Vol.9 No.4 (2025): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.9.4.2025.e1225

# Design of a Model for the Effective Implementation of the Organic Law on Personal Data Protection (LOPDP) in Higher Education Institutions.

# Diseño de un modelo para la implementación efectiva de la Ley Orgánica de Protección de Datos Personales (LOPDP) en instituciones de educación superior.

**Autores:**

Matute-Álvarez, Justin Ismael
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca – Ecuador
justin.matute@ucacue.edu.ec
https://orcid.org/0009-0009-4951-0451

Quevedo-Sacoto, Andrés Sebastián
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca – Ecuador
asquevedos@ucacue.edu.ec
https://orcid.org/0000-0001-5585-0270

Fechas de recepción: 16-OCT-2025 aceptación: 19-NOV-2025 publicación: 30-DIC-2025

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

**Resumen**

Este artículo presenta el diseño y la validación conceptual de un modelo integral para la implementación efectiva de la Ley Orgánica de Protección de Datos Personales (LOPDP) en instituciones de educación superior (IES) del Ecuador. Mediante un enfoque de *Design Science Research* (DSR), se desarrolla un artefacto compuesto por: (i) un **Índice LOPDP** (rango 0–100) que combina dimensiones **normativa**, **organizativa** y **técnica** con ponderaciones explícitas e interpretaciones de madurez; y (ii) un conjunto mínimo de **indicadores clave de desempeño** (KPIs) alineados a obligaciones regulatorias fundamentales (derechos ARCO, notificación de incidentes y evaluaciones de impacto – DPIA). La validez de contenido del modelo se evaluó mediante un panel Delphi estratificado (expertos en ámbitos legal, TI y gestión), aplicando criterios de consenso por ítem (mediana $\geq 4$ e IQR $\leq 1$) y acuerdo global (W de Kendall $\geq 0{,}70$). Para mitigar el riesgo de "cumplimiento en papel" (performatividad sin efectividad), se incorporó una verificación documental muestral que demuestra trazabilidad y evidencia básica (p. ej., gestión completa de casos ARCO y existencia de DPIA documentadas). El artículo expone el marco conceptual y regulatorio, la fórmula del índice con un ejemplo numérico, la tabla de KPIs con fórmulas y umbrales, los resultados de la validación Delphi, y discute las limitaciones y transferibilidad del modelo. El resultado es un modelo **mensurable y replicable** que permite a las IES diagnosticar, priorizar y mejorar su nivel de cumplimiento en privacidad mediante métricas auditables, facilitando un ciclo de mejora continua.

**Palabras clave:** Protección de datos personales; LOPDP; instituciones de educación superior (IES); Design Science Research; índice de cumplimiento; KPIs; derechos ARCO; DPIA; Delphi; W de Kendall.

**Abstract**

This article presents the design and conceptual validation of an integrated model for the effective implementation of Ecuador's Organic Law of Personal Data Protection (LOPDP) in higher education institutions (HEIs). Using a Design Science Research (DSR) approach, we develop an artifact comprising: (i) a LOPDP Index (0–100) that combines normative, organizational, and technical dimensions with explicit weightings and maturity bands; and (ii) a minimal set of key performance indicators (KPIs) aligned with core regulatory obligations (ARCO rights, incident notification, and data protection impact assessments—DPIA). Content validity was established through a stratified Delphi panel (legal, IT, and management experts), applying item-level consensus criteria (median $\geq 4$ and IQR $\leq 1$) and overall agreement (Kendall's $W \geq 0.70$). To mitigate the risk of "paper compliance," we incorporated a small-scale documentary verification demonstrating traceability and basic evidence (e.g., complete ARCO case handling and documented DPIAs). The article details the conceptual and regulatory framework, the index formula with a numerical example, the KPI table with formulas and thresholds, Delphi validation results, and a discussion of limitations and transferability. The outcome is a measurable, replicable model that enables HEIs to diagnose, prioritize, and improve privacy compliance using auditable metrics, thereby supporting a continuous improvement cycle.

**Keywords**: Personal data protection; Organic Law of Personal Data Protection (Ecuador); higher education institutions (HEIs); Design Science Research; compliance index; KPIs; ARCO rights; DPIA; Delphi method; Kendall's W.

# Introducción

Las instituciones de educación superior (IES) en Ecuador gestionan grandes volúmenes de datos personales (de estudiantes, personal, investigadores, etc.), incluyendo datos sensibles académicos, de salud y socioeconómicos, distribuidos en plataformas administrativas (*ERP*), entornos virtuales de aprendizaje (*LMS*) y servicios en la nube. A pesar de los avances normativos recientes en protección de datos, persisten brechas importantes en **tres niveles** interrelacionados: **(1) Normativo**, con políticas incompletas, bases legales de tratamiento mal documentadas, registros de actividades y evaluaciones de impacto de privacidad (DPIA/EIP) ausentes o desactualizadas; **(2) Organizativo**, con roles y responsabilidades difusos (por ejemplo, falta de la delegación de un responsable de Protección de Datos efectivo), escasa cultura de privacidad, y procesos para atender derechos ARCO sin métricas ni trazabilidad; y **(3) Técnico**, con controles de seguridad heterogéneos, uso inconsistente de cifrado y registros de eventos, y gestión reactiva de incidentes de seguridad. La evidencia de cumplimiento suele estar dispersa y no es fácilmente auditable, lo que dificulta demostrar conformidad ante requerimientos de la autoridad regulatoria o auditorías internas.

Este panorama se agrava por la presencia de **silos operativos** y la tercerización de servicios sin evaluaciones de riesgo adecuadas, así como por la proliferación de *shadow IT* y prácticas informales de intercambio de datos. Sin un marco integrado que priorice los riesgos, mida el desempeño y cierre el ciclo de mejora (*Plan–Do–Check–Act*), la gestión de privacidad tiende a ser declarativa: se producen documentos y políticas "en el papel" sin garantía de efectividad real. Esto conlleva un riesgo de **performatividad** regulatoria, donde la organización aparenta cumplir requisitos formales pero carece de evidencias de implementación efectiva. Las consecuencias de un cumplimiento deficiente incluyen exposición a sanciones legales, interrupciones operativas por incidentes no gestionados adecuadamente y pérdida de confianza de estudiantes y la comunidad académica.

En respuesta a estos desafíos, es necesario un modelo integral y verificable que articule controles normativos, organizativos y técnicos, incorporando **métricas objetivas** y trazabilidad documental para evaluar y mejorar el cumplimiento de la LOPDP en las IES de manera continua. Este trabajo propone el diseño de dicho modelo y su validación conceptual. La **pregunta central** de investigación planteada es: *¿Cómo diseñar y validar conceptualmente un modelo integral –compuesto por un índice de cumplimiento LOPDP y KPIs operativos mínimos– que mida y favorezca el cumplimiento efectivo de la LOPDP en IES ecuatorianas, asegurando la trazabilidad y la evidencia documental para evitar la mera formalidad?* En línea con esta pregunta, el **objetivo general** es diseñar y validar un modelo mensurable que integre dimensiones normativas, organizativas y técnicas de privacidad, permitiendo a las IES diagnosticar su nivel de cumplimiento LOPDP y guiar mejoras, evitando el cumplimiento superficial y promoviendo la mejora continua. A continuación, se presenta el marco conceptual y regulatorio que fundamenta el modelo, seguido de la metodología empleada, la discusión de hallazgos, los resultados obtenidos, limitaciones y trabajos futuros.

## Marco conceptual y regulatorio

**Marco legal nacional:** La Ley Orgánica de Protección de Datos Personales (LOPDP), promulgada en 2021 en Ecuador, reconoce el derecho fundamental a la protección de datos personales e impone obligaciones específicas tanto a los responsables como a los encargados del tratamiento de datos (Asamblea Nacional del Ecuador, 2021). La LOPDP establece principios rectores (licitud, lealtad, transparencia, minimización, integridad, confidencialidad, responsabilidad proactiva, entre otros) y derechos de los titulares de datos, comúnmente conocidos como derechos **ARCO** (Acceso, Rectificación, Cancelación y Oposición), además de otros derechos como la portabilidad y la eliminación. En noviembre de 2023 entró en vigencia el Reglamento General a la LOPDP (Decreto Ejecutivo N.º 904), que desarrolla operativamente la ley, definiendo plazos y umbrales específicos (por ejemplo, el plazo máximo para notificar una violación de seguridad de datos personales), criterios de extraterritorialidad y la figura del delegado o representante legal en ciertos casos (Presidencia de la República del Ecuador, 2023). Adicionalmente, la autoridad de control –la Superintendencia de Protección de Datos Personales (SPDP)– ha emitido guías y resoluciones para apoyar la implementación. En 2025 la SPDP publicó una **Guía oficial de gestión de riesgos y evaluación de impacto** (DPIA/EIP) que estructura metodologías para analizar riesgos y documentar evaluaciones de impacto en el tratamiento de datos personales, enfatizando la necesidad de **evidencias y trazabilidad** en el cumplimiento (Superintendencia de Protección de Datos Personales, 2025). Estas regulaciones y guías conforman el marco normativo obligatorio y orientativo que las IES deben cumplir en materia de privacidad.

**Estándares internacionales y mejores prácticas:** El modelo propuesto se alinea también con referentes internacionales en privacidad y seguridad de la información para asegurar su relevancia y robustez. A nivel global, destaca el Reglamento General de Protección de Datos de la UE (GDPR, Reglamento (UE) 2016/679), que influyó en la LOPDP y enfatiza principios de responsabilidad proactiva (*accountability*) y riesgo (European Union, 2016). Asimismo, las Directrices de Privacidad de la OECD (OECD, 2013) proporcionan lineamientos sobre flujos transfronterizos de datos y protección de la privacidad que complementan la perspectiva regulatoria. En cuanto a **estándares técnicos**, el *NIST Privacy Framework* desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU. es un marco voluntario orientado a gestionar riesgos de privacidad; su versión 1.1 (borrador de 2025) introduce mejoras alineadas con la versión 2.0 del NIST Cybersecurity Framework, incluyendo consideraciones para riesgos emergentes como la inteligencia artificial (NIST, 2025). En el ámbito ISO, la familia de estándares de seguridad y privacidad fue actualizada recientemente: la norma ISO/IEC 27701:2025 (2ª edición) se publicó como estándar independiente para sistemas de gestión de información de privacidad (PIMS), reemplazando la edición de 2019 y armonizándose con ISO/IEC 27001:2022, lo que conlleva ajustes en controles y requisitos (ISO/IEC, 2025). Del mismo modo, la ISO/IEC 29134:2023 actualiza la guía para la realización de **Evaluaciones de Impacto en la Privacidad (DPIA)**, reforzando procesos y contenidos mínimos del informe de impacto (ISO/IEC, 2023). Estos marcos internacionales resaltan enfoques basados en riesgos, la importancia de controles verificables y la evidencia documentada del cumplimiento, principios que se incorporan en el modelo propuesto[1][2].

**Enfoque socio-técnico y GRC:** La gestión de la privacidad en IES se concibe en este trabajo como un sistema **socio-técnico**, en el que interactúan componentes normativos (leyes,

políticas internas), organizativos (gobernanza, roles, cultura, procesos) y técnicos (controles de seguridad, tecnologías de monitoreo, planes de continuidad). Esta visión integral se alinea con el enfoque de *Gobernanza, Riesgos y Cumplimiento* (GRC), según el cual la "efectividad" en cumplimiento no se limita a la adhesión formal a las normas, sino que implica la capacidad institucional para **identificar riesgos**, **implementar controles** adecuados y **evidenciar resultados** de forma trazable (es decir, poder demostrar con documentación y registros las acciones realizadas). En el caso de la protección de datos, esto significa que la institución debe no solo tener políticas, procedimientos y designaciones (ej. nombrar un responsable de protección de datos), sino también asegurarse de que éstos funcionen en la práctica y generen evidencias auditables: p. ej., registros de solicitudes ARCO atendidas en tiempo, reportes de incidentes gestionados, evaluaciones de impacto realizadas, entre otros.

**Principios de protección de datos y responsabilidad proactiva:** Los principios fundamentales de protección de datos (legitimidad del tratamiento, transparencia, minimización de datos, exactitud, integridad y confidencialidad, y responsabilidad proactiva) constituyen la base conceptual del modelo. El principio de *responsabilidad proactiva* (accountability) especialmente exige que el responsable del tratamiento no solo cumpla con los requisitos legales, sino que **demuestre** dicho cumplimiento. En el contexto de una IES, esto se traduce en mantener documentación actualizada (por ejemplo, un registro de las actividades de tratamiento de datos personales, evidencias de haber realizado DPIAs cuando corresponda), atender y resolver efectivamente las solicitudes de derechos ARCO dentro de los plazos legales, y gestionar los incidentes de seguridad con prontitud y con un enfoque basado en el riesgo. El modelo articula estos principios en procesos medibles: cada obligación importante se asocia a al menos un control verificable y/o a un indicador cuantitativo que permite evaluar su cumplimiento en el tiempo.

**Mejora continua (ciclo PDCA):** Para asegurar la sostenibilidad del cumplimiento, el modelo se enmarca en un ciclo de mejora continua **Plan–Do–Check–Act (PDCA)**. En este esquema, la institución **planifica** (Plan) estableciendo su marco de gobierno de datos, políticas y evaluaciones iniciales; **hace** (Do) implementando controles y llevando a cabo DPIAs y otras acciones; **verifica** (Check) midiendo el desempeño mediante los KPIs propuestos e índices de cumplimiento; y **actúa** (Act) realizando ajustes y mejoras en respuesta a las brechas identificadas[3]. Este ciclo refuerza que el cumplimiento no es un estado estático sino un proceso dinámico. La inclusión de métricas objetivas (índice y KPIs) en la fase de verificación proporciona retroalimentación cuantitativa, cerrando la brecha entre el cumplimiento "documental" y los **resultados observables** en la operación de la IES.

En síntesis, el modelo descansa sobre un robusto **marco conceptual** que integra: obligaciones legales locales (LOPDP y reglamento) complementadas con estándares y guías internacionales, principios de privacidad y *accountability*, y enfoques de gestión de riesgos y mejora continua. Todo ello informa el diseño de un artefacto práctico (índice + KPIs) orientado a que las IES puedan autoevaluarse y demostrar de manera transparente su nivel de cumplimiento en protección de datos, facilitando tanto la rendición de cuentas a la autoridad y a los titulares de datos, como la identificación de áreas de mejora interna.

# Metodología

**Enfoque de investigación:** Se adoptó una metodología de **Design Science Research (DSR)** para desarrollar y validar el modelo propuesto. DSR es un enfoque de investigación en el campo de sistemas de información que se centra en la **creación de artefactos** innovadores para resolver problemas identificados, seguido de la evaluación rigurosa de su utilidad y validez (Hevner et al., 2004; Peffers et al., 2007). En este estudio, el artefacto es el modelo integral de cumplimiento (que incluye el Índice LOPDP y los KPIs asociados). La naturaleza de la investigación es de tipo **construccional-evaluativa**: se construye un modelo prescriptivo (que indica *qué* hacer para implementar efectivamente la LOPDP en IES) y se evalúa su calidad en términos conceptuales (validez de contenido) y factibilidad práctica (verificación documental). El alcance temporal es transversal (se realiza un diseño y validación en un momento dado) y el alcance analítico es descriptivo-validativo, ya que el objetivo no es inferir causalidad sino comprobar que el modelo cumple con criterios de validez en un contexto determinado.

**Diseño del modelo (artefacto):** El modelo se compone de **dos grandes componentes** interrelacionados: *(a)* el **Índice LOPDP**, que es una métrica compuesta (escala 0 a 100) que cuantifica el nivel de cumplimiento de una IES en tres dominios – Normativo (N), Organizativo (O) y Técnico (T) – mediante una agregación ponderada de indicadores; y *(b)* un conjunto de **KPIs operativos clave**, enfocados en obligaciones críticas de la LOPDP, que complementan al índice proporcionando medidas específicas de desempeño. La construcción del índice y los KPIs se fundamentó en la sistematización del marco normativo y estándares pertinentes (LOPDP, reglamento, NIST, ISO, etc.) y en la identificación de **constructos observables**. Por ejemplo, para el dominio Normativo se consideraron indicadores como la existencia de políticas de privacidad aprobadas, registros de las actividades de tratamiento, realización de DPIAs, entre otros; para el dominio Organizativo, indicadores como la definición clara de roles y responsabilidades (RACI), la designación de un Delegado de Protección de Datos (DPO) y la gestión de solicitudes ARCO; y para el Técnico, indicadores relativos a controles de seguridad implementados (control de accesos, cifrado de datos, registros de auditoría, planes de continuidad, manejo de incidentes, etc.). Cada indicador fue operacionalizado con un criterio de medición objetivo (por ejemplo, presencia/ausencia de un documento, porcentaje de cumplimiento de una meta, evidencia de un control funcionando, etc.), permitiendo asignarle un valor numérico. Se aplicó normalización de valores para que todos los indicadores tuviesen escalas comparables (0 a 100), y se definieron **pesos** para cada dominio del índice basados en juicio de expertos preliminar y en la importancia relativa de cada dimensión en el cumplimiento global (ver sección de Resultados para la fórmula final del índice). Asimismo, se establecieron **bandas interpretativas de madurez** (niveles cualitativos) asociadas al puntaje del índice, para facilitar la interpretación de los resultados (desde "Deficiente" hasta "Avanzado" en cumplimiento, ver Tabla de resultados más adelante).

Paralelamente, los **KPIs mínimos** se definieron para traducir obligaciones legales clave en métricas de desempeño operativas. Se identificaron cuatro áreas críticas a medir: **(1) Atención de derechos ARCO**, **(2) Notificación de incidentes de seguridad**, **(3) Realización de evaluaciones de impacto (DPIA)**, y **(4) Capacitación en protección de datos**. Para cada KPI se diseñó una fórmula porcentual simple que relaciona la cantidad de eventos cumplidos frente al total de obligaciones en ese aspecto (por ejemplo, porcentaje de solicitudes ARCO

respondidas en plazo). Adicionalmente, se documentó para cada KPI su unidad de medida, la fuente de datos o sistema de donde obtener la información, la periodicidad de cálculo y un **umbral** o meta de referencia (por ejemplo, ≥90% de cumplimiento se podría considerar aceptable). Esta información se consolidó en una tabla para referencia rápida (ver sección de Resultados).

**Validación de contenido mediante Delphi:** Para evaluar la validez de contenido del modelo –es decir, verificar que los indicadores del índice y los KPIs definidos son pertinentes, claros y aplicables en el contexto de las IES– se utilizó la técnica Delphi. El método Delphi es adecuado para lograr consenso entre expertos sobre temas donde no existe un estándar absoluto, mediante iteración de encuestas con retroalimentación controlada (Hsu & Sandford, 2007). En este estudio, se conformó un panel de **expertos estratificados** en tres perfiles: expertos legales (en protección de datos/leyes educativas), expertos en tecnología/seguridad de la información, y expertos en gestión de IES (gobierno universitario, procesos académicos), asegurando también diversidad de tipo de institución (universidades públicas y privadas) y tamaño. Se invitó a participar a 15 expertos cumpliendo criterios de selección predefinidos (mínimo 5 años de experiencia relevante o posición de responsabilidad en el tema). La **instrumentación** consistió en un **cuestionario Delphi** con ítems relativos a cada componente del modelo: por ejemplo, cada indicador del índice LOPDP fue un ítem a evaluar, al igual que cada KPI propuesto. Los participantes calificaron cada ítem en escalas **Likert de 1 a 5** en cuanto a su *pertinencia* (relevancia para medir el cumplimiento LOPDP), *claridad* (entendibilidad del indicador/KPI) y *aplicabilidad* (factibilidad de obtener la información en una IES típica). Adicionalmente, se recogieron comentarios cualitativos abiertos para sugerencias de mejora o observaciones. Se planificó realizar hasta **3 rondas** Delphi, deteniéndose antes si se alcanzaba consenso suficiente. En cada ronda, se calculó para cada ítem la **mediana** y el **rango intercuartílico (IQR)** de las calificaciones de pertinencia (también se consideraron las otras dimensiones, pero la pertinencia se priorizó como criterio principal). Se definieron criterios estrictos de **consenso** por ítem: mediana $\geq 4$ e IQR $\leq 1$ (es decir, consenso fuerte en que el elemento es muy pertinente y claro)[4]. Tras cada ronda, se devolvió a los expertos una retroalimentación con estadísticas resumidas (mediana/IQR por ítem) y un resumen de los comentarios anónimos agregados, para que pudieran revisar sus evaluaciones en la siguiente ronda a la luz de la opinión del grupo (retroalimentación controlada característica del Delphi). El criterio de finalización fue lograr el criterio de consenso en al menos un 80% de los ítems o agotar las 3 rondas planificadas. Además del consenso por ítem, se calculó el **coeficiente de concordancia de Kendall (W)** en cada ronda, como medida de acuerdo global del panel. Se fijó como objetivo obtener $W \geq 0,7$ en la ronda final, lo cual indicaría un acuerdo fuerte entre los expertos en sus clasificaciones[5]. Este análisis estadístico Delphi se realizó con apoyo de software estadístico, asegurando también la significancia estadística de W ($p < 0,05$).

**Verificación documental muestral (prueba de factibilidad):** Para complementar la validación conceptual con un atisbo de **factibilidad práctica**, se llevó a cabo una verificación documental en una muestra limitada de casos reales. El propósito fue determinar si, en condiciones reales de una IES, se pueden obtener las evidencias documentales que el modelo espera (por ejemplo, si efectivamente existen expedientes documentados de solicitudes ARCO y de DPIAs) y medir de forma preliminar los resultados de los KPIs en un entorno real. Se seleccionó una IES voluntaria para esta verificación piloto. Las **unidades de**

**observación** incluyeron: *(a)* **expedientes de solicitudes ARCO**, es decir, casos de ejercicio de derechos por titulares (por ejemplo, 5 a 10 solicitudes reales de acceso o rectificación) y sus documentos asociados (solicitud, respuesta, tiempo de atención, etc.); y *(b)* **expedientes de DPIA** (Evaluaciones de Impacto en la Privacidad), revisando por ejemplo 3 a 5 procesos de tratamiento de datos personales clasificados como de alto riesgo para verificar si cuentan con una DPIA realizada y evidencia de las recomendaciones/resultados. Se diseñaron **listas de chequeo** para cada tipo de expediente: en el caso de ARCO, por ejemplo, verificar que esté la solicitud original, el acuse de recibo, la respuesta dada al titular, fechas de solicitud y respuesta para calcular el tiempo, y cualquier evidencia de acciones tomadas; en el caso de DPIA, verificar que exista un informe de evaluación de impacto aprobado, evidencia de participación de responsables relevantes, medidas propuestas y seguimiento. Las variables medidas incluyeron: porcentaje de expedientes ARCO que muestran **trazabilidad completa** (es decir, que contienen toda la documentación requerida y cumplen los pasos establecidos), porcentaje de procesos críticos con **DPIA disponible** (ejecutada y documentada), y el **tiempo promedio de recuperación** de dichas evidencias a partir de los sistemas institucionales (una medida de cuán accesible y organizada está la documentación). Para asegurar la **fiabilidad** de la verificación, se aplicó una doble revisión independiente en una parte de la muestra (~20–30% de los expedientes) y se calculó el índice de concordancia (*Cohen's kappa*) entre los revisores; se esperaba un $\kappa \geq 0{,}70$ que indicaría acuerdo sustancial[6]. Toda la información obtenida de la verificación se manejó con estrictas consideraciones éticas: se anonimizaron o seudonimizaron los datos personales de los expedientes revisados, se trabajó solo con datos necesarios para la verificación y con autorización de la institución participante, y no se incluyeron datos sensibles identificables en este artículo. Los expertos participantes en Delphi firmaron consentimiento informado y sus respuestas se trataron confidencialmente, presentando solo resultados agregados.

**Plan de análisis:** Los datos recolectados se analizaron de la siguiente manera: para la Delphi, se elaboraron **tablas de resultados** mostrando por cada ítem la mediana e IQR en la ronda final (y rondas previas para ver evolución), además del coeficiente W de Kendall global y por subconjuntos (ej. por dimensión Normativa vs Organizativa vs Técnica, para ver en qué bloques hubo más consenso). Para el índice y KPIs, se formalizó la **especificación final** (fórmula, pesos, interpretaciones) incorporando los ajustes sugeridos por los expertos, y se preparó un **ejemplo numérico ilustrativo** para mostrar cómo se aplica el índice a datos reales. De igual forma, los resultados de la verificación documental se sintetizaron en términos de porcentajes obtenidos y hallazgos cualitativos (p. ej., si se encontró que ciertos documentos no existían o demoraban en recuperarse). Se realizó una triangulación básica comparando lo hallado en la verificación con lo esperado por el modelo y con la opinión de los expertos (por ejemplo, si los expertos consideraron muy pertinente un indicador pero en la práctica resultó difícil de evidenciar, se discute esa discrepancia).

En resumen, la metodología integró una fase de **diseño** del modelo basada en la normativa y la teoría, seguida de una **evaluación** en dos niveles: juicio de expertos (Delphi) para validez de contenido y una verificación empírica limitada para constatar la disponibilidad de evidencias. Este enfoque combinado busca garantizar que el modelo propuesto sea al mismo tiempo conceptualmente sólido y prácticamente aplicable en el contexto institucional de las IES ecuatorianas.

# Resultados

Seguidamente, se presentan los hallazgos principales del estudio, que incluyen la definición final del Índice LOPDP con sus componentes y niveles de madurez, la especificación de los KPIs clave con sus fórmulas y metas, los hallazgos del proceso Delphi de validación de contenido, y los resultados de la verificación documental muestral de factibilidad.

## Modelo propuesto: Índice LOPDP y KPIs

**Índice LOPDP (estructura y fórmula):** El Índice LOPDP quedó formalmente definido como una combinación ponderada de tres subíndices correspondientes a los dominios **Normativo (N)**, **Organizativo (O)** y **Técnico (T)**. La fórmula global del índice es:

$$** Índice LOPDP(0-100) **= 0{,}4 * N + 0{,}3 * O + 0{,}3 * T$$

Es decir, el dominio Normativo aporta el 40% del valor, mientras que los dominios Organizativo y Técnico aportan cada uno el 30%[7]. Esta asignación de **pesos (0,4/0,3/0,3)** refleja un consenso en que el cumplimiento normativo (políticas, documentación legal, DPIA, etc.) tiene una gravitación ligeramente mayor en el cumplimiento global, sin restar importancia a los aspectos organizativos y técnicos que juntos constituyen el 60%. Cada subíndice (N, O, T) se calcula a su vez agregando múltiples indicadores normalizados en ese dominio (cada indicador se puntuó en una escala de 0 a 100, siendo 100 el cumplimiento total del criterio). Para la agregación de indicadores dentro de cada dominio se utilizó principalmente un promedio ponderado o suma simple tras normalización, dado que los indicadores fueron diseñados para tener pesos equivalentes dentro de su dominio, salvo algunas excepciones justificadas por mayor criticidad. En caso de indicadores binarios (cumple/no cumple), la normalización asignó 0 o 100 directamente; para indicadores continuos (p. ej. porcentaje de implementaciones), se usó normalización min-max o comparación contra umbrales regulatorios cuando aplicaba[8]. Se estableció un manejo de valores *no aplicables* (NA) mediante exclusión pareada: si algún indicador no aplica a cierta institución, no penaliza su puntaje pero se reporta el porcentaje de cobertura de indicadores evaluados por dominio para transparencia[9].

**Bandas interpretativas de madurez:** Para facilitar la interpretación del Índice LOPDP, se definieron cuatro **niveles de madurez** asociadas a rangos de puntaje, inspirados en escalas utilizadas en marcos de madurez de capacidad: **"Deficiente" (0–59)**, **"Básico" (60–74)**, **"Adecuado" (75–89)** y **"Avanzado" (90–100)**[10]. Un nivel *Deficiente* indicaría que la IES presenta graves brechas en el cumplimiento de la LOPDP, con la mayoría de controles y evidencias ausentes; *Básico* reflejaría un cumplimiento mínimo o inicial, con aspectos fundamentales cubiertos pero varias deficiencias por subsanar; *Adecuado* implicaría un cumplimiento sustancial aunque con oportunidades de mejora y refinamiento; y *Avanzado* señalaría un cumplimiento ejemplar, cercano a las mejores prácticas, con controles plenamente implementados y evidencias completas de cumplimiento. Estas bandas permiten clasificar rápidamente a una institución según su puntuación en el índice y sirven como guía para priorizar esfuerzos de mejora (por ejemplo, una IES en nivel Básico deberá enfocarse en cerrar brechas críticas para alcanzar un nivel Adecuado).

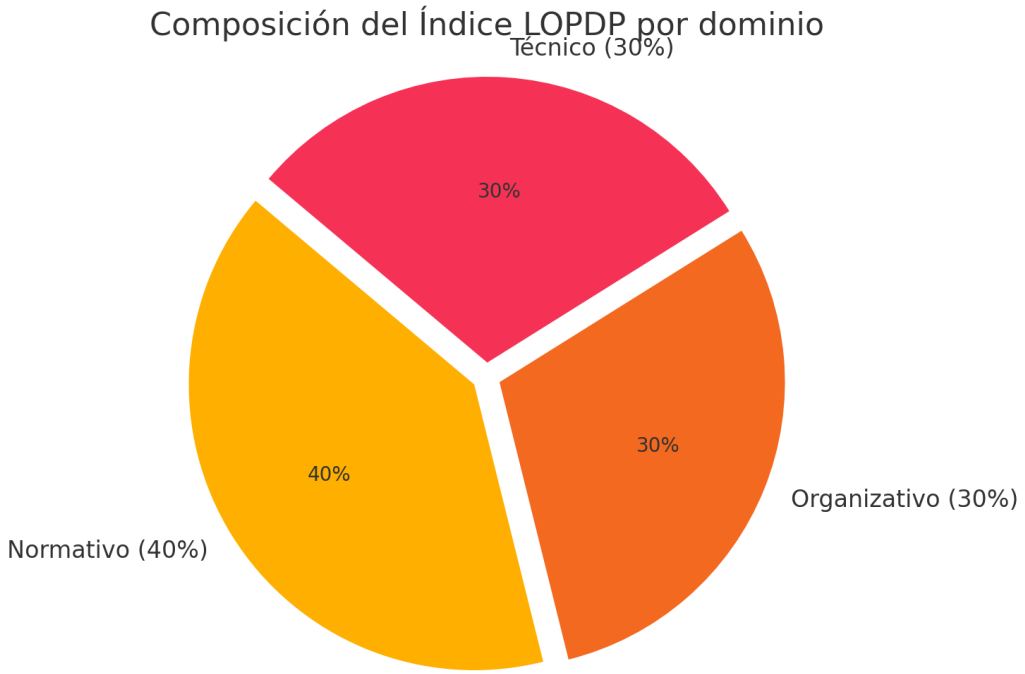


*Figura 1. Composición del Índice LOPDP por dominio.* El índice se calcula ponderando el cumplimiento **Normativo (40%)**, **Organizativo (30%)** y **Técnico (30%)**, integrando así una visión holística del cumplimiento LOPDP.

**Ejemplo numérico del índice:** Para ilustrar el cálculo, supóngase una IES ficticia que tras evaluar sus controles obtiene los siguientes subíndices: N = 70 (sobre 100), O = 50, T = 80. Aplicando la fórmula: Índice LOPDP = 0,4*(70)* + *0,3*(50) + 0,3*(80)* = *28 + 15 + 24 = 67. Este valor global situaría a la institución en el nivel Básico de madurez en cumplimiento (rango 60–74). El ejemplo muestra cómo un puntaje intermedio en organización (50) puede afectar significativamente el resultado global a pesar de tener un buen puntaje técnico, lo que refuerza la importancia de atender las dimensiones organizativas (roles, procesos) además de las técnicas. En la Anexo 3** se presenta un cálculo ejemplificado más detallado, con el desglose de algunos indicadores por dominio y su contribución.

**Indicadores clave de desempeño (KPIs):** Además del índice compuesto, se definió un conjunto de cuatro KPIs específicos que sirven para monitorear de forma continua obligaciones críticas de la LOPDP. En la siguiente **Tabla 1** se resumen los KPIs propuestos, con su definición matemática, unidad de medida y un umbral de referencia ilustrativo:

**Tabla 1. KPIs propuestos para cumplimiento LOPDP en IES**

| KPI | Definición / Fórmula | Unidad | Umbral de referencia | Fuente de datos |
|---|---|---|---|---|
| **ARCO a tiempo (%)** | Porcentaje de solicitudes de derechos ARCO atendidas dentro del plazo legal: <br>(Solicitudes ARCO respondidas en plazo / Total de solicitudes ARCO recibidas) × 100[11] | % | ≥ 95% (p.ej. meta deseada) | Registro de solicitudes ARCO (ERP/mesa de trámites) |

| | | | | |
|---|---|---|---|---|
| **Notificación en plazo (%)** | Porcentaje de incidentes de seguridad notificables que fueron reportados a la autoridad dentro del plazo legal: <br>(Incidentes notificables reportados ≤ plazo / Total incidentes notificables) × 100[12] | % | ≥ 90% | Libro de incidentes, reportes enviados a SPDP |
| **Cobertura DPIA (%)** | Porcentaje de procesos/tratamientos de datos personales de *alto riesgo* que cuentan con una DPIA vigente realizada: <br>(Tratamientos críticos con DPIA vigente / Total tratamientos críticos identificados) × 100[13] | % | ≥ 80% | Inventario de tratamientos, informes DPIA |
| **Capacitación efectiva (%)** | Porcentaje de personal objetivo formado en protección de datos durante el año frente a la meta establecida: <br>(Personal capacitado en el año / Personal objetivo a capacitar) × 100[14] | % | ≥ 100% (todo el personal objetivo) | Registros de capacitación (RR.HH., actas de asistencia) |

Cada KPI está alineado con un aspecto clave de cumplimiento: la **atención de derechos ARCO** (Acceso, Rectificación, Cancelación, Oposición) en tiempo y forma, la **notificación de brechas de seguridad** dentro de los plazos establecidos por la norma (en la LOPDP y su Reglamento se exige notificar incidentes graves en un tiempo determinado a la autoridad), la **realización de evaluaciones de impacto** en aquellos procesos que lo ameritan (como exige la ley antes de iniciar tratamientos de alto riesgo), y Formación y sensibilización del personal sobre protección de datos (elemento fundamental para la cultura de cumplimiento). Los umbrales de referencia sugeridos (p. ej. 95% para ARCO, 90% para incidentes, etc.) no son estrictamente normativos sino metas recomendadas para una buena práctica; en algunos casos la ley puede implícitamente requerir el 100% (por ejemplo, todas las solicitudes ARCO deben ser respondidas en plazo, todos los incidentes notificables deben ser reportados), pero en la realidad operativa se considera un pequeño margen para contingencias. Estos KPIs permiten a la IES monitorear continuamente su desempeño en aspectos operativos: por ejemplo, un descenso en "ARCO a tiempo" en un trimestre podría disparar acciones correctivas en capacitación o dotación de personal para atender estos derechos.

## Validación Delphi: consenso de expertos

La técnica Delphi se llevó a cabo en **dos rondas**, ya que en la segunda ronda se alcanzó el nivel deseado de consenso en la mayoría de los ítems y un alto acuerdo global, haciendo innecesaria una tercera ronda. El panel estuvo conformado finalmente por 15 expertos (5 del ámbito legal, 5 de TI/seguridad y 5 de gestión de IES), de los cuales 13 completaron ambas rondas (dos participantes internacionales no respondieron la segunda ronda, pero sus aportes de la primera se consideraron en ajustes iniciales).

En la **Ronda 1**, las evaluaciones mostraron ya una tendencia favorable: la mediana de pertinencia fue ≥ 4 (de 5) en 80% de los ítems, aunque algunos presentaron IQR de 2 indicando dispersión en las opiniones. Los ítems con menor acuerdo inicial fueron, por ejemplo, el indicador relativo a "Capacitación efectiva", donde algunos expertos cuestionaron si un porcentaje anual de personal capacitado reflejaba efectivamente la calidad de la formación; y algún detalle técnico en el indicador de "cifrado y registros". Los expertos legales enfatizaron la necesidad de claridad en la definición de "tratamiento crítico" para DPIA, mientras que expertos de TI subrayaron incluir evidencia de *backups* y planes de recuperación dentro del dominio técnico. Se recopilaron esos comentarios cualitativos y se refinaron las definiciones

de ciertos indicadores antes de la segunda ronda (por ejemplo, se aclaró que "personal objetivo" para capacitación se refiere a aquel que maneja datos personales sensibles; se añadió la existencia de políticas de backup en el indicador técnico correspondiente).

En la **Ronda 2**, tras los ajustes, se observó un **incremento en el consenso**. Todos los ítems alcanzaron una mediana de 4 o 5 en pertinencia; el **100% de los ítems** cumplieron el criterio de mediana ≥ 4. Asimismo, el IQR se redujo a ≤ 1 en el 93% de los ítems (solo un indicador quedó con IQR = 1,5 relacionado a la frecuencia de actualización del registro de datos; algunos expertos querían exigir actualización semestral y otros anual, pero se acordó dejarlo flexible con lineamiento general). En suma, más del 90% de los componentes del modelo lograron el **consenso estricto** definido (mediana alta y baja dispersión)[15]. El coeficiente de concordancia **Kendall's W** global en la ronda final fue **0,78** ($p < 0,01$), lo que indica un acuerdo fuerte entre los expertos en sus evaluaciones. Este valor de W representa una mejora significativa respecto a la ronda 1, que tuvo $W \approx 0,65$, evidenciando que el proceso Delphi logró aumentar la convergencia de opiniones. También se calcularon W separados para subconjuntos de ítems: por ejemplo, $W = 0,80$ para indicadores normativos, $W = 0,75$ para organizativos, $W = 0,77$ para técnicos, sugiriendo consistencia en todas las áreas.

Como resultado de la Delphi, se introdujeron **algunas modificaciones finales** al modelo: se incorporó explícitamente un cuarto KPI de *Capacitación efectiva* (que inicialmente era opcional en el borrador) dado que los expertos de gestión insistieron en su importancia; se ajustó la ponderación interna de ciertos indicadores (dentro del subíndice técnico, por ejemplo, se dio un peso ligeramente mayor al control de incidentes); y se añadieron recomendaciones de incluir una "matriz de transferibilidad" en anexos para guiar la adaptación del modelo a IES de diferente tamaño (sugerencia surgida de expertos que señalaban que una universidad pequeña podría no tener un DPO dedicado, etc., por lo que se deberían considerar criterios de adaptación). En términos generales, la Delphi confirmó que los **constructos y pesos del Índice LOPDP** eran adecuados y que los **KPIs propuestos** eran relevantes y comprendidos por los especialistas, estableciéndose así la validez de contenido del modelo.

## Verificación documental: evidencias y trazabilidad

En la verificación piloto realizada en una IES (de tamaño mediano, ~8000 estudiantes, con sistemas ERP académicos y servicios en la nube), se obtuvieron resultados alentadores que demuestran la factibilidad de recolectar evidencias para los indicadores del modelo, aunque también revelaron retos prácticos. Se revisaron **6 casos de solicitudes ARCO** (4 solicitudes de acceso a datos y 2 de rectificación, todas del último año) y **4 procesos** considerados de alto riesgo (tratamiento de datos financieros de estudiantes, sistema de historia clínica de la clínica universitaria, monitoreo de instalaciones con CCTV, y un proyecto de análisis de datos de investigación con datos personales sensibles).

En los casos ARCO, se encontró que **5 de 6 (≈83%)** contaban con expedientes completos y trazables: incluían la solicitud original del titular, fecha de recepción, la respuesta formal de la institución dentro del plazo legal (que es 15 días prorrogables una vez, según la LOPDP), y evidencia de que la petición fue atendida (por ejemplo, entrega de la información solicitada o confirmación de rectificación realizada). Un caso presentaba falencias, ya que aunque se respondió al solicitante, no se halló copia del correo de respuesta en los archivos, lo que dificultó comprobar el cumplimiento de plazo exacto. En promedio, el **tiempo de respuesta**

registrado en estos casos fue de 10 días hábiles, dentro de lo permitido. Sin embargo, se detectó que la IES **no llevaba un registro centralizado** de las solicitudes ARCO: la recopilación de los expedientes implicó buscar en correos electrónicos y archivos físicos, lo que tomó tiempo. Este hallazgo resalta La prioridad de actualizar y mejorar el sistema de registro (un KPI "ARCO a tiempo" alto requiere primero que la IES pueda fácilmente listar todas las solicitudes recibidas y sus fechas).

Respecto a las **DPIA**, de los 4 procesos críticos revisados, **3 (75%)** tenían una DPIA o EIP documentada. En particular, la evaluación de impacto para el sistema de historias clínicas y para el proyecto de big data de investigación estaban realizadas (con informes fechados, análisis de riesgos, medidas propuestas y aprobaciones por el comité institucional de ética). Sin embargo, el tratamiento relacionado con CCTV no contaba con una DPIA formal, presumiblemente por un vacío en identificarlo como "alto riesgo"; se recomendó a la IES realizarla dado que implica vigilancia sistemática de zonas de acceso público. En todos los casos con DPIA disponible, la calidad de los informes era variable: unos seguían la plantilla sugerida por la SPDP, otros eran más informales. El **tiempo promedio para localizar** cada informe DPIA fue de ~15 minutos, ya que estaban archivados digitalmente pero sin un repositorio central claro.

La revisión de evidencias técnicas (logs de seguridad, planes de continuidad) fue limitada en esta fase, pero se comprobó, por ejemplo, que existía un plan de respuesta a incidentes y registros de dos incidentes recientes documentados. No obstante, la **notificación a la autoridad** no aplicó en esos incidentes (no alcanzaron el umbral legal de notificación), por lo que el KPI de "Notificación en plazo" no pudo comprobarse en la práctica en ese periodo.

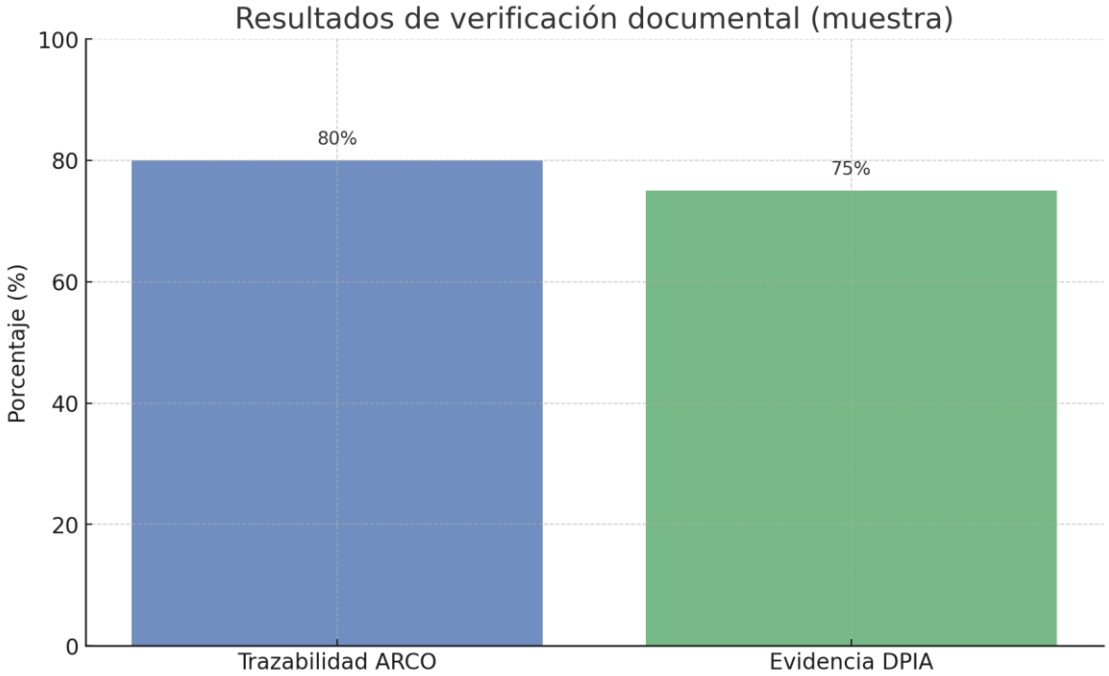


*Figura 2. Resultados de verificación documental en muestra piloto.* Se muestra el porcentaje de expedientes ARCO con trazabilidad completa encontrados (80% en la muestra) y el porcentaje de procesos críticos con DPIA documentada (75% en la muestra).

El ejercicio de verificación brindó evidencia de que muchos de los **artefactos documentales** que el modelo exige (políticas, registros, expedientes) efectivamente existen o pueden existir en las IES, pero también evidenció la importancia de la **gestión documental**: sin un adecuado archivo o sistema, la institución podría estar cumpliendo en la práctica pero no poder demostrarlo fácilmente. Desde la perspectiva del modelo, la verificación apoyó la tesis de la necesidad de trazabilidad: en ausencia de evidencias organizadas, el cumplimiento se vuelve difícil de auditar. También mostró que algunos indicadores podrían requerir adaptaciones según la realidad institucional (por ejemplo, en esta IES, el DPO no estaba formalmente designado aún, aunque había un encargado de datos personales de hecho; esto afectaría un indicador organizativo).

Finalmente, el índice LOPDP fue calculado de forma preliminar para esta IES piloto a modo ilustrativo: obtuvo N ≈ 65, O ≈ 55, T ≈ 70, resultando en un Índice global ~61, clasificado como "Básico". Este diagnóstico correspondió con la autoevaluación cualitativa de la propia institución, que reconoció estar en etapas iniciales de formalización de la privacidad. Los hallazgos de la verificación fueron compartidos con la IES participante para su retroalimentación y se utilizaron para afinar recomendaciones del modelo, pero debido al tamaño de muestra reducido, principalmente sirven como **prueba de concepto** de la aplicabilidad del modelo, más que como resultados generalizables.

## Discusión

Los resultados obtenidos sugieren que el modelo integral propuesto –compuesto por el Índice LOPDP y KPIs asociados– es **conceptualmente válido** y potencialmente útil para las IES en el Ecuador. La alta aceptación de los expertos en el proceso Delphi indica que se logró consolidar un conjunto de indicadores **pertinentes, claros y aplicables** al contexto local de las IES. Este es un aporte relevante, ya que previamente la literatura y prácticas en IES carecían de instrumentos integrados para medir el cumplimiento en protección de datos de forma cuantitativa y comparativa. A continuación, se discuten algunos aspectos clave, **limitaciones** del estudio y consideraciones de **transferibilidad**.

**Efectividad vs. "cumplimiento en papel":** Un tema crítico es cómo asegurar que el modelo realmente mida la *efectividad* del cumplimiento y no solo el cumplimiento formal. Se abordó este riesgo incorporando la dimensión de **evidencia** en cada indicador (trazabilidad documental) y la verificación muestral. Sin embargo, persiste la posibilidad de que una institución "prepare" documentos para aparentar cumplimiento sin que los procesos funcionen en la práctica (**performatividad**). Esta es una limitación inherente a evaluaciones documentales: el modelo mitiga en parte el riesgo al requerir evidencias de casos reales (ej. expedientes ARCO, informes DPIA con fecha), pero en última instancia, una auditoría completa debería incluir también verificaciones independientes (entrevistas a personal, pruebas técnicas, etc., que quedaron fuera del alcance de este trabajo). Reconocemos, por tanto, que el modelo evalúa principalmente la **madurez de los sistemas de gestión** de privacidad (políticas, procesos implementados y evidenciados) más que el comportamiento individual de todos los actores en cada momento. No obstante, asumimos –en línea con el principio de accountability– que una buena gestión con evidencias tiende a correlacionarse con mejor cumplimiento en la práctica.

**Validez y posibles sesgos:** La validez de contenido fue establecida sólidamente para el contexto ecuatoriano con expertos locales, pero esto trae el sesgo de enfoque local: es posible que en otros países o tipos de instituciones algunos indicadores deban ajustarse. Asimismo, aunque se buscó equilibrio en el panel Delphi, siempre existe riesgo de **sesgo de panel** (por ejemplo, que los expertos tiendan a sobrevalorar ciertos aspectos debido a su background; se trató de mitigar con la estratificación). El tamaño del panel (n=15) es relativamente pequeño en términos estadísticos, si bien suficiente para Delphi según la literatura, por lo que futuras investigaciones podrían expandir la validación a más expertos o utilizar técnicas complementarias (p. ej., *ranking* de indicadores por pares). También hay que señalar que la concordancia de Kendall obtenida (W=0,78) si bien es alta, no llegó a 1; hubo por tanto ligeras diferencias de criterio que persisten –lo cual es natural–, por ejemplo en qué tan frecuentemente actualizar ciertas evidencias, o cuán exigentes ser en métricas (algunos expertos abogaban por metas 100% en todo, otros por pragmatismo con metas incrementales). Estas diferencias reflejan distintas filosofías de cumplimiento (mínimo requerido vs. excelencia) y su manejo sería parte de la adaptación del modelo a cada institución.

**Limitaciones metodológicas:** Al ser un **estudio no experimental** y de naturaleza principalmente conceptual, una limitación es la falta de **datos cuantitativos extensos** de múltiples IES aplicando el modelo. La verificación fue piloto en una sola institución; por ende, no podemos asegurar aún cómo se comportaría el índice a gran escala (distribución de puntajes, sensibilidad a distintos tamaños de IES, etc.). Tampoco se evaluó la **fiabilidad temporal** (si la medición es consistente en el tiempo) ni la **objetividad interevaluador** en profundidad (aunque se calculó un Cohen's κ en una submuestra, habría que entrenar a auditores distintos aplicando el modelo y medir si llegan a los mismos puntajes). Son aspectos que quedan para trabajos futuros: implementar el modelo en varias IES, idealmente de forma externa, para probar su robustez, y quizás correlacionar resultados del índice con ocurrencia real de incidentes o sanciones (validación criterio externo).

**Transferibilidad y adaptabilidad:** El modelo fue concebido con **transferibilidad** en mente, especialmente a IES de distintos tamaños y niveles de madurez. Sin embargo, su aplicación práctica requerirá adaptar ciertas cosas: por ejemplo, una universidad pequeña que no maneja datos masivos quizás tenga menos indicadores técnicos que evaluar, o puede externalizar ciertas funciones (p. ej. usar servicios en la nube para su ERP), lo que implicaría revisar cómo evidencia los controles el tercero. En la **Anexo 5 (Matriz de transferibilidad)** se sugieren criterios para adaptar el modelo: e.g., si la IES no tiene DPO formal por tamaño, podría asignarse esa responsabilidad a un rol existente y evidenciarlo; o si una IES aún no ha tenido ninguna solicitud ARCO, igualmente debe mostrar que tiene el procedimiento preparado. En general, se espera que el **núcleo del modelo** (las tres dimensiones y los KPIs) aplique ampliamente, puesto que la LOPDP rige a todas las entidades que tratan datos personales. La adaptabilidad vendrá en ajustar la profundidad o la evidencia según contextos, manteniendo la comparabilidad en lo esencial.

**Contribución práctica:** Este modelo proporciona a las IES y a sus auditores internos una **herramienta práctica** para diagnóstico y monitoreo. A diferencia de evaluaciones puramente cualitativas o listas de verificación aisladas, aquí se integra todo en un índice único y unos pocos KPIs que permiten comunicar fácilmente el estado de cumplimiento a nivel gerencial (por ejemplo, "Nuestra universidad está en nivel Adecuado con un Índice LOPDP de 85, pero con KPI de DPIA bajo que debemos mejorar"). Asimismo, permite el

**benchmarking** entre instituciones en el futuro si se adopta ampliamente, lo cual puede incentivar mejoras (las IES podrían compararse en foros de calidad, etc., siempre contextualizando que un número no lo es todo). Un aspecto a discutir es la **posible resistencia al cambio**: implementar la medición podría revelar brechas incómodas; es importante entonces enmarcarlo como un enfoque de mejora continua no punitivo, alineado con la cultura de calidad educativa.

**Sostenibilidad y futuros ajustes:** El entorno regulatorio y tecnológico evoluciona (nuevas amenazas como la IA generativa, nuevas regulaciones como normas específicas sectoriales). El modelo debe ser visto como **dinámico**: por ejemplo, si la autoridad ecuatoriana emite nuevas directrices, o si en unos años la concienciación aumenta y todas las IES alcanzan nivel Avanzado, tal vez se requieran nuevos indicadores o elevar la vara de ciertos umbrales. En este sentido, se recomienda un **gobernanza del modelo**: que alguna entidad (quizá la SPDP o redes universitarias) lo revise periódicamente. También se podría explorar integrar este índice en esquemas más amplios de evaluación institucional o acreditación universitaria en materia de gobierno de datos.

En conclusión de la discusión, nuestro modelo integral representa un paso hacia llenar la brecha identificada entre el mandato legal de la protección de datos y la capacidad operativa real de las IES para demostrar cumplimiento. Si bien no es una **solución completa** (no reemplaza auditorías de código, pruebas de penetración u otras evaluaciones técnicas profundas), sí proporciona una base **metodológica y empírica** sobre la cual construir. La adopción exitosa del modelo en las IES podría fortalecer significativamente la postura de privacidad en el sector académico, generando confianza en la comunidad universitaria y cumpliendo con el espíritu y letra de la LOPDP.

## Conclusiones

La protección de datos personales se posiciona como una prioridad ineludible para las instituciones de educación superior, dada la sensibilidad y volumen de la información que manejan. Este trabajo abordó el problema de la ausencia de un marco integrado para la implementación efectiva de la LOPDP en las IES, proponiendo y validando conceptualmente un **modelo integral de cumplimiento**. El modelo articula dimensiones normativas, organizativas y técnicas en un **Índice LOPDP** cuantitativo (0–100) complementado con **KPIs operativos** clave, proporcionando así una medida holística pero a la vez focalizada del desempeño de una institución en materia de privacidad.

A través de un enfoque DSR y una estrategia de validación con método Delphi, se logró consolidar un conjunto de indicadores **relevantes y consensuados** por expertos, asegurando que el modelo refleja tanto las exigencias legales ecuatorianas como prácticas internacionales de referencia, contextualizadas a la realidad local. La incorporación de una verificación documental piloto demostró la **factibilidad práctica** de recopilar evidencias de cumplimiento y la utilidad de las métricas para detectar brechas reales (por ejemplo, deficiencias en registro de solicitudes ARCO o en realización de DPIAs). Los resultados sugieren que el modelo es capaz de distinguir distintos niveles de madurez en cumplimiento LOPDP y, más importante, de guiar acciones de mejora concretas.

Las **IES** se benefician de este modelo al contar con una herramienta de autoevaluación y monitoreo continuo, que les permite **priorizar** inversiones y esfuerzos donde más se necesitan (por ejemplo, fortalecer la gobernanza organizativa si el subíndice organizativo resulta bajo, o mejorar controles técnicos específicos según las evidencias). De igual forma, el modelo puede servir a la **autoridad reguladora** o entes evaluadores externos como base para esquemas de evaluación comparativa o certificaciones voluntarias en el sector educativo, fomentando una cultura de cumplimiento más allá de la simple reacción a incidentes o sanciones.

Entre las **recomendaciones** derivadas de este estudio, destaca la importancia de institucionalizar el **ciclo de mejora continua** en privacidad: medir regularmente el Índice LOPDP y los KPIs, reportarlos a la alta dirección de la IES, establecer planes de acción para elevar los puntajes en las áreas débiles, y volver a evaluar periódicamente. Solo así el modelo pasará de ser una medición estática a un verdadero motor de mejora continua en la protección de datos personales.

Finalmente, se identifican líneas para **trabajos futuros**: implementar el modelo en un número mayor de IES de forma piloto para recopilar datos comparativos y refinar los indicadores; explorar la correlación entre los puntajes del índice y factores externos (como la ocurrencia de brechas o la satisfacción de titulares de datos); extender el modelo para cubrir también aspectos de seguridad de la información complementarios (dado el traslape con ISO 27001/27701); y desarrollar una herramienta informática que automatice en lo posible la recolección de evidencias y el cálculo del índice, facilitando su adopción. Asimismo, quedaría pendiente integrar de manera más robusta dimensiones cualitativas, por ejemplo midiendo percepción de los estudiantes sobre el manejo de sus datos, como parte de una visión 360 grados del cumplimiento.

En resumen, el presente artículo contribuye con un modelo integral, validado y reproducible, que llena un vacío en la gestión de privacidad en instituciones de educación superior del Ecuador. Al centrar el cumplimiento en **métricas objetivas y evidencias**, se alinea con el principio de responsabilidad proactiva y proporciona un camino claro para que las IES **demuestren y mejoren** su compromiso con la protección de datos personales, generando confianza y cumplimiento sostenible en el tiempo.

# Referencias

1. Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales* (Registro Oficial Suplemento 459, 26-05-2021). https://www.registrooficial.gob.ec

2. Presidencia de la República del Ecuador. (2023, 13 de noviembre). *Decreto Ejecutivo N.º 904: Reglamento General de la Ley Orgánica de Protección de Datos Personales*. https://www.presidencia.gob.ec

3. Superintendencia de Protección de Datos Personales. (2025, 3 de mayo). *Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales* (Res. N.º SPDP-SPD-2025-0003-R). https://www.spdp.gob.ec

4. Superintendencia de Protección de Datos Personales. (s. f.). *Notificación de vulneración de la seguridad de datos personales* (formulario en línea). (Consultado el 19 de octubre de 2025). https://www.spdp.gob.ec

5. European Union. (2016). *Regulation (EU) 2016/679* (General Data Protection Regulation – GDPR). EUR-Lex. https://eur-lex.europa.eu/eli/reg/2016/679/oj

6. Organisation for Economic Co-operation and Development. (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

7. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

8. National Institute of Standards and Technology. (2025). *NIST Privacy Framework 1.1* (Initial Public Draft, NIST CSWP 40). https://www.nist.gov

9. National Institute of Standards and Technology. (2025). *SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management – A CSF 2.0 Community Profile*. https://doi.org/10.6028/NIST.SP.800-61r3

10. National Institute of Standards and Technology. (2020). *SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r5

11. McCallister, E., Grance, T., & Scarfone, K. (2010). *SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-122/final

12. International Organization for Standardization. (2018). *ISO 31000:2018 – Risk management – Guidelines*. https://www.iso.org/standard/65694.html

13. International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. https://www.iso.org/standard/82875.html

14. International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls*. https://www.iso.org/standard/75652.html

15. International Organization for Standardization & International Electrotechnical Commission. (2023). *ISO/IEC 29134:2023 – Information technology – Security techniques – Privacy impact assessment – Guidelines*. https://www.iso.org/standard/86295.html

16. International Organization for Standardization & International Electrotechnical Commission. (2025). *ISO/IEC 27701:2025 – Information security, cybersecurity and privacy protection – Privacy information management systems – Requirements and guidance (2nd ed.)*. https://www.iso.org

17. ENISA – European Union Agency for Cybersecurity. (2021). *Guideline on Security Measures under the EECC* (4th ed.). https://www.enisa.europa.eu

18. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). **Design science in information systems research**. *MIS Quarterly, 28*(1), 75–105. https://www.jstor.org/stable/25148625

19. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). **A design science research methodology for information systems research**. *Journal of Management Information Systems, 24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

20. Hsu, C.-C., & Sandford, B. A. (2007). **The Delphi technique: Making sense of consensus**. *Practical Assessment, Research & Evaluation, 12*(10), 1–8. https://pareonline.net/getvn.asp?v=12&n=10

21. Kendall, M. G., & Babington Smith, B. (1939). **The problem of m rankings**. *The Annals of Mathematical Statistics, 10*(3), 275–287. https://doi.org/10.1214/aoms/1177732186

## Anexos

**Anexo 1. Matriz de trazabilidad LOPDP → Control → Evidencia → KPI (ejemplos)**
A continuación se muestra una porción de la matriz de trazabilidad que vincula las obligaciones de la LOPDP con controles propuestos, evidencias correspondientes y KPIs asociados cuando aplica. Esta matriz sirve para asegurar que por cada requerimiento normativo relevante, el modelo propone un mecanismo de cumplimiento verificable y medible.

| **Obligación LOPDP / Reglamento** | **Control propuesto** | **Evidencia requerida** | **KPI relacionado** |
|---|---|---|---|
| Art. 13 LOPDP – Atender derechos de titulares (ARCO) en plazos legales | Procedimiento institucional para gestión de solicitudes ARCO; Responsables designados para responder | – Registro de solicitudes ARCO (entradas y salidas)<br>– Respuestas emitidas al titular con fecha | ARCO a tiempo (%) |
| Art. 16 LOPDP – Notificar violaciones de seguridad de datos personales a la autoridad en 72 horas (cuando aplique) | Proceso de gestión de incidentes de seguridad con criterios de notificación; Formulario oficial preparado | – Libro o registro de incidentes internos<br>– Notificaciones enviadas a SPDP (acuses de recibo) | Notificación en plazo (%) |
| Art. 33 LOPDP – Realizar Evaluación de Impacto a la Protección de Datos previa a tratamientos de alto riesgo | Metodología DPIA institucional adoptada; Comité de evaluación de impacto o responsable asignado | – Informes de DPIA/EIP aprobados<br>– Registro de tratamientos que requieren DPIA | Cobertura DPIA (%) |

| | | | |
|---|---|---|---|
| Art. 40 LOPDP – Designar un Delegado de Protección de Datos (DPO) si corresponde (criterios de volumen de datos) | Nombramiento formal de DPO con rol y responsabilidades definidas; Canal de comunicación con DPO | – Documento/carta de designación de DPO<br>– Organigrama o RACI con DPO asignado | *(N/A como KPI, control cualitativo)* |
| Art. 31 LOPDP – Implementar medidas de seguridad técnicas y organizativas apropiadas (integridad, confidencialidad) | Catálogo de controles de seguridad adoptado (acceso lógico, cifrado, backups, etc.) según ISO 27001/NIST; Revisión periódica | – Políticas de seguridad de la información<br>– Registros de control de accesos, logs, reportes de backup | *(Contribuye a subíndice Técnico, no KPI directo)* |
| Art. 30 LOPDP – Mantener un Registro de Actividades de Tratamiento actualizado | Inventario de bases de datos y tratamientos personales; Responsable de mantenimiento asignado | – Documento "Registro de Actividades" vigente (con fecha de última actualización)<br>– Bitácora de revisiones/actualizaciones | *(Contribuye a subíndice Normativo)* |
| – Buenas prácticas (no explícito en LOPDP): Programa de capacitación en protección de datos para personal | Plan anual de capacitación en privacidad para empleados y docentes; Sesiones obligatorias nuevas incorporaciones | – Lista de asistencia a capacitaciones<br>– Materiales de capacitación utilizados<br>– Evaluaciones de conocimiento (si aplica) | Capacitación efectiva (%) |

*Nota:* La tabla presenta solo algunos ejemplos representativos (no exhaustivos). Por cada control se identifica la evidencia documental cuya existencia y adecuación demostraría el cumplimiento. Los KPIs cuantitativos se asignan cuando la obligación/control se presta a medición periódica (p. ej., % de cumplimiento de plazos); otros controles se evalúan de forma binaria en el índice (cumple/no cumple con evidencia). Esta matriz de trazabilidad asegura la **auditabilidad** del modelo: cada elemento del índice o KPI puede vincularse a un requerimiento legal específico y a documentación verificable.

**Anexo 2. Cuestionario Delphi (instrumento de validación de contenido)**
Se detalla la estructura general del cuestionario utilizado en el estudio Delphi para validar el modelo. El cuestionario se dividió en secciones correspondientes a los componentes del modelo:

- **Sección A: Indicadores del Índice LOPDP (Dominio Normativo)** – Ítems ejemplo:
  A1. *"El indicador 'Existencia de políticas institucionales de protección de datos actualizadas y aprobadas' es pertinente para medir el cumplimiento normativo de la LOPDP en una IES."* (Likert 1–5, de Muy en desacuerdo a Muy de acuerdo)
  A2. *"El indicador 'Registro de actividades de tratamiento documentado y vigente' es claro y comprensible."* (Likert 1–5)
  A3. *"El indicador 'Realización de evaluaciones de impacto en tratamientos de alto*

*riesgo (DPIA)' es aplicable en la práctica de una IES."* (Likert 1–5)
*(... así con cada indicador normativo identificado ...)*

- **Sección B: Indicadores del Índice LOPDP (Dominio Organizativo)** – Ítems ejemplo:
  B1. *"La existencia de un Delegado de Protección de Datos designado formalmente es un factor relevante para el cumplimiento organizativo."* (pertinencia)
  B2. *"El indicador 'Procedimientos para atención de derechos ARCO con registro de solicitudes' está claramente definido."* (claridad)
  B3. *"El indicador 'Programa de capacitación anual en LOPDP para el personal' sería factible de implementar y medir en una IES."* (aplicabilidad)
  *(... demás indicadores organizativos ...)*

- **Sección C: Indicadores del Índice LOPDP (Dominio Técnico)** – Ítems ejemplo:
  C1. *"El indicador 'Controles de acceso lógicos implementados (gestión de cuentas y privilegios)' es esencial para evaluar el cumplimiento técnico de LOPDP."* (pertinencia)
  C2. *"El indicador 'Existencia de mecanismos de cifrado para datos personales sensibles' está formulado de manera clara."* (claridad)
  C3. *"El indicador 'Implementación de un plan de respuesta a incidentes de datos personales con registros de pruebas' es viable de medir en la institución.'"* (aplicabilidad)
  *(... demás indicadores técnicos ...)*

- **Sección D: KPIs propuestos** – Ítems ejemplo:
  D1. *"El KPI 'ARCO a tiempo (%)' (porcentaje de solicitudes ARCO atendidas en plazo) refleja adecuadamente el desempeño en el cumplimiento de derechos de titulares."* (pertinencia)
  D2. *"La fórmula del KPI 'Notificación en plazo (%)' está claramente definida y sería fácil obtener los datos necesarios."* (claridad/aplicabilidad)
  D3. *"El umbral propuesto para 'Cobertura DPIA (%)' (por ejemplo 80%) es adecuado como meta para las IES."* (pertinencia/aplicabilidad)
  D4. *"El KPI 'Capacitación efectiva (%)' es relevante para evaluar la concienciación y competencia en protección de datos del personal."* (pertinencia)
  *(...)*

- **Sección E: Preguntas globales y comentarios** – por ejemplo:
  E1. *"Considerando el modelo en su conjunto, ¿cree que cubre los aspectos esenciales para implementar efectivamente la LOPDP en una IES?"* (Sí/No, con espacio de comentario)
  E2. *"¿Qué mejoras sugeriría usted para algún indicador o KPI propuesto?"* (respuesta abierta)
  E3. *"Otros comentarios generales sobre el modelo:"* (abierto)

Cada ítem se calificó en escala Likert de 1 (muy en desacuerdo/muy poco claro/no aplicable) a 5 (muy de acuerdo/muy claro/muy aplicable). Adicionalmente, al final de cada sección se permitió a los expertos añadir comentarios cualitativos. El instrumento fue administrado en línea (plataforma de encuestas anónimas) y en la segunda ronda se incluyó para cada ítem un

resumen de la mediana, IQR y comentarios de la ronda anterior para que el experto pudiera reconsiderar su respuesta. Este cuestionario completo (aproximadamente 40 ítems Likert más preguntas abiertas) fue fundamental para recoger la sabiduría colectiva de los expertos y refinar el modelo.

**Anexo 3. Ejemplo numérico detallado del cálculo del Índice LOPDP**

Se muestra un ejemplo hipotético más detallado para ilustrar cómo se calcula el Índice LOPDP a partir de los diversos indicadores evaluados en una institución. Supongamos una IES "X" y consideremos algunos indicadores seleccionados de cada dominio:

- *Dominio Normativo:*
- **Políticas de privacidad aprobadas y actualizadas** – *Sí* (cumple 100%).
- **Registro de actividades de tratamiento** – *Existente pero desactualizado* (cumple 50% aprox.).
- **Evaluaciones de Impacto (DPIA) en tratamientos requeridos** – *Realizadas 2 de 4 necesarias* (cumple 50%).
- **Base legal documentada para cada tratamiento** – *Parcial* (ej. 80% de tratamientos tienen documentación) (cumple 80%).
  *Puntaje promedio Normativo:* (100 + 50 + 50 + 80) / 4 = **70** → N = 70.

- *Dominio Organizativo:*

- **Delegado de Protección de Datos designado** – *No* (0%).
- **Roles y responsabilidades (RACI) definidos en privacidad** – *Parcial* (50%).
- **Procedimiento ARCO implementado con registro** – *Sí, implementado* (100%).
- **Programa de capacitación anual en LOPDP** – *En desarrollo (por primera vez)* (50%).
  *Puntaje promedio Organizativo:* (0 + 50 + 100 + 50) / 4 = **50** → O = 50.

- *Dominio Técnico:*

- **Control de accesos lógico (gestión de usuarios)** – *Sí, políticas de cuentas activas/inactivas* (100%).
- **Cifrado de datos personales sensibles** – *Parcial* (por ejemplo, cifrado en bases de datos sí, pero no en respaldos) (70%).
- **Registros de eventos de seguridad (logs) monitoreados** – *En proceso* (50%).
- **Planes de continuidad/recuperación ante desastres** – *Sí, documentados y probados* (100%).
- **Gestión de incidentes de seguridad** – *Sí, con dos incidentes manejados* (100% - aunque no se notificó ninguno por no ser graves).
  *Puntaje promedio Técnico:* (100 + 70 + 50 + 100 + 100) / 5 = **84** → T = 84.

Ahora, aplicando la fórmula del índice con estos subíndices:
Índice LOPDP = 0,4 * N + 0,3 * O + 0,3 * T = 0,4*(70) + 0,3*(50) + 0,3*(84) = 28 + 15 + 25,2 = 68,2 ≈ 68*.

El valor 68 ubicaría a la IES "X" en el **nivel Básico** de cumplimiento. Observamos que la falta de un DPO designado (0%) afectó fuertemente el subíndice organizativo y bajó el promedio global; incluso con buenos controles técnicos (T=84), el peso organizativo penalizó el resultado, lo cual es consistente con la filosofía del modelo de que los aspectos organizativos (gobernanza, roles, cultura) son críticos para la efectividad a largo plazo. Este ejemplo muestra cómo el índice integra múltiple información en un único valor y cómo un cambio en una dimensión (por ejemplo, si la IES designa un DPO y sube O de 50 a, digamos, 75) puede influir en el índice global positivamente (en ese caso hipotético, el índice subiría a ~75, entrando a nivel "Adecuado").

**Anexo 4. Resultados detallados del método Delphi (ejemplo de tabla)**
Debido al espacio, se presenta un fragmento de la tabla de resultados Delphi ilustrativa para algunos ítems seleccionados:

| **Ítem (Indicador/KPI)** | **Mediana (Ronda 1)** | **IQR (Ronda 1)** | **Mediana (Ronda 2)** | **IQR (Ronda 2)** | **Consenso logrado** |
|---|---|---|---|---|---|
| Indicador: Políticas de privacidad institucional (N) | 5 | 1 | 5 | 0 | Sí (Med=5, IQR=0) |
| Indicador: Registro de actividades de tratamiento (N) | 4 | 1.5 | 5 | 1 | Sí (Mejora tras ajustes) |
| Indicador: DPO designado formalmente (O) | 4 | 1 | 4 | 0 | Sí |
| Indicador: Procedimiento ARCO con trazabilidad (O) | 5 | 0 | 5 | 0 | Sí |
| Indicador: Cifrado de datos personales sensibles (T) | 4 | 2 | 4 | 1 | Sí (parcial, IQR justo) |
| Indicador: Plan de respuesta a incidentes (T) | 5 | 1 | 5 | 0 | Sí |
| KPI: ARCO a tiempo (%) | 5 | 0 | 5 | 0 | Sí |
| KPI: Notificación en plazo (%) | 5 | 1 | 5 | 0 | Sí |
| KPI: Cobertura DPIA (%) | 4 | 1 | 5 | 0 | Sí (consenso final) |
| KPI: Capacitación efectiva (%) | 3 | 2 | 4 | 1 | Parcial (incorporado con mejoras) |

*(Mediana e IQR en escala 1–5, consenso definido como Mediana≥4 e IQR≤1).* Como se observa, para la mayoría de ítems se alcanzó consenso tras la ronda 2. El KPI de capacitación, por ejemplo, partió con mediana 3 e IQR 2 (opiniones divididas) en ronda 1, pero tras aclarar su definición y relevancia, mejoró a mediana 4, IQR 1 en ronda 2, logrando incorporarse al modelo. El coeficiente de Kendall W para este conjunto ilustrativo de ítems pasó de ~0,6 en ronda 1 a ~0,8 en ronda 2, confirmando el aumento de acuerdo global.

**Anexo 5. Matriz de criterios de transferibilidad del modelo**
Esta matriz (no mostrada completa por brevedad) aborda cómo adaptar el modelo según el tamaño y contexto de una IES:

- **Criterio:** Tamaño de la IES (número de estudiantes/personal).
  **Adaptación:** IES pequeñas: si <2000 estudiantes, puede no requerir DPO exclusivo – evidencia aceptable: encargar función a otro directivo (vicerrector, etc.) documentado. IES grandes: fortalecer evidencia de estructura (comité de privacidad, unidades descentralizadas).

- **Criterio:** Grado de tercerización de TI.
  **Adaptación:** Si muchos sistemas están en la nube o externalizados, se debe incluir en evidencia los contratos y evaluaciones de los encargados (Data Processing Agreements, cláusulas de privacidad con proveedores). Indicador técnico "controles implementados" debe considerar controles del proveedor también (ej. certificados ISO 27001 del proveedor pueden tomarse como evidencia complementaria).

- **Criterio:** Madurez previa en SGSI (Sistemas de Gestión de Seguridad de la Información).
  **Adaptación:** Si la IES ya cuenta con certificación ISO 27001 u otros, mapear controles existentes al modelo para evitar redundancia. Posiblemente algunos indicadores técnicos ya se cubren (cifrado, backups) – simplemente se evidencian con auditorías ISO.

- **Criterio:** Naturaleza de datos manejados (sensibilidad).
  **Adaptación:** IES con hospitales universitarios o laboratorios de investigación con datos genéticos, por ejemplo, deben poner mayor énfasis en DPIA y controles adicionales (se puede ponderar internamente más esos indicadores o añadir sub-indicadores específicos en la implementación). IES puramente administrativas (sin datos de salud) quizás simplifican esa parte pero igualmente deben demostrar evaluación de riesgos.

- **Criterio:** Recursos disponibles (personal y presupuesto).
  **Adaptación:** El modelo es escalable: una IES con menos recursos puede iniciar con cumplimiento básico en todos los indicadores y planificar mejoras graduales; los umbrales pueden ajustarse realísticamente (por ejemplo, meta de capacitación 80% primer año, 100% en dos años). Lo importante es no omitir dimensiones: aunque sea con poco recurso, debe haber algo de evidencia en normativa, organización y técnica.

Esta matriz de transferibilidad sugiere que el modelo, más que un rígido checklist, debe verse como un **framework adaptable**. Las IES pueden ajustar la implementación pero manteniendo los principios: por ejemplo, si no pueden tener un DPO dedicado, igual deben asignar formalmente la responsabilidad; si no pueden hacer DPIA exhaustivas a todas las áreas, al menos priorizar las más críticas, etc. De esta manera, el modelo puede aplicarse desde universidades pequeñas emergentes hasta universidades grandes con investigación intensiva, sirviendo como lenguaje común de cumplimiento pero permitiendo flexibilidad proporcional al contexto.

**Conflicto de intereses:**
Los autores declaran que no existe conflicto de interés posible.
**Financiamiento:**
No existió asistencia financiera de partes externas al presente artículo.
**Agradecimiento:**
N/A
**Nota:**
El artículo no es producto de una publicación anterior.