Brechas y pérdidas de datos en las Organizaciones: Dimensiones críticas e implicaciones para la gestión del riesgo[1]

Data breaches and losses in organizations: Critical dimensions and implications for risk management

Fernando Enrique Hernández Casco
Auditor Regional TI
ORCID: https://orcid.org/0009-0007-7046-327X

Fecha de recepción: 09.01.2026
Fecha de aceptación: 22.06.2026
Fecha de publicación en línea: octubre 2026

Resumen:

Las brechas y pérdidas de datos se han consolidado como uno de los riesgos más relevantes para las organizaciones, sin importar su tamaño, complejidad o sector, con efectos que trascienden el impacto técnico inmediato. Estudios recientes, como el Cost of a Data Breach Report 2024 de IBM, muestran que estos incidentes combinan costes directos de respuesta con pérdidas de negocio y efectos de largo plazo sobre la competitividad. Asimismo, estudios académicos y documentos de autoridades de protección de datos, incluyendo guías de la Agencia Española de Protección de Datos y del Supervisor Europeo de Protección de Datos, señalan que los impactos reputacionales, legales, operativos y sociales (en particular sobre los derechos y libertades de las personas) deben integrarse en la evaluación del riesgo. Por lo anterior, el documento desarrolla un marco conceptual que distingue seis dimensiones de impacto: económica, reputacional, operativa, legal/regulatoria, social/privacidad, e inteligencia artificial/automatización; proponiendo un modelo de costo esperado de consecuencias que combina impacto, probabilidad, eficacia de controles y apetito de riesgo organizacional. El estudio emplea investigación documental con datos secundarios, articulando análisis cualitativo de contenido e ilustración cuantitativa del modelo en tres escenarios, con el fin de apoyar decisiones de gestión, inversión y gobernanza de datos.

Abstract:

Data breaches and data loss have become one of the most significant risks for organizations, regardless of their size, complexity, or sector, with effects that extend far beyond the immediate technical impact. Recent studies, such as IBM's Cost of a Data Breach Report 2024, show that these incidents combine direct response costs with business losses and long-term effects on competitiveness. Likewise, academic studies and documents from data protection authorities, including guidelines from the Spanish Data Protection Agency and the European Data Protection Supervisor, indicate that reputational, legal, operational, and social impacts (particularly on the rights and freedoms of individuals) must be integrated into risk assessment. Therefore, this document develops a conceptual framework that distinguishes six dimensions of impact: economic, reputational, operational, legal/regulatory, social/privacy, and artificial intelligence/automation; proposing an expected cost-of-consequences model that combines impact, probability, effectiveness of controls, and organizational risk appetite. The study employs documentary research with secondary data, articulating qualitative content analysis and quantitative illustration of the model in three scenarios, in order to support data management, investment and governance decisions.

[1] Declaración de uso de la IA. En este manuscrito se ha utilizado de forma limitada el apoyo de herramientas de inteligencia artificial generativa (ChatGPT, Copilot, Gemini y Perplexity), exclusivamente para tareas de orientación, ordenamiento de ideas y mejora de la redacción formal. Las ideas, la formulación del problema, el análisis de los documentos de referencia, así como el desarrollo del marco conceptual, la propuesta del modelo de costo esperado de consecuencias y los escenarios cualitativos y cuantitativos han sido concebidos, definidos y validados por el autor, quien asume la responsabilidad plena sobre el contenido, su rigor metodológico y su originalidad.

Palabras clave:
Brechas de datos, pérdida de datos, gestión del riesgo, privacidad y protección de datos; e inteligencia artificial.

Sumario:
1. Introducción. **2.** Metodología. **2.1.** Hipótesis y objetivo general. **2.2.** Diseño metodológico y enfoque documental. **2.3.** Criterios de selección de fuentes. **2.4.** Integración del análisis cualitativo y cuantitativo. **3.** Marco conceptual. **3.1.** Brechas y pérdidas de datos en las organizaciones. **3.2.** Dimensiones de impacto. **3.3.** Modelo de costo esperado de consecuencias (MCEC). **3.3.1.** Componentes del modelo. **3.3.2.** Escenarios cualitativos y cuantitativos del MCEC. **4.** Resultados y discusión. **5.** Conclusiones y recomendaciones. Bibliografía.

Keywords:
Data breaches, data loss, risk management, privacy and data protection; and artificial intelligence.

Summary:
1. *Introduction.* ***2.*** *Methodology.* ***2.1.*** *Hypothesis and general objective.* ***2.2.*** *Methodological design and documentary approach.* ***2.3.*** *Criteria for source selection.* ***2.4.*** *Integration of qualitative and quantitative analysis.* ***3.*** *Conceptual framework.* ***3.1.*** *Data breaches and data loss in organizations.* ***3.2.*** *Impact dimensions.* ***3.3.*** *Expected cost of consequences model (ECCM).* ***3.3.1.*** *Model components.* ***3.3.2.*** *Qualitative and quantitative scenarios of the ECCM.* ***4.*** *Results and discussion.* ***5.*** *Conclusions and recommendations. Bibliography.*

1. Introducción

Las brechas y pérdidas de datos ocupan hoy una posición central en la agenda de gestión del riesgo de las organizaciones, no solo por sus efectos económicos inmediatos, sino también por sus implicaciones sobre la continuidad operativa, la confianza de los grupos de interés y el cumplimiento de obligaciones en materia de protección de datos. Este problema adquiere especial relevancia en organizaciones públicas y privadas que dependen de procesos digitalizados, tratan datos personales o estratégicos y cuentan con niveles intermedios de madurez en gestión del riesgo, donde la necesidad de priorizar decisiones con recursos limitados es particularmente visible.

Pese a la amplitud de literatura e informes técnicos disponibles, buena parte de los enfoques existentes examina estos incidentes de manera parcial o aislada, ya sea mediante métricas agregadas de coste, análisis centrados en sectores concretos o aproximaciones regulatorias enfocadas principalmente con el cumplimiento.

En ese contexto, persiste una necesidad metodológica y práctica, la cual se enfoca en una propuesta que permita articular en un mismo esquema de análisis los distintos efectos asociados a brechas y pérdidas de datos, sin depender de modelos altamente sofisticados ni de bases históricas extensas que muchas organizaciones no poseen. Esta carencia es particularmente importante cuando se busca apoyar decisiones de inversión en controles, definir prioridades de tratamiento del riesgo y fortalecer la gobernanza del dato bajo contextos de creciente presión regulatoria y tecnológica.

Por lo anterior, lo descrito en este documento pretende mostrar las principales dimensiones implicadas en las brechas y pérdidas de datos y propone un modelo de costo esperado de consecuencias como instrumento de apoyo para la valoración del riesgo en contextos organizativos concretos.

Por tanto, el contenido de este estudio se orienta principalmente a organizaciones públicas y privadas con dependencia significativa de datos, exposición a riesgos de seguridad y privacidad, y niveles intermedios de madurez en gestión del riesgo, especialmente cuando no disponen de modelos cuantitativos avanzados ni de bases históricas suficientes para estimaciones complejas. En ese sentido, la propuesta no pretende sustituir metodologías de impacto específicas, sino ofrecer una estructura analítica flexible para apoyar procesos de priorización, valoración y toma de decisiones.

2. Metodología

El estudio se ha desarrollado como una investigación de tipo documental, basada en el análisis de datos secundarios procedentes de informes técnicos, artículos académicos, así como guías de autoridades y organismos especializados en protección de datos, seguridad de la información e inteligencia artificial.

Bajo el contexto antes expuesto, permite aprovechar la evidencia existente sobre costes, impactos y marcos de gestión de brechas y pérdidas de datos, así como de prácticas de gobernanza de datos y evaluación de riesgos en tratamientos que incorporan tecnologías emergentes. Entre las fuentes

destacan el informe anual de costos de brechas de datos[2], estudios académicos sobre impactos económicos y organizacionales de las brechas de datos, investigaciones sobre confianza y privacidad; así como guías desarrolladas por la Agencia Española de Protección de Datos (AEPD)[3], del Supervisor Europeo de Protección de Datos (EDPS)[4] y de otros organismos especializados en gobernanza de datos e inteligencia artificial.

A su vez, la selección de fuentes siguió tres (3) criterios principales: i) relevancia temática, ii) actualidad y iii) diversidad de enfoques. En primer lugar, se priorizaron documentos que abordaran de forma directa las brechas y pérdidas de datos, sus impactos económicos, reputacionales, operativos, legales y sociales, y su relación con la gestión del riesgo y la protección de datos personales. En segundo lugar, se buscó incluir materiales recientes, con especial atención a informes y guías publicados en los últimos años, que recogieran la evolución de los incidentes y de los marcos regulatorios. En tercer lugar, se incorporaron tanto estudios académicos como informes técnicos y documentos de autoridades, con el fin de integrar evidencias, marcos conceptuales y orientaciones de política pública.

Asimismo, se tomó como referencia la edición más reciente del costo de extracción de datos de IBM, que aportan estadísticas globales sobre coste medio por brecha, distribución de costes por categorías (pérdida de negocio, respuesta técnica, notificación, sanciones) y diferencias por sector, tamaño de la organización y nivel de madurez de la seguridad, incluida la adopción de soluciones basadas en inteligencia artificial. A su vez, de estudios académicos, se consideraron los costes económicos y organizacionales de las brechas de datos[5]; así como investigaciones sobre el impacto de estos incidentes en la confianza[6], la conducta de auto-revelación de información y las preocupaciones por la privacidad[7].

En cuanto a referencias de documentos de autoridades y organismos especializados, se revisaron las guías de la AEPD sobre gestión de riesgos[8] y evaluación de impacto, orientaciones sobre tratamientos que incorporan inteligencia artificial[9], así como documentos relativos a espacios de datos y gobernanza del dato, junto con informes del EDPS sobre gestión del riesgo en sistemas de inteligencia artificial (IA)[10] y documentos europeos sobre implementación del Reglamento General de Protección de Datos (RGPD)[11]. Estas fuentes permiten conectar las dimensiones de impacto con obligaciones normativas, buenas prácticas de gobierno del dato y recomendaciones específicas sobre la evaluación y mitigación de riesgos.

2.1. Hipótesis y objetivo general

El presente documento parte de la hipótesis de que las brechas y pérdidas de datos producen consecuencias de carácter multidimensional que no pueden ser valoradas cuando el análisis se limita a métricas agregadas de coste o a aproximaciones centradas exclusivamente en el incumplimiento normativo. Sobre esa base, se sostiene que un modelo integrador, construido a partir de evidencia documental y articulado mediante variables de impacto, probabilidad, eficacia de controles y priorización organizacional, puede ofrecer una herramienta útil para aproximar el costo esperado de tales eventos en contextos donde no se dispone de modelos avanzados ni de series históricas robustas.

El objetivo general consiste en desarrollar un marco analítico que permita identificar, organizar y valorar las principales consecuencias asociadas a las brechas y pérdidas de datos en las organizaciones, así como proponer un modelo conceptual de costo esperado que contribuya a la gestión del riesgo y a la toma de decisiones. De este objetivo general se desprenden cuatro (4) objeti-

[2] IBM, Cost of a Data Breach Report 2024

[3] AEPD, Gestión de riesgo y evaluación de impacto en tratamientos de datos personales (2021)

[4] EDPS, Guidance for Risk Management of Artificial Intelligence systems

[5] Economic Costs and Impacts of Business Data Breaches", Issues in Information Systems, 2019, https://www.iacis.org/iis/2019/2_iis_2019_162-171.pdf

[6] The Effects of Privacy and Data Breaches on Consumers' Online Self-Disclosure, Protection Behavior, and Message Valence", SAGE Open, 2023, https://journals.sagepub.com/doi/10.1177/21582440231181395

[7] meta-análisis "Privacy concern and its consequences: A meta-analysis", https://www.sciencedirect.com/science/article/abs/pii/S0040162523004742 (2023)

[8] AEPD, Gestión de riesgo y evaluación de impacto en tratamientos de datos personales (2021)

[9] AEPD, Adecuación al RGPD de tratamientos que incorporan IA (2020)

[10] EDPS, Risk Management of AI Systems under the GDPR (2025)

[11] AESIA, Guía de datos y gobernanza de datos (2025)

vos específicos: i) identificar las dimensiones de impacto más relevantes descritas en la literatura especializada y en documentos técnicos de referencia; ii) examinar de manera crítica la forma en que dichas dimensiones han sido abordadas por estudios académicos, informes sectoriales y autoridades especializadas; iii) estructurar un modelo que articule impacto, probabilidad, controles y ponderación relativa de los riesgos; e iv) ilustrar el funcionamiento de esa propuesta mediante escenarios construidos con datos secundarios y supuestos consistentes con la evidencia revisada.

La propuesta busca servir como instrumento de apoyo para organizaciones que requieren aproximaciones razonadas al riesgo asociado a brechas y pérdidas de datos, especialmente en contextos de madurez intermedia en gestión del riesgo y gobernanza del dato. En consecuencia, este estudio se sitúa en un plano conceptual y aplicado, orientado a la construcción de una herramienta de apoyo a la decisión más que a la validación empírica de relaciones causales en una muestra de organizaciones.

2.2. Diseño metodológico y enfoque documental

El estudio busca integrar componentes cualitativos y cuantitativos, adecuado para examinar un problema cuya discusión se encuentra dispersa entre trabajos académicos, informes de industria, guías regulatorias y documentos de organismos especializados. Este tipo de diseño permite seleccionar, organizar, contrastar e interpretar información ya disponible para construir una propuesta conceptual fundada en evidencia previa, lo que resulta especialmente pertinente cuando el objetivo no es medir empíricamente un universo de casos, sino elaborar un marco analítico susceptible de ser utilizado y posteriormente validado en distintos entornos organizativos.

La elección del enfoque documental se justifica en dos aristas, i) por la naturaleza del objeto de estudio, donde las brechas y pérdidas de datos han sido abordadas desde perspectivas económicas, jurídicas, operativas, reputacionales y de privacidad, pero esas aproximaciones suelen encontrarse fragmentadas o segregadas entre fuentes de distinta procedencia, por lo que se identifica la necesidad de un diseño que permita integrar esas contribuciones en una misma estructura de análisis; y ii) el enfoque documental resulta coherente con el propósito del artículo, que no consiste en verificar un fenómeno mediante trabajo de campo, sino en construir una propuesta metodológica sustentada en conocimiento acumulado y en orientaciones técnicas ya consolidadas.

Por tanto y apoyado desde la perspectiva antes descrita, el componente cualitativo se orientó a la identificación y organización de categorías de análisis relacionadas con los tipos de consecuencias derivadas de brechas y pérdidas de datos, mientras que el componente cuantitativo se destinó a traducir esas categorías en una estructura de estimación aplicable a escenarios ilustrativos. La combinación de ambos planos responde a la necesidad de vincular la interpretación conceptual del riesgo con una formulación que pueda resultar operativa para la toma de decisiones informada, manteniendo el carácter exploratorio del estudio y sin pretender sustituir modelos complejos existentes.

2.3. Criterios de selección de fuentes

La selección de fuentes se realizó mediante criterios explícitos de relevancia, actualidad, autoridad, diversidad y utilidad analítica. Se priorizaron documentos directamente vinculados con brechas de datos, pérdida de información, gestión del riesgo, protección de datos personales, continuidad operativa, gobernanza del dato e impactos asociados al uso de inteligencia artificial en entornos organizativos. También, se favorecieron publicaciones recientes, especialmente aquellas emitidas en los últimos años, sin excluir trabajos anteriores cuya incorporación se consideró necesaria por su valor conceptual o por su influencia en la discusión especializada.

Asimismo, se valoró la autoridad y confiabilidad de las fuentes, dando preferencia a artículos académicos, informes técnicos ampliamente reconocidos y guías emitidas por autoridades u organismos especializados en protección de datos, seguridad de la información, gobernanza y evaluación del riesgo. De forma complementaria, se procuró mantener diversidad en la procedencia de los materiales con el fin de evitar una visión unidimensional del problema, integrando estudios académicos, informes sectoriales, documentos institucionales y orientaciones regulatorias. Este criterio de diversidad no tuvo una finalidad acumulativa, sino comparativa, ya que permitió contrastar enfoques, identificar coincidencias y reconocer vacíos o sesgos en la literatura revisada.

La revisión no se orientó a la construcción de un inventario exhaustivo de toda la producción existente, sino a la conformación de un conjunto suficiente y pertinente para fundamentar la propuesta del estudio. Es por ello que, la inclusión final de cada fuente dependió no solo de su cercanía temática, sino también de su capacidad para aportar elementos útiles a la definición de dimensio-

nes de análisis, a la justificación del modelo y a la formulación de escenarios ilustrativos.

2.4. Integración del análisis cualitativo y cuantitativo

En cuanto a la integración metodológica, se desarrolló en dos (2) niveles complementarios, donde: i) el análisis cualitativo permitió examinar el contenido de las fuentes seleccionadas para identificar patrones recurrentes, categorías de impacto, relaciones entre variables y criterios de valoración del riesgo presentes en la literatura y en los documentos técnicos revisados. Este proceso no se limitó a describir lo que cada documento señalaba de manera aislada, sino que buscó establecer conexiones entre enfoques económicos, regulatorios, organizativos y de privacidad, con el propósito de construir una base conceptual más articulada; y ii) el componente cuantitativo se orientó a la formulación de un modelo de costo esperado de consecuencias construido exclusivamente a partir de datos secundarios y de supuestos ilustrativos consistentes con la evidencia disponible.

La articulación de ambos niveles permitió que las categorías derivadas del análisis cualitativo sirvieran como fundamento del modelo cuantitativo, mientras que la formulación cuantitativa ofreció una vía para ordenar y hacer comparables las distintas consecuencias identificadas en la revisión documental.

3. Marco conceptual

El análisis de las brechas y pérdidas de datos requiere articular distintos planos de observación: la caracterización de los incidentes, la identificación de las consecuencias que producen en el entorno organizativo y social, y la forma en que esos efectos se integran en marcos de valoración del riesgo y de toma de decisiones. Este apartado presenta, en primer lugar, una síntesis de las principales aportaciones conceptuales sobre brechas y pérdidas de datos, en segundo término, las dimensiones de impacto identificadas en la literatura y en documentos técnicos, y, finalmente, el modelo de costo esperado de consecuencias propuesto en este trabajo.

3.1. Brechas y pérdidas de datos en las organizaciones

En el ámbito de la seguridad de la información y de la protección de datos personales, resulta útil distinguir entre brecha de datos y pérdida de datos, aunque en la práctica ambos fenómenos pueden presentarse de manera simultánea dentro de un mismo incidente[12]. Las guías especializadas suelen asociar la brecha de datos con el acceso, uso o divulgación no autorizados de información, mientras que la pérdida de datos remite a supuestos de indisponibilidad, borrado accidental, corrupción o destrucción de la información, incluso cuando no exista acceso ilegítimo por parte de terceros[13].

Desde la perspectiva organizacional, cada tipo de evento activa efectos distintos sobre la operación, la seguridad, la continuidad del negocio y el cumplimiento normativo. Los informes recientes sobre incidentes de seguridad muestran, además, que las organizaciones se enfrentan a escenarios cada vez más complejos, en los que convergen extracción no autorizada de información, errores de configuración, ataques de ransomware, fallos asociados a terceros y problemas en la cadena de suministro digital[14]. En estos contextos, la duración del ciclo de detección y contención adquiere especial relevancia, ya que un mayor tiempo de exposición tiende a ampliar las consecuencias económicas, operativas y reputacionales del incidente.

Desde el plano jurídico, tanto las brechas como determinadas formas de pérdida de datos pueden dar lugar a obligaciones de análisis, documentación y, en su caso, notificación a las autoridades competentes y a las personas afectadas, particularmente cuando la incidente entraña riesgos para los derechos y libertades de los interesados. Por ello, una aproximación adecuada al problema no puede limitarse a la ocurrencia del evento técnico, sino que debe considerar también sus efectos proyectados sobre la organización, sobre las personas afectadas y sobre el marco de responsabilidad aplicable.

[12] Véase la distinción conceptual desarrollada por la Agencia Española de Protección de Datos en su guía sobre gestión del riesgo y evaluación de impacto en tratamientos de datos personales. https://www.aepd.es/guias/gestion-riesgo-evaluacion-impacto-tratamientos

[13] Agencia Española de Protección de Datos, Gestión del riesgo y evaluación de impacto en tratamientos de datos personales (Madrid: AEPD, 2021), 20–24, 33 y 43–47; Agencia Española de Protección de Datos, Adecuación al RGPD de tratamientos que incorporan inteligencia artificial. (Madrid: AEPD, 2020), 9 y 49

[14] IBM Security, Cost of a Data Breach Report 2024 (Armonk, NY: IBM Corporation, 2024), 5–6, 10, 15–33.

3.2. Dimensiones de impacto

La revisión de literatura, los informes sectoriales y las guías de autoridades coinciden en que las brechas y pérdidas de datos producen consecuencias que no se agotan en una sola dimensión de análisis. Su impacto se despliega de forma simultánea en el plano económico, en la reputación institucional, en la continuidad operativa, en la exposición jurídica y regulatoria, en la esfera social y de privacidad, así como en los riesgos asociados al uso de inteligencia artificial y automatización[15]. Esta constatación justifica la adopción de un enfoque multidimensional y capaz de representar con mayor fidelidad la complejidad de estos eventos.

Las dimensiones que se desarrollan a continuación no deben entenderse como compartimentos rígidos ni mutuamente excluyentes. Se trata, más bien, de categorías analíticas que permiten ordenar consecuencias que en la práctica aparecen entrelazadas. Una misma brecha puede ocasionar pérdidas económicas directas, interrupciones de servicio, sanciones regulatorias, deterioro reputacional y afectaciones relevantes para los derechos de las personas.

- 1. Dimensión económica. La dimensión económica comprende tanto los costos directos derivados de la respuesta al incidente como los costos indirectos que se manifiestan con posterioridad. En el primer grupo suelen incluirse la investigación técnica, la contención, la recuperación de sistemas, la notificación y la gestión inmediata del evento. En el segundo se ubican, entre otros, la pérdida de negocio, la disminución de ingresos, la caída de productividad, los gastos de remediación prolongada y los efectos sobre la posición competitiva de la organización. Esta dimensión continúa siendo central en la literatura sobre brechas de datos, pero su análisis resulta insuficiente cuando se examina de forma aislada.

- 2. Dimensión reputacional. La dimensión reputacional hace referencia a las consecuencias que un incidente puede generar sobre la confianza de clientes, usuarios, socios, reguladores y demás grupos de interés. En entornos de alta exposición digital, la forma en que la organización comunica y gestiona una brecha influye de manera directa en la percepción pública del evento y en la persistencia del daño reputacional. El impacto en esta dimensión suele manifestarse en pérdida de confianza, reducción de la disposición a compartir información, debilitamiento del vínculo con la organización y necesidad de invertir recursos adicionales en reconstrucción institucional.

- 3. Dimensión operativa. La dimensión operativa se refiere a la afectación de los procesos, servicios y capacidades funcionales de la organización. Una brecha o pérdida de datos puede obligar a detener sistemas, limitar funcionalidades, ejecutar planes de recuperación, reasignar recursos críticos y operar temporalmente bajo condiciones degradadas. En este sentido, el daño no se expresa solo en términos de gasto, sino también en interrupciones, retrasos, ineficiencias y pérdida de capacidad de respuesta. Esta dimensión adquiere especial importancia en organizaciones cuya continuidad depende de la disponibilidad e integridad de la información.

- 4. Dimensión legal y regulatoria. La dimensión legal y regulatoria abarca las consecuencias vinculadas al incumplimiento de obligaciones jurídicas y de protección de datos, incluidas posibles sanciones administrativas, costes de defensa, reclamaciones y exigencias de corrección o reforzamiento de controles. No obstante, esta dimensión cumple además una función transversal, puesto que el marco normativo también opera como un factor que puede intensificar o atenuar la exposición global al riesgo. La gravedad de sus efectos dependerá, entre otros aspectos, del tipo de datos comprometidos, del sector en el que actúe la organización, de la diligencia acreditada y de la existencia de medidas técnicas y organizativas.

- 5. Dimensión social y de privacidad. Sitúa el análisis en las personas afectadas por el incidente y en las consecuencias que pueden recaer sobre sus derechos, libertades e intereses legítimos. Las brechas y pérdidas de datos pueden facilitar fraudes, suplantación de identidad, discriminación, usos no deseados de la información o pérdida de confianza en instituciones públicas y privadas. Desde la perspectiva de la protección de datos, esta dimensión obliga a la evaluación del perjuicio potencial que el incidente puede causar a los titulares de los datos.

- 6. Dimensión de inteligencia artificial y automatización. La dimensión de inteligencia artificial y automatización responde a la creciente presencia de sistemas automatizados tanto en la operación organizacional como en las estrategias de seguridad. Por un lado, determinadas

[15] Shirley S. Ho, Nga N. Ho-Dac y Ray-Bing Huang, "The Effects of Privacy and Data Breaches on Consumers' Online Self-Disclosure, Protection Behavior, and Message Valence," *SAGE Open* 13, no. 3 (2023). Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, rev. 01 (2017), 12; European Data Protection Supervisor, Risk Management of AI Systems under the GDPR (Brussels: EDPS, 2025), 9–12.

soluciones de inteligencia artificial pueden contribuir a reducir tiempos de detección, fortalecer capacidades de respuesta y disminuir el costo de algunos incidentes. Por otro, la incorporación de estas tecnologías abre nuevos vectores de riesgo, como el uso no autorizado de herramientas de inteligencia artificial (IA), la exposición de datos en entornos no gobernados, los ataques dirigidos a modelos o aplicaciones y la ampliación de superficies de vulnerabilidad asociadas a prácticas de "*shadow AI*"[16]. En consecuencia, esta dimensión también presenta una naturaleza dual: constituye un ámbito específico de impacto cuando el incidente involucra sistemas de IA, a su vez, actúa como un factor que puede mitigar o amplificar el riesgo residual según el nivel de gobernanza y control existente.

En conjunto, las seis (6) dimensiones propuestas permiten estructurar un entendimiento más completo de las consecuencias asociadas a brechas y pérdidas de datos. Su utilidad no radica en separar y analiza en silos aquellos elementos que puedan generar un impacto de forma individual, sino en ofrecer un marco ordenado para identificar prioridades de análisis, orientar decisiones de gestión del riesgo y fundamentar la formulación del modelo de costo esperado de consecuencias.

3.3. Modelo de costo esperado de consecuencias (MCEC)

La literatura sobre brechas y pérdidas de datos ha aportado evidencia relevante sobre el costo económico de estos incidentes, así como sobre sus efectos operativos, reputacionales, regulatorios y sociales. Sin embargo, buena parte de estas aproximaciones permanece distribuida entre métricas agregadas de coste, estudios sectoriales y marcos generales de gestión del riesgo que, aunque útiles, no siempre ofrecen una estructura integrada y operativa para organizaciones que necesitan aproximaciones razonadas sin disponer de modelos avanzados ni de grandes bases históricas de incidentes[17].

En ese contexto, el Modelo de Costo Esperado de Consecuencias (MCEC) se plantea como una instrumento conceptual y aplicada orientada a integrar, en una misma formulación, la magnitud potencial del impacto, la probabilidad de ocurrencia, la eficacia de los controles y la prioridad relativa que la organización asigna a cada dimensión de riesgo. Su finalidad es proporcionar una estructura flexible que pueda ser adaptada por organizaciones públicas y privadas con dependencia significativa de datos, exposición relevante a incidentes de seguridad y niveles intermedios de madurez en gestión del riesgo.

A diferencia de enfoques centrados exclusivamente en el coste promedio de una brecha, el MCEC parte como premisa de que las consecuencias no se distribuyen de forma uniforme ni afectan del mismo modo a todas las organizaciones. Del mismo modo, frente a marcos generales de gestión del riesgo, como FAIR[18], ISO 31000:2018[19] o NIST CSF 2.0[20], la propuesta se concentra específicamente en las brechas y pérdidas de datos y procura articular en un solo esquema dimensiones económicas, reputacionales, operativas, legales, sociales y asociadas a inteligencia artificial; manteniendo un nivel de complejidad menor que el exigido por modelos de cuantificación más robustos.

3.3.1. Componentes del modelo

El MCEC se apoya en las seis (6) dimensiones de impacto definidas previamente: i) económica, ii) reputacional, iii) operativa, iv) legal y regulatoria, v) social y de privacidad, e vi) inteligencia artificial y automatización. Para cada dimensión i se consideran cuatro (4) elementos: i) impacto, ii) probabilidad, iii) control y iv) peso; donde:

- a. Impacto$_i$: coste estimado si un incidente asociado a esa dimensión se materializa, expresado en términos monetarios; incluye, según la naturaleza de cada dimensión, pérdidas directas, costes de respuesta, sanciones, gastos de recuperación o valor aproximado del daño reputacional.

[16] European Data Protection Supervisor, Risk Management of AI Systems under the GDPR (Brussels: EDPS, 2025), 9–12.

[17] Agencia Española de Protección de Datos (AEPD), Gestión del riesgo y evaluación de impacto en tratamientos de datos personales (Madrid: AEPD, 2021), 33 y 43–47; Agencia Española de Protección de Datos (AEPD), Adecuación al RGPD de tratamientos que incorporan inteligencia artificial. (Madrid: AEPD, 2020), 9 y 49.

[18] FAIR Institute, The Importance and Effectiveness of Cyber Risk Quantification, acceso consultado en abril de 2026, https://www.fairinstitute.org/what-is-fair.

[19] ISO 31000:2018: Estándar internacional que proporciona principios, un marco de referencia y un proceso integral para gestionar riesgos en organizaciones de cualquier tamaño o sector. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

[20] NIST CSF 2.0: Marco de ciberseguridad que proporciona buenas prácticas y estándares para gestionar y reducir los riesgos de ciberseguridad. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

- b. Probabilidad$_i$: probabilidad de que ocurra un incidente relevante en esa dimensión durante el periodo de referencia, aproximada a partir de tasas observadas en informes de brechas, estadísticas sectoriales, escenarios internos o evidencia secundaria disponible.

- c. Control$_i$: nivel de eficacia de los controles existentes, expresado entre 0 y 1, que refleja el grado de mitigación alcanzado mediante medidas técnicas, organizativas y de gobernanza, incluida la adopción de capacidades de seguridad basadas en inteligencia artificial y automatización cuando corresponda.

- d. Peso$_i$: ponderación asignada a la dimensión según el apetito y la tolerancia al riesgo de la organización, de modo que sectores con alta sensibilidad regulatoria, social o reputacional puedan reflejar esa mayor exposición en la estructura del modelo.

Tomando en cuenta los elementos antes descritos, el costo esperado de consecuencias se expresa mediante la siguiente formulación:

$$CEC = \sum Peso_i \times Impacto_i \times Probabilidad_i \times (1 - Control_i)$$

La expresión resume la idea de que el riesgo residual depende simultáneamente de la magnitud potencial del daño, de la probabilidad de ocurrencia, del grado de mitigación aportado por los controles y de la relevancia relativa que la organización asigna a cada dimensión. En coherencia con lo señalado en la sección 3.2, las dimensiones legal y regulatoria, e inteligencia artificial y automatización, pueden además desempeñar un papel modulador del riesgo total, sin que ello obligue en esta etapa a alterar la formulación básica del modelo.

3.3.2. Escenarios cualitativos y cuantitativos del MCEC

Con el propósito de ilustrar la operatividad del modelo, se presentan escenarios cualitativos y cuantitativos para dicho modelo, donde:

a. Escenarios cualitativos. Tomando como referencia los patrones identificados en el informe Cost of a Data Breach 2024[21] y en la publicación del ISACA Journal[22] citada en el manuscrito base, se plantean tres (3) escenarios cualitativos que conservan la misma estructura dimensional, pero modifican el nivel de controles y los pesos para mostrar cómo distintas decisiones de gestión del riesgo alteran el costo esperado residual. Dichos escenarios se resumen en la Tabla 1.

- Escenario A: Controles tradicionales. La organización cuenta con controles convencionales, sin despliegue intensivo de soluciones de inteligencia artificial y automatización en sus capacidades de seguridad. En términos analíticos, este escenario representa un punto de referencia o situación base, con niveles moderados de eficacia de controles en las dimensiones económica, operativa y legal, y niveles relativamente bajos en la dimensión de inteligencia artificial y automatización.

- Escenario B: Alta seguridad con IA. La organización ha invertido de forma consistente en capacidades de seguridad basadas en inteligencia artificial y automatización, incluyendo detección temprana, orquestación de respuesta y monitorización continua. Este perfil se asocia a reducciones del coste medio de las brechas y del tiempo necesario para su identificación y contención, por lo que el modelo representa esta situación mediante niveles altos de control en las dimensiones económica, operativa y de IA.

- Escenario C: Shadow AI y gobernanza débil. La organización utiliza herramientas de IA sin una correcta gobernanza, incluyendo supuestos de shadow AI, servicios externos no evaluados formalmente o despliegues sin controles suficientes sobre tratamiento de datos. Este tipo de prácticas incrementa la probabilidad de incidentes vinculados a IA y puede amplificar de manera simultánea los riesgos legales, regulatorios y de privacidad, incluso cuando los controles tradicionales se mantienen en niveles intermedios.

[21] IBM Security, Cost of a Data Breach Report 2024 (Armonk, NY: IBM Corporation, 2024), 5–6, 10, 15–33.

[22] Freund, Jack y Natalie Jorion. "The True Cost of a Data Breach." *ISACA Journal*, vol. 1, 2023. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-1/the-true-cost-of-a-data-breach.

Tabla 1. Escenarios cualitativos del MCEC

#	Dimensión	Parámetros	Escenario A: Controles tradicionales	Escenario B: Alta seguridad con IA	Escenario C: Shadow AI y gobernanza débil
1	Económica	Impacto económico típico de una brecha; probabilidad anual	Controles básicos; prioridad estándar	Automatización y detección temprana; prioridad estándar	Controles irregulares; prioridad estándar
2	Reputacional	Pérdida de clientes e imagen de marca	Comunicación reactiva; prioridad media	Gestión proactiva de incidentes; prioridad media	Gestión deficiente; prioridad alta
3	Operativa	Paradas de servicio y costes de recuperación	Planes parciales de continuidad; prioridad estándar	Resiliencia mejorada; prioridad estándar	Planes incompletos; prioridad estándar
4	Legal y regulatoria	Multas y costes legales	Cumplimiento básico; prioridad media	Cumplimiento reforzado; prioridad media-alta	Riesgo de incumplimiento; prioridad alta
5	Social y privacidad	Daños a personas, impacto en derechos	Medidas parciales; prioridad media-alta	Salvaguardas reforzadas; prioridad alta	Salvaguardas débiles; prioridad muy alta
6	IA y automatización	Riesgos específicos de IA y shadow AI	Uso limitado de IA; prioridad estándar	IA gobernada orientada a seguridad; prioridad media-alta	Shadow AI extendida; prioridad alta

Fuente: Elaboración propia bajo análisis de reporte de IBM (2024) y publicación en ISACA Journal (2023).

A su vez, como complemento para entender y comprender el modelo de análisis cualitativo expuesto, se muestra en la Tabla 2 con valores ilustrativos de control y peso por dimensión para cada escenario. Estos valores son un ejemplo, creados bajo criterio y juicio experto, inspirados en la lógica de los informes de IBM y en el enfoque de ISACA sobre la descomposición de costes y la importancia de la madurez de control, los cuales están pensados para que cada organización los ajuste con datos propios.

Tabla 2. Valores de control y peso por dimensión y escenario

#	Dimensión	Parámetros clave (comunes)	Escenario A: Controles tradicionales	Escenario B: Alta seguridad con IA	Escenario C: Shadow AI y baja gobernanza
1	Económica	Impacto económico típico por brecha; probabilidad anual	Control = 0.4; Peso = 1.0	Control = 0.7; Peso = 1.0	Control = 0.3; Peso = 1.0
2	Reputacional	Pérdida estimada de clientes/ingresos futuros	Control = 0.3; Peso = 1.2	Control = 0.5; Peso = 1.2	Control = 0.2; Peso = 1.3
3	Operativa	Coste de paradas y recuperación	Control = 0.5; Peso = 1.0	Control = 0.8; Peso = 1.0	Control = 0.4; Peso = 1.0
4	Legal y regulatoria	Multas, costes legales	Control = 0.4; Peso = 1.1	Control = 0.6; Peso = 1.1	Control = 0.3; Peso = 1.2
5	Social y privacidad	Daños a personas, impacto en derechos	Control = 0.3; Peso = 1.3	Control = 0.5; Peso = 1.3	Control = 0.2; Peso = 1.4
6	IA y automatización	Riesgos específicos de IA (brechas de modelos, shadow AI)	Control = 0.2; Peso = 1.0	Control = 0.7; Peso = 1.1	Control = 0.1; Peso = 1.3

Fuente: Elaboración propia bajo análisis de reporte de IBM (2024) y publicación en ISACA Journal (2023).

b. Escenario cuantitativo. Este análisis se trata de una simulación ilustrativa construida exclusivamente con datos secundarios y destinada a facilitar la comparación entre escenarios, permitiendo mostrar la lógica del modelo. Por tanto, basado en el informe de IBM indica que el coste medio global de una brecha de datos se encuentra en un rango de $4.4 – $4.9 millones de dólares en los últimos años, con una descomposición en componentes como pérdida de negocio, respuesta técnica, notificación y sanciones. El artículo de ISACA muestra, además, que el coste puede representarse como porcentaje de los ingresos anuales y que los eventos más

habituales se sitúan por debajo de 0.4% de la facturación, con fuertes variaciones en función de factores como el sector, la presencia de litigios, el tipo de datos afectados o el uso de ransomware.

Por lo anterior y con base en estas referencias, se plantean tres (3) escenarios cuantitativos para una organización con ingresos anuales de 1,000 millones dólares (este valor se puede ajustar con base a la realidad de la organización), utilizando la fórmula del Costo Esperado de Consecuencias (CEC) y los valores de control y peso definidos en el MCEC. Los valores de impacto y probabilidad se fijan de manera prudente dentro de los rangos sugeridos por IBM e ISACA, con el objetivo de mostrar la lógica del modelo más que de producir estimaciones exactas.

A continuación, se describen los supuestos comunes para llevar a cabo los tres (3) escenarios: a. Ingresos anuales: $1,000.00 millones.

b. Impactos máximos por brecha, por dimensión (si el incidente se materializa): i. Económica: $5 millones (aprox. 0.5% de ingresos, alineado con el rango de IBM para coste medio más un margen adicional). ii. Reputacional: $3 millones (pérdida de clientes y campañas de reconstrucción de imagen). iii. Operativa: $4 millones (paradas de servicio, horas extra y recuperación). iv. Legal/regulatoria: $3 millones (multas y costes legales en un caso relevante). v. Social/privacidad: $2 millones (medidas de apoyo a afectados, reclamos, compensaciones). vi. IA y automatización: $2 millones (incidentes asociados a IA, incluyendo posibles filtraciones o mal funcionamiento de modelos). c. Probabilidad anual de al menos un incidente categorizado como "crítico o relevante" en cada dimensión en el escenario de referencia, cuyos valores de orientación son los siguientes: i. Económica: 0.30 ii. Reputacional: 0.25 iii. Operativa: 0.30 iv. Legal/regulatoria: 0.20 v. Social/privacidad: 0.25 vi. IA y automatización: 0.15

Estos parámetros reflejan, de forma agregada, la frecuencia observada de brechas y su potencial para activar distintas dimensiones de impacto, conforme a los patrones descritos por IBM e ISACA. En virtud de los parámetros antes descritos, se procede a desarrollar los tres (3) escenarios, mismos que se detallan a continuación:

- Escenario A: Controles tradicionales. En este escenario, se asumen niveles de control y pesos tal como se muestran en la Tabla 3 de valores ilustrativos del MCEC para controles tradicionales.

Tabla 3. Cálculo del CEC para Escenario A

#	Dimensión	Impacto (M)	Prob.	Control	Peso	CEC_i = Peso × Impacto × Prob × (1 − Control) (M)
1	Económica	5.0	0.30	0.40	1.0	1.0 × 5.0 × 0.30 × 0.60 = **0.90**
2	Reputacional	3.0	0.25	0.30	1.2	1.2 × 3.0 × 0.25 × 0.70 ≈ **0.63**
3	Operativa	4.0	0.30	0.50	1.0	1.0 × 4.0 × 0.30 × 0.50 = **0.60**
4	Legal/regulatoria	3.0	0.20	0.40	1.1	1.1 × 3.0 × 0.20 × 0.60 ≈ **0.40**
5	Social/privacidad	2.0	0.25	0.30	1.3	1.3 × 2.0 × 0.25 × 0.70 ≈ **0.46**
6	IA y automatización	2.0	0.15	0.20	1.0	1.0 × 2.0 × 0.15 × 0.80 = **0.24**
Total CEC						**≈ $3.23 millones**

En resumen, el costo esperado anual de consecuencias se sitúa en torno a $3.2 millones, lo que equivale aproximadamente a 0.32% de los ingresos anuales, dentro del orden de magnitud que ISACA identifica como habitual para la mayoría de los eventos. La mayor contribución proviene de las dimensiones económica, operativa y reputacional, coherente con las descomposiciones de coste reportadas por IBM.

- Escenario B: Alta seguridad con IA. Para este escenario, se asume que la organización despliega ampliamente soluciones de seguridad basadas en IA y automatización, así como capacidades maduras de respuesta, lo que se refleja en valores de control más altos en varias dimensiones. Se mantienen los mismos impactos y probabilidades, pero se ajustan los controles y se conserva la estructura de pesos, tal y como se muestran en la Tabla 4.

Tabla 4. Cálculo del CEC para Escenario B

#	Dimensión	Impacto (M)	Prob.	Control	Peso	CEC_i = Peso × Impacto × Prob × (1 - Control) (M)
1	Económica	5.0	0.30	0.70	1.0	1.0 × 5.0 × 0.30 × 0.30 = **0.45**
2	Reputacional	3.0	0.25	0.50	1.2	1.2 × 3.0 × 0.25 × 0.50 = **0.45**
3	Operativa	4.0	0.30	0.80	1.0	1.0 × 4.0 × 0.30 × 0.20 = **0.24**
4	Legal/regulatoria	3.0	0.20	0.60	1.1	1.1 × 3.0 × 0.20 × 0.40 ≈ **0.26**
5	Social/privacidad	2.0	0.25	0.50	1.3	1.3 × 2.0 × 0.25 × 0.50 ≈ **0.33**
6	IA y automatización	2.0	0.15	0.70	1.0	1.0 × 2.0 × 0.15 × 0.30 ≈ **0.14**
Total CEC						**≈ $1.83 millones**

El costo esperado anual desciende a unos $1.8 millones, es decir, alrededor de 0.18% de los ingresos, lo que implica una reducción cercana al 40% respecto del escenario de referencia. Esta magnitud es consistente con las reducciones de entre $1.8 y $2.2 millones por brecha asociadas por IBM a la adopción extensiva de IA y automatización de seguridad, y con el argumento de ISACA sobre el impacto de una mayor madurez de control en el coste total.

- Escenario C: Shadow AI y gobernanza débil. En este escenario, se asume un uso extensivo de herramientas de "shadow AI" sin gobernanza adecuada, junto con niveles de control más bajos en la dimensión de IA y un incremento de pesos en las dimensiones legal y social/privacidad. Se conservan los mismos impactos, pero se ajustan probabilidades y controles para reflejar una mayor exposición en IA y en las dimensiones jurídicas y sociales, tal y como se muestran en la Tabla 5.

Tabla 5. Cálculo del CEC para Escenario C

#	Dimensión	Impacto (M)	Prob.	Control	Peso	CEC_i = Peso × Impacto × Prob × (1 - Control) (M)
1	Económica	5.0	0.30	0.30	1.0	1.0 × 5.0 × 0.30 × 0.70 = **1.05**
2	Reputacional	3.0	0.25	0.20	1.3	1.3 × 3.0 × 0.25 × 0.80 ≈ **0.78**
3	Operativa	4.0	0.30	0.40	1.0	1.0 × 4.0 × 0.30 × 0.60 = **0.72**
4	Legal/regulatoria	3.0	0.20	0.30	1.2	1.2 × 3.0 × 0.20 × 0.70 ≈ **0.50**
5	Social/privacidad	2.0	0.25	0.20	1.4	1.4 × 2.0 × 0.25 × 0.80 ≈ **0.56**
6	IA y automatización	2.0	0.25	0.20	1.3	1.3 × 2.0 × 0.25 × 0.90 ≈ **0.59**
Total CEC						**≈ $4.20 millones**

Para el escenario 3, el costo esperado anual de consecuencias se aproxima a $4.2 millones, es decir, en el entorno de 0.42% de los ingresos, alineado con el umbral del 0.4% de facturación que ISACA identifica como referencia para la mayoría de los eventos, pero con mayor peso de componentes legales, sociales y de IA. El incremento respecto al escenario de referencia ilustra cómo la combinación de bajos niveles de control en IA, alta probabilidad de incidentes en esta dimensión y mayor sensibilidad legal y social puede elevar el riesgo residual incluso si otros controles se mantienen.

Estos tres (3) escenarios cuantitativos, desarrollados con parámetros coherentes con la información de magnitud reportadas por IBM e ISACA, muestran que el CEC: a. Permite descomponer el riesgo residual en dimensiones diferenciadas, ligando cada una a impactos, probabilidades, controles y pesos específicos. b. Produce resultados agregados (en torno a 0.2–0.4% de los ingresos) que son razonables y comparables con los rangos identificados por los modelos basados en datos históricos y regresiones econométricas descritos por ISACA. c. Ofrece una estructura flexible para incorporar nuevas variables o matices (por ejemplo, ransomware, tipo de datos afectados, litigios) sin perder la claridad de la formulación básica, lo que facilita su prueba, ajuste y mejora a medida que se disponga de más datos.

Desde esta perspectiva, el CEC se presenta como un modelo conceptual y operativo que, aunque no sustituye a modelos cuantitativos basados en regresión desarrollados sobre grandes bases de datos sobre eventos, incidentes u otros elementos asociados a los riesgos en datos, puede utilizarse en organizaciones que no disponen de esa información para aproximar su perfil de riesgo y evaluar el efecto de distintas decisiones de inversión y gobernanza en el costo esperado de brechas y pérdidas de datos.

A su vez, la comparación de los tres (3) escenarios muestra que el MCEC produce resultados cuantitativamente razonables y alineados con los órdenes de magnitud observados en el informe

de IBM y en el análisis econométrico de ISACA, al tiempo que permite visualizar el efecto de las decisiones de gestión del riesgo sobre el coste esperado de brechas y pérdidas de datos. Por tanto, el modelo muestra: a. Reducción del coste esperado cuando aumenta la eficacia de los controles, en especial cuando se incorporan soluciones de seguridad basadas en IA y automatización. b. El incremento del coste esperado cuando la organización despliega IA sin gobernanza adecuada y asume un mayor riesgo legal y social por el tratamiento de datos personales sensibles.

4. Resultados y discusión

Los escenarios cualitativos y cuantitativos desarrollados a partir del MCEC permiten identificar tres (3) aspectos principales. i) El modelo muestra que las consecuencias de las brechas y pérdidas de datos no se concentran exclusivamente en la dimensión económica, sino que se distribuyen entre componentes reputacionales, operativos, legales, sociales y asociados a inteligencia artificial, en línea con el marco conceptual desarrollado en la sección anterior[23]. ii) La comparación entre escenarios sugiere que la eficacia de los controles modifica de manera apreciable el costo esperado residual, especialmente cuando la organización combina capacidades de detección y respuesta con mecanismos de gobernanza sobre el uso de inteligencia artificial.[24] iii) Los resultados ponen de manifiesto que la ausencia de una correcta gobernanza sobre herramientas de IA puede desplazar el peso del riesgo hacia dimensiones que trascienden el costo directo, en particular las de privacidad, cumplimiento y exposición reputacional.

Desde una perspectiva cuantitativa, la ilustración desarrollada en el estudio sitúa el costo esperado anual de consecuencias en un rango aproximado de 0.18% a 0.42% de los ingresos anuales, según el escenario considerado. El escenario asociado a mayor madurez de control y uso gobernado de inteligencia artificial presenta el valor más bajo, mientras que el escenario caracterizado por shadow AI y debilidad de gobernanza arroja el valor más alto. Esta diferencia es consistente con la evidencia utilizada en este estudio, según la cual la reducción de tiempos de detección, la mejora de la respuesta y el fortalecimiento de controles tienden a disminuir el costo total de las brechas, mientras que la exposición a usos no controlados de IA incrementa la probabilidad de incidentes y sus efectos acumulados.

Estos resultados no deben interpretarse como una validación empírica definitiva del MCEC, sino como una demostración razonada de su utilidad analítica. Esta investigación se apoya en datos secundarios y en valores ilustrativos construidos a partir de literatura especializada, informes sectoriales y documentos de autoridades, por lo que el principal aporte del modelo reside en su capacidad para organizar y traducir distintas dimensiones de impacto en un esquema consistente de apoyo a la decisión. En este sentido, el MCEC resulta especialmente útil para organizaciones que no cuentan con grandes bases históricas de incidentes, pero necesitan aproximaciones estructuradas para priorizar controles, justificar inversiones y discutir el riesgo residual en términos comprensibles para la dirección y para las áreas de cumplimiento o auditoría interna.

La discusión del modelo también permite ubicar su alcance frente a otros enfoques de cuantificación. A diferencia de modelos econométricos construidos sobre grandes volúmenes de datos históricos, la propuesta no busca ofrecer una predicción estadística universal, sino una herramienta flexible y replicable para combinar impacto, probabilidad, control y peso de cada dimensión. Su principal fortaleza radica en que integra en una sola formulación elementos económicos y no económicos del daño, conservando al mismo tiempo una lógica suficientemente simple para ser ajustada por cada organización con sus propios datos o con referencias sectoriales.

Al mismo tiempo, los resultados sugieren que las dimensiones legal y regulatoria, e inteligencia artificial y automatización, desempeñan una función dual dentro del análisis. Por un lado, constituyen dimensiones de impacto con efectos propios; por otro, actúan como factores que amplifican o reducen el riesgo residual dependiendo del grado de diligencia organizacional, de la calidad de la gobernanza del dato y del nivel de supervisión sobre los sistemas automatizados.

[23] Wang, Ping, Hubert D'Cruze y David Wood, "Economic Costs and Impacts of Business Data Breaches," Issues in Information Systems 20, no. 2 (2019): 162–171; Freund, Jack y Natalie Jorion, "The True Cost of a Data Breach," ISACA Journal 1 (2023).

[24] IBM Security, Cost of a Data Breach Report 2024 (Armonk, NY: IBM, 2024), 5–6, 10, 15–33; Freund y Jorion, "The True Cost of a Data Breach." European Data Protection Supervisor, Risk Management of AI Systems under the GDPR (Brussels: EDPS, 2025), 9–12; Agencia Española de Protección de Datos, Adecuación al RGPD de tratamientos que incorporan inteligencia artificial (Madrid: AEPD, 2020), 9 y 49.

5. Conclusiones y recomendaciones

- a. Las brechas y pérdidas de datos deben entenderse como fenómenos de riesgo con efectos multidimensionales, cuyos impactos exceden el plano económico e inciden también en la reputación, la continuidad operativa, el cumplimiento normativo, los derechos y libertades de las personas y la gobernanza de la inteligencia artificial. Sobre esa base, el MCEC ofrece una propuesta conceptual y operativa que permite integrar estas dimensiones en un indicador único de costo esperado residual, adaptable a la realidad, tamaño y complejidad de cada organización.

- b. Los escenarios desarrollados sugieren que el modelo reproduce órdenes de magnitud creíbles y útiles para fines analíticos, al tiempo que visibiliza el efecto de distintos niveles de control y de gobernanza de IA sobre el costo esperado de brechas y pérdidas de datos. En consecuencia, su valor principal no reside en reemplazar modelos cuantitativos avanzados, sino en servir como instrumento de apoyo para la gestión del riesgo, la priorización de controles, la toma de decisiones informada y la comunicación con la Alta Dirección.

- c. Desde una perspectiva práctica, se recomienda a las organizaciones identificar de manera explícita las seis (6) dimensiones de impacto en sus procesos críticos y tratamientos de datos, utilizar el MCEC como marco inicial de estimación cuando no se disponga de series internas robustas, y reforzar las capacidades de detección, respuesta y gobernanza de inteligencia artificial para evitar la expansión de prácticas de shadow AI. Asimismo, conviene alinear la aplicación del modelo con las obligaciones de protección de datos, con los procesos de continuidad de negocio y con los esquemas institucionales de gestión del riesgo que puedan existir.

- d. Como línea de desarrollo futuro, el estudio señala que, de forma breve, el MCEC requiere validación empírica posterior con datos reales de diferentes sectores, así como ajustes específicos en pesos, probabilidades y variables complementarias según el contexto organizacional. Esta mención basta para atender el plano prospectivo sin extender en exceso la conclusión ni comprometer afirmaciones que el estudio, por su naturaleza documental, todavía no pretende demostrar de manera definitiva.

Bibliografía

Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679. Rev. 01. Brussels, 2017. Consultado el 6 de enero de 2026. https://ec.europa.eu/newsroom/article29/items/611236

Baruh, Lemi, Zeynep D. Aydoğan, y Zeynep A. Toker. "Privacy Concern and Its Consequences: A Meta-Analysis." Technological Forecasting and Social Change 196 (2023): 122789. Consultado el 6 de enero de 2026. https://doi.org/10.1016/j.techfore.2023.122789

European Commission. Implementing the General Data Protection Regulation: A First Step towards a New Opportunity for Europe. Brussels: European Commission, 2018. Consultado el 6 de enero de 2026. https://commission.europa.eu/publications/implementing-general-data-protection-regulation-gdpr_en

European Data Protection Supervisor. Risk Management of AI Systems under the GDPR. Brussels: EDPS, 2025. Consultado el 6 de enero de 2026. https://www.edps.europa.eu/

FAIR Institute. "What Is FAIR?" Consultado el 14 de abril de 2026. https://www.fairinstitute.org/what-is-fair

Freund, Jack, y Natalie Jorion. "The True Cost of a Data Breach." ISACA Journal 1 (2023). Consultado el 6 de enero de 2026. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-1/the-true-cost-of-a-data-breach

Ho, Shirley S., Nga N. Ho-Dac, y Ray-Bing Huang. "The Effects of Privacy and Data Breaches on Consumers' Online Self-Disclosure, Protection Behavior, and Message Valence." SAGE Open 13, no. 3 (2023). Consultado el 6 de enero de 2026. https://doi.org/10.1177/21582440231181395

IBM Security. Cost of a Data Breach Report 2024. Armonk, NY: IBM Security, 2024. Consultado el 6 de enero de 2026. https://www.ibm.com/reports/data-breach

International Organization for Standardization. ISO 31000:2018 Risk Management—Guidelines. Geneva: ISO, 2018. Consultado el 14 de abril de 2026. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

National Institute of Standards and Technology. Cybersecurity Framework 2.0. Gaithersburg, MD: NIST, 2024. Consultado el 14 de abril de 2026. https://www.nist.gov/cyberframework

Wang, Ping, Hubert D'Cruze, y David Wood. "Economic Costs and Impacts of Business Data Breaches." Issues in Information Systems 20, no. 2 (2019): 162–171. Consultado el 6 de enero de 2026. https://doi.org/10.48009/2_iis_2019_162-171