Gestión de riesgos y protección de datos: la tecnificación normativa ecuatoriana frente al paradigma europeo

Risk Management and Data Protection: Ecuadorian Normative Technification versus the European GDPR Paradigm

Darío Echeverría Muñoz
Abogado, Docente en Derecho Digital

Resumen:

El presente artículo analiza la evolución del marco regulatorio de protección de datos personales en la República del Ecuador, con especial énfasis en la estrategia de implementación técnica desplegada por la Superintendencia de Protección de Datos Personales (SPDP). A través de una metodología analítica-comparativa —que combina análisis documental de fuentes normativas primarias, revisión bibliográfica de literatura especializada y estudio de casos de herramientas regulatorias concretas— se examina el espectro regulatorio que transita desde un modelo garantista basado en derechos, pasando por el enfoque basado en riesgos del Reglamento General de Protección de Datos (RGPD), hasta consolidarse en un modelo de metarregulación. El estudio deconstruye la normativa ecuatoriana y sus guías de gestión de riesgos cuantitativa (FAIR, Monte Carlo), contrastando este enfoque prescriptivo con la flexibilidad operativa del modelo europeo representado por el sistema GESTIONA de la Agencia Española de Protección de Datos (AEPD) y el marco de la CNIL francesa. La investigación concluye que Ecuador apuesta por una objetivación matemática del cumplimiento, transformando obligaciones jurídicas abstractas en requisitos de ingeniería prescriptivos para cerrar la brecha de implementación regional, distanciándose del modelo de confianza europeo. Este enfoque, si bien reduce la incertidumbre jurídica, conlleva riesgos de rigidez normativa y exclusión de actores con recursos limitados.

Palabras clave:

LOPDP; RGPD; Metarregulación; Gestión de Riesgos; Análisis Comparado.

Abstract:

This article analyzes the evolution of the personal data protection regulatory framework in the Republic of Ecuador, with special emphasis on the technical implementation strategy deployed by the Superintendence of Personal Data Protection (SPDP). Through an analytical-comparative methodology — combining documentary analysis of primary normative sources, bibliographic review of specialized literature, and case studies of concrete regulatory tools— the regulatory spectrum is examined, transitioning from a guarantee-oriented rights-based model, through the GDPR's risk-based approach, to consolidate into a meta-regulation model. The study deconstructs the Ecuadorian regulations and quantitative risk management guides (FAIR, Monte Carlo), contrasting this prescriptive approach with the operational flexibility of the European model represented by the GESTIONA system of the Spanish Data Protection Agency (AEPD) and the French CNIL framework. The research concludes that Ecuador is betting on mathematical objectification of compliance, transforming abstract legal obligations into prescriptive engineering requirements to bridge the regional implementation gap, distancing itself from the European trust-based model. While this approach reduces legal uncertainty, it carries risks of normative rigidity and exclusion of actors with limited resources.

Keywords:

LOPDP; GDPR; Meta-regulation; Risk Management; Comparative Analysis.

1. Introducción

La protección de datos personales ha dejado de ser una disciplina jurídica periférica para convertirse en el eje central de la gobernanza digital contemporánea. En la República del Ecuador, esta transformación posee una dimensión profundamente constitucional. El artículo 66, numeral 19 de la Constitución de la República reconoce y garantiza el derecho a la protección de datos de carácter personal, elevando este mandato a un nivel de garantía fundamental.[1]

Sin embargo, la materialización de este derecho ha sufrido una metamorfosis acelerada que merece análisis riguroso. Si bien la Ley Orgánica de Protección de Datos Personales (LOPDP) de 2021 fue influenciada por el denominado «Efecto Bruselas» —fenómeno mediante el cual la Unión Europea extiende su poder regulatorio más allá de sus fronteras territoriales— y el RGPD, la implementación regulatoria liderada por la Superintendencia de Protección de Datos Personales (SPDP) en el periodo 2024-2025, y consolidada con la actualización a la versión 2 de su guía técnica en 2026, marca un hito disruptivo: el paso hacia una metarregulación.

Esta transformación no ocurre en un vacío regional. América Latina ha experimentado una ola de convergencia regulatoria en materia de protección de datos durante la última década. Brasil promulgó su *Lei Geral de Proteção de Dados* (LGPD) en 2018, estableciendo la *Autoridade Nacional de Proteção de Dados* (ANPD) en 2020. Chile actualizó su normativa mediante la Ley 21.096 de 2018, mientras que Colombia ha avanzado significativamente en la aplicación de su Ley 1581 de 2012. Argentina, pionera regional con su Ley 25.326 de 2000, obtuvo en 2019 la declaración de adecuación por parte de la Comisión Europea, reconociendo un nivel de protección esencialmente equivalente al europeo.

En este contexto regional, Ecuador se distingue no por ser el primero en regular, sino por la estrategia de implementación adoptada. A diferencia del modelo europeo, que descansa en la ponderación jurídica y el análisis cualitativo de riesgos bajo el principio de *accountability*, Ecuador ha optado por una estrategia que impone una ingeniería de la privacidad cuantificable. Este nuevo paradigma busca reducir la incertidumbre jurídica mediante la precisión de la ingeniería de datos, integrando estándares internacionales (ISO 27001, ISO 27701, NIST) y modelos matemáticos (FAIR, Monte Carlo) directamente en la normativa secundaria.[2]

La pregunta central que articula esta investigación es: ¿Constituye el modelo ecuatoriano una evolución necesaria del paradigma basado en riesgos del RGPD, o representa una sobre-tecnificación que podría comprometer la flexibilidad y adaptabilidad que caracterizan al enfoque europeo? Para responderla, el artículo adopta una metodología analítica-comparativa basada en:

[1] Asamblea Constituyente de la República del Ecuador, Constitución de la República del Ecuador, Registro Oficial 449 (Quito: 20 de octubre de 2008), art. 66, num. 19.

[2] Superintendencia de Protección de Datos Personales del Ecuador, *Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales – Versión 2* (Quito: SPDP, 2026), p. 12.

- i) Análisis documental de fuentes normativas primarias —textos legales, resoluciones y guías técnicas—
- ii) Revisión sistemática de literatura académica y regulatoria especializada; y
- iii) Estudio comparado de herramientas concretas de supervisión (GESTIONA-AEPD, metodología PIA-CNIL).

Esta triangulación metodológica permite contrastar principios abstractos con implementaciones operativas, superando los límites del análisis puramente dogmático.

2. De la Burocracia Legal a la Ingeniería Regulatoria

Para comprender el modelo ecuatoriano, es necesario desmitificar la idea de que representa una invención normativa absoluta. Más que situarse en una vanguardia inédita, la regulación ecuatoriana se distingue por adoptar un modelo híbrido que fusiona el garantismo jurídico tradicional con la ingeniería de datos aplicada. Esta estrategia operacionaliza los paradigmas existentes de manera prescriptiva y técnicamente específica para suplir carencias institucionales y de cultura de cumplimiento, marcando una diferencia pragmática respecto a jurisdicciones con mayor madurez.

2.1. Evolución de los Modelos de Regulación

La teoría regulatoria contemporánea identifica tres modelos fundamentales que han estructurado históricamente la protección de datos personales, cada uno respondiendo a contextos tecnológicos, políticos y epistemológicos específicos.

2.1.1. Modelo Basado en Derechos (Rights-Based Model)

El enfoque histórico fundacional, anclado en la dignidad humana y los derechos fundamentales, concibe la protección de datos como un derecho autónomo derivado del derecho a la intimidad pero con sustantividad propia. Este modelo encuentra su expresión paradigmática en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.[3]

El considerando 1 del RGPD establece que "[l]a protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental."[4] De manera análoga, el artículo 66, numeral 19, de la Constitución ecuatoriana reconoce y garantiza este derecho fundamental.[5] La LOPDP, en su Capítulo III (arts. 12-23), despliega un amplio catálogo de derechos que incluyen información, acceso, rectificación, actualización, eliminación, oposición, portabilidad, y el derecho a no ser objeto de decisiones basadas únicamente en valoraciones automatizadas.[6]

Sin embargo, el modelo basado en derechos no escala adecuadamente con el riesgo tecnológico y depende excesivamente de la capacidad de ejercicio del titular, quien frecuentemente carece de los conocimientos técnicos, recursos o información necesaria para activar efectivamente sus facultades frente a organizaciones con asimetrías de poder significativas.

2.1.2. Modelo Basado en Riesgos (Risk-Based Model y Accountability)

El segundo estadio evolutivo representa un cambio de paradigma: del enfoque reactivo centrado en el titular hacia un modelo proactivo centrado en el responsable del tratamiento. El artículo 5.2 del RGPD establece que "[e]l responsable del tratamiento será responsable del cumplimiento

[3] Parlamento Europeo y Consejo de la Unión Europea, "Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos", *Diario Oficial de las Comunidades Europeas* L 281 (1995).

[4] Parlamento Europeo y Consejo de la Unión Europea, "Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)", *Diario Oficial de la Unión Europea* L 119 (2016), considerando 1.

[5] Asamblea *Constituyente, Constitución de la República del Ecuador*, art. 66, num. 19.

[6] Asamblea Nacional del Ecuador, *Ley Orgánica de Protección de Datos Personales*, Registro Oficial Suplemento 459 (Quito: 26 de mayo de 2021), arts. 12-23.

de lo dispuesto en el apartado 1 y capaz de demostrarlo (responsabilidad proactiva)."[7] Esta responsabilidad proactiva se operacionaliza mediante la gestión de riesgos: el responsable debe evaluar continuamente los riesgos y adoptar medidas técnicas y organizativas apropiadas.[8]

Un ejemplo paradigmático de la maduración de este enfoque es el Marco de Ciberseguridad del NIST (NIST CSF 2.0), actualizado en febrero de 2024, que elevó la «Gobernanza» (GOVERN) como función central y transversal.[9] La función GOVERN abarca seis categorías: Contexto Organizacional (GV.OC), Estrategia de Gestión de Riesgos (GV.RM), Roles, Responsabilidades y Autoridades (GV.RR), Política (GV.PO), Supervisión (GV.OV), y Gestión de Riesgos de la Cadena de Suministro (GV.SC).[10]

En Europa, la AEPD desarrolló el sistema GESTIONA[11], herramienta digital que guía a las organizaciones en la realización de análisis de riesgos mediante metodologías estructuradas pero flexibles, manteniendo un significativo grado de discrecionalidad metodológica que permite a las organizaciones adaptar sus sistemas a sus circunstancias específicas.

2.1.3. Modelo Basado en Estándares (Standards-Based Model)

Como respuesta directa a la ambigüedad inherente de los principios legales abstractos, surge un tercer estadio evolutivo: el modelo basado en estándares técnicos internacionales. Este enfoque recurre a normas desarrolladas por organismos como ISO/IEC, NIST o CIS para establecer métricas objetivas, procedimientos de ingeniería auditables y niveles de madurez verificables.

Por ejemplo, el mandato legal de «garantizar la confidencialidad de los datos» se traduce en controles concretos: Control ISO 27001:2022 A.8.24 (uso de criptografía), Control NIST SP 800-53 Rev. 5 SC-8 (protección de integridad en tránsito), y CIS Control 3 (protección de datos mediante cifrado en reposo y en tránsito). Estos controles son medibles, auditables y permiten la certificación por terceros independientes.

Sus ventajas —objetividad, interoperabilidad, mejora continua y transferencia de conocimiento— coexisten con limitaciones igualmente relevantes: rigidez ante innovaciones disruptivas, costos prohibitivos para organizaciones pequeñas, riesgo de tecnocracia que privilegie el cumplimiento formal sobre la protección efectiva, y dependencia regulatoria de estándares anglosajones. Ecuador, consciente de estas tensiones, construye un modelo híbrido que preserva el marco garantista de la LOPDP mientras instrumentaliza el cumplimiento mediante estándares técnicos.

2.2. Tipologías Regulatorias

Para caracterizar con precisión la estrategia ecuatoriana, es fundamental distinguir las tipologías de intervención estatal que la componen: heterorregulación, autorregulación y metarregulación.

2.2.1. Heterorregulación

La heterorregulación representa la intervención estatal directa mediante normas de comando y control. En Ecuador, el fundamento heterorregulatorio parte del reconocimiento constitucional del artículo 66, numeral 19. Ejemplos paradigmáticos en la LOPDP incluyen: la prohibición de tratar datos sensibles sin consentimiento explícito (art. 26),[12] la prohibición de transferencias internacionales a países sin nivel adecuado de protección (art. 35),[13] y el régimen sancionatorio con multas de hasta el 5% de los ingresos anuales (art. 56).[14]

---

[7] Parlamento Europeo y Consejo de la Unión Europea, "Reglamento (UE) 2016/679", *Diario Oficial de la Unión Europea* L 119 (2016), art. 5.2.

[8] Parlamento Europeo, "RGPD", art. 32.1.

[9] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0* (Gaithersburg, MD: NIST, 2024), https://doi.org/10.6028/NIST.CSWP.29

[10] Ibid.

[11] Agencia Española de Protección de Datos, "La AEPD presenta su herramienta Gestiona como ayuda para realizar análisis de riesgos y evaluaciones de impacto en la protección de datos", nota de prensa, AEPD, accedido el 29 de diciembre de 2025, https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-presenta-su-herramienta-gestiona-como-ayuda-para

[12] Asamblea Nacional, LOPDP, art. 26.

[13] Asamblea Nacional, LOPDP, art. 35.

[14] Asamblea Nacional, LOPDP, art. 56.

2.2.2. Autorregulación

El RGPD europeo fomenta explícitamente la autorregulación a través de códigos de conducta sectoriales (art. 40), supervisión del cumplimiento por organismos acreditados (art. 41), y mecanismos de certificación (arts. 42-43).[15] Ecuador, en contraste, integra la autorregulación como un mecanismo subordinado de cumplimiento técnico. Los artículos 52-53 de la LOPDP y los artículos 68-70 del Reglamento General[16] permiten códigos de conducta sectoriales, pero los sujetan explícitamente a verificación y aprobación por la SPDP, lo que evita el riesgo de captura regulatoria o disminución encubierta de estándares.[17]

2.2.3. Metarregulación

La innovación distintiva de Ecuador radica en la implementación sistemática de la metarregulación: el Estado no dicta cada micro-conducta operativa, sino que supervisa los sistemas de gestión interna que las organizaciones diseñan para cumplir con los fines públicos establecidos en la ley. Mientras Europa mantiene una metarregulación abierta y metodológicamente flexible, Ecuador apuesta por una metarregulación técnicamente prescriptiva que exige metodologías cuantitativas específicas (FAIR, Monte Carlo) para tratamientos de alto riesgo, jerarquía metodológica obligatoria, documentación de *rationales* con evidencia trazable, y la integración de marcos internacionales (ISO 27001/27701, NIST SP 800-53).

Esta estrategia responde a un diagnóstico pragmático: en contextos institucionales débiles, la flexibilidad puede devenir en arbitrariedad o simulación. Al prescribir métodos técnicos, Ecuador reduce la incertidumbre epistémica del cumplimiento, facilitando tanto la implementación por parte de los responsables como la verificación por la autoridad. El riesgo —sobre-prescripción generadora de rigidez y costos desproporcionados para organizaciones pequeñas— es reconocido expresamente por la propia guía de la SPDP.

2.3. Gobernanza Dual: Responsable, CISO y DPO

El paradigma híbrido de metarregulación requiere una estructura de roles claramente diferenciada. El Responsable del Tratamiento —conforme al artículo 24 del RGPD[18] y los artículos 4, 10 y 40 de la LOPDP—[19] ostenta la responsabilidad última de garantizar el cumplimiento y asignar los recursos necesarios para ello.

El Oficial de Seguridad de la Información (CISO) actúa como encargado técnico: diseña, implementa y supervisa los controles de seguridad conforme a los estándares prescritos (ISO 27001, NIST CSF),[20] sin asumir por ello la responsabilidad jurídica de garantía de derechos fundamentales, que permanece en la esfera del Responsable.

El Delegado de Protección de Datos (DPO), regulado en los artículos 37-39 del RGPD[21] y los artículos 47-51 de la LOPDP,[22] opera con independencia funcional garantizada: el artículo 38.3 del RGPD establece que no puede recibir instrucciones sobre el desempeño de sus funciones.[23] Su función es de segunda línea de defensa: valida que los controles implementados por el CISO y las decisiones del Responsable se alineen con la normativa de protección de datos.

Esta estructura tripartita (Responsable-CISO-DPO) es crítica en el modelo ecuatoriano: el Responsable decide e invierte, el CISO ejecuta técnicamente con base en estándares prescritos,

[15] Parlamento Europeo, "RGPD", arts. 40-43.

[16] Presidencia de la República del Ecuador, *Reglamento General a la Ley Orgánica de Protección de Datos Personales*, Decreto Ejecutivo 904, Registro Oficial Tercer Suplemento 435 (Quito: 13 de noviembre de 2023), arts. 68-70.

[17] Asamblea Nacional, LOPDP, art. 52.

[18] Parlamento Europeo, "RGPD", art. 24.

[19] Asamblea Nacional, LOPDP, arts. 4, 10 y 40.

[20] International Organization for Standardization, *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (Ginebra: ISO, 2022), Anexo A.

[21] Parlamento Europeo, "RGPD", arts. 37-39.

[22] Asamblea Nacional, LOPDP, arts. 47-51.

[23] Parlamento Europeo, "RGPD", art. 38.3.

y el DPO supervisa el cumplimiento normativo documentando evidencia para demostrar *accountability*. La confusión de roles entre el CISO y el DPO —uno de los errores más frecuentes en la implementación práctica— genera dilución de responsabilidades que la SPDP considera sancionable.

3. El Núcleo Operativo de la Metarregulación

La Resolución No. SPDP-SPD-2025-0003-R, que aprueba la Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales (cuya actualización a la versión 2 en 2026 reafirma esta postura prescriptiva), constituye el instrumento operativo central del modelo ecuatoriano. Esta guía materializa prescriptivamente el artículo 40 de la LOPDP —que obliga a implementar medidas de seguridad adaptadas al riesgo— y el artículo 42, que regula la Evaluación de Impacto en la Protección de Datos (EIPD). El análisis comparativo frente al sistema GESTIONA de la AEPD y las metodologías de la CNIL revela convergencias estructurales y divergencias metodológicas que ilustran la apuesta ecuatoriana por la cuantificación como vehículo de certeza jurídica.

3.1. Taxonomía de la Incertidumbre

Una de las contribuciones conceptuales más sofisticadas de la guía ecuatoriana es la distinción explícita entre dos tipos fundamentales de incertidumbre que deben gestionarse diferenciadamente.[24]

La incertidumbre aleatoria (*aleatoric uncertainty*) se refiere a la variabilidad intrínseca e irreducible de los eventos futuros, originada en la naturaleza estocástica de ciertos fenómenos: desastres naturales, fallas aleatorias de hardware, comportamiento humano impredecible, ataques oportunistas no dirigidos. Su gestión se centra en el modelado probabilístico basado en datos históricos, la cuantificación de impactos y la transferencia de riesgos mediante seguros cibernéticos.

La incertidumbre epistemológica, en contraste, es *reducible*: deriva de la falta de conocimiento sobre el propio sistema —desconocimiento del inventario de datos, ignorancia sobre vulnerabilidades, ausencia de inteligencia de amenazas, incomprensión de flujos de datos—. La guía ecuatoriana interpreta el artículo 40 de la LOPDP[25] como una obligación de reducir activamente esta incertidumbre mediante auditorías técnicas, mapeo de procesos y análisis forense, incluso la versión 2 de la guía ecuatoriana es tajante al respecto, estableciendo como objetivo primordial reducir esta incertidumbre epistemológica frente a escenarios de amenaza. Ignorarla se considera negligencia sancionable. Esta distinción no aparece explícitamente en las guías europeas (GESTIONA-AEPD, metodología PIA-CNIL), aunque ambas operan implícitamente bajo el mismo presupuesto.

3.2. Metodologías de Análisis

La guía ecuatoriana impone una jerarquía metodológica que vincula el nivel de riesgo del tratamiento con el tipo de análisis requerido, contrastando marcadamente con la flexibilidad europea.

3.2.1. El Problema del «Ruido» en Evaluaciones Cualitativas

Las evaluaciones cualitativas basadas en juicios subjetivos presentan limitaciones severas que la guía de la SPDP reconoce explícitamente: ambigüedad semántica (¿qué significa «probabilidad alta»?), compresión de rangos en matrices 3×3, sesgo de anclaje hacia eventos recientes y manipulabilidad de las clasificaciones. Para combatir este ruido decisional, la guía exige la documentación obligatoria de *rationales*: justificaciones explícitas y basadas en evidencia —fuentes de información, supuestos explicitados, metodología de cálculo y registro de revisiones— y métricas significativas para cada decisión o valor asignado.

3.2.2. Métodos Cualitativos y sus Condiciones de Uso

La guía permite métodos cualitativos para tratamientos de riesgo bajo o medio —matrices de riesgo clásicas, análisis de escenarios y método Delphi—, bajo condiciones estrictas: el tratamiento no involucra datos sensibles a gran escala, no utiliza tecnologías emergentes, el impacto potencial sobre derechos fundamentales es limitado, y existe documentación exhaustiva de los *rationales* para cada estimación.

[24] SPDP, *Guía de Gestión de Riesgos*, p. 18.

[25] Asamblea Nacional, LOPDP, art. 40.

3.2.3. Métodos Cuantitativos para Alto Riesgo

Para tratamientos que entrañan riesgo alto —conforme al artículo 42 de la LOPDP—,[26] la guía ecuatoriana impulsa y en la práctica exige el uso de modelos matemáticos avanzados: el estándar FAIR (*Factor Analysis of Information Risk*) y las simulaciones de Monte Carlo.

FAIR descompone el riesgo en factores primitivos cuantificables: Riesgo = Probabilidad de Evento de Pérdida × Magnitud de Pérdida. Permite expresar el riesgo en términos financieros anualizados (por ejemplo, «Pérdida Anual Esperada de USD 500.000 con 90% de confianza»), adaptándolo a protección de datos como número de titulares afectados o gravedad de vulneración de derechos.[27] Monte Carlo, por su parte, simula miles de escenarios posibles ante la incertidumbre en las variables, generando distribuciones de probabilidad del resultado. La guía introduce además el Pd-VaR (*Personal Data Value at Risk*), análogo al VaR financiero, que expresa la máxima pérdida probable en términos de derechos afectados con un nivel de confianza dado.

La versión 2 (2026) de la guía profundiza esta exigencia, rechazando explícitamente las lógicas de cumplimiento normativo "en el papel" basadas en listas de verificación documentales (checklists), exigiendo en su lugar la construcción de modelos de riesgo alimentados por datos confiables y dictámenes de expertos calibrados[28]. Jurídicamente, esto significa que la justificación de una medida de seguridad deja de ser un argumento retórico-legal para convertirse en una demostración analítica obligatoria.

3.2.4. Comparación con el Marco Europeo: Flexibilidad vs. Prescripción

El contraste con el enfoque europeo es marcado. El sistema GESTIONA de la AEPD[29] guía al responsable a través de un análisis de riesgos fundamentalmente cualitativo: identificación de activos y amenazas, evaluación en escalas bajo/medio/alto, y mapeo automático a controles del Esquema Nacional de Seguridad o ISO 27001. No calcula pérdidas esperadas ni emplea simulaciones estocásticas. Su fortaleza es la accesibilidad para cualquier pequeña empresa; su debilidad, la limitada precisión para tratamientos complejos.

La metodología PIA de la CNIL[30] también es predominantemente cualitativa: proporciona escalas (negligible / limitada / importante / máxima) sin exigir cuantificación matemática. La apuesta ecuatoriana por la cuantificación obligatoria para alto riesgo representa un *trade-off* claro: Ecuador sacrifica accesibilidad y flexibilidad a cambio de objetividad y verificabilidad.

3.3. El Proceso de Gestión de Riesgos

La gestión de riesgos requiere un objeto de análisis definido. Por ello, la normativa ecuatoriana estructura el proceso partiendo de una base documental obligatoria: el Registro de Actividades de Tratamiento (RAT).

3.3.1. Registro de Actividades de Tratamiento (RAT)

El RAT —exigido por el artículo 38 del Reglamento General de la LOPDP, concordante con el artículo 30 del RGPD—[31] es el inventario vivo y dinámico de los flujos de datos de la organización. Sin un RAT actualizado que detalle qué datos personales se tratan, para qué finalidades, quién los trata, dónde se almacenan, cómo se protegen, cuándo se eliminan y hacia dónde fluyen, resulta imposible identificar riesgos con precisión.

Ecuador eleva el RAT de herramienta útil a requisito de validez técnica, cerrando la posibilidad de presentar evaluaciones de riesgos «de escritorio» desconectadas de la realidad operativa. La guía

[26] Asamblea Nacional, LOPDP, art. 42; SPDP, *Guía de Gestión de Riesgos*, p. 35.

[27] The FAIR Institute, "FAIR Standard for Privacy Risk", White Paper (2020), p. 5. Véase también Luis Enríquez, "FAIR Model Privacy Uncertainty Quantification GDPR", *The FAIR Institute* (blog), 3 de diciembre de 2024, accedido el 14 de enero de 2026, https://www.fairinstitute.org/blog/fair-model-privacy-uncertainty-quantification-gdpr

[28] SPDP, Guía de *Gestión de Riesgos*, p. 2.

[29] Agencia Española de Protección de Datos, "GESTIONA: Manual de Usuario" (2019). Herramienta disponible en: https://www.aepd.es/guias-y-herramientas/herramientas/facilita-rgpd. Accedido el 15 de diciembre de 2024.

[30] Commission Nationale de l'Informatique et des Libertés, *Privacy Impact Assessment (PIA): Methodology* (París: CNIL, 2018). Accedido el 29 de diciembre de 2025. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

[31] Presidencia de la República, *Reglamento General LOPDP*, art. 38.

establece explícitamente que cualquier evaluación realizada sin RAT previo y actualizado carece de validez técnica y no satisface las obligaciones de *accountability*. Esta posición es más estricta que la europea: ni la AEPD ni la CNIL invalidan automáticamente evaluaciones realizadas sin RAT formal, aunque ambas reconocen su utilidad instrumental.

3.3.2. El Ciclo de Gestión de Riesgos: Cinco Etapas

Sobre la base del RAT, la guía de la SPDP estandariza el flujo de trabajo en cinco fases secuenciales inspiradas en ISO 31000:2018 y NIST SP 800-39:

- Etapa 1 — Establecimiento del Contexto: Define los parámetros del análisis, incluyendo el contexto externo (marco legal, obligaciones contractuales, panorama de amenazas), el contexto interno (estructura organizacional, cultura de cumplimiento, recursos disponibles), el alcance (global, por proceso, por proyecto o por incidente) y los criterios de aceptación de riesgo (apetito de riesgo). Es responsabilidad de la alta dirección —no del CISO ni del DPO— definir formalmente qué nivel de riesgo está dispuesta a tolerar.

- Etapa 2 — Identificación de Riesgos: Construye un inventario exhaustivo de amenazas (humanas intencionales, humanas no intencionales, tecnológicas y ambientales) y vulnerabilidades, combinando talleres multidisciplinarios, listas de verificación basadas en estándares, revisión de incidentes históricos y análisis de brecha.

- Etapa 3 — Análisis de Riesgos: Estima la probabilidad de ocurrencia y la magnitud del impacto para cada escenario. Para métodos cuantitativos, el riesgo se calcula como Pérdida Anual Esperada (LAE) = Frecuencia Anual × Magnitud de Pérdida; con Monte Carlo se obtiene una distribución de probabilidad del resultado.

- Etapa 4 — Evaluación de Riesgos: Compara el nivel calculado contra los criterios de aceptación definidos en la Etapa 1, clasificando cada riesgo como aceptable, tolerable o inaceptable. Si el riesgo residual es alto para los derechos y libertades de los titulares, se activa la obligatoriedad de EIPD conforme al artículo 42 de la LOPDP.

- Etapa 5 — Tratamiento de Riesgos: Selección e implementación de controles mediante las estrategias de mitigación (controles técnicos, organizativos y físicos), transferencia (seguros, contratos con encargados), evitación (no iniciar el tratamiento) o aceptación consciente (con aprobación formal de la alta dirección y documentación del rationale). El ciclo PDCA integrado garantiza la revisión periódica y actualización del RAT.

3.4. La Evaluación de Impacto en la Protección de Datos (EIPD)

La EIPD —regulada en el artículo 42 de la LOPDP, análogo al artículo 35 del RGPD—[32] representa una iteración más profunda de la gestión de riesgos, enfocada exclusivamente en los riesgos para los derechos y libertades de las personas físicas.

3.4.1. Disparadores de Obligatoriedad

La EIPD es obligatoria cuando el tratamiento presenta al menos dos de los criterios de alto riesgo establecidos en las Directrices del Grupo de Trabajo del Artículo 29 (WP29), adoptadas por el EDPB:[33] (1) evaluación o puntuación/*scoring*; (2) decisiones automatizadas con efectos jurídicos significativos; (3) observación sistemática a gran escala; (4) datos sensibles a gran escala; (5) datos tratados a gran escala; (6) cruce de datos de diversas fuentes; (7) datos de personas vulnerables; (8) uso innovador o aplicación de nuevas tecnologías (IA, biometría, IoT); (9) transferencias internacionales fuera de países con decisión de adecuación; y (10) tratamientos que impidan ejercer derechos o acceder a servicios esenciales.

3.4.2. Contenido Mínimo y Consulta Previa

Una EIPD completa requiere: (1) descripción sistemática del tratamiento basada en el RAT; (2) evaluación de necesidad y proporcionalidad, incluyendo análisis de legitimación, minimización y

[32] Asamblea Nacional, LOPDP, art. 42.

[33] Grupo de Trabajo del Artículo 29, "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento 'entraña probablemente un alto riesgo' a efectos del Reglamento (UE) 2016/679", WP248 rev.01, adoptadas el 4 de octubre de 2017, accedido el 29 de diciembre de 2025, https://www.aepd.es/documento/wp248rev01-es.pdf

compatibilidad de finalidades; (3) gestión de riesgos detallada con documentación completa de rationales; (4) especificación de medidas de seguridad y garantías; (5) consulta formal al DPO y, cuando sea apropiado, a partes interesadas; y (6) conclusión y plan de acción con responsables, plazos y métricas de seguimiento.

Cuando, tras realizar la EIPD, el riesgo residual sigue siendo alto y el responsable no puede mitigarlo suficientemente, el artículo 43 de la LOPDP (equivalente al art. 36 del RGPD) exige consultar a la SPDP *antes de iniciar el tratamiento*. Este mecanismo de control preventivo (*ex ante*) permite a la autoridad revisar la EIPD, solicitar información adicional, recomendar medidas adicionales o, en casos extremos, prohibir el tratamiento. La EIPD no es un documento estático; debe revisarse y actualizarse ante cambios en las circunstancias del tratamiento, nuevas amenazas, brechas de seguridad, o periódicamente —al menos cada tres años para tratamientos de alto riesgo—.

4. Análisis Comparativo Estructural: Ecuador vs. RGPD

El análisis comparado entre el RGPD y la LOPDP revela una divergencia fundamental en la filosofía de implementación. Aunque ambos cuerpos normativos comparten un ADN principialista común y buscan la tutela del mismo derecho fundamental, las estrategias para operacionalizar este mandato difieren sustancialmente.

4.1. Divergencia en los Principios Rectores: Granularidad vs. Condensación

Es un error común asumir una equivalencia exacta entre los principios del RGPD (art. 5) y los de la LOPDP (art. 10). El RGPD condensa sus mandatos en seis principios materiales más el de accountability. La LOPDP despliega trece principios rectores explícitos, decisión que no es meramente retórica, sino que tiene consecuencias jurídicas operativas:

- Autonomía de la Transparencia y la Lealtad: Al separar la «Transparencia» (art. 10.c) de la «Lealtad» (art. 10.b), Ecuador impide que la mera disponibilidad de avisos de privacidad justifique prácticas desleales.
- Seguridad vs. Confidencialidad: La LOPDP distingue el principio de «Confidencialidad» (art. 10.g) del de «Seguridad» (art. 10.k), clarificando que la obligación de secreto es distinta de la obligación técnica de protección integral (CID).
- Aplicación Favorable al Titular: El literal (l) del artículo 10 introduce explícitamente el principio pro homine digital, que en Europa es construcción jurisprudencial del TJUE, mientras que en Ecuador es mandato de ley positiva.

4.2. Flexibilidad vs. Prescripción: El Costo de la Certeza y sus Límites

La diferencia más profunda radica en cómo cada sistema gestiona la incertidumbre del cumplimiento. El modelo europeo se basa en la neutralidad tecnológica y la madurez institucional: asume que las organizaciones poseen (o pueden contratar) el criterio necesario para determinar qué medidas son «apropiadas». Esta flexibilidad favorece la innovación, pero genera inseguridad jurídica para las PYME.

El modelo ecuatoriano, diagnosticando una falta de madurez en la cultura de cumplimiento regional, opta por la reducción de incertidumbre mediante prescripción. Al exigir metodologías cuantitativas como FAIR y Monte Carlo para riesgos altos, la SPDP elimina la ambigüedad del término «apropiado»: si el análisis matemático demuestra que la probabilidad de pérdida excede el apetito de riesgo, la medida es inapropiada; si lo reduce por debajo del umbral, es conforme.

Este enfoque ofrece objetividad y verificabilidad, pero impone barreras significativas: la implementación de modelos estocásticos y estándares ISO requiere recursos financieros y técnicos —actuarios, ingenieros de datos— fuera del alcance de la mayoría de las empresas locales. Ecuador, paradójicamente, construye un sistema de *compliance* de élite en una economía en desarrollo, apostando a que la exigencia técnica elevará el nivel del mercado, aunque a riesgo de asfixiar a los actores más pequeños que no puedan costear la «ingeniería de la privacidad». La evaluación definitiva de este modelo requerirá evidencia empírica sobre su efectividad en la protección real de derechos versus los costos de cumplimiento generados.

Un límite adicional que merece profunda reflexión crítica es el riesgo de que la sofisticación técnica desplace la centralidad de los derechos fundamentales y desborde la propia capacidad institucional

del Estado. Si una gran corporación tecnológica presenta una Evaluación de Impacto sustentada en un complejo modelo estocástico alimentado por inteligencia artificial que legitima un tratamiento intrusivo, cabe preguntarse si la SPDP cuenta con el músculo auditor, los actuarios y científicos de datos necesarios para refutar y deconstruir dicho modelo. Cuando el cumplimiento se convierte en un intrincado ejercicio matemático, la objetivación cuantitativa de la privacidad puede reproducir, a una escala inaudita, el cumplimiento cosmético y excluyente que buscaba erradicar.

5. Conclusiones

La evolución normativa de la protección de datos en Ecuador, cristalizada en la LOPDP y su desarrollo reglamentario y técnico entre 2021 al 2026, representa un caso de estudio singular en el derecho comparado. Lejos de una simple trasplantación del RGPD europeo, Ecuador ha reconfigurado el modelo de *accountability* para adaptarlo a una realidad institucional distinta, transitando desde un garantismo abstracto hacia una metarregulación.

En primer lugar, el análisis evidencia que Ecuador ha abandonado la neutralidad metodológica europea. La imposición de jerarquías analíticas que obligan al uso de métodos cuantitativos (FAIR, Monte Carlo) y rechazan las listas de verificación documentales para tratamientos de alto riesgo busca cerrar la brecha de implementación mediante su objetivación. Se asume que, ante la falta de una cultura de cumplimiento orgánica, la matemática actuarial ofrece un refugio de certeza jurídica superior a la discrecionalidad cualitativa.

En segundo lugar, la estructura de gobernanza de la LOPDP refuerza el control estatal sobre la autorregulación. Al convertir el RAT en un requisito de validez técnica y al subordinar los códigos de conducta a verificación estricta, el regulador ecuatoriano transforma el modelo de «cumplir y demostrar» en «documentar, cuantificar y demostrar».

En tercer lugar, la comparación estructural con el RGPD revela que la tecnificación normativa ecuatoriana es una espada de doble filo. Ofrece métricas claras y reduce la ambigüedad interpretativa, lo que constituye un avance deseable para la seguridad jurídica. Sin embargo, eleva sustancialmente los costos de transacción y las barreras de entrada al cumplimiento, con el riesgo adicional de que la sofisticación técnica desplace la efectividad sustantiva de la protección de derechos.

El éxito de este modelo dependerá de si la sofisticación técnica exigida logra ser internalizada por el tejido empresarial —o si, por el contrario, deriva en un cumplimiento formalista de élite que deja desprotegida a la gran masa de titulares cuyos datos son tratados por actores incapaces de costear la ingeniería de privacidad prescrita—, y de si la SPDP mantiene una supervisión sustantiva orientada a la efectividad real de los derechos, más allá de la verificación formal de los modelos matemáticos. Ecuador ha apostado por la ciencia de datos como garante del derecho; el tiempo dirá si la fórmula es sostenible.

Bibliografía

Agencia Española de Protección de Datos. "Directrices sobre la evaluación de impacto en la protección de datos (wp248 rev.01)." Madrid: AEPD. Accedido el 29 de diciembre de 2025. https://www.aepd.es/documento/wp248rev01-es.pdf.

Agencia Española de Protección de Datos. "Facilita RGPD." Herramienta digital. Madrid: AEPD. Accedido el 15 de diciembre de 2025. https://www.aepd.es/guias-y-herramientas/herramientas/facilita-rgpd.

Agencia Española de Protección de Datos. "La AEPD presenta su herramienta Gestiona como ayuda para realizar análisis de riesgos y evaluaciones de impacto en la protección de datos." Nota de prensa. Madrid: AEPD. Accedido el 29 de diciembre de 2025. https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-presenta-su-herramienta-gestiona-como-ayuda-para

Asamblea Constituyente de la República del Ecuador. *Constitución de la República del Ecuador*. Registro Oficial 449. Quito: 20 de octubre de 2008. Accedido el 15 de diciembre de 2025 https://www.lexis.com.ec/biblioteca/constitucion-republica-ecuador.

Asamblea Nacional del Ecuador. *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento 459. Quito: 26 de mayo de 2021. Accedido el 15 de diciembre de 2025 https://www.lexis.com.ec/biblioteca/ley-organica-proteccion-datos-personales.

Commission Nationale de l'Informatique et des Libertés (CNIL). "PIA, methodology." París: CNIL. Accedido el 29 de diciembre de 2025. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf.

Comité Europeo de Protección de Datos. "Guidelines 3/2019 on processing of personal data through video devices." Version 2.0. Bruselas: EDPB, 2020. Accedido el 29 de diciembre de 2025. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

Cox, Louis Anthony Jr. "What's Wrong with Risk Matrices?" *Risk Analysis* 28, no. 2 (2008): 497-512. Accedido el 29 de diciembre de 2025. https://doi.org/10.1111/j.1539-6924.2008.01030.x.

Enríquez, Luis. "FAIR Model Privacy Uncertainty Quantification GDPR." *The FAIR Institute* (blog), 3 de diciembre de 2025. Accedido el 14 de enero de 2026. https://www.fairinstitute.org/blog/fair-model-privacy-uncertainty-quantification-gdpr.

Hoepman, Jaap-Henk. "Privacy Design Strategies." En *ICT Systems Security and Privacy Protection: 29th IFIP TC 11 International Conference*, editado por Nora Cuppens-Boulahia et al., 446-459. Cham: Springer, 2014. Accedido el 16 de enero de 2026. https://doi.org/10.1007/978-3-642-55415-5_38.

International Organization for Standardization. *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Ginebra: ISO, 2022. Accedido el 10 de enero de 2026.

International Organization for Standardization. *ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*. Ginebra: ISO, 2019. Accedido el 10 de enero de 2026.

International Organization for Standardization. *ISO 31000:2018 Risk management — Guidelines*. Ginebra: ISO, 2018. Accedido el 10 de enero de 2026.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0*. Gaithersburg, MD: NIST, 2024. Accedido el 10 de enero de 2026. https://doi.org/10.6028/NIST.CSWP.29.

National Institute of Standards and Technology. *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0*. Gaithersburg, MD: NIST, 2020. Accedido el 10 de enero de 2026. https://doi.org/10.6028/NIST.CSWP.01162020.

National Institute of Standards and Technology. *Zero Trust Architecture*. NIST Special Publication 800-207. Gaithersburg, MD: NIST, 2020. Accedido el 11 de enero de 2026. https://doi.org/10.6028/NIST.SP.800-207.

National Institute of Standards and Technology. *Guide for Conducting Risk Assessments*. NIST Special Publication 800-30 Revision 1. Gaithersburg, MD: NIST, 2012. Accedido el 11 de enero de 2026. https://doi.org/10.6028/NIST.SP.800-30r1.

Parlamento Europeo y Consejo de la Unión Europea. "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos." *Diario Oficial de la Unión Europea* L 119 (2016). Accedido el 15 de diciembre de 2025. https://www.boe.es/doue/2016/119/L00001-00088.pdf.

Presidencia de la República del Ecuador. *Reglamento General a la Ley Orgánica de Protección de Datos Personales*. Decreto Ejecutivo 904. Registro Oficial Tercer Suplemento 435. Quito: 13 de noviembre de 2023. Accedido el 15 de diciembre de 2025. https://www.gob.ec/sites/default/files/regulations/2025-01/02%20Reglamento%20General%20a%20la%20Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos%20Personales_0.pdf.

Superintendencia de Protección de Datos Personales del Ecuador. *Resolución No. SPDP-SPD-2025-0003-R: Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales*. Quito: SPDP, 2025. Accedido el 15 de diciembre de 2025. https://spdp.gob.ec/wp-content/uploads/2025/05/GUIA-DE-GESTION-DE-RIESGOS-E-IMPACTO-VERSION-1.pdf.

Superintendencia de Protección de Datos Personales del Ecuador. *Guía de Gestión de Riesgos y Evaluación de Impacto del Tratamiento de Datos Personales – Versión 2*. Quito: SPDP, 2026. Accedido el 20 de marzo de 2026. https://spdp.gob.ec/wp-content/uploads/2026/03/ggrispdp2026v2.pdf