determinados resultados sin revelar necesariamente los datos originales a las demás partes. Este enfoque modifica la relación entre privacidad, confianza y control porque reduce la exposición directa de información durante procesos colaborativos (Agahari et al., 2022). Sin embargo, estas soluciones tecnológicas no sustituyen el análisis jurídico. Aunque una técnica disminuya la cantidad de información compartida, sigue siendo necesario determinar la finalidad del procesamiento, las responsabilidades de los participantes y los riesgos residuales asociados al tratamiento conjunto.

La comunicación de datos puede adquirir mayor complejidad cuando intervienen plataformas que integran numerosos servicios y proveedores. Una sola interacción del usuario puede activar procesos de autenticación, almacenamiento, medición, publicidad o análisis ejecutados por diferentes entidades. Esta estructura dificulta que el titular identifique quién recibe su información y para qué la utiliza. Los análisis de privacidad aplicados a aplicaciones digitales muestran que la existencia de múltiples permisos y conexiones con servicios externos puede incrementar los riesgos cuando las prácticas de recopilación y transferencia no son suficientemente transparentes (Kim et al., 2023). Por ello, la evaluación debe considerar el ecosistema completo y no únicamente la aplicación visible para el usuario.

La transferencia también puede convertirse en una fuente de riesgo cuando se combina con conservación prolongada o análisis automatizado. Un tercero que recibe datos puede integrarlos con información obtenida de otras fuentes y generar perfiles o inferencias que no existían en el contexto original. Esta posibilidad amplía el impacto del tratamiento porque el titular pierde capacidad para anticipar los resultados derivados de la combinación de información. La privacidad predictiva muestra que grandes conjuntos de datos pueden utilizarse para inferir características o comportamientos que exceden el contenido explícito de los registros transferidos (Mühlhoff, 2021). El control jurídico debe extenderse, por tanto, a los usos posteriores previsibles de la información comunicada.

La transferencia de datos personales exige finalmente mecanismos que permitan conservar trazabilidad sobre quién recibió la información, con qué fundamento y para qué finalidad. La pérdida de trazabilidad dificulta el ejercicio de derechos y la atribución de responsabilidades cuando ocurre una vulneración. En sistemas digitales complejos, la protección efectiva requiere documentar relaciones entre responsables, encargados y destinatarios, además de establecer

límites técnicos de acceso. La comunicación a terceros debe concebirse como una operación sometida a los mismos principios que rigen el resto del tratamiento. Su legitimidad depende de que preserve finalidad, transparencia, proporcionalidad, seguridad y capacidad efectiva del titular para ejercer control sobre sus datos.

2.7 Tratamiento de datos personales en redes sociales y aplicaciones digitales

Las redes sociales y las aplicaciones digitales realizan un tratamiento continuo de datos personales durante el registro, uso y permanencia del usuario en el servicio. Este tratamiento puede incluir información identificativa, datos de contacto, ubicación, fotografías, preferencias, interacciones, historial de actividad e identificadores técnicos. La relevancia jurídica no depende únicamente de los datos que la persona introduce voluntariamente, sino también de aquellos que la plataforma obtiene mediante el funcionamiento del servicio. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, comprende dentro del tratamiento cualquier operación realizada sobre datos personales mediante procedimientos automatizados o no automatizados, lo que incluye estas actividades digitales.

La recolección de información en aplicaciones puede comenzar desde el momento en que el usuario instala el servicio y concede determinados permisos. Acceso a ubicación, cámara, micrófono, contactos o almacenamiento puede ampliar considerablemente la información disponible para el proveedor. La legitimidad de estas operaciones exige verificar si cada dato resulta necesario para la finalidad declarada. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, los principios de pertinencia y minimización obligan a limitar el tratamiento a información adecuada y estrictamente necesaria. La solicitud indiscriminada de permisos puede aumentar innecesariamente la exposición del titular frente a usos posteriores (Kim et al., 2023).

Las redes sociales presentan además una característica particular: gran parte de los datos se genera mediante interacciones aparentemente cotidianas. Publicaciones, reacciones, comentarios, fotografías, vínculos sociales y horarios de conexión pueden revelar aspectos personales más amplios de lo que el usuario pretendía comunicar. El concepto de datos incidentales permite explicar cómo determinados contenidos públicos o semipúblicos pueden mostrar indirectamente ubicación, rutinas, relaciones o características privadas. La utilización posterior de esta información por terceros puede producir riesgos incluso cuando el contenido fue publicado voluntariamente, porque la accesibilidad técnica no determina por sí sola la legitimidad de todos los usos posibles (Kutschera, 2023).

El deber de transparencia adquiere especial importancia en este contexto debido a la cantidad de operaciones que pueden permanecer invisibles para el usuario. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, el titular debe recibir información sobre los fines del tratamiento, su base jurídica, el tiempo de conservación, los destinatarios o categorías de destinatarios y otros elementos necesarios para comprender cómo serán utilizados sus datos. En redes sociales y aplicaciones, esta obligación debe abarcar prácticas de seguimiento, personalización, análisis y comunicación a terceros cuando formen parte del funcionamiento del servicio. La información excesivamente compleja puede dificultar el ejercicio efectivo de los derechos.

Las aplicaciones también pueden recopilar datos derivados de la actividad del usuario sin que este los proporcione de forma consciente. Frecuencia de uso, tiempo de permanencia, patrones de desplazamiento, contenido consultado o respuestas a determinadas recomendaciones pueden convertirse en señales utilizadas para clasificar comportamientos. Estos registros permiten construir perfiles cada vez más detallados cuando se combinan durante períodos prolongados. La analítica predictiva demuestra que la agregación de información conductual puede permitir inferir intereses, características o probabilidades que no aparecen explícitamente en los datos originales (Mühlhoff, 2021). El tratamiento digital debe considerar, por ello, tanto la información observada como las inferencias generadas posteriormente.

La personalización de contenidos constituye una de las aplicaciones más comunes de estos datos. Los sistemas algorítmicos pueden seleccionar publicaciones, recomendaciones o publicidad a partir de perfiles contruidos mediante la actividad previa del usuario. Desde el punto de vista jurídico, la personalización no elimina la obligación de respetar finalidad, proporcionalidad y transparencia. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige que los propósitos sean determinados, explícitos y legítimos. Si una aplicación utiliza información recopilada para prestar un servicio con el fin adicional de elaborar perfiles comerciales o conductuales, debe existir una base jurídica que permita ese tratamiento y una información suficientemente clara para el titular.

El tratamiento en redes sociales puede involucrar asimismo a terceros que participan en publicidad, medición, alojamiento, autenticación o análisis. La información puede circular entre diferentes organizaciones mediante herramientas integradas en una misma aplicación, lo que dificulta identificar quién interviene en cada operación. Los modelos de intercambio de datos muestran que el control puede distribuirse entre múltiples participantes y que la protección depende de delimitar funciones, accesos y finalidades específicas (Agahari et al.,

2022). Esta complejidad exige que la plataforma no se limite a informar sobre su propio tratamiento, sino que establezca mecanismos de control sobre aquellos terceros que reciben o procesan información dentro de su ecosistema.

La seguridad constituye otro componente esencial porque las cuentas sociales y aplicaciones concentran información capaz de revelar múltiples dimensiones de la vida personal. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, obliga a responsables y encargados a adoptar medidas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas para proteger los datos. En aplicaciones digitales, estas medidas deben considerar autenticación, control de accesos, gestión de permisos, protección de comunicaciones y reducción de exposición innecesaria. La seguridad insuficiente puede permitir que un incidente afecte simultáneamente datos de identidad, contenido privado, contactos, ubicación y hábitos, aumentando considerablemente la gravedad de una vulneración.

La publicación voluntaria de información tampoco elimina los riesgos asociados con la reutilización fuera de contexto. Una fotografía o comentario compartido para determinados contactos puede ser capturado, replicado, analizado o combinado posteriormente con otras fuentes. Las investigaciones sobre redes sociales muestran que los datos disponibles pueden utilizarse para obtener información no prevista inicialmente por la persona que publicó el contenido (Kutschera, 2023). Esta posibilidad obliga a diferenciar entre hacer visible una información en un contexto específico y autorizar cualquier tratamiento posterior. La protección de datos debe considerar la finalidad, la expectativa razonable del usuario y las condiciones bajo las cuales terceros reutilizan información obtenida de plataformas sociales.

Las aplicaciones móviles presentan además diferencias significativas en sus prácticas de privacidad. Algunas solicitan numerosos permisos, integran herramientas de terceros o recopilan información que excede la función principal ofrecida al usuario. La evaluación automatizada de miles de aplicaciones ha mostrado que es posible identificar niveles distintos de riesgo mediante indicadores asociados con prácticas de recopilación, permisos y tratamiento de información personal (Kim et al., 2023). Este tipo de análisis evidencia que el riesgo no depende únicamente de la categoría del servicio, sino de las decisiones concretas tomadas durante su diseño. Una aplicación aparentemente sencilla puede generar una exposición considerable si incorpora mecanismos de recopilación desproporcionados.

El tratamiento de datos personales en redes sociales y aplicaciones debe analizarse, por tanto, como un proceso continuo que combina recopilación, observación, inferencia,

almacenamiento, perfilado y eventual comunicación a terceros. El usuario puede percibir únicamente la interfaz visible mientras numerosas operaciones se ejecutan en segundo plano. Esta asimetría exige reforzar transparencia, minimización, seguridad y control sobre finalidades durante todo el ciclo del tratamiento. La protección jurídica no busca impedir el funcionamiento de servicios digitales, sino limitar aquellas prácticas que amplían innecesariamente la exposición de las personas. En este contexto, la eficacia de las garantías depende de que las operaciones técnicas permanezcan sometidas a criterios jurídicos verificables.

Figura 5

Tratamiento de datos personales en redes sociales y aplicaciones digitales



Nota. El esquema muestra cómo las plataformas recopilan, procesan y comparten información durante la interacción del usuario, y relaciona estas operaciones con los principales riesgos y garantías aplicables al tratamiento de datos personales.

2.8 Riesgos asociados al tratamiento masivo y automatizado de datos

El tratamiento masivo y automatizado de datos incrementa la capacidad de recopilar, relacionar y analizar información personal a una escala difícil de alcanzar mediante procedimientos tradicionales. El riesgo jurídico aparece cuando grandes volúmenes de datos permiten construir perfiles, inferir características o adoptar decisiones que afectan a las personas sin suficiente transparencia. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige que todo tratamiento respete los principios de finalidad, minimización, proporcionalidad, seguridad y responsabilidad proactiva. Estos principios funcionan como límites frente a prácticas que podrían ampliar innecesariamente la exposición de los titulares o utilizar datos más allá de los propósitos inicialmente definidos.

La acumulación prolongada de información constituye uno de los principales riesgos porque permite reconstruir comportamientos, relaciones y trayectorias personales. Registros de comunicaciones, ubicación o actividad digital pueden adquirir un significado distinto cuando se conservan durante largos períodos y se analizan conjuntamente. El estudio de los sistemas de retención masiva muestra que la amplitud temporal y material del almacenamiento puede generar tensiones importantes con la privacidad, especialmente cuando afecta a grandes grupos de personas sin una diferenciación suficiente entre situaciones de riesgo y actividades ordinarias (Mitsilegas et al., 2023). Por ello, la conservación debe limitarse mediante criterios de necesidad, proporcionalidad y finalidad.

El perfilado automatizado introduce otro riesgo porque transforma datos existentes en inferencias que pueden no haber sido proporcionadas directamente por el titular. Los algoritmos pueden estimar intereses, preferencias, comportamientos futuros o atributos sensibles a partir de patrones estadísticos. La privacidad predictiva demuestra que estas inferencias pueden afectar a personas incluso cuando los datos empleados no parecen sensibles de manera aislada (Mühlhoff, 2021). En términos jurídicos, el problema no se limita a la recopilación inicial, sino también a la capacidad del sistema para generar nueva información y utilizarla posteriormente para clasificar, segmentar o evaluar a una persona sin una comprensión suficiente de las consecuencias del tratamiento.

Los modelos de aprendizaje automático añaden riesgos específicos porque pueden retener o revelar información relacionada con los datos utilizados durante su entrenamiento. Se han identificado ataques que permiten inferir si una persona formó parte de un conjunto de datos, reconstruir determinados atributos o extraer información de los modelos. Estas

vulnerabilidades amplían el concepto tradicional de filtración porque la exposición puede producirse incluso cuando la base original se encuentra protegida (Rigaki & Garcia, 2023). La seguridad del tratamiento automatizado debe abarcar, por tanto, no solo las bases de datos, sino también los modelos, interfaces, registros intermedios y mecanismos mediante los cuales se generan resultados.

La utilización masiva de información también puede aumentar la opacidad del tratamiento. Cuando intervienen múltiples plataformas, proveedores, sistemas de análisis y destinatarios, el titular puede desconocer dónde se encuentran sus datos o qué entidades participan en su procesamiento. Esta fragmentación dificulta ejercer derechos y atribuir responsabilidades cuando se produce una vulneración. Los modelos de intercambio de datos muestran que la distribución del procesamiento entre varios actores puede reducir el control directo sobre la información y exigir mecanismos adicionales de gobernanza, trazabilidad y delimitación de responsabilidades (Agahari et al., 2022). La automatización no debe convertirse en una justificación para debilitar la identificación de los sujetos que intervienen.

Tabla 6

Riesgos derivados del tratamiento masivo y automatizado de datos personales

Riesgo	Forma en que se manifiesta	Posible afectación
Acumulación excesiva	Conservación de grandes volúmenes de datos durante períodos prolongados.	Pérdida de privacidad y ampliación de la exposición.
Perfilado automatizado	Clasificación e inferencia de características personales.	Discriminación, segmentación o decisiones desfavorables.
Reutilización incompatible	Empleo de datos para finalidades distintas de las iniciales.	Pérdida de control por parte del titular.
Opacidad algorítmica	Dificultad para comprender cómo se genera un resultado.	Limitación del ejercicio de derechos y de la capacidad de impugnación.
Ataques a modelos	Extracción o reconstrucción de información desde sistemas de aprendizaje automático.	Revelación de datos sensibles o inferidos.
Interconexión de bases	Cruce de registros procedentes de fuentes diferentes.	Identificación indirecta y generación de perfiles detallados.
Transferencia entre múltiples actores	Circulación de información en ecosistemas digitales complejos.	Dificultad para determinar responsabilidades.
Automatización de decisiones	Uso de resultados algorítmicos para adoptar decisiones relevantes.	Afectación de derechos sin intervención humana suficiente.

Nota. La tabla resume los principales riesgos que surgen cuando grandes volúmenes de información se procesan mediante sistemas automatizados y se combinan con otras fuentes.

La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce el derecho a no ser objeto de decisiones basadas única o parcialmente en valoraciones automatizadas cuando produzcan efectos jurídicos o afecten derechos y libertades fundamentales, salvo los supuestos permitidos por la normativa. Esta garantía resulta particularmente importante en escenarios de tratamiento masivo, donde una misma lógica algorítmica puede aplicarse simultáneamente a numerosos titulares. El riesgo aumenta cuando las decisiones se basan en perfiles contruidos con datos incompletos, desactualizados o inferidos, porque los errores pueden reproducirse de manera sistemática y afectar a grupos amplios de personas.

La evaluación de riesgos debe realizarse antes de que el tratamiento produzca consecuencias. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, responsables y encargados deben aplicar medidas administrativas, técnicas, físicas, organizativas y jurídicas, además de metodologías para analizar y gestionar riesgos. Esta obligación cobra especial relevancia cuando se utilizan sistemas automatizados capaces de procesar grandes cantidades de información. La responsabilidad proactiva exige identificar posibles escenarios de afectación, valorar su gravedad y adoptar controles preventivos. No basta con reaccionar después de una filtración o decisión perjudicial; el riesgo debe formar parte del diseño y supervisión del tratamiento.

La evaluación automatizada de aplicaciones y servicios digitales también muestra que los riesgos pueden identificarse mediante indicadores relacionados con permisos, recopilación, finalidades y prácticas de privacidad. Estos métodos permiten detectar diferencias significativas entre servicios que aparentemente cumplen funciones similares y evidencian que el nivel de exposición depende de decisiones concretas sobre diseño y tratamiento (Kim et al., 2023). Este enfoque resulta útil para controlar sistemas masivos porque facilita revisar prácticas de manera sistemática. Sin embargo, la evaluación técnica debe complementarse con un análisis jurídico que determine si las operaciones son necesarias, proporcionales y compatibles con los derechos reconocidos al titular.

El tratamiento masivo y automatizado requiere protección durante todo el ciclo de vida de los datos. El riesgo no depende solo del volumen de información, sino de su combinación, las inferencias generadas y las decisiones algorítmicas derivadas. Por ello, seguridad, transparencia, minimización y trazabilidad deben integrarse para preservar el control jurídico, las finalidades, las responsabilidades y los límites de cada operación automatizada realizada.



Capítulo 3

Consentimiento, transparencia y derechos de los titulares

David Israel Báez Herrera

3.1 Consentimiento como fundamento para el tratamiento de datos personales

El consentimiento constituye una de las bases que pueden legitimar el tratamiento de datos personales cuando la voluntad del titular autoriza determinadas operaciones sobre su información. Su importancia radica en que permite vincular el tratamiento con una decisión consciente de la persona y limita la posibilidad de utilizar los datos más allá de aquello que fue aceptado. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 8, establece que los datos personales pueden tratarse y comunicarse cuando existe una manifestación de voluntad del titular para hacerlo. Esta regulación convierte al consentimiento en un mecanismo jurídico de control sobre la información personal.

El consentimiento no debe entenderse como una autorización general e ilimitada. Su función consiste en habilitar un tratamiento concreto dentro de condiciones previamente determinadas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, lo define como una manifestación de voluntad libre, específica, informada e inequívoca mediante la cual el titular autoriza al responsable a tratar sus datos personales. Esta definición relaciona directamente el consentimiento con la autonomía individual y exige que la persona conozca suficientemente qué tratamiento acepta. En aplicaciones que manejan información íntima o sensible, la calidad de esa decisión adquiere particular importancia debido a las consecuencias que puede tener la utilización posterior de los datos (Alaattinoğlu, 2022).

Para que el consentimiento funcione como fundamento legítimo debe estar vinculado con finalidades concretas. Una persona no puede adoptar una decisión suficientemente informada si desconoce para qué serán utilizados sus datos o si la autorización comprende propósitos formulados de manera excesivamente amplia. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 8, exige que el consentimiento sea específico respecto de los medios y fines del tratamiento. Esta característica impide utilizar una aceptación genérica para justificar operaciones sustancialmente diferentes de aquellas que fueron presentadas al titular. La especificidad permite además evaluar posteriormente si el responsable respetó los límites establecidos al momento de obtener la autorización.

La libertad constituye otra condición esencial porque una autorización obtenida mediante presión, engaño o ausencia real de alternativas no expresa adecuadamente la voluntad del titular. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 8, el consentimiento debe ser libre y encontrarse exento de vicios. Esta exigencia obliga a examinar las circunstancias concretas bajo las cuales una persona acepta el tratamiento. En

determinados servicios digitales, la dependencia de una plataforma o la vinculación entre acceso al servicio y aceptación de usos adicionales puede dificultar una decisión verdaderamente autónoma. El análisis del consentimiento en aplicaciones que procesan datos íntimos muestra precisamente la importancia de valorar las condiciones reales de elección (Alaattinoğlu, 2022).

La condición de informado exige que el titular conozca previamente los elementos relevantes del tratamiento. No basta con presentar un botón de aceptación si la información esencial permanece oculta, fragmentada o redactada de forma incomprensible. El artículo 8 de la Ley Orgánica de Protección de Datos Personales (2021) vincula expresamente el consentimiento informado con el principio de transparencia. Esta exigencia se complementa con el artículo 12 de la misma ley, que reconoce el derecho a recibir información sobre finalidades, base jurídica, tiempo de conservación, tipos de tratamiento y destinatarios, entre otros elementos. La decisión del titular debe sustentarse, por tanto, en información suficiente para comprender el alcance de la autorización.

La manifestación también debe ser inequívoca, de manera que no existan dudas razonables sobre si el titular realmente autorizó el tratamiento. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 8, incorpora esta condición como requisito de validez. El Reglamento General a la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo No. 904, 2023), en su artículo 5, desarrolla este criterio y señala que el consentimiento debe reflejar indudablemente la aceptación mediante una declaración, pronunciamiento o acción afirmativa clara. Esta exigencia limita prácticas basadas en silencio, inactividad o mecanismos ambiguos que no permitan demostrar de forma suficiente la voluntad del titular.

La responsabilidad de demostrar que el consentimiento fue obtenido correctamente corresponde a quien sustenta el tratamiento en esa autorización. El Reglamento General a la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo No. 904, 2023), en su artículo 5, dispone que el responsable debe poder demostrar el consentimiento obtenido cuando sea requerido por la autoridad competente. Esta obligación refuerza la responsabilidad proactiva porque exige mantener evidencia verificable de la decisión del titular. En los entornos digitales, esta documentación puede incluir registros de la aceptación, versiones de la información presentada y condiciones existentes en el momento en que se produjo la autorización. La trazabilidad permite comprobar posteriormente la legitimidad del tratamiento.

El consentimiento adquiere mayor exigencia cuando se procesan datos sensibles. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 26, establece como regla general la prohibición del tratamiento de datos sensibles y contempla entre sus excepciones la existencia de consentimiento explícito del titular para fines claramente especificados. Esta protección reforzada responde al potencial impacto que pueden tener datos sobre salud, orientación sexual, identidad, biometría u otras características especialmente vinculadas con la vida privada. El estudio de aplicaciones dedicadas al seguimiento menstrual muestra que solicitar consentimiento para información íntima requiere considerar tanto la sensibilidad del dato como las condiciones reales bajo las cuales el usuario acepta su procesamiento (Alaattinoğlu, 2022).

El consentimiento tampoco es irrevocable. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 8, reconoce que puede revocarse en cualquier momento sin necesidad de justificar la decisión. El responsable debe proporcionar mecanismos gratuitos, ágiles y sencillos, semejantes a los utilizados para obtener inicialmente la autorización. La revocación no afecta retroactivamente la licitud del tratamiento realizado antes de que esta se produzca, pero obliga a revisar la continuidad de las operaciones que dependían de esa base. Esta facultad evita que una autorización otorgada en un momento determinado se convierta en una cesión permanente del control sobre los datos personales.

El consentimiento debe analizarse además junto con las demás condiciones que legitiman el tratamiento y no como una fórmula aplicable automáticamente a cualquier situación. La existencia de una aceptación formal no corrige prácticas incompatibles con principios como finalidad, minimización, proporcionalidad o transparencia. Un responsable podría obtener una manifestación de voluntad y, aun así, incurrir en un tratamiento problemático si recopila información excesiva o presenta las finalidades de forma poco comprensible. Por ello, la validez jurídica del consentimiento depende tanto de las condiciones en que se obtiene como de la forma en que posteriormente se respetan los límites comunicados al titular (Alaattinoğlu, 2022).

El consentimiento constituye, en consecuencia, una expresión concreta de la capacidad del titular para intervenir en el tratamiento de sus datos. Su valor jurídico no radica simplemente en registrar una aceptación, sino en garantizar que la decisión sea libre, específica, informada e inequívoca y que pueda ser demostrada y posteriormente revocada. En los entornos digitales, donde las operaciones de tratamiento pueden multiplicarse y permanecer poco visibles, estas condiciones adquieren una función protectora frente a autorizaciones genéricas o poco

comprensibles. La articulación entre la Ley Orgánica de Protección de Datos Personales y su Reglamento convierte al consentimiento en un mecanismo de control sujeto a requisitos verificables y no en una formalidad administrativa.

3.2 Requisitos para la validez del consentimiento

La validez del consentimiento depende de que la manifestación del titular reúna condiciones suficientes para demostrar una decisión auténtica sobre el tratamiento de sus datos. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 8, establece que el consentimiento debe ser libre, específico, informado e inequívoco. Estos requisitos funcionan de manera conjunta: la ausencia de cualquiera de ellos puede debilitar la legitimidad del tratamiento cuando esta se sustenta precisamente en la autorización del titular. El consentimiento válido, por tanto, no se reduce a una aceptación formal, sino que requiere condiciones materiales que permitan comprobar que la persona comprendió y autorizó efectivamente el tratamiento.

La libertad exige que el titular pueda decidir sin presiones, condicionamientos indebidos o consecuencias desproporcionadas derivadas de negarse. Una aceptación obtenida en un contexto donde el usuario carece de alternativas reales puede resultar problemática, aunque exista una manifestación formal. El artículo 8 de la Ley Orgánica de Protección de Datos Personales (2021) exige que el consentimiento se encuentre libre de vicios. Esta condición resulta especialmente importante cuando se tratan datos íntimos o sensibles mediante aplicaciones digitales, pues la relación entre acceso al servicio y autorización para usos adicionales puede afectar la autonomía de la decisión. El análisis de *menstruapps* evidencia precisamente estas tensiones (Alaattinoğlu, 2022).

La especificidad exige que el consentimiento se refiera a finalidades concretas y suficientemente delimitadas. El titular debe poder distinguir para qué operaciones está autorizando el uso de sus datos y no quedar sometido a fórmulas generales que permitan tratamientos indefinidos. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 8, dispone que el consentimiento debe ser específico respecto de los medios y fines del tratamiento. Esta exigencia impide agrupar de manera indiscriminada finalidades diferentes dentro de una sola autorización. Cuando existen varios propósitos claramente diferenciables, la persona debe poder comprenderlos y decidir sobre ellos sin que una aceptación genérica absorba actividades posteriores no previstas.

El carácter informado requiere que la decisión se adopte después de recibir información comprensible sobre las condiciones esenciales del tratamiento. Esta exigencia se relaciona directamente con el artículo 12 de la Ley Orgánica de Protección de Datos Personales (2021), que reconoce al titular el derecho a conocer finalidades, base jurídica, tiempo de conservación, tipos de tratamiento y destinatarios, entre otros elementos. La información debe proporcionarse antes de obtener la autorización y no después de iniciar el tratamiento. La transparencia cumple aquí una función sustantiva: permite que el consentimiento se base en conocimiento real y no únicamente en la aceptación mecánica de términos extensos o difíciles de interpretar.

La inequívocidad exige que la conducta del titular permita concluir claramente que autorizó el tratamiento. El Reglamento General a la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo No. 904, 2023), en su artículo 5, desarrolla esta condición al exigir una declaración, pronunciamiento o acción afirmativa clara que refleje indudablemente la aceptación. Esta regla excluye interpretaciones basadas exclusivamente en silencio o inactividad cuando no existe una manifestación suficiente de voluntad. La exigencia resulta particularmente relevante en interfaces digitales, donde el diseño de botones, casillas o configuraciones puede influir en la decisión del usuario y generar dudas sobre si la aceptación fue realmente consciente.

Tabla 7

Requisitos para la validez del consentimiento en el tratamiento de datos personales

Requisito	Contenido jurídico	Riesgo si no se cumple
Libertad	La decisión debe adoptarse sin presión ni condicionamiento indebido.	El consentimiento puede no reflejar una voluntad auténtica.
Especificidad	La autorización debe referirse a finalidades y medios determinados.	Se habilitan usos más amplios de los que el titular pretendía aceptar.
Información previa	El titular debe conocer las condiciones esenciales antes de decidir.	La aceptación se produce sin comprensión suficiente del tratamiento.
Inequivocidad	Debe existir una manifestación clara de aceptación.	Puede confundirse silencio o inactividad con autorización.
Expresividad reforzada	Determinados tratamientos, como los relativos a datos sensibles, exigen consentimiento explícito cuando esta sea la base aplicable.	Se reduce la protección frente a tratamientos de mayor impacto.
Demostrabilidad	El responsable debe poder acreditar que obtuvo válidamente el consentimiento.	Dificultad para demostrar la legitimidad del tratamiento.

Requisito	Contenido jurídico	Riesgo si no se cumple
Revocabilidad	El titular debe poder retirar posteriormente su autorización.	La aceptación se transforma en una autorización prácticamente permanente.

Nota. La tabla organiza las condiciones que permiten diferenciar una autorización jurídicamente válida de una aceptación meramente formal o insuficientemente informada.

La demostrabilidad constituye otro elemento relevante porque la validez no debe presumirse únicamente por la afirmación del responsable. El Reglamento General a la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo No. 904, 2023), en su artículo 5, establece que el responsable debe estar en condiciones de demostrar el consentimiento obtenido. En entornos digitales, esta obligación exige conservar registros suficientes sobre la acción afirmativa realizada, las condiciones presentadas y la versión de la información disponible en ese momento. La trazabilidad permite verificar posteriormente si el consentimiento existió realmente y si correspondía a las finalidades para las que los datos fueron utilizados.

Cuando se tratan datos sensibles, los requisitos se intensifican debido a las posibles consecuencias sobre la intimidad, igualdad y otros derechos. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 26, el tratamiento de datos sensibles está prohibido como regla general, salvo que concurra alguna de las excepciones previstas, entre ellas el consentimiento explícito del titular para fines claramente especificados. Esta exigencia obliga a diferenciar entre una aceptación genérica y una manifestación expresa respecto de información especialmente protegida. El estudio de aplicaciones que recopilan datos íntimos demuestra que la sensibilidad de la información condiciona la calidad y profundidad que debe tener la autorización (Alaattinoğlu, 2022).

La revocabilidad completa el conjunto de condiciones porque el consentimiento no produce una autorización irrevocable. El artículo 8 de la Ley Orgánica de Protección de Datos Personales (2021) reconoce al titular la posibilidad de retirar su consentimiento en cualquier momento y exige que existan mecanismos gratuitos, ágiles y sencillos para hacerlo. Esta facultad preserva la capacidad de decisión durante el tratamiento y no únicamente en el momento inicial. La retirada obliga a revisar las operaciones cuya legitimidad dependía de la autorización, aunque no convierte automáticamente en ilícito el tratamiento realizado con anterioridad mientras el consentimiento válido se encontraba vigente.

La validez del consentimiento debe evaluarse, en consecuencia, a partir de las condiciones reales en las que se obtuvo y de la forma en que se documentó, utilizó y mantuvo posteriormente. Libertad, especificidad, información e inequívocidad constituyen exigencias

sustantivas y no simples formalidades. La existencia de un registro electrónico de aceptación no demuestra por sí sola que el titular comprendió el tratamiento o dispuso de una alternativa efectiva. En servicios digitales complejos, la evaluación jurídica debe considerar también el diseño de la interfaz, la claridad de las finalidades y la facilidad para revocar la autorización, de modo que el consentimiento conserve su función como expresión auténtica de autodeterminación informativa.

Figura 6

Requisitos para la validez del consentimiento en el tratamiento de datos personales



Nota. El esquema sintetiza las condiciones esenciales que permiten considerar válido el consentimiento y destaca su relación con el control que conserva el titular sobre el uso de sus datos personales.

3.3 Información previa y deber de transparencia frente al titular

La información previa constituye una condición esencial para que el titular comprenda cómo serán tratados sus datos personales antes de que la organización inicie determinadas operaciones. Su finalidad no consiste únicamente en cumplir una formalidad documental, sino en reducir la asimetría existente entre quien recopila la información y quien la proporciona. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, reconoce el derecho del titular a recibir información clara sobre el tratamiento. Esta exigencia permite que la persona conozca qué datos serán utilizados, con qué propósito, durante cuánto tiempo y bajo qué condiciones jurídicas se desarrollará el tratamiento.

La transparencia exige que esa información sea accesible, comprensible y suficientemente precisa. Una política extensa o redactada con lenguaje excesivamente técnico puede cumplir formalmente con la obligación de informar y, sin embargo, dificultar la comprensión real del titular. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, incorpora la transparencia como uno de los principios rectores del tratamiento y exige que la información relacionada con los datos personales sea clara y de fácil comprensión. Este principio adquiere especial relevancia en plataformas digitales donde múltiples operaciones se ejecutan en segundo plano y no siempre resultan visibles para el usuario.

El contenido de la información previa debe permitir identificar los elementos esenciales del tratamiento. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, el titular debe conocer, entre otros aspectos, las finalidades, la base jurídica, los tipos de tratamiento, el tiempo de conservación, la identidad y datos de contacto del responsable, los destinatarios o categorías de destinatarios y la posibilidad de ejercer sus derechos. Esta obligación permite que la persona evalúe las consecuencias del tratamiento antes de proporcionar información o continuar utilizando un servicio. La transparencia, por tanto, debe reflejar las condiciones reales de funcionamiento y no únicamente declaraciones generales.

El deber de informar adquiere mayor complejidad cuando intervienen sistemas automatizados o inteligencia artificial. En estos casos, el titular puede conocer que sus datos serán utilizados, pero no comprender cómo se generarán perfiles, inferencias o decisiones. La literatura sobre divulgaciones relacionadas con inteligencia artificial muestra que muchas organizaciones proporcionan información limitada o poco útil sobre la lógica y consecuencias del tratamiento automatizado, lo que reduce la capacidad de comprensión del usuario (Wulf & Seizov, 2024).

La transparencia debe incluir, por tanto, información suficientemente significativa sobre el funcionamiento del tratamiento cuando este pueda producir efectos relevantes sobre la persona.

La información previa también debe mantenerse actualizada cuando cambian las condiciones del tratamiento. Si una organización incorpora nuevas finalidades, nuevos destinatarios o modifica de forma sustancial el uso de los datos, la información proporcionada inicialmente puede dejar de ser suficiente. El principio de transparencia exige coherencia entre lo comunicado y lo efectivamente realizado. Cuando el tratamiento se amplía sin informar adecuadamente al titular, se debilita la capacidad de control y se afecta la legitimidad de las decisiones adoptadas sobre los datos. Esta necesidad de información permanente resulta especialmente evidente en servicios digitales que evolucionan rápidamente y añaden nuevas funciones o mecanismos de análisis.

Tabla 8

Contenido de la información previa al titular

Elemento informativo	Contenido que debe comunicarse	Finalidad
Identidad del responsable	Nombre y datos de contacto de quien determina el tratamiento.	Permitir identificar al sujeto responsable.
Finalidad	Propósitos específicos para los que se utilizarán los datos.	Delimitar los usos legítimos de la información.
Base jurídica	Fundamento que habilita el tratamiento.	Explicar por qué la operación resulta jurídicamente válida.
Tipo de tratamiento	Operaciones principales realizadas sobre los datos.	Permitir comprender cómo se utilizará la información.
Conservación	Tiempo previsto o criterios utilizados para determinarlo.	Evitar retenciones indefinidas o desconocidas.
Destinatarios	Personas o categorías de terceros que recibirán los datos.	Informar sobre la circulación de la información.
Derechos del titular	Acceso, rectificación, eliminación, oposición y demás derechos aplicables.	Facilitar su ejercicio efectivo.
Tratamiento automatizado	Existencia de perfilado o decisiones automatizadas cuando corresponda.	Permitir comprender posibles efectos del sistema.

Nota. La tabla organiza los elementos que permiten al titular conocer de manera anticipada las condiciones esenciales bajo las cuales serán tratados sus datos personales.

La transparencia no se limita a entregar información, sino que exige que esta sea útil para adoptar decisiones y ejercer derechos. La investigación sobre divulgaciones de inteligencia artificial obligatorias en materia de protección de datos muestra que las organizaciones pueden cumplir parcialmente con requisitos formales y, al mismo tiempo, ofrecer explicaciones que no permiten comprender suficientemente el tratamiento (Wulf & Seizov, 2024). Este problema

demuestra que la calidad de la información resulta tan importante como su existencia. Una comunicación jurídicamente adecuada debe permitir que el titular identifique los elementos relevantes sin necesidad de interpretar documentos técnicos o ambiguos.

La transparencia adquiere una dimensión adicional cuando la información no ha sido obtenida directamente del titular. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 12, contempla la necesidad de informar sobre el origen de los datos cuando estos provienen de otras fuentes. Esta exigencia resulta especialmente relevante en entornos donde empresas reciben información de proveedores, plataformas asociadas o bases de datos externas. Si el titular desconoce cómo una organización obtuvo sus datos, se dificulta el ejercicio de acceso, rectificación u oposición. La trazabilidad del origen constituye, por tanto, una condición necesaria para mantener control sobre la circulación de información personal.

El deber de transparencia también se relaciona con las decisiones automatizadas. Los estudios sobre información significativa en sistemas algorítmicos muestran que la persona necesita comprender, al menos en términos funcionales, qué lógica interviene y qué consecuencias puede generar el tratamiento sobre su situación (Dexe et al., 2022). Esta exigencia no implica revelar necesariamente todos los detalles técnicos del algoritmo, pero sí proporcionar información suficiente para que el titular pueda evaluar la decisión, cuestionarla o ejercer los derechos correspondientes. La opacidad tecnológica no debe convertirse en una barrera para el ejercicio de garantías reconocidas por la normativa de protección de datos.

La información previa y la transparencia constituyen, en consecuencia, condiciones que acompañan todo el tratamiento y no únicamente el momento inicial de recopilación. Su función es permitir que el titular conozca quién utiliza sus datos, con qué fundamento, para qué finalidad, durante cuánto tiempo y con qué posibles consecuencias. En tratamientos digitales y automatizados, esta obligación adquiere mayor importancia debido a la complejidad técnica y a la participación de múltiples actores. La protección efectiva exige que la información jurídica y técnica se traduzca en explicaciones comprensibles que permitan ejercer control real sobre los datos personales y reaccionar frente a usos incompatibles con los derechos del titular (Wulf & Seizov, 2024; Dexe et al., 2022).

3.4 Derecho de acceso a los datos personales

El derecho de acceso permite que el titular conozca qué información personal mantiene una organización sobre él y comprenda las condiciones en las que esa información está siendo tratada. Su ejercicio constituye una herramienta básica de control porque posibilita verificar la

existencia de datos, identificar posibles errores y conocer las finalidades asociadas al tratamiento. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 13, reconoce al titular el derecho a conocer y obtener gratuitamente del responsable acceso a todos sus datos personales, así como a la información prevista en el artículo precedente, sin necesidad de presentar una justificación para ejercerlo.

El acceso se relaciona directamente con la autodeterminación informativa porque una persona difícilmente puede controlar información que desconoce. La Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, reconoce expresamente que el derecho a la protección de datos personales incluye el acceso y la decisión sobre información y datos de esta naturaleza. Esta garantía constitucional otorga al acceso una dimensión que supera la mera consulta administrativa. Conocer los datos que posee una entidad constituye una condición previa para determinar si su recopilación, conservación y utilización resultan compatibles con los derechos del titular y con las finalidades que justificaron originalmente el tratamiento.

El artículo 13 de la Ley Orgánica de Protección de Datos Personales (2021) establece además que el acceso debe proporcionarse gratuitamente. Esta característica evita que los costos económicos se conviertan en una barrera para conocer la información propia. La misma disposición determina que el titular no necesita justificar por qué solicita acceso, lo que refuerza el carácter autónomo del derecho. El responsable debe establecer métodos razonables para facilitar su ejercicio y atender la solicitud dentro del plazo de quince días. De este modo, la legislación no se limita a reconocer una facultad abstracta, sino que incorpora condiciones concretas destinadas a garantizar una respuesta efectiva.

El contenido del acceso comprende más que la entrega aislada de los datos almacenados. Al remitirse al artículo 12 de la Ley Orgánica de Protección de Datos Personales (2021), el artículo 13 permite conocer también información relacionada con finalidades, base jurídica, tiempo de conservación, destinatarios y características relevantes del tratamiento. Esta amplitud es necesaria porque un listado de datos puede resultar insuficiente para comprender cómo afectan realmente al titular. El derecho adquiere sentido cuando permite reconstruir el contexto del tratamiento y establecer quién utiliza la información, para qué propósito y durante cuánto tiempo, facilitando posteriormente el ejercicio de rectificación, eliminación u oposición cuando resulte procedente.

En entornos automatizados, el acceso adquiere una complejidad adicional porque el titular puede solicitar información relacionada con procesos que generan perfiles o decisiones a partir

de sus datos. Custers y Heijne (2022) muestran que el alcance del derecho de acceso frente a decisiones automatizadas plantea interrogantes sobre qué información debe proporcionarse acerca de la lógica utilizada, los datos considerados y los efectos previstos. El problema no consiste únicamente en entregar registros existentes, sino en ofrecer información suficientemente útil para comprender cómo intervienen los datos personales dentro del procedimiento automatizado. El acceso cumple así una función de transparencia frente a sistemas cuya operación puede resultar difícil de observar externamente.

La posibilidad de comprender el tratamiento automatizado también depende de la calidad de las explicaciones proporcionadas. Las investigaciones sobre decisiones algorítmicas evidencian que la información ofrecida al titular puede variar considerablemente entre organizaciones y jurisdicciones, especialmente respecto de la lógica y significado de los resultados producidos (Dexe et al., 2022). Una respuesta excesivamente general puede satisfacer formalmente una solicitud sin permitir que la persona comprenda realmente cómo se utilizó su información. El derecho de acceso exige, por ello, un equilibrio entre la complejidad técnica del sistema y la necesidad de proporcionar información inteligible que permita evaluar las consecuencias del tratamiento sobre la situación individual.

La transparencia de las respuestas es igualmente relevante en sistemas de inteligencia artificial. Wulf y Seizov (2024) identifican limitaciones en determinadas comunicaciones realizadas para explicar tratamientos automatizados, particularmente cuando las organizaciones alegan que no pueden proporcionar mayor información. Esta dificultad demuestra que reconocer jurídicamente un derecho de acceso no garantiza por sí mismo su utilidad práctica. La información debe ser suficientemente concreta para permitir al titular entender las operaciones que afectan sus datos. Cuando la respuesta se limita a descripciones genéricas del sistema o evita explicar los elementos relevantes del tratamiento, disminuye la capacidad de la persona para cuestionar resultados y ejercer otros derechos derivados.

El acceso también cuenta con protección jurisdiccional en Ecuador mediante la acción de hábeas data. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 92, toda persona tiene derecho a conocer la existencia y acceder a documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma o sus bienes consten en entidades públicas o privadas. Esta garantía amplía la protección cuando el acceso no puede obtenerse mediante los mecanismos ordinarios. La Constitución permite además conocer el uso, finalidad, origen, destino y tiempo de vigencia de los archivos o bancos donde permanece la información personal.

La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), en su artículo 49, desarrolla esta garantía y establece que la acción de hábeas data tiene como objeto garantizar judicialmente el acceso a documentos, datos genéticos, bancos o archivos de datos personales que se encuentren en poder de entidades públicas o personas naturales o jurídicas privadas. La disposición reconoce también el derecho a conocer el uso de la información, su finalidad, origen, destino y tiempo de vigencia. Esta protección permite que el titular disponga de una vía jurisdiccional cuando el control sobre sus propios datos no pueda ejercerse adecuadamente mediante una solicitud directa.

La legislación establece, sin embargo, que el derecho de acceso tampoco puede utilizarse abusivamente. El artículo 13 de la Ley Orgánica de Protección de Datos Personales (2021) dispone expresamente que su ejercicio no podrá efectuarse de forma que constituya abuso del derecho. Esta limitación no altera su carácter fundamental, pero permite evitar solicitudes utilizadas de manera manifiestamente contraria a su finalidad. El responsable debe diferenciar entre una solicitud legítima, incluso cuando sea amplia, y un comportamiento abusivo debidamente acreditado. La existencia de esta limitación exige una interpretación cuidadosa para impedir que se utilice como argumento general para dificultar o restringir injustificadamente el acceso del titular.

El derecho de acceso funciona finalmente como punto de conexión con otros derechos de protección de datos. Una persona necesita conocer qué información existe antes de determinar si debe solicitar su rectificación, actualización, eliminación o cuestionar una decisión automatizada. Su eficacia depende de que la respuesta sea gratuita, completa, comprensible y proporcionada dentro del plazo legal. En sistemas digitales complejos, el acceso permite hacer visible un tratamiento que normalmente permanece bajo control técnico de organizaciones y plataformas. Por esta razón, constituye una garantía esencial para reducir la asimetría informativa y proporcionar al titular herramientas concretas para supervisar el uso de sus datos personales (Custers & Heijne, 2022; Dexe et al., 2022).

3.5 Rectificación y actualización de información personal

El derecho de rectificación y actualización permite al titular corregir información personal que no refleja adecuadamente su situación. Su importancia radica en que los datos almacenados por instituciones y plataformas pueden influir en decisiones administrativas, comerciales, laborales o automatizadas, por lo que una información incorrecta puede producir consecuencias concretas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 14,

reconoce el derecho a obtener del responsable la rectificación y actualización de los datos personales inexactos o incompletos. Esta facultad constituye una expresión del control del titular sobre su información y obliga a mantener correspondencia entre los registros utilizados y la realidad que pretenden representar.

La rectificación se aplica cuando la información registrada presenta errores, mientras que la actualización responde a datos que fueron correctos inicialmente, pero dejaron de reflejar una situación vigente. Esta diferencia resulta relevante en bases que contienen domicilios, información laboral, datos de contacto, antecedentes administrativos o cualquier otro registro susceptible de modificarse con el tiempo. El artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021), mediante el principio de calidad y exactitud, exige que los datos sean exactos, íntegros, precisos, completos, comprobables y, cuando corresponda, debidamente actualizados. La obligación alcanza así tanto la corrección de errores como el mantenimiento adecuado de la información utilizada.

La capacidad de corregir los datos tiene además fundamento constitucional. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 66, numeral 19, el derecho a la protección de datos personales comprende el acceso y la decisión sobre información de este carácter. La posibilidad de decidir perdería eficacia si el titular pudiera conocer que un registro es incorrecto, pero careciera de mecanismos para modificarlo. La rectificación complementa, por tanto, al derecho de acceso: primero permite identificar qué información posee una entidad y posteriormente posibilita corregir aquella que resulte falsa, incompleta o desactualizada. Ambos derechos fortalecen la capacidad individual de controlar la representación informativa de la propia persona.

El ejercicio del derecho está sujeto a un procedimiento que permite al responsable verificar la modificación solicitada. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 14, señala que el titular deberá presentar los justificativos correspondientes cuando resulte pertinente y dispone que el responsable atienda el requerimiento dentro de quince días. Esta exigencia busca evitar modificaciones arbitrarias y garantizar que los registros mantengan calidad y veracidad. La presentación de justificativos no debe transformarse, sin embargo, en una barrera desproporcionada para corregir errores evidentes. El procedimiento debe orientarse a comprobar la información necesaria y resolver efectivamente la inconsistencia detectada por el titular.

La corrección también debe extenderse a quienes hayan recibido previamente los datos. El artículo 14 de la Ley Orgánica de Protección de Datos Personales (2021) establece que, dentro del mismo plazo previsto para atender la solicitud, el responsable debe informar al destinatario sobre la rectificación para que este actualice la información correspondiente. Esta obligación resulta esencial en ecosistemas digitales donde un dato puede haber sido comunicado a diferentes organizaciones o incorporado a múltiples sistemas. Corregir únicamente la base original dejaría subsistente el error en otros registros. La actualización efectiva exige, por ello, mecanismos de trazabilidad capaces de identificar a los destinatarios y comunicar oportunamente las modificaciones realizadas.

La exactitud adquiere mayor relevancia cuando los datos intervienen en sistemas automatizados. Una información incorrecta puede incorporarse a perfiles, clasificaciones o decisiones y producir resultados aparentemente objetivos que parten de premisas equivocadas. Custers y Heijne (2022) muestran que el ejercicio de los derechos sobre datos utilizados en decisiones automatizadas presenta dificultades particulares debido a la necesidad de conocer qué información intervino en el proceso y cómo fue utilizada. En estos contextos, el acceso y la rectificación mantienen una relación estrecha: el titular necesita identificar los datos empleados para poder cuestionar aquellos que sean incorrectos y reducir la posibilidad de que el sistema reproduzca continuamente una clasificación basada en información defectuosa.

La actualización también resulta necesaria porque la exactitud de un dato depende del contexto temporal. Una dirección, condición laboral, situación económica o circunstancia personal puede modificarse y convertir un registro anteriormente correcto en información desactualizada. El principio de calidad y exactitud previsto en el artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021) exige adoptar medidas razonables para rectificar o suprimir sin dilación los datos inexactos respecto de las finalidades para las que son tratados. La obligación no debe entenderse exclusivamente como una respuesta a solicitudes individuales, sino también como un criterio para que los responsables gestionen preventivamente la calidad de sus bases de información.

La rectificación adquiere particular importancia cuando una organización utiliza datos para adoptar decisiones que afectan significativamente al titular. En sistemas automatizados, una variable incorrecta puede modificar una valoración y trasladar el error a resultados posteriores. Las investigaciones sobre información y decisiones automatizadas evidencian que la posibilidad de comprender los datos considerados constituye una condición para cuestionar adecuadamente los resultados producidos por estos sistemas (Dexe et al., 2022). La corrección

de datos debe realizarse antes de que información incorrecta continúe siendo utilizada en nuevas operaciones. De lo contrario, el error inicial puede adquirir mayor alcance mediante la automatización y afectar sucesivamente distintas decisiones relacionadas con una misma persona.

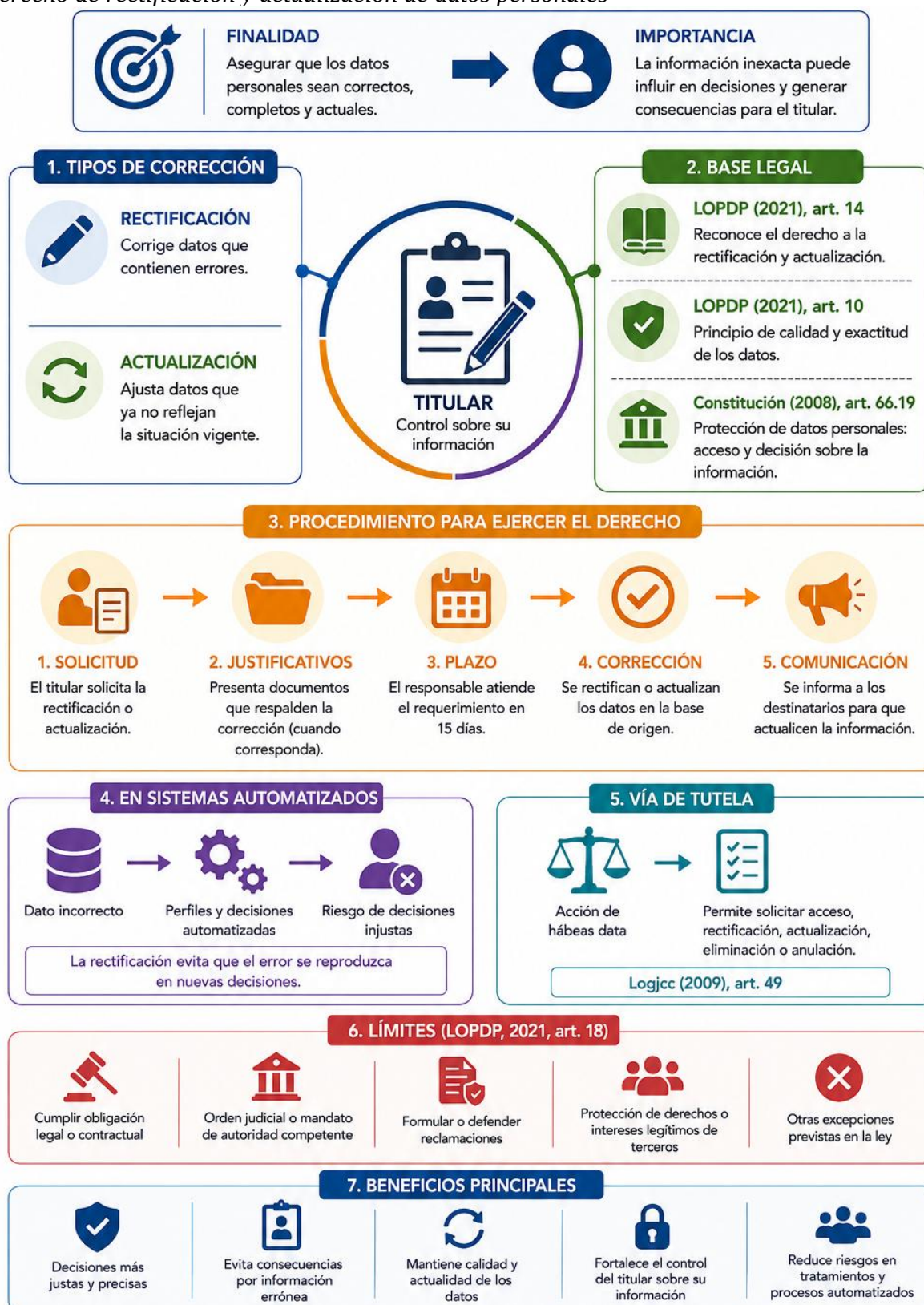
El derecho de rectificación cuenta también con una vía de tutela constitucional. De acuerdo con la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), en su artículo 49, la acción de hábeas data permite acceder a datos personales y solicitar su actualización, rectificación, eliminación o anulación cuando corresponda. Esta garantía resulta relevante cuando el responsable no atiende adecuadamente una solicitud o persiste una afectación relacionada con información personal. La existencia de una vía jurisdiccional refuerza el carácter exigible del derecho y evita que la corrección dependa exclusivamente de la voluntad de la entidad que administra la base de datos. La calidad informativa se convierte así en una cuestión jurídicamente tutelable.

El derecho tampoco opera de manera absoluta. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 18, establece excepciones aplicables a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad. Entre ellas se encuentran situaciones en las que los datos resulten necesarios para cumplir una obligación legal o contractual, atender una orden judicial o mandato de autoridad competente, formular o defender reclamaciones, o cuando la solicitud pueda perjudicar derechos o intereses legítimos de terceros en las condiciones previstas por la norma. Estas limitaciones deben aplicarse de manera justificada, pues una excepción no convierte automáticamente en correcta una información que objetivamente resulte inexacta.

La rectificación y actualización cumplen finalmente una función preventiva dentro del sistema de protección de datos. Mantener información correcta reduce la posibilidad de decisiones injustificadas, errores administrativos y tratamientos posteriores basados en registros que ya no representan adecuadamente al titular. En entornos digitales, esta obligación adquiere mayor alcance porque un mismo dato puede replicarse, transferirse o incorporarse a procesos automatizados con rapidez. El derecho exige, por ello, que la corrección produzca efectos sobre las distintas operaciones vinculadas con la información y no únicamente sobre el registro visible para el usuario. La calidad de los datos constituye una condición indispensable para que transparencia, acceso y autodeterminación informativa tengan eficacia práctica.

Figura 7

Derecho de rectificación y actualización de datos personales



Nota. El esquema organiza las principales vías para corregir o actualizar información personal y muestra su relación con el ejercicio del derecho, la tutela jurídica y la prevención de decisiones basadas en datos inexactos o desactualizados.

3.6 Supresión, eliminación y derecho al olvido

El derecho de supresión permite al titular solicitar que determinados datos personales sean eliminados cuando ya no exista una razón legítima para mantenerlos dentro de un sistema de tratamiento. Su finalidad consiste en evitar que la información permanezca disponible de forma indefinida y pueda utilizarse fuera del contexto que justificó su recopilación. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 15, reconoce el derecho a la eliminación cuando el tratamiento no cumpla con los principios previstos en la normativa, haya cumplido su finalidad o haya vencido el plazo de conservación, entre otros supuestos establecidos legalmente.

La eliminación se relaciona directamente con el principio de conservación. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, establece que los datos deben conservarse únicamente durante el tiempo necesario para cumplir las finalidades que justificaron su tratamiento. Cuando esa finalidad desaparece, la permanencia de la información requiere una nueva justificación jurídica. Este criterio resulta especialmente importante en entornos digitales, donde la capacidad técnica permite conservar grandes volúmenes de información durante períodos prolongados. Mantener datos sin necesidad incrementa los riesgos de acceso, reutilización, filtración o combinación con otros registros y debilita el control del titular sobre su propia información.

El derecho al olvido se vincula con la posibilidad de limitar la permanencia o difusión de información personal cuando su mantenimiento ya no resulta justificado. No debe entenderse como un derecho absoluto a borrar cualquier referencia sobre una persona, porque su aplicación exige ponderar otros derechos y obligaciones. En entornos digitales, este derecho adquiere relevancia debido a la capacidad de los buscadores, redes sociales y plataformas para mantener accesible información durante largos períodos. El análisis del sharenting muestra que contenidos difundidos por terceros pueden permanecer disponibles y afectar posteriormente a la persona concernida, especialmente cuando se trata de menores cuyos datos fueron publicados sin una decisión propia suficientemente formada (Bessant & Schnebbe, 2022).

La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 15, contempla distintos supuestos que pueden justificar la eliminación. Entre ellos se encuentran el incumplimiento de principios, la desaparición de la finalidad, el vencimiento del plazo de conservación y la revocación del consentimiento cuando no exista otra base que legitime el tratamiento. La supresión no depende, por tanto, únicamente de que el titular cambie de

opinión, sino también de que desaparezcan las condiciones jurídicas que justificaban mantener los datos. Esta regulación obliga al responsable a revisar la vigencia de las finalidades y evita que la información se convierta en un activo conservado automáticamente por tiempo indefinido.

La eliminación efectiva puede resultar técnicamente compleja cuando los datos han sido replicados, transferidos o almacenados en diferentes sistemas. Una misma información puede encontrarse en bases operativas, respaldos, servicios en la nube o sistemas de terceros. Por ello, la supresión no debe limitarse a ocultar el dato en la interfaz visible para el usuario. El responsable debe identificar dónde permanece almacenada la información y aplicar procedimientos que permitan retirar o bloquear su utilización cuando corresponda. Esta exigencia se vuelve especialmente relevante en plataformas digitales, donde la circulación de datos puede ser amplia y la trazabilidad resulta indispensable para garantizar que la eliminación produzca efectos reales.

Tabla 9
Supuestos y efectos de la supresión de datos personales

Supuesto	Fundamento	Efecto esperado
Finalidad cumplida	El dato dejó de ser necesario para el propósito original.	Eliminación o bloqueo de la información.
Plazo de conservación vencido	Ya no existe justificación temporal para mantener el dato.	Retiro del registro de los sistemas activos.
Tratamiento contrario a principios	Se incumplen legalidad, finalidad, minimización u otros principios.	Cese del tratamiento y eliminación cuando proceda.
Revocación del consentimiento	El titular retira la autorización y no existe otra base jurídica.	Interrupción del tratamiento sustentado en consentimiento.
Datos desactualizados o innecesarios	La información dejó de ser pertinente.	Revisión y eventual eliminación.
Publicación digital persistente	La información continúa accesible sin justificación suficiente.	Evaluación de retiro, desindexación o supresión.
Existencia de obligación legal	La conservación sigue siendo exigida por una norma.	El dato puede mantenerse mientras subsista la obligación.

Nota. La tabla diferencia los principales escenarios en los que la supresión puede resultar procedente y los casos en que la conservación puede mantenerse por una obligación jurídica.

El derecho de supresión no opera de manera automática en todos los casos. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 18, establece excepciones aplicables cuando la información resulta necesaria para cumplir una obligación legal o contractual, atender una orden judicial, formular o defender reclamaciones o proteger determinados derechos e intereses legítimos. Estas limitaciones muestran que la eliminación exige analizar el contexto jurídico completo. Una solicitud puede ser legítima y, sin embargo, no producir una

supresión inmediata si existe una obligación superior que justifique temporalmente la conservación de los datos.

La supresión también se relaciona con el derecho a la intimidad y con la posibilidad de evitar que información antigua continúe condicionando la vida presente de una persona. Este problema adquiere especial relevancia en redes sociales y plataformas donde contenidos publicados años atrás pueden permanecer accesibles mediante búsquedas o replicaciones. Bessant y Schnebbe (2022) muestran que el derecho de eliminación puede funcionar como una herramienta importante frente a contenidos difundidos por terceros, aunque su efectividad depende de factores como la edad del titular, el contexto de publicación y la existencia de otros intereses jurídicamente protegidos.

La acción de hábeas data ofrece además una vía de tutela cuando una persona necesita obtener la eliminación de información que permanece en archivos o bases de datos. De acuerdo con la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), en su artículo 49, esta garantía permite solicitar actualización, rectificación, eliminación o anulación de datos personales cuando corresponda. La posibilidad de acudir a una vía jurisdiccional refuerza el carácter exigible de la supresión y evita que la eliminación dependa únicamente de procedimientos internos de la entidad responsable.

La supresión y el derecho al olvido cumplen, finalmente, una función de equilibrio entre memoria digital y control individual. La tecnología facilita que la información permanezca disponible durante períodos muy superiores a los previstos inicialmente, pero esa capacidad no convierte la conservación en jurídicamente legítima. La protección de datos exige revisar periódicamente la necesidad de mantener información y garantizar mecanismos eficaces para retirarla cuando desaparezca su fundamento. En este sentido, la eliminación no constituye una negación de la memoria, sino una herramienta para evitar que datos innecesarios continúen produciendo efectos sobre la vida privada y la autonomía del titular.

3.7 Oposición y limitación del tratamiento de datos personales

El derecho de oposición permite al titular manifestar que no desea que sus datos continúen siendo tratados en determinadas circunstancias. Su función consiste en preservar la capacidad de control cuando el tratamiento, aunque inicialmente pueda contar con una base jurídica, entra en conflicto con intereses, derechos o libertades de la persona. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 16, reconoce expresamente el derecho a oponerse o negarse al tratamiento en los casos previstos por la norma. Esta facultad resulta especialmente

relevante cuando el tratamiento se basa en interés legítimo o cuando los datos son utilizados para actividades de mercadotecnia directa.

La oposición no produce los mismos efectos en todos los supuestos. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 16, el titular puede oponerse cuando la ley lo permita, siempre que no se afecten derechos y libertades fundamentales de terceros y no se trate de información pública, de interés público o cuyo tratamiento esté ordenado legalmente. La norma también contempla la oposición frente a tratamientos sustentados en interés legítimo, siempre que la persona justifique su situación concreta. Esta regulación exige ponderar las razones del titular frente a los motivos que sustentan la continuidad del tratamiento.

La mercadotecnia directa constituye uno de los ámbitos en los que el derecho de oposición recibe una protección especialmente clara. El artículo 16 de la Ley Orgánica de Protección de Datos Personales (2021) establece que el titular puede oponerse en cualquier momento al tratamiento de sus datos con fines de mercadotecnia directa, incluida la elaboración de perfiles vinculada con esos propósitos. Cuando se ejerce este derecho, los datos deben dejar de ser tratados para dichas finalidades. Esta previsión limita la posibilidad de mantener campañas comerciales o segmentaciones dirigidas contra la voluntad expresa de la persona y refuerza su capacidad para controlar usos secundarios de información personal.

La limitación o suspensión del tratamiento cumple una función distinta a la oposición. En lugar de exigir necesariamente la eliminación definitiva de los datos, permite restringir temporalmente determinadas operaciones mientras se resuelve una circunstancia concreta. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 19, reconoce el derecho a obtener la suspensión cuando el titular impugna la exactitud de los datos, cuando el tratamiento es ilícito y prefiere limitar su uso antes que eliminarlos, cuando necesita conservarlos para formular o defender reclamaciones o mientras se resuelve una oposición. Esta medida evita que el tratamiento continúe produciendo efectos durante una controversia.

La oposición y la suspensión protegen al titular de manera complementaria. La primera cuestiona la legitimidad de continuar determinados tratamientos, mientras que la segunda restringe temporalmente su utilización sin eliminar necesariamente la información. Esta diferencia resulta importante en entornos digitales, donde los datos pueden intervenir en múltiples operaciones simultáneas. La suspensión puede ser adecuada cuando todavía debe verificarse la exactitud de un registro o resolverse una reclamación. Custers y Heijne (2022)

muestran que el ejercicio de derechos frente a tratamientos automatizados depende en gran medida de que las personas puedan conocer y cuestionar cómo sus datos intervienen en procesos que producen consecuencias sobre ellas.

Tabla 10

Diferencias entre oposición y limitación del tratamiento de datos personales

Derecho	Supuesto principal	Efecto sobre el tratamiento	Finalidad protectora
Oposición general	El titular cuestiona un tratamiento permitido por la ley en las condiciones previstas.	Puede determinar el cese del tratamiento.	Proteger intereses, derechos y libertades del titular.
Oposición a mercadotecnia directa	Los datos se utilizan para publicidad o perfilado asociado.	El tratamiento debe cesar para esos fines.	Evitar usos comerciales contrarios a la voluntad del titular.
Oposición frente a interés legítimo	El tratamiento se sustenta en interés legítimo y existe una situación particular del titular.	Requiere ponderar los intereses en conflicto.	Evitar afectaciones desproporcionadas.
Suspensión por inexactitud	El titular cuestiona la exactitud de los datos.	Se limita el uso mientras se verifica la información.	Evitar decisiones basadas en datos posiblemente incorrectos.
Suspensión por tratamiento ilícito	El titular rechaza la supresión y solicita limitar el uso.	Los datos permanecen, pero su utilización queda restringida.	Conservar información sin permitir un tratamiento amplio.
Suspensión por reclamaciones	Los datos ya no son necesarios para el responsable, pero sí para el titular.	Se mantienen para fines de reclamación.	Preservar medios necesarios para ejercer derechos.
Suspensión durante una oposición	Se discute si prevalecen los motivos del responsable o del titular.	El tratamiento se restringe mientras se resuelve la controversia.	Evitar efectos mientras se determina la legitimidad del tratamiento.

Nota. La tabla diferencia los efectos de la oposición y de la suspensión según la causa que justifica restringir o detener el tratamiento de datos personales.

El responsable no puede ignorar automáticamente una oposición basada en una situación particular del titular. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 16, establece que deberá dejar de tratar los datos salvo que demuestre motivos legítimos e imperiosos que prevalezcan sobre los intereses, derechos y libertades de la persona o que resulten necesarios para formular, ejercer o defender reclamaciones. La solicitud debe ser atendida dentro de quince días. Este mecanismo introduce una carga de justificación para la

continuidad del tratamiento y exige que el responsable explique por qué sus motivos deben prevalecer en el caso concreto.

La suspensión implica además restricciones concretas sobre el uso de la información. Según el artículo 19 de la Ley Orgánica de Protección de Datos Personales (2021), los datos sometidos a suspensión solo pueden tratarse en determinados supuestos, como la formulación, ejercicio o defensa de reclamaciones, la protección de derechos de otra persona o razones importantes de interés público. Cuando el titular impugna la exactitud de los datos, debe dejarse constancia de esa inconformidad mientras se realiza la verificación. Esta regla impide que información controvertida continúe utilizándose normalmente como si su exactitud hubiera sido confirmada.

La aplicación de estos derechos presenta especial relevancia frente a tratamientos automatizados. Una oposición o suspensión puede impedir que datos controvertidos sigan alimentando perfiles o decisiones mientras se evalúa su legitimidad. Las investigaciones sobre transparencia algorítmica muestran que la posibilidad de cuestionar un tratamiento depende de que el titular reciba información suficientemente comprensible sobre cómo se utilizan sus datos y qué consecuencias pueden producirse (Dexe et al., 2022; Wulf & Seizov, 2024). Cuando los procesos son opacos, el ejercicio de oposición pierde eficacia práctica porque la persona puede desconocer incluso que existe un tratamiento susceptible de ser cuestionado.

La oposición y la limitación refuerzan, en consecuencia, la posición activa del titular frente al tratamiento de información personal. No se limitan a permitir acceso o corrección, sino que ofrecen mecanismos para detener o restringir usos que generan controversias jurídicas. Su efectividad depende de procedimientos claros, respuestas oportunas y una adecuada ponderación entre los intereses del responsable y los derechos de la persona. En sistemas digitales y automatizados, estos mecanismos adquieren mayor relevancia porque una operación puede reproducirse rápidamente y afectar múltiples decisiones. La protección exige, por tanto, que el titular pueda intervenir antes de que un tratamiento cuestionado continúe produciendo consecuencias sobre su esfera jurídica.

3.8 Portabilidad de datos y decisiones automatizadas

La portabilidad de datos permite al titular recibir su información personal en un formato estructurado, de uso común y lectura mecánica, y trasladarla a otro responsable cuando concurren las condiciones previstas por la normativa. Esta facultad busca reducir la dependencia tecnológica respecto de una sola plataforma y facilitar que la persona conserve

cierto control sobre sus datos al cambiar de proveedor o servicio. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 17, reconoce el derecho a la portabilidad y establece que el titular puede solicitar la transmisión de sus datos a otro responsable cuando el tratamiento se base en consentimiento o contrato y se realice por medios automatizados.

La portabilidad no debe confundirse con el simple derecho de acceso. El acceso permite conocer y obtener los datos que mantiene una organización, mientras que la portabilidad añade la posibilidad de recibirlos en condiciones técnicas que faciliten su reutilización o traslado. Esta diferencia resulta especialmente importante en servicios digitales donde la información acumulada puede representar años de actividad, preferencias o configuraciones. Turner y Tanczer (2024) muestran que, en la práctica, los usuarios valoran la portabilidad como una herramienta para reducir barreras al cambio entre servicios, aunque su implementación depende de estándares técnicos y de la capacidad real para transferir información de manera interoperable.

El ejercicio de este derecho está sujeto a determinadas condiciones jurídicas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 17, dispone que la portabilidad procede cuando el tratamiento se basa en consentimiento o contrato y se efectúa mediante medios automatizados. También establece que el derecho no debe afectar negativamente los derechos y libertades de terceros. Estas condiciones evitan interpretar la portabilidad como una obligación irrestricta de trasladar cualquier información contenida en los sistemas. El responsable debe evaluar qué datos corresponden efectivamente al titular y cuáles podrían involucrar información de otras personas o contenidos sometidos a limitaciones jurídicas específicas.

La utilidad práctica de la portabilidad depende también del formato en el que se entregan los datos. Un archivo técnicamente legible, pero difícil de reutilizar, puede reducir el alcance real del derecho. La finalidad consiste en que la información pueda ser utilizada en otro entorno sin procesos desproporcionados de conversión. Turner y Tanczer (2024) identifican precisamente una brecha entre el reconocimiento jurídico del derecho y las dificultades prácticas para ejercerlo en ecosistemas tecnológicos heterogéneos. La interoperabilidad, los formatos estandarizados y la compatibilidad entre servicios se convierten así en condiciones técnicas que influyen directamente en la eficacia jurídica de la portabilidad.

La portabilidad puede contribuir además a fortalecer la autonomía del titular en mercados digitales donde los efectos de dependencia son significativos. Cuando una persona pierde

acceso a su historial, configuraciones o registros al abandonar una plataforma, el costo de cambiar de proveedor aumenta. El derecho permite reducir esa dependencia al facilitar la continuidad de la información bajo otro responsable. Sin embargo, no todas las categorías de datos tienen la misma facilidad de traslado. Información proporcionada directamente por el titular puede ser más sencilla de portar que datos inferidos o perfiles elaborados internamente por un sistema. Esta distinción requiere analizar cuidadosamente el alcance material de la solicitud (Turner & Tanczer, 2024).

Las decisiones automatizadas constituyen otro ámbito relevante dentro de los derechos del titular porque pueden producir efectos jurídicos o consecuencias significativas sin intervención humana sustancial. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 20, reconoce el derecho a no ser objeto de decisiones basadas única o parcialmente en valoraciones automatizadas cuando estas produzcan efectos jurídicos o afecten derechos y libertades fundamentales. La norma introduce así una garantía específica frente a procedimientos que utilizan perfiles, puntuaciones o predicciones para determinar resultados sobre una persona. El objetivo es evitar que la automatización elimine por completo la posibilidad de revisión, explicación o intervención humana.

La transparencia resulta indispensable para que este derecho pueda ejercerse de manera efectiva. Una persona difícilmente puede cuestionar una decisión automatizada si desconoce que fue sometida a un proceso de esa naturaleza. Dexe et al. (2022) señalan que la información significativa sobre la lógica utilizada, la relevancia del tratamiento y sus posibles consecuencias constituye un componente central de la protección frente a decisiones automatizadas. No se trata necesariamente de revelar todos los detalles técnicos del algoritmo, sino de ofrecer una explicación suficiente que permita comprender cómo los datos influyeron en el resultado y qué posibilidades existen para solicitar una revisión.

El derecho de acceso también se conecta directamente con las decisiones automatizadas. Custers y Heijne (2022) analizan cómo el acceso puede utilizarse para conocer la información empleada en procedimientos automatizados y evaluar si la persona recibió una explicación suficiente sobre la lógica aplicada. Esta relación resulta especialmente importante cuando el resultado depende de múltiples variables o de modelos complejos. La posibilidad de acceder a los datos permite identificar errores, información desactualizada o inferencias incorrectas que pudieron influir en la decisión. En este sentido, acceso, rectificación y revisión de decisiones automatizadas funcionan como derechos complementarios dentro del sistema de protección.

La calidad de las explicaciones ofrecidas por las organizaciones también condiciona la eficacia de estas garantías. Wulf y Seizov (2024) muestran que algunas divulgaciones sobre inteligencia artificial pueden ser demasiado generales, incompletas o poco útiles para el titular. Cuando la información se limita a indicar que existe un sistema automatizado sin explicar de manera comprensible su papel en la decisión, la transparencia pierde eficacia práctica. La obligación de informar debe permitir que la persona identifique la existencia del tratamiento automatizado, comprenda sus consecuencias principales y disponga de elementos suficientes para cuestionarlo cuando considere que afecta indebidamente sus derechos.

La portabilidad y las decisiones automatizadas se relacionan en un punto común: ambas buscan reducir la asimetría de poder informacional entre titulares y organizaciones. La primera facilita que la persona pueda trasladar sus datos y disminuir la dependencia respecto de un proveedor; la segunda limita la posibilidad de que sistemas automatizados adopten decisiones relevantes sin mecanismos de explicación o revisión. Estas garantías reflejan una evolución del derecho de protección de datos desde la simple confidencialidad hacia formas más activas de control. El titular no solo debe saber que sus datos están protegidos, sino también disponer de herramientas para moverlos, comprender su uso y cuestionar resultados automatizados.

La eficacia de estos derechos depende finalmente de que existan procedimientos técnicos y jurídicos capaces de hacerlos operativos. La portabilidad requiere formatos compatibles, canales seguros y delimitación clara de los datos transferibles; las decisiones automatizadas exigen transparencia, acceso, revisión y posibilidad de intervención humana cuando corresponda. En ambos casos, la complejidad tecnológica no puede utilizarse como argumento para vaciar de contenido los derechos reconocidos por la normativa. La protección de datos en entornos digitales exige que las capacidades técnicas de las organizaciones se acompañen de mecanismos que permitan al titular conservar control sobre la información y sobre las consecuencias derivadas de su tratamiento.



Capítulo 4

Responsabilidad jurídica por vulneraciones de datos personales

Adriana Carolina Calderón Muñoz

4.1 Vulneraciones de seguridad y exposición de datos personales

Las vulneraciones de seguridad de datos personales comprenden incidentes que afectan la confidencialidad, integridad o disponibilidad de la información y pueden provocar pérdida, alteración, destrucción, acceso o divulgación no autorizada. Su importancia jurídica deriva de que una falla técnica puede transformarse en una afectación directa a los derechos del titular cuando permite que terceros conozcan o utilicen información sin autorización. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, incorpora el principio de seguridad y exige a responsables y encargados adoptar medidas adecuadas frente a riesgos, amenazas y vulnerabilidades. La protección debe responder a la naturaleza y contexto concreto del tratamiento.

La exposición de datos puede originarse por causas diversas, entre ellas errores humanos, configuraciones incorrectas, credenciales comprometidas, ataques informáticos, pérdida de dispositivos o deficiencias en los procedimientos internos. Una vulneración no exige necesariamente que exista intención de causar daño, pues también puede producirse como consecuencia de controles insuficientes. El análisis de comunicaciones posteriores a brechas de datos muestra que la responsabilidad organizacional comprende tanto las condiciones de seguridad existentes antes del incidente como la manera en que se informa y responde después de detectarlo (Thomas et al., 2022). Esta perspectiva obliga a considerar la seguridad como un proceso permanente y no como una actuación posterior al incidente.

La gravedad de una vulneración depende de factores como la cantidad de titulares afectados, la naturaleza de los datos expuestos, la duración del incidente y las posibilidades de utilización posterior de la información. Una filtración de datos identificativos puede producir consecuencias distintas de la exposición de información sanitaria, financiera o especialmente sensible. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, obliga a utilizar metodologías de análisis y gestión de riesgos y a adoptar medidas para prevenir, impedir, reducir, mitigar y controlar las vulneraciones identificadas. Esta obligación exige relacionar las medidas aplicadas con las características específicas de cada tratamiento.

La exposición pública de una brecha introduce además efectos que trascienden la pérdida inmediata de confidencialidad. La divulgación del incidente puede afectar la confianza de usuarios, clientes o pacientes y generar consecuencias económicas o reputacionales para la organización. El análisis de vulneraciones en el sector sanitario muestra que la publicación de brechas puede asociarse con reacciones económicas y con mayores exigencias de respuesta

institucional, especialmente cuando la información comprometida presenta una naturaleza sensible (Bohn & Schiereck, 2023). Estos efectos evidencian que la seguridad de datos forma parte de la gestión jurídica y organizacional, pues una vulneración puede generar consecuencias simultáneas para titulares y responsables.

Las organizaciones también enfrentan riesgos cuando sus sistemas dependen de proveedores, plataformas o infraestructuras externas. La distribución de operaciones entre diferentes actores puede dificultar la identificación del punto concreto donde se produjo la vulneración y complicar la atribución de responsabilidades. El análisis de ecosistemas digitales demuestra que los proveedores de plataformas pueden desempeñar funciones relevantes en tratamientos ilícitos o deficientemente controlados, especialmente cuando determinan condiciones tecnológicas que afectan el acceso y circulación de información (Kurtz et al., 2022). Por ello, la seguridad debe evaluarse a lo largo de toda la cadena de tratamiento y no limitarse únicamente a la infraestructura controlada directamente por el responsable.

La obligación de seguridad incorpora una dimensión preventiva claramente definida en la normativa ecuatoriana. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, responsables y encargados deben implementar herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, además de verificar periódicamente su eficacia y realizar evaluaciones de adecuación al nivel de seguridad antes del tratamiento. Estas obligaciones impiden interpretar el cumplimiento como una simple reacción frente a incidentes consumados. El responsable debe demostrar que identificó previamente los riesgos previsibles y que adoptó medidas coherentes con ellos, de modo que la prevención forme parte de la gestión ordinaria de los datos personales.

Una vez producida una vulneración, la rapidez con que la organización detecta y evalúa el incidente influye en la posibilidad de reducir sus consecuencias. La respuesta debe determinar qué datos resultaron afectados, qué titulares podrían encontrarse en riesgo y qué medidas son necesarias para contener la exposición. Thomas et al. (2022) señalan que las comunicaciones sobre brechas constituyen una dimensión de la responsabilidad porque permiten valorar si la organización explica adecuadamente lo ocurrido, las consecuencias previsibles y las acciones adoptadas. Una gestión deficiente del incidente puede ampliar el daño inicial si los titulares desconocen que su información ha quedado expuesta y no pueden adoptar medidas protectoras.

La legislación ecuatoriana contempla expresamente la comunicación al titular cuando la vulneración puede comprometer sus derechos. La Ley Orgánica de Protección de Datos

Personales (2021), en su artículo 46, establece que el responsable debe notificar sin dilación la vulneración cuando esta conlleve un riesgo para los derechos fundamentales y libertades individuales, dentro del término de tres días desde que tuvo conocimiento del riesgo. La misma disposición contempla determinadas excepciones cuando las medidas aplicadas sean efectivas, el riesgo haya sido neutralizado o la comunicación individual exija un esfuerzo desproporcionado, supuesto en el cual procede una comunicación pública.

Las vulneraciones de datos también permiten evaluar la eficacia real de las políticas de seguridad existentes. La existencia de normas internas o herramientas tecnológicas no demuestra por sí sola que el riesgo haya sido adecuadamente controlado. El estudio empírico de Fan (2023) sobre políticas de seguridad y brechas evidencia la necesidad de analizar si las medidas regulatorias producen efectos preventivos efectivos y si las sanciones generan incentivos suficientes para reducir incidentes. Esta cuestión resulta importante porque el cumplimiento meramente formal puede coexistir con vulnerabilidades persistentes. La prevención jurídica exige comprobar que las medidas implementadas funcionan en la práctica y se adaptan a las amenazas que enfrenta cada organización.

La exposición de datos personales puede generar además responsabilidades distintas según la causa y las consecuencias del incidente. Una misma vulneración puede originar obligaciones administrativas derivadas del incumplimiento de medidas de seguridad, responsabilidades frente a los titulares afectados e incluso consecuencias penales cuando existen conductas ilícitas deliberadas. Por ello, identificar el origen del incidente resulta esencial para determinar si existió negligencia, incumplimiento organizativo, acceso indebido o actuación dolosa. Las organizaciones deben conservar evidencias suficientes sobre las condiciones del sistema y las acciones realizadas después de detectar la vulneración, pues la trazabilidad facilita establecer responsabilidades y evaluar si la respuesta fue proporcional al nivel de riesgo.

La gestión de vulneraciones exige finalmente integrar prevención, detección, contención, documentación y comunicación. Ninguna medida aislada garantiza una protección completa, porque los incidentes pueden originarse tanto en componentes tecnológicos como en fallas organizativas o humanas. El artículo 47 de la Ley Orgánica de Protección de Datos Personales (2021) exige precisamente una combinación de herramientas y procesos destinados a prevenir y controlar riesgos, mientras que el artículo 46 regula la comunicación al titular cuando la afectación alcanza un nivel relevante. La responsabilidad jurídica comienza, por tanto, antes de la brecha y continúa durante su gestión posterior, de modo que la seguridad debe entenderse como una obligación continua y demostrable.

4.2 Responsabilidad de responsables y encargados del tratamiento

La responsabilidad jurídica en materia de protección de datos depende de la función que cada sujeto desempeña dentro del tratamiento. El responsable decide las finalidades y condiciones esenciales bajo las cuales se utilizará la información, mientras que el encargado realiza operaciones por cuenta de aquel. Esta diferencia condiciona la distribución de obligaciones y permite determinar quién debe responder cuando se produce un tratamiento ilícito o una vulneración de seguridad. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 4, distingue expresamente ambas figuras y las vincula con niveles diferentes de decisión, ejecución y control dentro del ciclo de tratamiento de datos personales.

El responsable debe garantizar que el tratamiento se ajuste a la normativa desde su planificación. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, exige adoptar medidas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas para garantizar y demostrar el cumplimiento. Esta obligación incluye la aplicación de políticas internas, la evaluación de riesgos y la adopción de controles adecuados a la naturaleza de los datos. La responsabilidad no surge únicamente después de una vulneración, porque el deber jurídico comprende anticipar los riesgos previsibles y establecer mecanismos que reduzcan su probabilidad e impacto antes de iniciar o modificar un tratamiento.

El encargado también asume obligaciones propias, aunque actúe siguiendo instrucciones del responsable. Su intervención puede abarcar almacenamiento, alojamiento, soporte tecnológico, análisis, procesamiento o gestión de bases de datos. El artículo 47 de la Ley Orgánica de Protección de Datos Personales (2021) incluye expresamente a responsables y encargados dentro de las obligaciones de seguridad y cumplimiento. Esta previsión impide que el encargado se considere un mero ejecutor sin responsabilidad sobre las condiciones técnicas y organizativas de su actuación. Cuando controla infraestructura, credenciales o mecanismos de acceso, sus decisiones pueden influir directamente en la confidencialidad, integridad y disponibilidad de la información personal.

La responsabilidad se vuelve más compleja en ecosistemas digitales donde intervienen plataformas, proveedores tecnológicos y servicios conectados. Kurtz et al. (2022) muestran que la atribución de responsabilidad puede depender de la capacidad real de cada actor para influir sobre las condiciones del tratamiento, especialmente cuando una plataforma determina aspectos técnicos o contractuales que afectan a otros participantes. En estos escenarios, la identificación formal de un responsable no siempre basta para comprender cómo se distribuye

el poder efectivo sobre los datos. El análisis jurídico debe considerar quién decide, quién ejecuta y quién controla elementos esenciales capaces de prevenir o facilitar un tratamiento contrario a la normativa.

La actuación diligente exige además documentar decisiones y demostrar que las medidas adoptadas eran adecuadas al nivel de riesgo. La responsabilidad proactiva implica conservar evidencia sobre evaluaciones, políticas, procedimientos, controles de acceso y mecanismos de respuesta frente a incidentes. Thomas et al. (2022) destacan que la rendición de cuentas también se refleja en la forma en que las organizaciones explican públicamente una brecha, reconocen responsabilidades y comunican las acciones adoptadas. La documentación permite reconstruir el comportamiento anterior y posterior al incidente y facilita determinar si el responsable y el encargado actuaron con la diligencia exigible según las características del tratamiento.

Tabla 11
Responsabilidades principales del responsable y del encargado del tratamiento

Sujeto	Función principal	Obligaciones relevantes	Riesgo jurídico ante incumplimiento
Responsable	Determina finalidades y condiciones esenciales del tratamiento.	Definir bases jurídicas, finalidades, políticas y medidas de seguridad.	Responder por tratamientos ilícitos o controles insuficientes.
Encargado	Trata datos por cuenta del responsable.	Cumplir instrucciones y aplicar medidas técnicas y organizativas.	Responder por actuaciones contrarias a instrucciones o deberes propios.
Responsable y encargado	Participan conjuntamente en la protección operativa.	Gestionar riesgos, documentar medidas y prevenir vulneraciones.	Responsabilidad por deficiencias en seguridad o gestión.
Responsable	Supervisa la relación con terceros.	Seleccionar proveedores adecuados y delimitar obligaciones.	Falta de control sobre tratamientos externalizados.
Encargado	Administra procesos o infraestructura delegada.	Restringir accesos y mantener confidencialidad.	Exposición o uso indebido de información.
Ambos	Deben colaborar frente a incidentes.	Detectar, contener, documentar y comunicar vulneraciones.	Agravamiento de consecuencias por respuesta tardía o deficiente.

Nota. La tabla diferencia las obligaciones asociadas con la capacidad de decisión del responsable y con la ejecución técnica u operativa del encargado dentro del tratamiento.

La relación entre responsable y encargado debe estructurarse de manera que las obligaciones no queden indefinidas. Cuando se externalizan servicios tecnológicos, el responsable debe

asegurarse de que el encargado ofrece garantías suficientes para proteger los datos y cumplir las instrucciones acordadas. La existencia de un contrato no elimina la necesidad de supervisión, especialmente cuando el proveedor administra infraestructura crítica o maneja categorías sensibles de información. Kurtz et al. (2022) muestran que las relaciones entre plataformas y proveedores pueden crear zonas de responsabilidad compartida o difusa si las funciones no se delimitan correctamente, lo que aumenta los riesgos para los titulares.

La responsabilidad también se evalúa por la capacidad de reaccionar frente a una vulneración. Una organización que detecta un incidente debe identificar su alcance, contenerlo y adoptar medidas para reducir los efectos sobre los titulares. Thomas et al. (2022) señalan que las comunicaciones de brechas permiten observar si la organización asume responsabilidad, explica lo ocurrido y proporciona información útil sobre las acciones posteriores. Esta dimensión comunicativa no sustituye las medidas técnicas, pero forma parte de la rendición de cuentas porque demuestra si la entidad reconoce el incidente y actúa de forma coherente con sus obligaciones de protección y transparencia.

La existencia de medidas preventivas tampoco excluye responsabilidad cuando estas resultan insuficientes frente a riesgos previsibles. El análisis debe considerar la naturaleza de los datos, el volumen tratado, la tecnología utilizada y las amenazas identificables. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, exige que las medidas sean apropiadas y que su eficacia se verifique periódicamente. Esto implica que los controles deben actualizarse cuando cambian las condiciones del tratamiento. Una política que fue adecuada en un momento puede dejar de serlo si aumenta el volumen de datos, se incorporan nuevos proveedores o aparecen vulnerabilidades relevantes.

La responsabilidad de responsables y encargados se configura, en consecuencia, como una obligación continua de prevención, control y demostración. El responsable conserva la posición central porque define el tratamiento, mientras que el encargado debe ejecutar sus funciones respetando instrucciones y obligaciones propias de seguridad. En ecosistemas complejos, la protección efectiva depende de que ambos mantengan trazabilidad, delimiten competencias y cooperen frente a incidentes. La atribución de responsabilidad no debe basarse únicamente en denominaciones contractuales, sino en la intervención real de cada actor y en su capacidad para influir sobre las condiciones que determinaron el tratamiento y la eventual vulneración.

Figura 8
Responsabilidad del responsable y del encargado del tratamiento



Nota. El esquema diferencia las funciones y obligaciones de ambos sujetos y muestra los criterios que permiten atribuir responsabilidad según su capacidad de decisión, control, prevención, documentación y respuesta frente a incumplimientos o incidentes.

4.3 Responsabilidad por acceso, uso o divulgación no autorizada de datos

El acceso no autorizado a datos personales constituye una vulneración cuando una persona consulta, obtiene o utiliza información sin contar con habilitación jurídica o autorización suficiente. La responsabilidad puede recaer sobre quien accede indebidamente y también sobre la organización que permitió el acceso por ausencia de controles adecuados. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, exige a responsables y encargados aplicar medidas técnicas, administrativas, físicas, organizativas y jurídicas apropiadas para proteger la información. Esta obligación implica establecer mecanismos de autenticación,

permisos diferenciados y controles internos capaces de limitar el acceso únicamente a quienes necesitan utilizar los datos.

El uso no autorizado puede producirse incluso cuando el acceso inicial fue legítimo. Un empleado, proveedor o tercero puede disponer de autorización para consultar determinada información y, sin embargo, utilizarla posteriormente para fines distintos de los previstos. En estos casos, el problema no reside en la entrada al sistema, sino en la desviación de finalidad. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige que el tratamiento respete los principios de finalidad, lealtad y confidencialidad. El incumplimiento de estos principios puede generar responsabilidad cuando los datos se utilizan fuera del propósito informado o en beneficio de intereses ajenos al tratamiento autorizado.

La divulgación no autorizada representa una forma especialmente grave de afectación porque amplía el número de personas que pueden acceder a información personal. De acuerdo con el COIP (2014), en su artículo 229, la revelación ilegal de información registrada en ficheros, archivos, bases de datos o medios semejantes puede generar responsabilidad penal cuando se vulneran el secreto, la intimidad y la privacidad. La norma evidencia que determinadas conductas no se agotan en una infracción administrativa, sino que pueden adquirir relevancia penal cuando existe una divulgación ilícita y voluntaria. La naturaleza de los datos expuestos influye además en la gravedad de las consecuencias.

El acceso indebido puede originarse también por deficiencias organizativas y no únicamente por ataques externos. Contraseñas compartidas, permisos excesivos, falta de segregación de funciones o ausencia de registros de actividad pueden facilitar que personas autorizadas excedan el ámbito de sus funciones. Thomas et al. (2022) muestran que la responsabilidad frente a brechas de datos debe analizarse considerando tanto las causas técnicas como las deficiencias de gestión que permitieron el incidente. Esta perspectiva resulta importante porque una organización puede contar con herramientas de seguridad y, aun así, mantener prácticas internas que dificulten identificar quién accedió a los datos y con qué finalidad.

La responsabilidad se vuelve más compleja cuando el tratamiento se distribuye entre plataformas y proveedores externos. En estos ecosistemas, un tercero puede acceder a datos mediante interfaces, servicios integrados o infraestructura administrada por otra entidad. Kurtz et al. (2022) señalan que la determinación de responsabilidad requiere observar qué actor controla realmente las condiciones técnicas y organizativas que permiten el tratamiento. La atribución no debe depender únicamente del nombre asignado en un contrato, sino de la

capacidad efectiva de decidir, restringir accesos o modificar el funcionamiento del sistema. Esta evaluación permite identificar con mayor precisión qué sujeto pudo prevenir la utilización o divulgación no autorizada.

Tabla 12

Formas de acceso, uso y divulgación no autorizada de datos personales

Conducta	Manifestación	Posible responsabilidad
Acceso sin autorización	Consulta de datos sin permiso válido.	Administrativa y, según el caso, penal.
Exceso de privilegios	Uso de permisos superiores a los necesarios.	Responsabilidad organizativa por controles insuficientes.
Uso distinto de la finalidad	Empleo de datos para propósitos no autorizados.	Incumplimiento de finalidad y lealtad.
Divulgación a terceros	Comunicación de información sin base jurídica.	Responsabilidad administrativa, civil o penal.
Difusión pública	Publicación de datos personales sin habilitación.	Afectación de intimidad y privacidad.
Acceso interno indebido	Consulta por empleados sin necesidad funcional.	Responsabilidad individual y organizacional.
Transferencia no controlada	Entrega de datos a proveedores o destinatarios no autorizados.	Responsabilidad del sujeto que permite o ejecuta la transferencia.
Falta de trazabilidad	Imposibilidad de identificar quién accedió a la información.	Dificultad para demostrar cumplimiento y asignar responsabilidades.

Nota. La tabla distingue conductas que pueden comprometer la confidencialidad de los datos y generar responsabilidades según la forma, finalidad y contexto en que se produce el acceso o la divulgación.

La obligación de confidencialidad acompaña todo el tratamiento. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, exige preservar la reserva de los datos incluso después de finalizar la relación con el titular o con la organización que participó en el tratamiento. Esta obligación limita el uso posterior de información conocida por razón de funciones laborales, profesionales o contractuales. Una persona que deja de prestar servicios no adquiere libertad para conservar, utilizar o divulgar los datos a los que tuvo acceso. La permanencia del deber de confidencialidad constituye una barrera jurídica frente a usos posteriores que podrían afectar la privacidad del titular.

La responsabilidad por acceso indebido también puede surgir cuando el responsable no controla adecuadamente las credenciales y permisos concedidos. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, exige verificar periódicamente la eficacia de las medidas implementadas y evaluar su adecuación al nivel de riesgo. Esta obligación implica revisar perfiles de acceso, retirar permisos innecesarios y actualizar

mecanismos de autenticación. La falta de mantenimiento puede convertir controles inicialmente adecuados en medidas insuficientes. La responsabilidad, por tanto, no depende únicamente de haber instalado mecanismos de seguridad, sino de mantenerlos actualizados y adaptados a los cambios en personal, tecnología y tratamiento.

Cuando la divulgación produce una brecha de seguridad, la organización debe además gestionar el incidente de manera documentada y proporcional. Thomas et al. (2022) destacan que la comunicación posterior permite valorar si la entidad identificó correctamente el alcance de la exposición, asumió responsabilidades y adoptó medidas de respuesta. Esta actuación resulta relevante porque el daño puede aumentar si los titulares desconocen que su información fue divulgada. La gestión adecuada exige identificar qué datos fueron afectados, quién pudo acceder a ellos y qué medidas deben adoptarse para contener su utilización posterior. La transparencia posterior forma parte de la responsabilidad frente a la vulneración.

La responsabilidad por acceso, uso o divulgación no autorizada exige finalmente combinar reglas preventivas, deberes de confidencialidad y mecanismos de sanción. El responsable debe controlar quién puede acceder, el encargado debe limitar su actuación a las instrucciones legítimas y cualquier tercero debe contar con una base suficiente para recibir información. Cuando estas condiciones fallan, pueden concurrir responsabilidades de distinta naturaleza según la conducta y el daño producido. La protección efectiva depende de que las organizaciones puedan demostrar quién accedió a cada dato, con qué finalidad y bajo qué autorización, evitando que la complejidad tecnológica diluya la responsabilidad de los sujetos involucrados.

4.4 Incidentes de seguridad, filtraciones y deber de notificación

Los incidentes de seguridad comprenden eventos que comprometen o pueden comprometer la confidencialidad, integridad o disponibilidad de los datos personales. Pueden originarse en ataques externos, errores humanos, fallas de configuración, pérdida de dispositivos, accesos indebidos o vulnerabilidades en sistemas y proveedores. La relevancia jurídica aparece cuando el incidente afecta efectivamente la protección de la información y genera riesgos para los titulares. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 46, regula la notificación de vulneraciones de seguridad cuando estas puedan implicar riesgo para los derechos fundamentales y libertades individuales, lo que obliga al responsable a evaluar la gravedad del evento.

Una filtración de datos se produce cuando información personal queda expuesta o accesible para personas que no estaban autorizadas a conocerla. Esta exposición puede ser pública o limitada a determinados terceros, pero en ambos casos requiere determinar qué datos fueron afectados, durante cuánto tiempo estuvieron comprometidos y qué consecuencias podrían derivarse. Thomas et al. (2022) muestran que la gestión de brechas no debe limitarse a describir el incidente, sino que también debe explicar las medidas adoptadas, las responsabilidades identificadas y las acciones destinadas a reducir el impacto. La calidad de la respuesta institucional influye directamente en la capacidad de los titulares para protegerse frente a consecuencias posteriores.

La obligación de notificar responde a la necesidad de evitar que el titular permanezca ignorante frente a una exposición que pueda perjudicarlo. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 46, el responsable debe comunicar la vulneración al titular sin dilación y, en todo caso, dentro del término previsto por la norma cuando exista riesgo para sus derechos y libertades. Esta comunicación debe permitir que la persona conozca lo ocurrido y adopte medidas razonables, como cambiar credenciales, vigilar movimientos financieros o extremar precauciones frente a intentos de suplantación, fraude u otras formas de aprovechamiento de la información filtrada.

El deber de notificación no significa que todo evento técnico deba comunicarse de manera automática al titular. La valoración jurídica exige identificar si la vulneración genera un riesgo real para sus derechos. La naturaleza de los datos, el volumen de información comprometida, el número de personas afectadas y la posibilidad de reidentificación son factores relevantes. Una filtración de datos sensibles puede requerir una respuesta más urgente que un incidente limitado a información de bajo impacto. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 46, vincula precisamente la obligación de notificar con la existencia de riesgo para derechos fundamentales y libertades individuales.

La notificación debe contener información suficiente para que el titular comprenda la naturaleza del incidente. Una comunicación vaga puede cumplir formalmente con el envío, pero no permite evaluar qué medidas conviene adoptar. Thomas et al. (2022) destacan que las comunicaciones sobre brechas deberían explicar qué ocurrió, qué datos fueron comprometidos y qué acciones fueron implementadas para contener el incidente. Desde la perspectiva jurídica, esta claridad forma parte de la rendición de cuentas, porque la organización debe demostrar que evaluó el evento y actuó de manera proporcional. La transparencia posterior a una filtración constituye, por tanto, una extensión del deber general de protección de datos.

La comunicación a los titulares también se relaciona con la confianza institucional. Bohn y Schiereck (2023) muestran que la publicación de brechas puede generar efectos reputacionales y económicos, especialmente en sectores donde los datos tratados son altamente sensibles, como la salud. Sin embargo, la posibilidad de consecuencias negativas para la organización no justifica ocultar el incidente cuando existe una obligación jurídica de informar. La protección del titular debe prevalecer sobre el interés reputacional de la entidad. Una comunicación temprana y clara puede reducir daños posteriores, mientras que el retraso injustificado puede agravar la exposición y aumentar la responsabilidad asociada con la gestión deficiente del incidente.

La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, complementa el deber de notificación con la obligación de gestionar riesgos y aplicar medidas preventivas. Esto implica que la organización debe disponer de procedimientos internos para detectar vulneraciones, clasificarlas, documentarlas y decidir cuándo corresponde comunicar el evento. Un sistema que carece de mecanismos de monitoreo puede descubrir una filtración demasiado tarde, cuando la información ya ha circulado ampliamente. La responsabilidad no comienza en el momento de la comunicación, sino en la capacidad previa para identificar señales de riesgo y activar protocolos de respuesta antes de que el impacto aumente.

Las organizaciones que operan con proveedores externos deben coordinar también la detección y comunicación de incidentes. Cuando un encargado del tratamiento detecta una vulneración en sistemas que administra por cuenta del responsable, debe existir un procedimiento que permita informar rápidamente y aportar los datos necesarios para evaluar el riesgo. La complejidad de los ecosistemas digitales puede retrasar la respuesta si las responsabilidades no están definidas. Kurtz et al. (2022) muestran que las relaciones entre plataformas y proveedores pueden generar zonas de responsabilidad difusa, por lo que la claridad contractual y técnica resulta esencial para determinar quién detecta, comunica y mitiga una vulneración.

La documentación del incidente cumple una función probatoria y de aprendizaje. Registrar la fecha de detección, los sistemas afectados, los datos comprometidos, las medidas aplicadas y las comunicaciones realizadas permite demostrar cómo actuó la organización. Esta información también sirve para revisar las causas y corregir deficiencias que podrían repetirse. La responsabilidad proactiva exige que las decisiones frente a una brecha puedan justificarse posteriormente. Thomas et al. (2022) subrayan que la rendición de cuentas se fortalece cuando la organización explica de manera estructurada su respuesta y demuestra que no se limitó a

contener el daño inmediato, sino que adoptó acciones para reducir la probabilidad de incidentes similares.

Las filtraciones también pueden activar consecuencias sancionatorias cuando revelan incumplimientos de las obligaciones de seguridad. Fan (2023) muestra que la eficacia de las normas depende en parte de que existan mecanismos de cumplimiento capaces de generar incentivos preventivos. Una vulneración no implica necesariamente que la organización haya actuado ilícitamente, pero puede evidenciar negligencia si los riesgos eran previsibles y las medidas claramente insuficientes. Por ello, el análisis jurídico debe distinguir entre incidentes inevitables pese a controles razonables y eventos facilitados por fallas de gestión, ausencia de protocolos o decisiones que ignoraron vulnerabilidades conocidas.

El deber de notificación cumple, finalmente, una función protectora y no meramente administrativa. Informar a tiempo permite al titular adoptar medidas, facilita la supervisión de la autoridad y obliga a la organización a asumir responsabilidad por la gestión del incidente. La eficacia del sistema depende de que la comunicación sea oportuna, comprensible y proporcional al riesgo. Una notificación tardía o incompleta puede aumentar el daño, especialmente cuando los datos expuestos permiten fraude, suplantación o afectaciones reputacionales. La gestión de incidentes exige, por tanto, integrar prevención, detección, evaluación, documentación y comunicación dentro de un mismo proceso de responsabilidad jurídica.

4.5 Daños derivados de las vulneraciones de datos personales

Las vulneraciones de datos personales pueden producir daños de naturaleza económica, reputacional, emocional y jurídica, dependiendo del tipo de información afectada y de las consecuencias derivadas de su exposición o uso indebido. No toda brecha genera automáticamente el mismo nivel de perjuicio, porque deben considerarse factores como sensibilidad de los datos, número de titulares afectados, duración del incidente y posibilidad de explotación posterior. La responsabilidad jurídica exige analizar la relación entre la vulneración y el daño producido. En este sentido, las organizaciones deben valorar no solo la pérdida directa de información, sino también las consecuencias previsibles que puede sufrir el titular después del incidente (Thomas et al., 2022).

Los daños económicos pueden manifestarse mediante fraude, suplantación de identidad, utilización indebida de medios de pago o costos asociados con la recuperación del control sobre cuentas y servicios. Cuando una brecha compromete credenciales, números de identificación u

otra información susceptible de explotación, el titular puede verse obligado a modificar contraseñas, bloquear cuentas o adoptar medidas adicionales de seguridad. La gravedad dependerá del acceso efectivo que terceros hayan obtenido y de la utilización posterior de los datos. Bohn y Schiereck (2023) muestran que las brechas también pueden generar consecuencias económicas para las organizaciones afectadas, especialmente cuando la divulgación del incidente modifica la confianza del mercado o de sus usuarios.

El daño reputacional constituye otra consecuencia posible cuando información privada se hace pública o circula fuera del contexto para el que fue recopilada. Datos relativos a salud, relaciones personales, antecedentes o actividades privadas pueden modificar la percepción que otras personas o instituciones tienen del titular. La difusión puede resultar particularmente difícil de revertir en entornos digitales, donde la información puede copiarse, indexarse o replicarse rápidamente. El derecho a la intimidad reconocido por la Constitución de la República del Ecuador (2008), en su artículo 66, numeral 20, ofrece un fundamento para valorar este tipo de afectaciones cuando la exposición compromete aspectos reservados de la vida personal o familiar.

Las vulneraciones también pueden generar daños derivados de discriminación o exclusión. Cuando se exponen datos sensibles, la información puede utilizarse para clasificar a una persona, negarle oportunidades o tratarla de manera desfavorable. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 25, reconoce categorías especiales de datos cuya naturaleza exige una protección reforzada, precisamente porque su uso indebido puede afectar derechos y libertades. El riesgo aumenta cuando la información expuesta se combina con otros registros y permite construir perfiles detallados. La evaluación del daño debe considerar, por ello, no solo la divulgación inicial, sino también los posibles usos posteriores de la información.

Los datos sanitarios ilustran con claridad la amplitud de los perjuicios posibles. Una filtración de información médica puede revelar diagnósticos, tratamientos o condiciones que el titular pretendía mantener en reserva. Esa exposición puede afectar relaciones laborales, personales o sociales y generar consecuencias difíciles de revertir. La sensibilidad de estos datos exige controles reforzados y respuestas rápidas cuando ocurre una vulneración. La investigación sobre incidentes en servicios de salud muestra que las organizaciones deben valorar tanto el impacto material como la pérdida de confianza y las expectativas de reparación de las personas afectadas (Masuch et al., 2021).

El daño también puede derivarse de la pérdida de control sobre la información, incluso cuando no exista una pérdida económica inmediata. Saber que datos personales circulan entre terceros desconocidos puede generar incertidumbre respecto de cómo serán utilizados en el futuro. Esta pérdida de control resulta especialmente relevante cuando la información puede permanecer disponible durante períodos prolongados. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 46, vincula la notificación de vulneraciones con el riesgo para los derechos y libertades del titular. Esta exigencia reconoce implícitamente que el perjuicio puede manifestarse de maneras distintas y que la exposición debe evaluarse atendiendo a sus consecuencias potenciales.

La gravedad del daño depende también de la respuesta adoptada por la organización después de la brecha. Una comunicación tardía puede impedir que los titulares adopten medidas para reducir consecuencias posteriores. Thomas et al. (2022) señalan que la forma en que una entidad comunica el incidente influye en la percepción de responsabilidad y en la capacidad de las personas para reaccionar. La transparencia posterior a la vulneración permite disminuir ciertos riesgos, mientras que el silencio o la información insuficiente pueden agravarlos. La gestión del daño exige, por tanto, identificar rápidamente el alcance del incidente y proporcionar orientaciones útiles a quienes puedan resultar afectados.

Las medidas de reparación pueden incluir compensación económica, asistencia al titular, restitución de servicios o acciones destinadas a reducir el impacto. Masuch et al. (2021) analizan específicamente el papel de las disculpas y la compensación después de brechas de datos en servicios sanitarios y muestran que las respuestas institucionales influyen en la evaluación que las personas realizan del incidente. Estas medidas no sustituyen las obligaciones legales, pero pueden formar parte de una estrategia de reparación cuando existe un perjuicio. La adecuación de la respuesta debe considerar la naturaleza del daño y evitar soluciones meramente simbólicas cuando las consecuencias para el titular sean significativas.

La existencia de sanciones tampoco debe confundirse con la reparación individual. Una autoridad puede imponer una multa por incumplimiento normativo y, al mismo tiempo, el titular afectado puede requerir otros mecanismos para obtener reparación por los perjuicios sufridos. Los análisis de aplicación del régimen europeo muestran que las sanciones administrativas cumplen principalmente funciones de cumplimiento y disuasión, mientras que la compensación responde a la afectación concreta de la persona (Ruohonen & Hjerppe, 2022). Esta diferencia resulta importante porque una sanción institucional no elimina

automáticamente las consecuencias económicas, reputacionales o personales que permanecen después de una vulneración.

La prevención del daño exige evaluar riesgos antes de que ocurra el incidente. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, obliga a responsables y encargados a implementar metodologías de análisis y gestión de riesgos y a adoptar medidas para prevenir, reducir y controlar vulneraciones. Esta obligación implica considerar qué consecuencias produciría una eventual exposición y no únicamente la probabilidad técnica de que ocurra. Un mismo incidente puede tener impactos muy distintos según la sensibilidad y el contexto de los datos. La evaluación preventiva debe, por tanto, incorporar la perspectiva del titular y las posibles afectaciones sobre sus derechos.

Los daños derivados de las vulneraciones de datos muestran finalmente que la protección de la información personal no puede reducirse a una cuestión técnica. Una falla de seguridad puede traducirse en consecuencias económicas, sociales, reputacionales y jurídicas que persisten después de controlar el incidente. La responsabilidad exige identificar el daño, limitar su extensión y establecer medidas de reparación adecuadas. La respuesta institucional debe combinar notificación, asistencia, corrección de las causas y, cuando corresponda, compensación. El análisis de brechas demuestra que la eficacia de la protección depende tanto de evitar incidentes como de contar con mecanismos capaces de responder de forma proporcional cuando estos se producen (Masuch et al., 2021; Bohn & Schiereck, 2023).

4.6 Infracciones y sanciones en materia de protección de datos

El régimen de infracciones y sanciones en materia de protección de datos cumple una función de control frente al incumplimiento de las obligaciones impuestas a responsables, encargados y demás sujetos sometidos a la normativa. No toda irregularidad tiene la misma gravedad, por lo que la Ley Orgánica de Protección de Datos Personales diferencia conductas leves y graves según su naturaleza y efectos. Esta clasificación permite graduar la respuesta administrativa y relacionarla con el nivel de afectación producido. Los estudios sobre aplicación de sanciones muestran que la eficacia del régimen depende de combinar proporcionalidad, capacidad disuasoria y criterios consistentes para valorar la conducta infractora (Ruohonen & Hjerppe, 2022).

Las infracciones leves del responsable están previstas en el artículo 67 de la Ley Orgánica de Protección de Datos Personales (2021). Entre ellas se encuentran no tramitar, tramitar fuera de plazo o negar injustificadamente solicitudes o quejas del titular; no implementar protección de

datos desde el diseño y por defecto; no mantener disponibles políticas de protección de datos acordes con el tratamiento; seleccionar un encargado que no ofrezca garantías suficientes; e incumplir medidas correctivas dispuestas por la autoridad. Estas conductas reflejan deficiencias de cumplimiento que, aunque clasificadas como leves, pueden afectar la capacidad del titular para ejercer efectivamente sus derechos.

Las infracciones graves del responsable se encuentran en el artículo 68 de la Ley Orgánica de Protección de Datos Personales (2021). La norma contempla, entre otras conductas, la ausencia de medidas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas; el uso de datos para fines distintos de los declarados; el incumplimiento de obligaciones relacionadas con derechos de los titulares; y determinadas omisiones vinculadas con seguridad, registro, delegados y supervisión. La gravedad responde a que estas conductas pueden afectar directamente principios esenciales del tratamiento o impedir el funcionamiento de mecanismos de protección. El régimen exige, por ello, una actuación preventiva y verificable del responsable.

Los encargados del tratamiento tienen también un régimen específico. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 69, considera infracciones leves conductas como no colaborar con el responsable para atender solicitudes de titulares, no facilitar información necesaria para demostrar cumplimiento, obstaculizar auditorías o incumplir medidas correctivas. El artículo 70 tipifica infracciones graves, entre ellas tratar datos sin observar principios y derechos, actuar en contra de las condiciones acordadas con el responsable, omitir cláusulas de confidencialidad o no implementar mecanismos adecuados para preservar confidencialidad, integridad, disponibilidad y resiliencia. La responsabilidad del encargado es, por tanto, autónoma respecto de determinadas obligaciones propias.

La imposición de sanciones debe responder a criterios de proporcionalidad y a las características concretas de la conducta. El análisis empírico de decisiones sancionadoras muestra que elementos como gravedad de la infracción, principios afectados y circunstancias del incumplimiento influyen en la respuesta administrativa (Ruohonen & Hjerpe, 2022). La finalidad del régimen no consiste únicamente en castigar después de una vulneración, sino también en generar incentivos para que responsables y encargados incorporen el cumplimiento dentro de su gestión ordinaria. Fan (2023) advierte que la existencia formal de normas y sanciones no garantiza por sí misma una reducción de las brechas, por lo que su eficacia debe evaluarse también desde su capacidad preventiva.

Tabla 13*Infracciones y consecuencias sancionatorias en materia de protección de datos*

Categoría	Ejemplos de conductas	Sujeto principal	Consecuencia jurídica
Infracción leve	No atender adecuadamente solicitudes del titular.	Responsable	Sanción administrativa proporcional.
Infracción leve	No aplicar protección de datos desde el diseño y por defecto.	Responsable	Medidas correctivas y eventual multa.
Infracción grave	No implementar medidas adecuadas de seguridad y cumplimiento.	Responsable	Sanción correspondiente a infracción grave.
Infracción grave	Utilizar datos para finalidades distintas de las declaradas.	Responsable	Multa y medidas correctivas.
Infracción leve	No colaborar en el ejercicio de derechos del titular.	Encargado	Sanción administrativa.
Infracción grave	Tratar datos contrariando principios, derechos o instrucciones aplicables.	Encargado	Sanción por infracción grave.
Incumplimiento reiterado	Persistencia en conductas previamente corregidas o sancionadas.	Responsable o encargado	Agravamiento de la respuesta administrativa.
Conductas con relevancia penal	Acceso o divulgación ilícita en los supuestos previstos por el COIP.	Persona responsable de la conducta	Posible responsabilidad penal independiente.

Nota. La tabla diferencia las principales categorías de incumplimiento y muestra que la respuesta jurídica depende de la gravedad, del sujeto obligado y de la naturaleza concreta de la conducta.

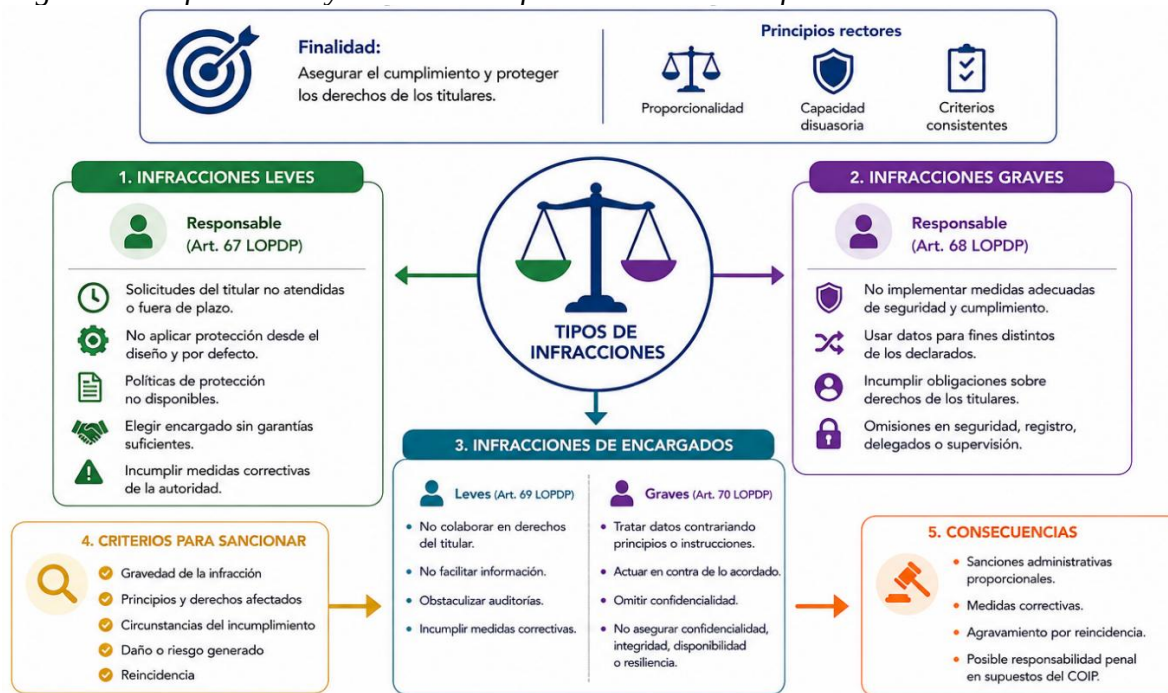
Las sanciones por infracciones leves están reguladas en el artículo 71 de la Ley Orgánica de Protección de Datos Personales (2021). Para servidores o funcionarios públicos responsables de una infracción leve, la norma prevé multas de uno a diez salarios básicos unificados, sin perjuicio de la responsabilidad extracontractual del Estado. Cuando el responsable, encargado o tercero sea una entidad de derecho privado o una empresa pública, la multa puede oscilar entre el 0,1 % y el 0,7 % del volumen de negocio correspondiente al ejercicio económico inmediatamente anterior. La autoridad debe aplicar criterios de proporcionalidad al determinar la sanción concreta.

Las infracciones graves reciben una respuesta superior. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 72, los servidores o funcionarios públicos pueden ser sancionados con multas de diez a veinte salarios básicos unificados. Para responsables, encargados o terceros que sean entidades de derecho privado o empresas públicas, la multa se sitúa entre el 0,7 % y el 1 % del volumen de negocio correspondiente al

ejercicio económico anterior. La diferencia respecto de las infracciones leves refleja el mayor impacto potencial de conductas que comprometen principios, derechos o medidas esenciales de seguridad y cumplimiento.

Figura 9

Régimen de infracciones y sanciones en protección de datos personales



Nota. El esquema diferencia las infracciones leves y graves aplicables a responsables y encargados, junto con los criterios utilizados para valorar su gravedad y las principales consecuencias derivadas del incumplimiento normativo.

El régimen administrativo no excluye otras formas de responsabilidad cuando la conducta presenta características distintas. Una infracción relacionada con protección de datos puede coincidir con actos que lesionen penalmente la intimidad o impliquen revelación ilícita de información. En esos casos, la sanción administrativa responde al incumplimiento del régimen de protección de datos, mientras que la responsabilidad penal se analiza según los elementos propios del tipo correspondiente. Esta coexistencia permite responder de forma diferenciada a conductas organizativas deficientes y a actuaciones deliberadas de mayor gravedad. La eficacia del sistema depende de mantener claridad sobre la naturaleza de cada responsabilidad y evitar equiparar automáticamente toda vulneración con un delito.

Las infracciones y sanciones cumplen finalmente una función preventiva dentro del sistema de protección de datos. Su efectividad depende de que responsables y encargados perciban el incumplimiento como un riesgo jurídico real y adopten medidas antes de que ocurra una vulneración. La evidencia comparada muestra que las multas pueden reforzar el cumplimiento,

pero su efecto depende de la consistencia de la supervisión y de la relación entre sanción, gravedad y conducta infractora (Ruohonen & Hjerpe, 2022). A su vez, Fan (2023) señala que las políticas sancionadoras deben acompañarse de mecanismos efectivos de seguridad y control, pues la amenaza de sanción no sustituye una gestión preventiva de los riesgos.

4.7 Reparación y mecanismos de reclamación frente a vulneraciones de privacidad

La reparación frente a una vulneración de privacidad busca restablecer, en la medida de lo posible, la posición jurídica del titular afectado y responder a las consecuencias derivadas del tratamiento indebido de sus datos. La reparación puede adoptar formas distintas según la naturaleza del daño, como corrección de información, eliminación de datos, cese del tratamiento, compensación económica o adopción de medidas destinadas a evitar nuevas afectaciones. La Ley Orgánica de Protección de Datos Personales (2021) reconoce mecanismos de tutela que permiten al titular reclamar frente a incumplimientos y exigir respuestas por parte de responsables y encargados cuando sus derechos han sido vulnerados.

La primera vía de reclamación suele consistir en ejercer directamente los derechos reconocidos por la normativa frente al responsable del tratamiento. Dependiendo del problema, el titular puede solicitar acceso, rectificación, actualización, eliminación, oposición, suspensión o portabilidad. Estos mecanismos permiten corregir determinadas afectaciones sin necesidad de acudir inicialmente a una instancia jurisdiccional. Su utilidad radica en que ofrecen respuestas específicas según el tipo de vulneración. Cuando una organización atiende adecuadamente la solicitud, puede reducir el impacto del incidente y evitar que el daño continúe produciéndose. La efectividad de estos derechos depende de que existan procedimientos accesibles, plazos claros y respuestas motivadas.

La acción de hábeas data constituye una garantía jurisdiccional especialmente relevante cuando los mecanismos ordinarios resultan insuficientes. De acuerdo con la Constitución de la República del Ecuador (2008), en su artículo 92, toda persona tiene derecho a conocer la existencia y acceder a documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma o sus bienes consten en entidades públicas o privadas. La misma disposición permite conocer el uso, finalidad, origen, destino y tiempo de vigencia de la información, así como solicitar su actualización, rectificación, eliminación o anulación cuando corresponda.

La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), en su artículo 49, desarrolla esta garantía y establece que la acción de hábeas data tiene por objeto proteger

judicialmente el acceso y control sobre datos personales. Esta vía permite reclamar cuando la información permanece incorrecta, desactualizada, utilizada de forma indebida o conservada sin justificación. La existencia de un mecanismo judicial resulta fundamental porque evita que la tutela dependa únicamente de la voluntad del responsable. El titular puede acudir a una autoridad jurisdiccional para obtener una decisión vinculante cuando la respuesta administrativa o interna no ha sido suficiente para restablecer sus derechos.

La reparación también puede requerir medidas distintas a la eliminación o rectificación. En algunos casos, el daño ya se produjo y no puede revertirse únicamente modificando una base de datos. Las investigaciones sobre respuestas posteriores a brechas muestran que la compensación y las disculpas pueden influir en la percepción de justicia y en la recuperación de la confianza de las personas afectadas (Masuch et al., 2021). Estas medidas no sustituyen las obligaciones legales ni eliminan automáticamente la responsabilidad, pero pueden formar parte de una respuesta más amplia cuando existe perjuicio material o inmaterial derivado de la vulneración.

La compensación económica puede resultar procedente cuando la vulneración produce daños cuantificables o afectaciones que justifican una reparación patrimonial. El análisis debe considerar la relación entre la conducta, el daño y la responsabilidad atribuible al sujeto que intervino en el tratamiento. La existencia de una sanción administrativa no necesariamente repara al titular, porque la multa impuesta por una autoridad responde al incumplimiento normativo y no directamente a la restitución individual. Ruohonen y Hjerpe (2022) muestran que los regímenes sancionadores cumplen principalmente funciones de cumplimiento y disuasión, mientras que la reparación individual requiere mecanismos específicos orientados a responder al perjuicio sufrido.

La reclamación también puede producirse mediante procedimientos ante la autoridad competente en materia de protección de datos. Estos mecanismos permiten denunciar incumplimientos, solicitar intervención institucional y promover medidas correctivas. Su función es distinta de la acción judicial, porque se orienta a la supervisión administrativa del cumplimiento y a la adopción de decisiones dentro del ámbito regulatorio. La efectividad de esta vía depende de que la autoridad pueda investigar, requerir información, ordenar medidas y aplicar sanciones cuando corresponda. La existencia de un órgano especializado facilita que los conflictos relacionados con tratamiento de datos sean analizados desde criterios técnicos y jurídicos específicos.

La reparación exige además medidas de no repetición cuando la vulneración revela fallas estructurales. Una respuesta limitada a compensar al titular puede resultar insuficiente si la organización mantiene las mismas deficiencias que originaron el incidente. Thomas et al. (2022) destacan que la rendición de cuentas posterior a una brecha debe incluir explicación del evento, acciones correctivas y medidas para evitar nuevos incidentes. Esto implica revisar controles de acceso, políticas internas, procedimientos de respuesta, formación del personal y sistemas de seguridad. La reparación adquiere así una dimensión preventiva, porque busca corregir tanto el daño individual como las condiciones organizativas que permitieron la vulneración.

La comunicación transparente con los afectados también forma parte de una reparación adecuada. Una persona necesita comprender qué ocurrió, qué datos fueron expuestos y qué acciones puede adoptar. La falta de información puede prolongar el daño al impedir que el titular tome medidas protectoras. Masuch et al. (2021) muestran que las estrategias de respuesta influyen en la valoración que los afectados realizan de la organización después de una brecha. Una comunicación clara, acompañada de medidas concretas, puede contribuir a reducir incertidumbre y restaurar parcialmente la confianza, aunque no elimina la necesidad de asumir responsabilidades por el incidente.

Los mecanismos de reclamación deben ser accesibles y comprensibles para evitar que la complejidad jurídica se convierta en una barrera. El titular debe saber a quién dirigirse, qué derecho ejercer y qué información presentar para sustentar su solicitud. Cuando los procedimientos son excesivamente técnicos, largos o poco transparentes, la protección pierde eficacia práctica. La tutela de la privacidad exige que las vías administrativas y jurisdiccionales puedan utilizarse de forma razonable por las personas afectadas. La existencia formal de derechos no resulta suficiente si el costo, la dificultad o la falta de información impiden su ejercicio efectivo frente a una vulneración.

La reparación frente a vulneraciones de privacidad debe entenderse, en consecuencia, como un conjunto de respuestas complementarias. Puede incluir rectificación, supresión, suspensión del tratamiento, intervención de la autoridad, hábeas data, sanciones, compensación y medidas de no repetición. La elección del mecanismo depende de la naturaleza de la afectación y del resultado que se busca obtener. La protección efectiva requiere que el titular pueda detener el tratamiento indebido, corregir sus consecuencias y exigir responsabilidad cuando corresponda. En este sentido, reparación y reclamación forman parte de una tutela integral que combina restitución, control institucional y prevención de nuevas vulneraciones.



Capítulo 5

Cumplimiento normativo y tutela de la privacidad

Galo Fernando Almeida Casanova

5.1 Sistemas de cumplimiento en materia de protección de datos personales

Los sistemas de cumplimiento en materia de protección de datos personales constituyen estructuras organizativas destinadas a garantizar que las actividades de tratamiento se ajusten de manera permanente a las obligaciones jurídicas aplicables. Su funcionamiento comprende políticas, procedimientos, responsabilidades internas, mecanismos de control, evaluación de riesgos y acciones correctivas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, exige a responsables y encargados implementar medidas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas para garantizar y demostrar el cumplimiento. Esta exigencia convierte la protección de datos en una responsabilidad continua que debe integrarse en la gestión ordinaria de las organizaciones.

Un sistema de cumplimiento eficaz no puede limitarse a disponer de documentos formales o cláusulas generales de privacidad. Debe existir correspondencia entre las reglas internas y las operaciones reales mediante las cuales se recolectan, almacenan, consultan, transfieren y eliminan datos personales. Prados et al. (2024) destacan que la gobernanza de la privacidad requiere componentes coordinados que permitan establecer responsabilidades, estructuras de decisión y mecanismos para controlar el cumplimiento de las exigencias legales. Desde esta perspectiva, la protección de datos debe incorporarse a la administración institucional como una función transversal, vinculada con los procesos tecnológicos, jurídicos, operativos y de supervisión.

La responsabilidad proactiva constituye uno de los fundamentos de estos sistemas porque exige demostrar que las medidas de protección fueron efectivamente implementadas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, incorpora la responsabilidad proactiva y demostrada entre los principios aplicables al tratamiento. Esto implica que el cumplimiento no se presume simplemente por la existencia de declaraciones institucionales, sino que debe poder comprobarse mediante registros, políticas, evaluaciones, evidencias de capacitación y controles periódicos. La documentación adquiere así una función probatoria, ya que permite reconstruir las decisiones adoptadas y verificar si la organización actuó de manera coherente con los riesgos asociados al tratamiento.

La asignación clara de responsabilidades internas constituye otro componente esencial. Cada organización debe determinar qué unidades o personas intervienen en la gestión de datos, quién autoriza tratamientos, quién supervisa medidas de seguridad y quién responde ante solicitudes o incidentes. La ausencia de responsabilidades definidas puede generar duplicidad de

funciones, omisiones y demoras en la respuesta frente a vulneraciones. Prados et al. (2024) señalan que la gobernanza de privacidad requiere articular funciones, procesos y mecanismos de rendición de cuentas dentro de la estructura institucional. Esta distribución permite transformar las obligaciones normativas en actividades concretas susceptibles de seguimiento, revisión y mejora.

El cumplimiento también requiere conocer qué datos posee la organización y para qué los utiliza. Sin un inventario actualizado de tratamientos resulta difícil determinar bases jurídicas, períodos de conservación, destinatarios, medidas de seguridad o riesgos específicos. La gestión sistemática de la información permite identificar tratamientos innecesarios, duplicados o incompatibles con las finalidades inicialmente establecidas. Issaoui et al. (2023), al analizar el cumplimiento de protección de datos en servicios en la nube, muestran que la complejidad tecnológica y la intervención de proveedores externos pueden dificultar la identificación de responsabilidades y condiciones de tratamiento. Esto exige fortalecer la trazabilidad sobre los flujos de información.

Los sistemas de cumplimiento deben incorporar además mecanismos de evaluación periódica. Las condiciones bajo las cuales se tratan los datos pueden cambiar por incorporación de nuevas tecnologías, modificaciones organizativas, ampliación de servicios o contratación de proveedores. Una medida adecuada en determinado momento puede volverse insuficiente frente a nuevas amenazas o transformaciones del tratamiento. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, exige verificar periódicamente la eficacia de las medidas implementadas. Esta revisión impide que el cumplimiento sea entendido como una actividad ejecutada una sola vez y obliga a mantener un proceso continuo de identificación, evaluación y corrección de deficiencias.

La formación del personal forma parte del sistema porque gran parte de las operaciones de tratamiento depende de decisiones humanas. Un trabajador puede provocar una vulneración al enviar información al destinatario equivocado, utilizar credenciales de manera inadecuada o conservar datos fuera de los sistemas autorizados. Las políticas internas requieren, por tanto, programas de capacitación relacionados con confidencialidad, seguridad, ejercicio de derechos y respuesta frente a incidentes. Prados et al. (2024) vinculan la gobernanza de privacidad con componentes organizacionales que permitan trasladar las reglas de protección a las prácticas cotidianas. La capacitación contribuye a reducir la distancia entre las obligaciones formales y las actuaciones concretas del personal.

La contratación de servicios externos representa un desafío adicional para los sistemas de cumplimiento. Una organización puede delegar almacenamiento, procesamiento o infraestructura, pero continúa necesitando controles sobre las condiciones en que sus datos son tratados. Issaoui et al. (2023) muestran que el cumplimiento en entornos de nube exige atender aspectos relacionados con responsabilidades compartidas, transparencia y control sobre proveedores. Por ello, antes de contratar un servicio debe evaluarse si el proveedor ofrece garantías suficientes y si sus prácticas son compatibles con las obligaciones del responsable. Los contratos deben acompañarse de mecanismos de supervisión capaces de verificar que las condiciones acordadas se mantienen durante la relación.

La automatización también puede apoyar determinadas actividades de cumplimiento cuando el volumen y complejidad de los tratamientos dificultan una revisión exclusivamente manual. Lorè et al. (2023) proponen un marco basado en inteligencia artificial orientado a apoyar decisiones relacionadas con cumplimiento, mostrando que las herramientas automatizadas pueden facilitar la identificación de requisitos, inconsistencias y riesgos regulatorios. Sin embargo, estos sistemas no eliminan la responsabilidad humana ni sustituyen la interpretación jurídica. Su utilidad depende de la calidad de los datos, criterios y reglas incorporados. La organización debe mantener capacidad de revisión para evitar que la automatización genere una falsa apariencia de conformidad normativa.

Los sistemas de cumplimiento deben incluir mecanismos de respuesta frente a desviaciones e incidentes. Detectar una deficiencia sin aplicar medidas correctivas reduce el valor del control interno y permite que el riesgo permanezca activo. La gestión debe establecer procedimientos para investigar incumplimientos, determinar sus causas, corregir controles y documentar las decisiones adoptadas. Esta lógica permite aprender de errores y fortalecer progresivamente las medidas existentes. La eficacia del sistema no se mide por la ausencia absoluta de incidentes, sino también por su capacidad para identificarlos oportunamente, contener sus efectos y modificar procesos cuando se demuestra que una práctica resulta incompatible con las obligaciones de protección de datos.

Un sistema de cumplimiento consolidado integra finalmente gobernanza, documentación, gestión de riesgos, capacitación, supervisión de proveedores y revisión continua. Su finalidad no consiste únicamente en evitar sanciones, sino en establecer condiciones organizativas que permitan utilizar información personal sin debilitar los derechos de los titulares. La responsabilidad demostrada exige que cada decisión relevante pueda justificarse mediante evidencia verificable y que los controles evolucionen junto con los tratamientos realizados. La

combinación de estructuras de gobernanza, herramientas tecnológicas y procedimientos de supervisión permite transformar la protección de datos en una práctica institucional permanente, capaz de responder tanto a exigencias normativas como a cambios tecnológicos y organizativos (Prados et al., 2024; Lorè et al., 2023).

5.2 Políticas internas y procedimientos para la gestión de información personal

Las políticas internas de protección de datos establecen los criterios que orientan la actuación de una organización cuando recolecta, utiliza, almacena, comparte o elimina información personal. Su función consiste en traducir las obligaciones jurídicas generales en reglas concretas aplicables a procesos, sistemas y personas. Una política eficaz debe determinar finalidades autorizadas, responsabilidades, niveles de acceso, períodos de conservación y procedimientos frente a incidentes o solicitudes de titulares. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, exige la adopción de medidas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, por lo que las políticas internas forman parte del cumplimiento demostrable.

La elaboración de políticas requiere partir de las actividades reales de tratamiento y no de modelos genéricos desconectados de la operación institucional. Cada organización administra categorías diferentes de datos, utiliza tecnologías particulares y mantiene relaciones específicas con proveedores, usuarios o trabajadores. Por ello, las reglas internas deben responder al contexto y al nivel de riesgo existente. Prados et al. (2024) sostienen que la gobernanza de la privacidad depende de la articulación entre estructuras, responsabilidades y procedimientos capaces de convertir las exigencias legales en prácticas verificables. Una política demasiado general puede resultar insuficiente para orientar decisiones concretas y demostrar que los controles fueron diseñados según necesidades identificadas.

Los procedimientos complementan las políticas porque describen cómo deben ejecutarse determinadas actuaciones. Mientras la política establece qué debe protegerse y bajo qué criterios, el procedimiento determina quién interviene, qué pasos debe seguir, qué documentación debe generar y qué controles debe aplicar. Esta distinción es importante para actividades como la atención de derechos, autorización de accesos, eliminación de información, gestión de proveedores o respuesta ante vulneraciones. Los procedimientos permiten reducir decisiones improvisadas y mantener criterios relativamente uniformes entre distintas unidades. Además, facilitan la supervisión posterior porque dejan evidencia sobre las

actuaciones realizadas y permiten comparar la práctica institucional con las reglas previamente aprobadas.

La gestión de accesos constituye uno de los ámbitos que requieren procedimientos detallados. No todo trabajador necesita consultar toda la información administrada por una organización, por lo que deben asignarse permisos según funciones y necesidades concretas. Las políticas deberían definir criterios para crear, modificar y retirar credenciales, revisar privilegios y registrar actividades relevantes. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, reconoce los principios de confidencialidad y seguridad, que obligan a preservar la información frente a accesos o usos incompatibles con el tratamiento autorizado. La gestión interna debe impedir que la disponibilidad técnica de los datos se convierta en autorización indiscriminada para utilizarlos.

Los períodos de conservación también deben incorporarse a las políticas institucionales. Mantener datos indefinidamente aumenta la superficie de exposición y dificulta justificar tratamientos cuya finalidad ya terminó. Los procedimientos deben establecer criterios para revisar archivos, eliminar información innecesaria y conservar únicamente aquello que continúe siendo legítimamente requerido. Estas decisiones deben aplicarse tanto a documentos principales como a copias, respaldos y sistemas secundarios. Una gestión adecuada evita que información aparentemente eliminada permanezca disponible en repositorios olvidados. El cumplimiento requiere, por tanto, vincular cada categoría de datos con una finalidad, un período de conservación y una forma segura de eliminación cuando desaparezca la necesidad que justificó su tratamiento.

Las políticas deben regular igualmente la relación con proveedores y encargados externos. La contratación de servicios de almacenamiento, nube, soporte o procesamiento puede trasladar operaciones técnicas, pero no elimina la necesidad de controlar cómo se administra la información. Issaoui et al. (2023) identifican dificultades de cumplimiento en servicios en la nube relacionadas con distribución de responsabilidades, transparencia y control sobre proveedores. Por ello, los procedimientos internos deben incluir criterios de selección, revisión contractual, delimitación de instrucciones, gestión de accesos y supervisión periódica. La organización necesita conocer dónde se procesan sus datos, quién puede acceder a ellos y qué medidas existen para responder ante incidentes o terminación del servicio.

La capacitación debe integrarse a estas políticas porque las reglas escritas resultan insuficientes si el personal desconoce cómo aplicarlas. Los procedimientos deberían especificar qué

personas reciben formación, con qué periodicidad y sobre qué aspectos de protección de datos. La capacitación puede abarcar confidencialidad, manejo de documentos, prevención de errores, reconocimiento de incidentes y atención de solicitudes. Prados et al. (2024) destacan que una estructura de gobernanza requiere mecanismos capaces de incorporar la privacidad a la actuación organizacional. Esto supone transformar las obligaciones jurídicas en comportamientos cotidianos y establecer responsabilidades cuando una persona utiliza información fuera de las funciones que le fueron asignadas.

En las entidades sometidas a obligaciones de transparencia, las políticas internas deben además diferenciar claramente entre información pública e información que no puede divulgarse libremente. La Ley Orgánica de Transparencia y Acceso a la Información Pública (2023), en su artículo 4, numeral 5, define la información confidencial e incluye aquella vinculada con la privacidad y los datos personales cuya difusión requiere consentimiento, remitiendo su tratamiento a la legislación de protección de datos. Esta distinción exige procedimientos de revisión antes de publicar o entregar documentos, de manera que el cumplimiento del deber de transparencia no provoque una divulgación indebida de información personal.

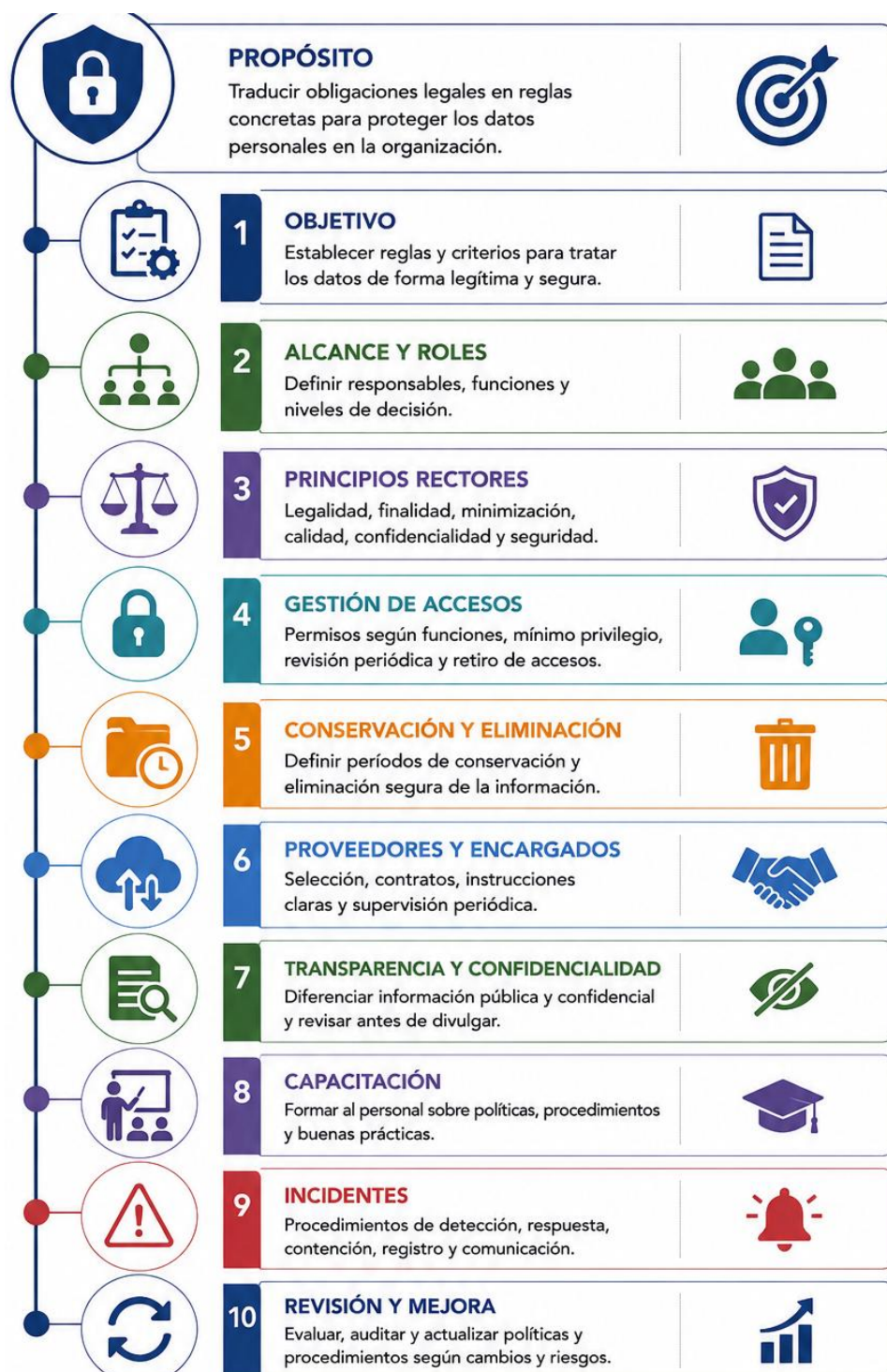
La gestión documental debe incorporar controles capaces de aplicar esa diferenciación en la práctica. Antes de divulgar expedientes, bases de datos o documentos administrativos, la organización debe identificar si contienen información personal, determinar si existe fundamento para su entrega y aplicar, cuando corresponda, mecanismos de anonimización, ocultamiento o separación de contenidos. La transparencia y la privacidad no deben abordarse como obligaciones aisladas, porque pueden coincidir dentro de un mismo documento. Un procedimiento interno bien diseñado permite entregar aquello que tiene carácter público sin exponer información que pertenece al ámbito protegido del titular. Esta revisión previa reduce conflictos y fortalece la coherencia entre distintas obligaciones institucionales.

Las políticas internas necesitan mecanismos de actualización porque los tratamientos y riesgos cambian con el tiempo. Nuevos sistemas, modificaciones legales, cambios de proveedores o incorporación de herramientas automatizadas pueden volver insuficientes procedimientos anteriormente adecuados. La revisión periódica debe identificar desviaciones entre lo establecido y la práctica, evaluar incidentes y adaptar controles cuando existan nuevas condiciones. Un sistema de cumplimiento maduro utiliza auditorías, registros y resultados de evaluaciones para modificar sus políticas. La finalidad no consiste en acumular documentos, sino en mantener reglas operativas capaces de responder a las condiciones reales bajo las cuales

se gestiona la información personal y demostrar que las decisiones adoptadas poseen fundamento verificable.

Figura 10

Políticas internas para la gestión y protección de datos personales



Nota. El esquema organiza los principales componentes que orientan la gestión interna de la información personal, desde la definición de responsabilidades y controles hasta la capacitación, respuesta a incidentes y mejora continua.

La eficacia de las políticas depende finalmente de su integración con la estructura institucional. Deben existir responsables identificables, recursos suficientes, procedimientos conocidos y mecanismos para controlar su aplicación. Una política que no determina quién debe actuar frente a una solicitud, una brecha o una eliminación pendiente pierde utilidad práctica. La gestión de información personal requiere conectar normas internas con actividades concretas y establecer evidencia de cumplimiento en cada etapa. Esta articulación permite reducir riesgos, asignar responsabilidades y corregir prácticas inconsistentes. Las políticas se convierten así en instrumentos de gobernanza que ordenan el tratamiento y hacen posible demostrar que la privacidad forma parte de la gestión cotidiana de la organización (Prados et al., 2024).

5.3 Protección de datos desde el diseño y por defecto

La protección de datos desde el diseño supone incorporar las exigencias de privacidad desde las primeras etapas de planificación de productos, servicios, procesos y sistemas que impliquen tratamiento de información personal. Su finalidad es evitar que la protección se añada únicamente después de que aparezcan riesgos o incidentes. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 39, establece que el responsable debe considerar desde las fases iniciales de concepción y diseño los riesgos que determinados tratamientos pueden generar para los derechos de los titulares e implementar medidas técnicas, organizativas y de otra naturaleza orientadas al cumplimiento normativo.

Este enfoque exige integrar criterios jurídicos y técnicos durante la definición de funcionalidades, arquitectura, permisos, almacenamiento y circulación de los datos. La privacidad deja así de funcionar como un control posterior y se convierte en una condición del propio diseño. Von Grafenstein et al. (2022) sostienen que una protección efectiva desde el diseño requiere métodos interdisciplinarios capaces de conectar objetivos jurídicos con decisiones concretas de diseño y experiencia de usuario. Esta integración es especialmente importante al definir finalidades, porque una formulación imprecisa puede conducir a recolección excesiva, usos secundarios y configuraciones que dificulten al titular comprender o controlar el tratamiento realizado.

La protección por defecto complementa este enfoque mediante configuraciones iniciales orientadas a limitar el tratamiento a lo estrictamente necesario. El artículo 39 de la Ley Orgánica de Protección de Datos Personales (2021) dispone que, por defecto, solo deben tratarse los datos personales necesarios para cada una de las finalidades establecidas. Esto significa que una persona no debería tener que modificar opciones complejas para alcanzar un

nivel razonable de privacidad. La configuración inicial debe evitar recolecciones innecesarias, accesos indiscriminados o difusión excesiva, colocando la minimización de datos como condición ordinaria del funcionamiento del sistema y no como una alternativa que dependa de la iniciativa del titular.

La aplicación práctica de estos principios requiere analizar qué información resulta indispensable para cada función. Un formulario digital, por ejemplo, no debería solicitar datos que no sean necesarios para prestar el servicio previsto, mientras que una plataforma debería restringir inicialmente la visibilidad de la información a los destinatarios requeridos. Von Grafenstein et al. (2022) muestran que la especificación efectiva de las finalidades puede fortalecerse mediante metodologías centradas en el usuario, porque permiten relacionar los objetivos del tratamiento con los procesos concretos donde se capturan y utilizan datos. Esta perspectiva ayuda a evitar que las decisiones técnicas amplíen silenciosamente el alcance inicialmente previsto.

La protección desde el diseño también exige anticipar escenarios de riesgo antes de implementar un sistema. Entre las decisiones relevantes se encuentran la forma de autenticar usuarios, separar bases de datos, establecer tiempos de conservación, gestionar permisos y reducir posibilidades de reidentificación. El responsable debe valorar tanto el estado de la técnica como la naturaleza y finalidad del tratamiento, conforme dispone el artículo 39 de la Ley Orgánica de Protección de Datos Personales (2021). El análisis temprano permite modificar un proyecto cuando todavía resulta viable hacerlo, evitando que deficiencias estructurales se consoliden y requieran posteriormente intervenciones más costosas o menos eficaces.

Tabla 14
Aplicación de la protección de datos desde el diseño y por defecto

Dimensión	Aplicación desde el diseño	Aplicación por defecto
Recolección	Determinar previamente qué datos son necesarios.	Solicitar inicialmente solo la información indispensable.
Acceso	Diseñar perfiles y permisos según funciones.	Mantener restringido el acceso salvo habilitación justificada.
Finalidad	Definir usos específicos antes de desarrollar el tratamiento.	Evitar activación automática de usos adicionales.
Conservación	Incorporar períodos y mecanismos de eliminación.	No conservar datos más tiempo del necesario.
Visibilidad	Diseñar controles sobre divulgación y destinatarios.	Mantener la configuración menos expansiva de exposición.

Dimensión	Aplicación desde el diseño	Aplicación por defecto
Seguridad	Integrar medidas técnicas y organizativas desde el proyecto.	Activar inicialmente las protecciones necesarias.
Derechos	Facilitar mecanismos de acceso, rectificación y demás derechos.	Presentar opciones comprensibles sin configuraciones innecesariamente complejas.
Evaluación	Examinar riesgos antes de implementar cambios o servicios.	Mantener configuraciones coherentes con la minimización del tratamiento.

Nota. La tabla diferencia la incorporación preventiva de garantías durante el desarrollo de un tratamiento y las configuraciones iniciales que limitan automáticamente el uso de datos a lo necesario.

La minimización constituye uno de los efectos más relevantes de la protección por defecto. Reducir el volumen de información tratada disminuye tanto la exposición ante incidentes como las posibilidades de utilización incompatible con la finalidad original. Este criterio debe aplicarse a cantidad, alcance, accesibilidad y tiempo de conservación. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 39, vincula expresamente la configuración por defecto con el tratamiento exclusivo de los datos necesarios para cada finalidad. La obligación, por tanto, no se limita a interfaces visibles para el usuario, sino que también alcanza decisiones internas sobre sistemas, bases de datos y procesos automatizados.

El diseño debe considerar además la comprensión del titular. Una interfaz puede ofrecer formalmente opciones de privacidad y, al mismo tiempo, dificultar su utilización mediante configuraciones confusas o decisiones predeterminadas excesivamente invasivas. Von Grafenstein et al. (2022) destacan la importancia de integrar enfoques centrados en el usuario para lograr que las exigencias jurídicas puedan materializarse efectivamente en la interacción con los sistemas. Esto implica diseñar opciones comprensibles, evitar recorridos innecesariamente complejos y relacionar las decisiones del usuario con finalidades claramente determinadas. La eficacia de la privacidad depende también de que las garantías puedan utilizarse en condiciones reales y no únicamente de que aparezcan formalmente disponibles.

La protección desde el diseño debe mantenerse durante todo el ciclo de vida del tratamiento. Una aplicación inicialmente adecuada puede incorporar posteriormente nuevas funciones, integraciones o fuentes de información capaces de alterar sus riesgos. Cada modificación relevante exige revisar si continúan siendo suficientes las medidas adoptadas y si las configuraciones predeterminadas siguen limitando el tratamiento a lo necesario. Esta lógica enlaza el diseño con la responsabilidad proactiva, porque obliga a justificar las decisiones técnicas y organizativas a medida que evoluciona el sistema. La protección no termina con el

lanzamiento del producto o servicio, sino que requiere revisión permanente frente a cambios funcionales, tecnológicos y organizativos.

La incorporación de privacidad desde el diseño y por defecto modifica, finalmente, la manera de entender el cumplimiento. En lugar de corregir vulnerabilidades cuando el tratamiento ya está funcionando, obliga a preguntarse desde el inicio qué datos son necesarios, quién debe acceder a ellos, cuánto tiempo deben conservarse y qué riesgos generan para las personas. El artículo 39 de la Ley Orgánica de Protección de Datos Personales (2021) convierte esta lógica preventiva en una obligación concreta del responsable, mientras que la evidencia académica muestra que su aplicación efectiva exige coordinación entre disciplinas jurídicas, técnicas y de diseño (von Grafenstein et al., 2022).

5.4 Evaluación de riesgos e impacto en la privacidad

La evaluación de riesgos permite identificar anticipadamente las condiciones que pueden comprometer la confidencialidad, integridad, disponibilidad o uso legítimo de los datos personales. Su propósito no consiste únicamente en reconocer amenazas técnicas, sino en determinar cómo un tratamiento puede afectar los derechos y libertades de las personas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 40, exige que responsables y encargados utilicen una metodología de análisis que considere las particularidades del tratamiento, las partes involucradas, las categorías y el volumen de datos utilizados. Esta valoración constituye una base necesaria para adoptar medidas de seguridad proporcionales al riesgo identificado.

El análisis debe contemplar tanto la probabilidad de que ocurra un evento como la gravedad de sus posibles consecuencias. Un tratamiento de información identificativa básica no presenta necesariamente el mismo riesgo que uno basado en datos sensibles, perfiles automatizados o grandes volúmenes de información. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 41, establece que la determinación de medidas de seguridad debe considerar los resultados del análisis de riesgos, la naturaleza de los datos, las características de las partes involucradas y antecedentes relacionados con pérdida, destrucción, divulgación o accesos no autorizados. De esta manera, seguridad y riesgo quedan jurídicamente vinculados.

Cuando el tratamiento puede generar un alto riesgo para los titulares, el análisis general debe complementarse con una evaluación de impacto en protección de datos. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 42, establece que el responsable debe realizarla cuando, debido a la naturaleza, contexto o finalidades del tratamiento, exista

probabilidad de alto riesgo para los derechos y libertades del titular o cuando lo requiera la autoridad competente. Esta evaluación tiene carácter preventivo porque busca identificar consecuencias antes de ejecutar o mantener tratamientos cuya complejidad, alcance o sensibilidad exige un nivel superior de análisis.

La evaluación de impacto adquiere especial relevancia cuando las organizaciones manejan información sensible o utilizan infraestructuras tecnológicas complejas. Georgiou y Lambrinoudakis (2021), al analizar evaluaciones de impacto en organizaciones sanitarias basadas en servicios de nube, muestran que la identificación estructurada de amenazas y consecuencias facilita seleccionar salvaguardas apropiadas para tratamientos donde confluyen datos sensibles, proveedores tecnológicos y riesgos de seguridad. Este enfoque permite pasar de una protección genérica a decisiones basadas en escenarios concretos. La evaluación debe considerar procesos, tecnologías, actores y posibles efectos sobre las personas, evitando que el cumplimiento se reduzca a una revisión exclusivamente documental.

La normativa ecuatoriana identifica circunstancias en las que la evaluación de impacto es obligatoria. El artículo 42 de la Ley Orgánica de Protección de Datos Personales (2021) incluye la evaluación sistemática y exhaustiva de aspectos personales basada en tratamiento automatizado cuando sustenta decisiones con efectos jurídicos, el tratamiento a gran escala de categorías especiales de datos o información relativa a condenas e infracciones penales y la observación sistemática a gran escala de zonas de acceso público. Estos supuestos reflejan escenarios donde el alcance o la sensibilidad del tratamiento incrementan considerablemente las posibles consecuencias para los titulares y justifican controles preventivos reforzados.

Tabla 15
Componentes de la evaluación de riesgos e impacto en la privacidad

Componente	Aspecto analizado	Finalidad dentro de la evaluación
Naturaleza del tratamiento	Tipo y sensibilidad de los datos utilizados.	Determinar el nivel de protección requerido.
Alcance	Volumen de datos, número de titulares y extensión del tratamiento.	Identificar la magnitud de una posible afectación.
Contexto	Entorno tecnológico, organizativo y relación entre los actores.	Reconocer circunstancias que modifican el riesgo.
Finalidad	Objetivos para los cuales se realiza el tratamiento.	Comprobar necesidad y coherencia del uso de los datos.
Amenazas	Acceso indebido, pérdida, alteración, filtración o uso incompatible.	Identificar eventos capaces de producir una afectación.
Consecuencias	Posibles efectos sobre derechos y libertades.	Estimar la gravedad de los impactos.

Componente	Aspecto analizado	Finalidad dentro de la evaluación
Probabilidad	Posibilidad de materialización de cada riesgo.	Priorizar riesgos que requieren intervención.
Salvaguardas	Medidas técnicas, organizativas y jurídicas previstas.	Reducir probabilidad o impacto del riesgo.
Riesgo residual	Nivel que permanece después de aplicar controles.	Determinar si resulta necesario adoptar medidas adicionales.

Nota. La tabla organiza los elementos que permiten relacionar las características del tratamiento con sus posibles consecuencias y con las medidas destinadas a reducir los riesgos para los titulares.

Una evaluación de impacto no debe convertirse en un documento estático preparado únicamente para demostrar cumplimiento. Su utilidad depende de que pueda modificar decisiones reales sobre el tratamiento. El Reglamento General a la Ley Orgánica de Protección de Datos Personales (2023), en su artículo 30, concibe esta evaluación como un instrumento preventivo orientado a identificar riesgos, describir acciones para gestionarlos y fortalecer una cultura preventiva de protección de datos. Esto implica que los resultados deben influir en la arquitectura tecnológica, las configuraciones de seguridad, los procedimientos y las condiciones bajo las cuales se autoriza un tratamiento.

El contenido de la evaluación debe permitir comprender por qué el tratamiento resulta necesario y cómo se pretende controlar sus consecuencias. El Reglamento General a la Ley Orgánica de Protección de Datos Personales (2023), en su artículo 32, exige incluir una descripción sistemática de las operaciones y finalidades, la justificación de su necesidad y proporcionalidad, la evaluación de riesgos para los derechos y libertades y las medidas previstas para afrontarlos. Estas exigencias conectan el análisis jurídico con decisiones técnicas y organizativas verificables. La evaluación no se limita a enumerar amenazas, sino que debe justificar por qué las salvaguardas seleccionadas resultan adecuadas frente a los riesgos identificados.

La evaluación requiere también revisión cuando cambian significativamente las condiciones del tratamiento. La incorporación de nuevas fuentes de información, proveedores, algoritmos, finalidades o tecnologías puede modificar riesgos que anteriormente habían sido considerados aceptables. Georgiou y Lambrinoudakis (2021) muestran que los entornos tecnológicos dinámicos requieren metodologías capaces de revisar periódicamente amenazas y controles. Esto impide asumir que una evaluación inicial continúa siendo válida indefinidamente. La gestión de privacidad debe funcionar como un ciclo en el que identificación, valoración,

mitigación y seguimiento se actualicen conforme evoluciona el tratamiento y aparezcan nuevas posibilidades de afectación para los titulares.

La evaluación de riesgos e impacto permite, finalmente, justificar decisiones antes de que una vulneración ocurra. Su valor jurídico y organizativo radica en demostrar que el responsable comprendió las características del tratamiento, anticipó consecuencias previsibles y seleccionó medidas proporcionales. Cuando el riesgo resulta elevado, la evaluación de impacto profundiza ese examen y obliga a relacionar cada amenaza con salvaguardas específicas. La combinación de los artículos 40, 41 y 42 de la Ley Orgánica de Protección de Datos Personales (2021) configura así una secuencia preventiva: identificar riesgos, determinar medidas y profundizar el análisis cuando las posibles afectaciones alcanzan un nivel especialmente significativo.

5.5 Medidas técnicas y organizativas para la seguridad de los datos

Las medidas técnicas y organizativas constituyen el núcleo operativo de la seguridad de los datos personales porque permiten reducir la probabilidad de accesos indebidos, pérdidas, alteraciones o divulgaciones no autorizadas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 10, establece el principio de seguridad y exige implementar medidas adecuadas y necesarias, atendiendo al estado de la técnica, la naturaleza de los datos y el contexto del tratamiento. Esta obligación impide aplicar soluciones idénticas a todos los escenarios, pues la intensidad de los controles debe responder al nivel concreto de riesgo que enfrenta cada organización.

Las medidas técnicas comprenden mecanismos incorporados directamente a sistemas, redes y dispositivos. Entre ellas pueden incluirse autenticación robusta, cifrado, copias de respaldo, segmentación de redes, registro de actividades, actualización de software y controles destinados a detectar comportamientos anómalos. Selzer (2021) sostiene que la adecuación de las medidas de seguridad no puede determinarse mediante una lista rígida de controles, sino que requiere valorar riesgos, capacidades tecnológicas y circunstancias específicas del tratamiento. Esta lógica resulta especialmente importante porque una herramienta técnicamente avanzada puede ser insuficiente si no responde a las amenazas reales o si se implementa de manera incorrecta dentro de la infraestructura.

Las medidas organizativas actúan sobre personas, responsabilidades y procedimientos. Incluyen asignación de funciones, políticas de acceso, capacitación, protocolos para incidentes, revisión de permisos, gestión de proveedores y mecanismos de supervisión. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, obliga al responsable a

implementar herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, además de verificar periódicamente su eficiencia, eficacia y efectividad. La norma exige también adoptar medidas destinadas a prevenir, impedir, reducir, mitigar y controlar los riesgos y vulneraciones identificados, reforzando la necesidad de combinar distintas capas de protección.

La elección de controles debe partir de una evaluación de riesgo y no de la simple disponibilidad de herramientas tecnológicas. Una organización que maneja datos sensibles, grandes volúmenes de información o servicios accesibles desde Internet necesita considerar amenazas diferentes a las de un tratamiento reducido y exclusivamente interno. Selzer (2021) plantea que la proporcionalidad entre riesgo y medida resulta esencial para determinar si las salvaguardas adoptadas pueden considerarse apropiadas. Este enfoque obliga a revisar continuamente las decisiones de seguridad, pues cambios en tecnologías, vulnerabilidades o formas de tratamiento pueden modificar el nivel de protección requerido y dejar obsoletas medidas anteriormente suficientes.

La seguridad también depende de las condiciones impuestas a proveedores y servicios externos. Cuando almacenamiento, procesamiento o infraestructura son delegados, el responsable necesita evaluar las garantías del proveedor y mantener mecanismos de supervisión. Issaoui et al. (2023) muestran que los servicios en la nube plantean dificultades vinculadas con distribución de responsabilidades, transparencia y control sobre medidas de privacidad. La externalización no elimina el riesgo ni convierte automáticamente al proveedor en único responsable de la seguridad. La organización debe conocer cómo se protegen los datos, quién puede acceder a ellos y qué procedimientos existen para detectar, comunicar y responder frente a incidentes.

Tabla 16
Medidas técnicas y organizativas para la seguridad de los datos personales

Tipo de medida	Aplicación	Riesgo que contribuye a reducir
Control de acceso	Asignación de permisos según funciones y necesidad.	Consulta o modificación no autorizada.
Autenticación	Verificación de identidad antes del ingreso a sistemas.	Uso indebido de credenciales.
Cifrado	Protección de información almacenada o transmitida.	Lectura de datos por terceros no autorizados.
Copias de respaldo	Conservación de versiones recuperables de información.	Pérdida o destrucción de datos.

Tipo de medida	Aplicación	Riesgo que contribuye a reducir
Registro de actividades	Conservación de evidencias sobre accesos y operaciones.	Falta de trazabilidad frente a incidentes.
Actualización tecnológica	Corrección de vulnerabilidades conocidas.	Explotación de fallas de seguridad.
Capacitación	Formación del personal sobre prácticas seguras.	Errores humanos y usos inadecuados.
Gestión de proveedores	Evaluación y supervisión de terceros.	Riesgos derivados de tratamientos externalizados.
Respuesta a incidentes	Procedimientos para detectar, contener y corregir eventos.	Ampliación de los efectos de una vulneración.

Nota. La tabla relaciona controles tecnológicos y organizativos con los riesgos que buscan reducir dentro de una estrategia integral de seguridad.

El control de acceso debe responder al principio de necesidad funcional. La posibilidad técnica de consultar información no significa que todas las personas de una organización deban disponer de esa facultad. Los privilegios deben concederse según responsabilidades y revisarse cuando cambian las funciones, termina una relación laboral o desaparece la necesidad que justificó el acceso. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, exige además suscribir compromisos de confidencialidad y manejo adecuado con quienes intervienen en el tratamiento. De esta forma, los controles tecnológicos se complementan con obligaciones organizativas destinadas a limitar el uso indebido de información.

La resiliencia constituye otra dimensión importante de la seguridad. No basta con impedir accesos indebidos; los sistemas deben mantener o recuperar funciones esenciales cuando ocurre una falla, ataque o pérdida de información. Las copias de seguridad, planes de continuidad y procedimientos de recuperación reducen el impacto de incidentes que afectan disponibilidad o integridad. Selzer (2021) destaca que la adecuación de las medidas requiere considerar no solo mecanismos preventivos, sino también la capacidad para enfrentar materializaciones del riesgo. Esta perspectiva reconoce que ninguna arquitectura elimina completamente las vulnerabilidades y que la protección debe incluir respuestas capaces de preservar la continuidad y restablecer condiciones seguras.

La eficacia de las medidas necesita verificarse periódicamente. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, obliga a implementar procesos de verificación, evaluación y valoración periódica de los controles adoptados. Esto puede traducirse en revisiones de permisos, pruebas de recuperación, auditorías, análisis de vulnerabilidades o evaluación de procedimientos internos. Una medida que nunca es comprobada puede generar

una apariencia de seguridad sin ofrecer protección efectiva. La revisión permite detectar configuraciones deficientes, controles obsoletos y cambios en el entorno que requieren ajustes antes de que se conviertan en causas de una vulneración.

Las medidas técnicas y organizativas deben funcionar finalmente como un sistema integrado y no como controles independientes. La tecnología puede limitar accesos, pero pierde eficacia cuando existen contraseñas compartidas, procedimientos deficientes o proveedores sin supervisión. Del mismo modo, una política interna resulta insuficiente si los sistemas permiten operaciones incompatibles con ella. La seguridad exige relacionar riesgo, tecnología, personal, procesos y supervisión para construir capas complementarias de protección. Este enfoque permite que las medidas evolucionen conforme cambian las amenazas y las condiciones del tratamiento, manteniendo un nivel de protección proporcional y demostrable frente a los riesgos identificados (Selzer, 2021; Issaoui et al., 2023).

5.6 Supervisión, auditoría y control del cumplimiento normativo

La supervisión del cumplimiento permite verificar si las políticas, procedimientos y medidas de protección de datos funcionan realmente dentro de la organización. Su propósito no consiste únicamente en detectar incumplimientos, sino también en identificar desviaciones antes de que produzcan una vulneración. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, exige implementar procesos de verificación, evaluación y valoración periódica de las medidas adoptadas. Esta obligación transforma la supervisión en una actividad continua vinculada con la responsabilidad demostrada, pues el responsable debe disponer de evidencias que permitan comprobar que los controles establecidos permanecen adecuados frente a los riesgos del tratamiento.

La auditoría constituye un mecanismo más estructurado para examinar el cumplimiento de obligaciones jurídicas, técnicas y organizativas. Puede abarcar políticas internas, registros de tratamiento, controles de acceso, contratos con encargados, gestión de incidentes, atención de derechos y medidas de seguridad. Prados et al. (2024) destacan que una gobernanza efectiva de la privacidad requiere mecanismos de seguimiento capaces de verificar responsabilidades y evaluar si las estructuras adoptadas funcionan conforme a los objetivos previstos. La auditoría permite identificar diferencias entre lo establecido documentalmente y las prácticas efectivamente desarrolladas, evitando que la conformidad normativa se limite a políticas que no se aplican en las operaciones cotidianas.

El alcance de una auditoría debe responder a las características del tratamiento. Una revisión superficial puede resultar insuficiente cuando la organización administra datos sensibles, grandes bases de información, sistemas automatizados o servicios externalizados. Deben establecerse criterios de evaluación relacionados con finalidad, minimización, conservación, seguridad, ejercicio de derechos y gestión de proveedores. Issaoui et al. (2023) muestran que los entornos de servicios en la nube dificultan el control directo sobre determinadas operaciones y exigen mayor claridad respecto de responsabilidades y garantías. Por ello, la auditoría debe extenderse también a aquellos tratamientos ejecutados por terceros cuando puedan afectar el cumplimiento del responsable.

El control normativo requiere disponer de indicadores que permitan observar cambios y detectar posibles desviaciones. Entre ellos pueden considerarse solicitudes de titulares pendientes, incidentes registrados, accesos indebidos, resultados de pruebas de seguridad, períodos de conservación incumplidos o deficiencias identificadas en proveedores. Estos indicadores no sustituyen el análisis jurídico, pero permiten priorizar áreas que requieren revisión. Lorè et al. (2023) muestran que herramientas basadas en inteligencia artificial pueden apoyar determinadas decisiones relacionadas con evaluación de cumplimiento, facilitando el análisis de grandes conjuntos de requisitos. Su utilización, sin embargo, debe mantenerse bajo supervisión humana y no convertirse en una decisión automática sobre conformidad normativa.

Los resultados de la supervisión deben traducirse en medidas correctivas. Identificar una vulnerabilidad sin establecer responsables, plazos y acciones concretas deja intacto el riesgo que motivó la revisión. El seguimiento posterior debe comprobar que las deficiencias fueron efectivamente corregidas y que las modificaciones no generaron nuevos problemas. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 47, vincula la responsabilidad con la evaluación periódica de la eficacia de las medidas implementadas. Esta exigencia permite entender la auditoría como parte de un ciclo de mejora en el que revisión, corrección y nueva verificación se suceden de manera sistemática.

Tabla 17

Mecanismos de supervisión, auditoría y control del cumplimiento normativo

Mecanismo	Aspecto examinado	Evidencia esperada	Resultado esperado
Supervisión periódica	Aplicación cotidiana de políticas y procedimientos.	Registros, reportes e indicadores internos.	Detección temprana de desviaciones.
Auditoría de cumplimiento	Adecuación de procesos a obligaciones jurídicas.	Informes, matrices y documentos verificables.	Identificación de incumplimientos y áreas de mejora.

Mecanismo	Aspecto examinado	Evidencia esperada	Resultado esperado
Revisión de accesos	Permisos asignados a usuarios y perfiles.	Registros de autenticación y autorizaciones.	Eliminación de privilegios innecesarios.
Control de proveedores	Cumplimiento de encargados y terceros.	Contratos, reportes y evidencias técnicas.	Reducción de riesgos externalizados.
Evaluación de incidentes	Causas y respuesta frente a vulneraciones.	Registros de incidentes y acciones adoptadas.	Corrección de fallas recurrentes.
Revisión de conservación	Permanencia de información en sistemas y archivos.	Inventarios y cronogramas de eliminación.	Supresión de datos innecesarios.
Seguimiento correctivo	Cumplimiento de acciones derivadas de auditorías.	Planes, responsables y plazos de mejora.	Cierre verificable de deficiencias.
Control automatizado	Identificación asistida de requisitos o inconsistencias.	Reportes generados y revisión humana.	Apoyo al análisis sistemático del cumplimiento.

Nota. La tabla organiza mecanismos complementarios de control y muestra las evidencias que permiten verificar si las obligaciones de protección de datos se aplican efectivamente.

La independencia y objetividad fortalecen la utilidad de la auditoría. Cuando una misma unidad diseña, aplica y evalúa todos sus controles sin ninguna revisión adicional, aumenta el riesgo de normalizar deficiencias o ignorar conflictos de interés. La supervisión puede combinar controles internos con revisiones especializadas según la complejidad de la organización. Prados et al. (2024) relacionan la gobernanza de privacidad con la definición clara de responsabilidades y mecanismos de rendición de cuentas. Lo importante es que la evaluación pueda cuestionar prácticas existentes, solicitar evidencias y formular acciones correctivas sin reducirse a una comprobación formal destinada únicamente a confirmar decisiones previamente adoptadas.

La trazabilidad resulta indispensable para demostrar cumplimiento durante una revisión. Las organizaciones deben conservar evidencias suficientes sobre decisiones, autorizaciones, evaluaciones de riesgos, incidentes, solicitudes de titulares, capacitaciones y modificaciones de controles. Sin documentación resulta difícil determinar si una actuación fue adecuada o reconstruir las circunstancias que originaron un incumplimiento. El principio de responsabilidad proactiva y demostrada previsto en el artículo 10 de la Ley Orgánica de Protección de Datos Personales (2021) refuerza esta exigencia. El cumplimiento no depende solo de realizar correctamente una actividad, sino también de poder acreditar posteriormente qué se hizo, por qué se hizo y qué controles respaldaron la decisión.

Figura 11

Supervisión, auditoría y control del cumplimiento normativo



Nota. El esquema sintetiza el proceso continuo de revisión, evaluación, corrección y documentación que permite verificar la eficacia de las medidas de protección de datos y demostrar el cumplimiento normativo.

La tecnología puede mejorar la supervisión cuando permite identificar anomalías, organizar evidencias o comparar prácticas con criterios previamente definidos. Lorè et al. (2023) muestran que los sistemas automatizados pueden apoyar la evaluación de requisitos regulatorios y facilitar procesos de decisión relacionados con cumplimiento. Sin embargo, una herramienta no puede determinar por sí sola la adecuación jurídica de todos los tratamientos, pues conceptos como proporcionalidad, necesidad o riesgo requieren interpretación contextual. La automatización debe utilizarse como apoyo a profesionales responsables de evaluar

resultados, verificar excepciones y justificar decisiones, evitando sustituir la rendición de cuentas por una conclusión generada únicamente mediante reglas computacionales.

La supervisión y la auditoría adquieren verdadero valor cuando forman parte de un proceso continuo de mejora. Cada hallazgo debe permitir revisar causas, modificar procedimientos y comprobar posteriormente si la corrección resultó eficaz. Una organización que audita únicamente cuando enfrenta una inspección o una vulneración mantiene un enfoque reactivo incompatible con la responsabilidad demostrada. El artículo 47 de la Ley Orgánica de Protección de Datos Personales (2021) exige precisamente evaluación periódica de las medidas implementadas. El control normativo debe funcionar, por tanto, como un mecanismo permanente que conecte evidencia, riesgo, corrección y aprendizaje institucional para sostener niveles adecuados de protección a lo largo del tiempo.

5.7 Mecanismos institucionales y jurídicos para la tutela efectiva de la privacidad

La tutela efectiva de la privacidad requiere mecanismos capaces de prevenir vulneraciones, controlar el cumplimiento y ofrecer respuestas cuando los derechos de los titulares resultan afectados. Su eficacia depende de la articulación entre responsables del tratamiento, autoridades administrativas y órganos jurisdiccionales, pues cada instancia cumple una función distinta dentro del sistema. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 1, establece entre sus finalidades garantizar el ejercicio del derecho a la protección de datos personales mediante principios, derechos, obligaciones y mecanismos de tutela. Esta configuración impide reducir la protección a reglas preventivas y exige disponer de vías concretas para exigir su cumplimiento.

La primera forma de tutela se desarrolla ante el propio responsable del tratamiento. El titular puede ejercer directamente los derechos reconocidos sobre su información y exigir que determinadas actuaciones sean corregidas cuando resulten incompatibles con la normativa. Este nivel resulta importante porque permite solucionar controversias sin acudir inmediatamente a instancias administrativas o judiciales. Para que funcione adecuadamente, las organizaciones deben disponer de canales accesibles, identificar responsables de atención y documentar las respuestas proporcionadas. Los mecanismos internos de cumplimiento fortalecen esta capacidad cuando asignan responsabilidades y conectan el ejercicio de derechos con procedimientos verificables de gestión, supervisión y corrección de tratamientos inadecuados (Prados et al., 2024).

Cuando el responsable no responde al requerimiento del titular o lo niega, la tutela puede trasladarse al ámbito administrativo. La Ley Orgánica de Protección de Datos Personales (2021), en su artículo 64, reconoce la posibilidad de presentar el correspondiente reclamo ante la Autoridad de Protección de Datos Personales, sin perjuicio de las acciones civiles, penales o constitucionales que puedan resultar procedentes. Esta vía permite que una controversia deje de depender exclusivamente de la respuesta de quien administra la información y sea examinada por un órgano especializado. La coexistencia de distintos mecanismos amplía las posibilidades de protección según la naturaleza y gravedad de la vulneración producida.

La Autoridad de Protección de Datos Personales ocupa una posición central dentro del sistema institucional de tutela. El artículo 76 de la Ley Orgánica de Protección de Datos Personales (2021) la configura como órgano de control y vigilancia y le atribuye, entre otras funciones, supervisar y evaluar tratamientos, ejercer potestad sancionadora, conocer reclamos, realizar o delegar auditorías técnicas y emitir normativa necesaria para garantizar este derecho. Estas facultades permiten intervenir tanto antes como después de una vulneración. La protección institucional combina así supervisión preventiva, investigación, corrección y sanción, evitando que la actuación de la autoridad quede limitada únicamente a imponer consecuencias después del incumplimiento.

La actuación administrativa puede comenzar incluso antes de que exista un procedimiento sancionador. De acuerdo con la Ley Orgánica de Protección de Datos Personales (2021), en su artículo 75, la Autoridad de Protección de Datos Personales puede iniciar de oficio o a petición del titular actuaciones previas destinadas a conocer las circunstancias de un caso y determinar la conveniencia de iniciar el procedimiento correspondiente. Esta facultad fortalece la capacidad institucional para examinar hechos que podrían revelar tratamientos contrarios a la normativa. La tutela adquiere así un carácter dinámico, porque permite investigar circunstancias relevantes sin exigir que toda intervención comience necesariamente con una infracción plenamente determinada.

La protección administrativa se complementa con mecanismos constitucionales cuando la afectación requiere intervención jurisdiccional. La Constitución de la República del Ecuador (2008), en su artículo 92, reconoce la acción de hábeas data para conocer la existencia de información personal, acceder a ella y determinar su uso, finalidad, origen, destino y tiempo de vigencia. También permite solicitar actualización, rectificación, eliminación o anulación de los datos. La disposición establece además que, si la solicitud no es atendida, el titular puede acudir ante la autoridad judicial y reclamar por los perjuicios ocasionados. Esta garantía

convierte el control sobre los datos personales en un derecho susceptible de protección jurisdiccional directa.

La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), en su artículo 49, desarrolla el objeto del hábeas data y garantiza judicialmente el acceso y control sobre información personal que se encuentre en poder de entidades públicas o personas naturales o jurídicas privadas. La norma permite solicitar acceso, actualización, rectificación, eliminación o anulación y establece que la reparación integral puede comprender obligaciones materiales e inmateriales determinadas judicialmente. Esta dimensión resulta relevante porque la tutela no se limita a reconocer que ocurrió una vulneración. El mecanismo debe ofrecer una respuesta capaz de corregir sus consecuencias y restablecer, dentro de lo jurídicamente posible, el ejercicio efectivo del derecho afectado.

La existencia simultánea de mecanismos administrativos y jurisdiccionales permite responder a vulneraciones de distinta naturaleza. Un incumplimiento relacionado con la atención de derechos puede requerir intervención de la autoridad especializada, mientras que una afectación constitucional puede justificar el hábeas data. La propia Ley Orgánica de Protección de Datos Personales (2021), en su artículo 64, preserva expresamente la posibilidad de ejercer acciones civiles, penales o constitucionales. Esta pluralidad no implica duplicar automáticamente procedimientos, sino reconocer que una misma conducta puede producir consecuencias jurídicas diferentes. La elección del mecanismo debe relacionarse con el derecho afectado, el tipo de reparación requerida y las características específicas de la actuación cuestionada.

La tutela institucional también depende de la capacidad de supervisar tratamientos tecnológicos complejos. La expansión de servicios digitales, infraestructuras externas y procesos automatizados dificulta verificar el cumplimiento exclusivamente mediante controles documentales. Lorè et al. (2023) muestran que las herramientas de inteligencia artificial pueden apoyar decisiones relacionadas con evaluación de conformidad, aunque requieren interpretación y supervisión humana. La autoridad y las organizaciones necesitan, por tanto, combinar competencias jurídicas con capacidad técnica suficiente para comprender cómo se procesan los datos. Una tutela formalmente disponible pierde eficacia cuando quienes deben aplicarla no pueden identificar las operaciones tecnológicas que generan el riesgo o determinar las responsabilidades correspondientes.

La protección efectiva también requiere conciliar privacidad y transparencia cuando una entidad administra información de interés público que contiene datos personales. La Ley Orgánica de Transparencia y Acceso a la Información Pública (2023) distingue la información pública de aquella de carácter confidencial vinculada con datos personales, de modo que las obligaciones de apertura no autorizan una difusión indiscriminada. Esta relación exige examinar cada solicitud según su contenido y aplicar mecanismos que permitan proteger información personal sin impedir injustificadamente el acceso legítimo a información pública. La tutela de la privacidad adquiere así una dimensión institucional transversal, porque debe operar incluso dentro de procesos cuya finalidad principal es garantizar otros derechos relacionados con información y control ciudadano.

La tutela efectiva de la privacidad se consolida cuando prevención, reclamación, supervisión administrativa y protección judicial funcionan de manera complementaria. El responsable constituye la primera instancia para corregir tratamientos, la Autoridad de Protección de Datos Personales supervisa y controla el cumplimiento, y el hábeas data proporciona una garantía jurisdiccional frente a afectaciones que requieren intervención judicial. La eficacia del sistema depende de que estos mecanismos sean accesibles, oportunos y capaces de producir resultados verificables. La protección de datos deja entonces de ser una declaración normativa abstracta y se convierte en un sistema de garantías mediante el cual el titular puede controlar su información, exigir correcciones y obtener respuesta frente a vulneraciones de su privacidad.

Conclusión

La protección de datos personales se ha consolidado como una garantía indispensable para preservar la privacidad, la intimidad y la capacidad de las personas para ejercer control sobre la información que las identifica. En la sociedad digital, esta protección adquiere especial relevancia porque los datos circulan constantemente entre instituciones públicas, empresas, plataformas, proveedores tecnológicos y sistemas automatizados. El reconocimiento jurídico del derecho resulta necesario, pero su eficacia depende de que existan mecanismos concretos capaces de limitar tratamientos injustificados, establecer obligaciones para quienes administran información y proporcionar herramientas que permitan al titular intervenir cuando sus datos son utilizados de forma contraria a sus derechos.

El tratamiento de datos personales debe analizarse como un proceso continuo que comprende recolección, almacenamiento, utilización, comunicación, conservación y eliminación. Cada una de estas etapas puede generar riesgos particulares cuando se ejecuta sin finalidad determinada, con información excesiva o mediante condiciones que dificultan conocer quién accede a los datos. Los entornos digitales han ampliado además las posibilidades de combinar registros, elaborar perfiles y producir inferencias a partir de información aparentemente aislada. Esta capacidad exige superar una concepción limitada de la privacidad basada únicamente en el secreto y reconocer que la afectación puede producirse también mediante análisis, reutilización o circulación de información previamente recopilada.

El consentimiento y la transparencia adquieren importancia dentro de este escenario porque permiten que el titular conozca determinadas condiciones del tratamiento y ejerza facultades sobre sus datos. Sin embargo, el consentimiento no puede utilizarse como mecanismo para trasladar toda la responsabilidad a la persona. Su eficacia depende de información comprensible, finalidades específicas y posibilidades reales de elección. De igual manera, derechos como acceso, rectificación, actualización, eliminación, oposición, limitación y portabilidad permiten corregir situaciones que pueden producir efectos perjudiciales. La protección efectiva requiere que estos derechos puedan ejercerse mediante procedimientos accesibles y que las organizaciones respondan de forma oportuna, motivada y verificable.

Las decisiones automatizadas y la elaboración de perfiles introducen desafíos adicionales porque pueden producir consecuencias significativas a partir del análisis de grandes cantidades de información. La utilización de inteligencia artificial no elimina las obligaciones existentes en materia de protección de datos ni transforma automáticamente en legítimos los tratamientos

realizados mediante sistemas complejos. Cuando las decisiones dependen de modelos algorítmicos, adquieren mayor importancia la transparencia, la calidad de los datos, la proporcionalidad y la posibilidad de cuestionar resultados. La innovación tecnológica necesita integrarse dentro de estructuras jurídicas y organizativas que impidan que la automatización reduzca la capacidad de las personas para comprender y controlar tratamientos que afectan su esfera personal.

Las vulneraciones de seguridad evidencian que los riesgos de privacidad no se limitan a tratamientos jurídicamente injustificados. Incluso una operación legítima puede producir daños cuando existen accesos indebidos, filtraciones, pérdidas o divulgaciones no autorizadas. Estas situaciones pueden generar afectaciones económicas, reputacionales, sociales y personales cuya intensidad depende de la sensibilidad y utilización posterior de los datos comprometidos. La responsabilidad de responsables y encargados exige, por ello, establecer controles antes del incidente, detectar oportunamente las vulneraciones y responder de manera proporcional cuando estas ocurren. La seguridad constituye una obligación permanente vinculada con prevención, documentación, comunicación y corrección de las causas identificadas.

El régimen de responsabilidad demuestra también que las vulneraciones pueden generar consecuencias administrativas, civiles, constitucionales e incluso penales según la naturaleza de la conducta. Las sanciones cumplen una función importante, pero no representan por sí solas una reparación suficiente para el titular. La tutela requiere mecanismos capaces de detener tratamientos indebidos, corregir información, eliminar datos cuando corresponda y responder frente a los perjuicios ocasionados. En este sentido, los procedimientos de reclamación y las garantías jurisdiccionales permiten trasladar el conflicto desde la relación privada con el responsable hacia instancias especializadas o judiciales cuando la respuesta inicial resulta insuficiente para restablecer los derechos afectados.

El cumplimiento normativo constituye una dimensión preventiva que permite reducir la distancia entre las disposiciones jurídicas y las prácticas reales de las organizaciones. Políticas internas, asignación de responsabilidades, capacitación, gestión de proveedores y documentación de decisiones son elementos necesarios para mantener un sistema capaz de demostrar cómo se protegen los datos. La privacidad desde el diseño y por defecto fortalece esta lógica al incorporar garantías desde la planificación de productos, servicios y procesos. Esta perspectiva resulta más efectiva que corregir posteriormente sistemas contruidos sin criterios de protección, porque permite limitar desde el inicio la recolección, accesibilidad, conservación y utilización de información personal.

La evaluación de riesgos, las medidas técnicas y organizativas, las auditorías y los mecanismos de supervisión completan esta estructura de cumplimiento. La protección adecuada no puede basarse en medidas estáticas, pues los riesgos evolucionan con las tecnologías, amenazas, proveedores y finalidades utilizadas. Las organizaciones deben revisar periódicamente sus controles y modificar aquellos que hayan perdido eficacia. Asimismo, la intervención de autoridades especializadas y mecanismos jurisdiccionales fortalece la tutela cuando los controles internos fallan. El sistema alcanza mayor eficacia cuando prevención, supervisión, reclamación y reparación funcionan de manera coordinada y permiten determinar responsabilidades sin que la complejidad tecnológica se convierta en un obstáculo para el ejercicio de derechos.

La protección de datos personales debe asumirse finalmente como una condición para el desarrollo responsable de la sociedad digital. El uso creciente de información puede generar beneficios para servicios públicos, investigación, salud, educación, comercio e innovación, pero esos beneficios no justifican tratamientos ilimitados ni la pérdida de control individual sobre los datos. El desafío consiste en mantener un equilibrio en el que las capacidades tecnológicas puedan desarrollarse dentro de límites jurídicos claros, controles efectivos y mecanismos de tutela accesibles. La privacidad se fortalece cuando el tratamiento de información responde a finalidades legítimas, minimiza riesgos y reconoce que detrás de cada conjunto de datos existe una persona cuyos derechos deben permanecer protegidos.

Bibliografía

- Agahari, W., Ofe, H., & de Reuver, M. (2022). It is not (only) about privacy: How multi-party computation redefines control, trust, and risk in data sharing. *Electronic Markets*, 32(3), 1577-1602. <https://doi.org/10.1007/s12525-022-00572-w>
- Alaattinoğlu, A. (2022). Rethinking Explicit Consent and Intimate Data: The Case of Menstruapps. *Feminist Legal Studies*, 30(2), 157-179. <https://doi.org/10.1007/s10691-021-09486-y>
- Bessant, C., & Schnebbe, M. (2022). Does the GDPR offer a solution to the ‘problem’ of sharenting? *Datenschutz und Datensicherheit*, 46(6), 352-356. <https://doi.org/10.1007/s11623-022-1618-3>
- Bohn, L., & Schiereck, D. (2023). Regulation of data breach publication: the case of US healthcare and the HITECH act. *Journal of Economics and Finance*, 47(2), 386-399. <https://doi.org/10.1007/s12197-022-09607-6>
- COIP. (2014). *Código Orgánico Integral Penal*. Suplemento del Registro Oficial No. 180, 10 de febrero de 2014: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf
- Constitución de la República del Ecuador*. (2008). Registro Oficial No. 449, 20 de octubre de 2008: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf
- Convención Americana sobre Derechos Humanos (Pacto de San José)*. (1969). San José, Costa Rica, 22 de noviembre de 1969: <https://www.oas.org/es/cidh/mandato/documentos-basicos/convencion-americana-derechos-humanos.pdf>
- Custers, B., & Heijne, A.-S. (2022). The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice. *Computer Law & Security Review*, 46, 105727. <https://doi.org/10.1016/j.clsr.2022.105727>
- Declaración Universal de Derechos Humanos*. (1948). Resolución 217 A (III) de la Asamblea General, 10 de diciembre de 1948: <https://www.un.org/es/about-us/universal-declaration-of-human-rights>
- Dexe, J., Franke, U., Söderlund, K., van Berkel, N., Jensen, R., Lepinkäinen, N., & Vaiste, J. (2022). Explaining automated decision-making: a multinational study of the GDPR

- right to meaningful information. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 47(3), 669-697. <https://doi.org/10.1057/s41288-022-00271-9>
- Fan, J. (2023). Legal Policies Failing on Data Breaches?—An Empirical Study of U.S. Information Security Law Implementations. *Procedia Computer Science*, 221, 971-978. <https://doi.org/10.1016/j.procs.2023.08.076>
- Georgiou, D., & Lambrinoudakis, C. (2021). Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations. *Future Internet*, 13(3), 66. <https://doi.org/10.3390/fi13030066>
- Issaoui, A., Örtensjö, J., & Islam, M. (2023). Exploring the General Data Protection Regulation (GDPR) compliance in cloud services: insights from Swedish public organizations on privacy compliance. *Future Business Journal*, 9, 107. <https://doi.org/10.1186/s43093-023-00285-2>
- Kim, N., Oh, H., & Choi, J. (2023). A privacy scoring framework: Automation of privacy compliance and risk evaluation with standard indicators. *Journal of King Saud University - Computer and Information Sciences*, 35(1), 514-525. <https://doi.org/10.1016/j.jksuci.2022.12.019>
- Kurtz, C., Wittner, F., Semmann, M., Schulz, W., & Böhmman, T. (2022). Accountability of platform providers for unlawful personal data processing in their ecosystems – A socio-techno-legal analysis of Facebook and Apple's iOS according to GDPR. *Journal of Responsible Technology*, 9, 100018. <https://doi.org/10.1016/j.jrt.2021.100018>
- Kutschera, S. (2023). Incidental data: observation of privacy compromising data on social media platforms. *International Cybersecurity Law Review*, 4(1), 91-114. <https://doi.org/10.1365/s43439-022-00071-w>
- Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional*. (2009). Segundo Suplemento del Registro Oficial No. 52, 22 de octubre de 2009: <https://isspol.org.ec/wp-content/uploads/2026/04/LEY-ORGANICA-DE-GARANTIAS-JURISDICCIONALES-Y-CONTROL-CONSTITUCIONAL.pdf>
- Ley Orgánica de Protección de Datos Personales*. (2021). Quinto Suplemento del Registro Oficial No. 459, 26 de mayo de 2021: https://isspol.org.ec/wp-content/uploads/2025/05/LEY_ORGA_NICA_DE_PROTECCIA_N_DE_DATOS_PERSONALES-1.pdf

- Ley Orgánica de Transparencia y Acceso a la Información Pública*. (2023). Segundo Suplemento del Registro Oficial No. 245, 7 de febrero de 2023: <https://www.gob.ec/sites/default/files/regulations/2023-10/Lotaip-2023.pdf>
- Lorè, F., Basile, P., Appice, A., de Gemmis, M., Malerba, D., & Semeraro, G. (2023). An AI framework to support decisions on GDPR compliance. *Journal of Intelligent Information Systems*, 61(2), 541-568. <https://doi.org/10.1007/s10844-023-00782-4>
- Martínez-Jara, J., & Pérez-Ycaza, J. (2022). Protección de datos personales en la historia clínica electrónica bajo el marco legal ecuatoriano. *IUSTITIA SOCIALIS*, 7(1), 776-801. <https://doi.org/10.35381/racji.v7i1.2203>
- Masuch, K., Greve, M., & Trang, S. (2021). What to do after a data breach? Examining apology and compensation as response strategies for health service providers. *Electronic Markets*, 31(4), 829-848. <https://doi.org/10.1007/s12525-021-00490-3>
- Mitsilegas, V., Guild, E., Kuskonmaz, E., & Vavoula, N. (2023). Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *European Law Journal*, 29(1-2), 176-211. <https://doi.org/10.1111/eulj.12417>
- Moran Barreto, I. (2023). La Ley de protección de datos y su incidencia en los derechos digitales en Ecuador en el año 2022. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, 7(48), 57-66. <https://doi.org/10.29018/issn.2588-1000vol7iss48.2023pp57-66>
- Mühlhoff, R. (2021). Predictive privacy: towards an applied ethics of data analytics. *Ethics and Information Technology*, 23(4), 675-690. <https://doi.org/10.1007/s10676-021-09606-x>
- Ojeda Bello, Z., & Cutié Mustelier, D. (2021). El derecho a la protección de datos personales en Cuba: desafíos en la era digital. *Revista IUS*, 15(48), 243-257. <https://doi.org/10.35487/rius.v15i48.2021.689>
- Ordellin Font, J. (2022). La protección de datos personales en tiempos de pandemia: aspectos controvertidos desde la relación público-privada. *Estudios en Derecho a la Información*, 1(14), 29-56. <https://doi.org/10.22201/ij.25940082e.2022.14.16892>
- Ordóñez Pineda, L., Correa Quezada, L., & Correa Conde, A. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. *Estado & Comunes*, 2(15), 77-97. https://doi.org/10.37228/estado_comunes.v2.n15.2022.270

- Pacto Internacional de Derechos Civiles y Políticos*. (1966). Resolución 2200 A (XXI) de la Asamblea General, 16 de diciembre de 1966: <https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
- Prados, L., Rabello, A., Souza Neto, J., & Orlandi, T. (2024). Componentes de governança da privacidade frente aos requisitos da Lei Geral de Proteção de Dados Pessoais. *Perspectivas em Gestão & Conhecimento*, 14(2), 24-49. <https://doi.org/10.22478/ufpb.2236-417X.2024v14n2.59683>
- Reglamento General a la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo No. 904)*. (2023). Tercer Suplemento del Registro Oficial No. 435, 13 de noviembre de 2023: https://www.cosede.gob.ec/wp-content/uploads/2023/12/REGLAMENTO-GENERAL-A-LA-LEY-ORG%C3%81NICA-DE-PROTECCION-DE-DATOS-PERSONALES_compressed-1.pdf
- Rigaki, M., & Garcia, S. (2023). A Survey of Privacy Attacks in Machine Learning. *ACM Computing Surveys*, 56(4), 1-34. <https://doi.org/10.1145/3624010>
- Ruohonen, J., & Hjerpe, K. (2022). The GDPR enforcement fines at glance. *Information Systems*, 106, 101876. <https://doi.org/10.1016/j.is.2021.101876>
- Selzer, A. (2021). The appropriateness of technical and organisational measures under Article 32 GDPR. *European Data Protection Law Review*, 7(1), 120-128. <https://doi.org/10.21552/edpl/2021/1/16>
- Thomas, L., Gondal, I., Oseni, T., & Firmin, S. (2022). A framework for data privacy and security accountability in data breach communications. *Computers & Security*, 116, 102657. <https://doi.org/10.1016/j.cose.2022.102657>
- Turner, S., & Tanczer, L. (2024). In principle vs in practice: User, expert and policymaker attitudes towards the right to data portability in the internet of things. *Computer Law & Security Review*, 52, 105912. <https://doi.org/10.1016/j.clsr.2023.105912>
- von Grafenstein, M., Jakobi, T., & Stevens, G. (2022). Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods. *Computer Law & Security Review*, 46, 105722. <https://doi.org/10.1016/j.clsr.2022.105722>

- Wulf, A., & Seizov, O. (2024). "Please understand we cannot provide further information": evaluating content and transparency of GDPR-mandated AI disclosures. *AI & SOCIETY*, 39(2), 235-256. <https://doi.org/10.1007/s00146-022-01424-z>
- Zambrano, A. D., Cedeño-Valarezo, L. C., Loor Morales, M. E., & Zambrano Zambrano, J. A. (2023). Análisis de los derechos a la intimidad y privacidad sobre los datos personales en la legislación Ecuatoriana. *Informática y Sistemas*, 7(1), 7-18. <https://doi.org/10.33936/isrtic.v7i1.5793>



ISBN: 978-9907-848-08-3




CIDPROS
EDITORIAL