SEI SABER ESTRATÉGICO INTERNACIONAL

https://doi.org/10.70577/s.e.v4i3.51

Fecha de recepción: 2026-04-22
Fecha de aceptación: 2026-07-20
Fecha de publicación: 2026-08-14
Periodicidad: Trimestral, Vol.: 4, No. 3, pág. 324-341
ISSN: 3121-2956

Responsabilidad jurídica de las empresas ante la filtración de datos personales

Legal responsibility of companies in the event of a breach of personal data

Alex Joe Alvia Pacheco[1]
Universidad Laica Eloy Alfaro de Manabí. Manta, Ecuador
e1350262927@live.uleam.edu.ec
https://orcid.org/0009-0001-8387-0428

Javier Andrés Espinoza Suárez[2]
Universidad Laica Eloy Alfaro de Manabí. Manta, Ecuador
javier.espinoza@uleam.edu.ec
https://orcid.org/0009-0000-8126-4400

Cómo citar:
Alvia Pacheco, A. J., & Espinoza Suárez, J. A. (2026). Responsabilidad jurídica de las empresas ante la filtración de datos personales. *Saber Estratégico Internacional*, *4*(3), 324–341. https://doi.org/10.70577/s.e.v4i3.51

RESUMEN

La creciente digitalización empresarial ha incrementado la exposición de los datos personales a accesos no autorizados, filtraciones y ciberataques, generando riesgos jurídicos para las organizaciones y afectaciones a los derechos de los titulares. El estudio tuvo como objetivo analizar la responsabilidad jurídica de las empresas ante la filtración de datos personales en Ecuador, considerando el marco constitucional, legal y reglamentario, las obligaciones preventivas, la gestión de incidentes y las responsabilidades administrativas, civiles y penales. Se aplicó un enfoque cualitativo con apoyo cuantitativo, mediante investigación documental y bibliográfica, método analítico-sintético y dogmático-jurídico, complementado con 60 registros analizados mediante coeficiente phi, regresión logística y conglomerados jerárquicos. Los resultados mostraron que las deficiencias en seguridad y notificación presentaron la mayor asociación con consecuencias jurídicas, ambas con φ = 0,312; además, el incumplimiento de notificación alcanzó una razón de probabilidades de 2,675. El grupo de alta exposición concentró 57,1% de consecuencias jurídicas, frente a 25,9% del grupo bajo. Se determinó que la responsabilidad empresarial dependió no solo de la filtración, sino también de la prevención, gestión del riesgo, respuesta oportuna y protección efectiva de los titulares.

Palabras clave: Protección de datos personales, filtración de datos, responsabilidad empresarial, seguridad de la información, gestión de riesgos.

ABSTRACT

The growing business digitalization has increased the exposure of personal data to unauthorized access, leaks and cyber-attacks, generating legal risks for organizations and impacts on the rights of the owners. The study aimed to analyze the legal responsibility of companies in the face of personal data leaks in Ecuador, considering the constitutional, legal and regulatory framework, preventive obligations, incident management and administrative, civil and criminal responsibilities. A qualitative approach was applied with quantitative support, through documentary and bibliographic research, analytical-synthetic and dogmatic-legal method, complemented with 60 records analyzed using phi coefficient, logistic regression and hierarchical clusters. The results showed that deficiencies in security and notification had the greatest association with legal consequences, both with φ = 0.312; Furthermore, failure to report reached an odds ratio of 2.675. The high exposure group accounted for 57.1% of legal consequences, compared to 25.9% in the low group. It was determined that corporate responsibility depended not only on the leak, but also on prevention, risk management, timely response and effective protection of the owners.

Keywords: Protection of personal data, data breach, corporate responsibility, information security, risk management.

https://doi.org/10.70577/s.e.v4i3.51

INTRODUCCIÓN

La era digital es una realidad a la que la sociedad se adapta de manera progresiva, debido a que el acelerado desarrollo de las tecnologías de la información y la comunicación ha transformado significativamente la forma en que las personas, empresas e instituciones recopilan, almacenan, gestionan y comparten información. Si bien estas herramientas han permitido optimizar procesos, incrementar la eficiencia operativa y facilitar el acceso a servicios digitales, también han generado nuevos desafíos en materia de seguridad y protección de datos personales. En este sentido, Klöckner et al. (2022), a partir del análisis de 219 anuncios de filtraciones de datos de empresas estadounidenses que cotizaban en bolsa, determinaron una reacción negativa significativa del mercado durante los dos días posteriores a la divulgación del incidente, demostrando que una vulneración de información puede trascender el ámbito tecnológico y afectar directamente el valor empresarial. De manera complementaria, Bamiatzi et al. (2023) analizaron 230 empresas afectadas por incidentes cibernéticos y comprobaron que las organizaciones con menores niveles de responsabilidad corporativa presentaron consecuencias financieras significativamente más desfavorables después de una filtración.

A escala internacional, la creciente dependencia de plataformas tecnológicas y sistemas de almacenamiento digital ha incrementado la exposición de la información a accesos no autorizados, ciberataques, errores humanos y filtraciones que pueden comprometer derechos fundamentales y ocasionar consecuencias económicas, reputacionales y jurídicas para las organizaciones responsables de su tratamiento. Al respecto, Zhu et al. (2024) sostienen que las filtraciones pueden deteriorar la moral de los empleados, la reputación corporativa, las relaciones con clientes y proveedores y el desempeño financiero, por lo que la responsabilidad empresarial debe comprender medidas preventivas y actuaciones posteriores al incidente. Así mismo, Naidoo et al. (2024), después de examinar 378 comunicados empresariales sobre vulneraciones de ciberseguridad, identificaron cuatro formas principales de respuesta organizacional: reconocimiento empático, demostración de capacidad para gestionar el incidente, recuperación de la confianza y restablecimiento de la lealtad de los afectados.

Desde una perspectiva más específica sobre la responsabilidad posterior al incidente, la filtración no termina con la identificación de la vulnerabilidad, puesto que obliga a la empresa a comunicar oportunamente, mitigar daños y adoptar acciones coherentes con las características del hecho. En esta línea, Nikkhah y Grover (2025) estudiaron experimentalmente a 849 participantes y analizaron información correspondiente a 307 filtraciones ocurridas entre 2006 y 2022, evidenciando que clientes e inversionistas valoran de manera diferente la responsabilidad de la organización según la causa, el grado de control empresarial sobre el incidente y la forma en que este es comunicado. De igual manera, Humphreys et al. (2024) advierten que la incorporación acelerada de nuevas tecnologías sin medidas suficientes de seguridad puede ampliar la exposición corporativa, recordando casos en los cuales llegaron a exponerse 38 terabytes de información privada, situación que reafirma el deber empresarial de evaluar los riesgos tecnológicos antes de implementar sistemas capaces de procesar información sensible.

En el contexto ecuatoriano, la problemática adquiere especial relevancia debido a que el crecimiento de los servicios digitales exige que las empresas adapten sus procedimientos internos al régimen jurídico de protección de datos. Sobre este aspecto, Astudillo et al. (2024) identificaron entre los principales retos del sector empresarial privado las amenazas de acceso no autorizado, la ciberdelincuencia, el manejo

https://doi.org/10.70577/s.e.v4i3.51

inadecuado de información, el desconocimiento de aspectos legales y la ausencia de políticas empresariales suficientes.

Entre las dificultades se encuentra “la ambigüedad en las normativas y la falta de políticas y adecuación empresarial” (Astudillo r et al., 2024, p. 567), lo cual demuestra que el cumplimiento jurídico requiere trasladar las disposiciones legales hacia protocolos efectivos de prevención, control y respuesta organizacional. En concordancia con ello, Barahona et al. (2024) señalan que, aunque Ecuador reconoce jurídicamente la protección de los datos personales, su efectividad enfrenta obstáculos relacionados con la limitada cultura de privacidad, las capacidades institucionales y la constante evolución tecnológica.

En el plano normativo nacional, la protección de los datos personales parte del artículo 66, numeral 19, de la Constitución de la República del Ecuador, que reconoce el derecho a la protección de datos de carácter personal y establece garantías respecto de su acceso, tratamiento y difusión. Este reconocimiento fue desarrollado posteriormente mediante la Ley Orgánica de Protección de Datos Personales, cuyo artículo 10 incorpora el principio de seguridad y exige a responsables y encargados adoptar medidas organizativas, técnicas y de otra naturaleza que resulten adecuadas frente a riesgos, amenazas y vulnerabilidades. A su vez, el Reglamento General de esta ley complementa el régimen aplicable a la gestión y seguridad de la información. Desde una perspectiva reciente, Andrade et al. (2026) explican que la protección ecuatoriana se estructura mediante mecanismos constitucionales y administrativos complementarios, manteniéndose la tutela constitucional junto con la actuación técnica y administrativa de la autoridad especializada.

La responsabilidad empresarial adquiere especial trascendencia cuando la vulneración produce daños al titular de la información, porque las consecuencias del incumplimiento no se limitan a las medidas administrativas, sino que pueden proyectarse hacia otros ámbitos jurídicos. En particular, Zambrano et al. (2024) analizan la responsabilidad civil derivada del incumplimiento de la normativa ecuatoriana y explican que el responsable del tratamiento puede responder incluso por actuaciones atribuibles a terceros sometidos a su vigilancia, además de señalar la relevancia de los daños extrapatrimoniales ocasionados por un tratamiento inadecuado de información personal. Por otra parte, Bermeo et al. (2024) resaltan, desde el sector financiero popular y solidario ecuatoriano, la necesidad de establecer sistemas de gestión que articulen la normativa nacional con medidas institucionales de protección, particularmente cuando las organizaciones administran información sensible de usuarios y clientes. De este modo, la responsabilidad empresarial debe ser comprendida desde una perspectiva integral que incluya prevención, seguridad, detección, comunicación del incidente, reparación del daño y determinación de las consecuencias jurídicas correspondientes.

Frente a esta problemática, persiste la necesidad de delimitar hasta dónde alcanza la responsabilidad de una empresa cuando los datos personales bajo su custodia son expuestos, sustraídos o divulgados sin autorización, especialmente al diferenciar las obligaciones preventivas de las consecuencias que surgen después de una vulneración. Por ello, el objetivo del estudio es analizar la responsabilidad jurídica de las empresas ante la filtración de datos personales mediante el estudio del marco constitucional, legal y reglamentario aplicable en Ecuador, considerando las obligaciones preventivas, los mecanismos de gestión de incidentes y las responsabilidades administrativas, civiles y penales que puedan generarse como consecuencia de vulneraciones de seguridad. Con este enfoque se pretende establecer que la

https://doi.org/10.70577/s.e.v4i3.51

protección de datos no son únicamente una obligación formal de cumplimiento normativo, sino un deber permanente de diligencia empresarial destinado a prevenir vulneraciones, responder oportunamente ante incidentes y garantizar los derechos de los titulares de la información.

Tutela jurídica, gobernanza y sujetos intervinientes en el tratamiento de datos personales

El concepto de protección de datos personales se ha fortalecido como uno de los principales desafíos jurídicos de la era digital, debido a que el crecimiento de las tecnologías y la circulación continua de información han ampliado las posibilidades de aprovechamiento de los datos y los riesgos para la privacidad. Desde una perspectiva organizacional, Thomas et al. (2022) explican que la rendición de cuentas sobre privacidad y seguridad requiere integrar responsabilidades, procedimientos de respuesta y comunicación verificable, de modo que una organización pueda demostrar cómo protege la información antes y después de un incidente. De manera complementaria, Wang y Ngai (2022), mediante información longitudinal de empresas cotizadas durante doce años, evidenciaron que la estructura organizacional y las capacidades gerenciales guardan relación con la probabilidad de experimentar filtraciones, lo cual demuestra que la protección no constituye únicamente una cuestión tecnológica, sino también jurídica y administrativa.

En Ecuador, esta concepción encuentra su fundamento superior en el artículo 66, numeral 19, de la Constitución de la República del Ecuador, que reconoce el derecho a la protección de los datos de carácter personal e incluye el acceso y decisión respecto de esa información, así como su correspondiente protección. La disposición constitucional determina, además, que la recolección, archivo, procesamiento, distribución o difusión requiere autorización de su titular o mandato legal. En este sentido, Chen et al. (2022) demostraron que la presencia de conocimientos especializados en tecnologías de la información dentro de los órganos de supervisión empresarial disminuye la exposición a vulneraciones, mientras que Chen et al. (2023) encontraron que la información revelada sobre riesgos de ciberseguridad después de una filtración posee contenido relevante para evaluar la situación de las empresas. Estos aportes respaldan la interpretación de que el deber de protección exige controles verificables y no solamente declaraciones formales de cumplimiento.

El artículo 92 de la Constitución reconoce la acción de hábeas data como una garantía destinada a permitir que las personas conozcan la existencia y accedan a documentos, datos genéticos, bancos o archivos de información personal e informes sobre sí mismas o sus bienes, pudiendo solicitar su actualización, rectificación, eliminación o anulación cuando corresponda. Por consiguiente, una filtración de información no debe entenderse exclusivamente como la falla técnica de un sistema informático, sino como un acontecimiento capaz de afectar directamente un derecho constitucional. Desde una perspectiva comparada, Hof (2024) sostiene que la protección desde el diseño y la actuación de las autoridades de control son necesarias para transformar los principios jurídicos de privacidad en exigencias concretas, mientras que Zuiderveen et al. (2024) señalan que las reglas de notificación de brechas favorecen la transparencia, la rendición de cuentas y los incentivos para mejorar la seguridad institucional.

La regulación constitucional fue desarrollada mediante la Ley Orgánica de Protección de Datos Personales, publicada en 2021, que configuró un sistema especializado de principios, derechos, obligaciones, autoridades y consecuencias jurídicas. Su aplicación no se limita a archivos digitales, pues comprende el tratamiento de datos personales contenido en cualquier soporte cuando corresponda al

https://doi.org/10.70577/s.e.v4i3.51

ámbito material previsto por la ley; igualmente, contempla reglas de aplicación territorial que pueden alcanzar determinadas operaciones realizadas fuera de Ecuador. En correspondencia con esta tendencia regulatoria, Gider et al. (2026) advierten que los sistemas modernos de protección de datos combinan bases jurídicas para el tratamiento, evaluación de impacto, seguridad, notificación de incidentes y mecanismos de cumplimiento, mientras que Khan et al. (2025) sostienen que la gestión corporativa de privacidad constituye una dimensión de responsabilidad social, debido a los efectos que una protección insuficiente puede generar sobre clientes y otros grupos de interés.

En cuanto a la información protegida, la Ley Orgánica de Protección de Datos Personales considera dato personal a aquel que identifica o hace identificable, directa o indirectamente, a una persona natural. Esta definición permite comprender que nombres, números de identificación, direcciones, correos electrónicos, registros financieros, localización y otros elementos pueden quedar sujetos al régimen jurídico cuando posibiliten identificar a una persona. A ello se suman categorías cuya naturaleza exige mayores salvaguardas, particularmente los datos sensibles, biométricos, de salud y aquellos vinculados con personas pertenecientes a grupos que requieren especial protección. Al respecto, Nemec et al. (2024), mediante una revisión sistemática de 99 investigaciones, comprobaron que los controles de acceso, el almacenamiento seguro y las medidas de protección de información sensible son componentes recurrentes para disminuir filtraciones, mientras que Pina et al. (2024) destacan que la administración responsable de bases de datos demanda integrar privacidad, ética, seguridad y limitación del uso de información.

Dentro de este régimen resulta fundamental diferenciar a los sujetos que intervienen en el tratamiento. El titular es la persona natural a quien pertenecen los datos; el responsable del tratamiento determina los fines y medios utilizados; y el encargado del tratamiento procesa la información por cuenta del responsable y dentro de sus instrucciones. Además, intervienen destinatarios, corresponsables, terceros y el delegado de protección de datos personales. La Superintendencia de Protección de Datos Personales aclaró en 2025 que las relaciones entre responsable y encargado previstas en los artículos 34 y 35 de la Ley Orgánica de Protección de Datos Personales se complementan con el artículo 43 de su Reglamento General, precisamente para impedir vacíos de responsabilidad cuando un tercero accede a información dentro de una relación de prestación de servicios.

Como puede observarse en la Tabla 1, la delimitación de los roles permite establecer quién decide sobre el tratamiento, quién ejecuta determinadas operaciones y quién debe responder por obligaciones específicas frente a la utilización o exposición de información personal.

Tabla 1

Principales sujetos y obligaciones dentro del tratamiento de datos personales

Sujeto	Función esencial	Responsabilidad principal
Titular de los datos	Persona natural a quien corresponde la información	Ejercer sus derechos de acceso, rectificación, actualización, eliminación, oposición y demás derechos reconocidos legalmente
Responsable del tratamiento	Determina la finalidad y los medios del tratamiento	Garantizar licitud, seguridad, gestión de riesgos y cumplimiento de las obligaciones legales
Encargado del tratamiento	Trata información por	Cumplir las instrucciones lícitas del

https://doi.org/10.70577/s.e.v4i3.51

	cuenta del responsable	responsable y proteger los datos bajo su acceso
Corresponsables	Determinan conjuntamente finalidades y medios	Distribuir contractualmente y cumplir las obligaciones derivadas del tratamiento conjunto
Destinatario o tercero	Recibe datos conforme a una comunicación autorizada	Utilizar la información respetando la finalidad y fundamento jurídico correspondiente
Delegado de protección de datos personales	Asesora y supervisa el cumplimiento	Mantener independencia, vigilar el cumplimiento y servir como punto de contacto con la autoridad
Superintendencia de Protección de Datos Personales	Autoridad pública de supervisión	Controlar, regular, investigar, adoptar medidas correctivas y ejercer la potestad sancionadora

Nota. Información de la Ley Orgánica de Protección de Datos Personales, su Reglamento General y los criterios interpretativos de la Superintendencia de Protección de Datos Personales.

En esta relación, la responsabilidad del responsable no desaparece por el simple hecho de contratar a un tercero. La normativa exige formalizar las relaciones de tratamiento y establecer obligaciones sobre objeto, duración, naturaleza, categorías de información, titulares, instrucciones, confidencialidad y medidas de seguridad. Además, mediante la Resolución número SPDP-SPD-2025-0006-R, la Superintendencia de Protección de Datos Personales estableció reglas para incorporar cláusulas de protección de datos personales en contratos celebrados dentro del territorio ecuatoriano. Desde el ámbito organizacional, Zhou y Huang (2024) comprobaron que las filtraciones producen efectos posteriores sobre los sistemas de control interno de las empresas, mientras que Rezaee et al. (2024), utilizando 24.456 observaciones empresariales correspondientes al periodo 2005-2018, identificaron una asociación positiva significativa entre comportamientos corporativos socialmente irresponsables y la ocurrencia de filtraciones.

El sistema jurídico también contempla consecuencias administrativas cuando se incumplen estas obligaciones. En el sector privado, la Ley Orgánica de Protección de Datos Personales establece para determinadas infracciones leves multas comprendidas entre el 0,1% y el 0,7% del volumen de negocio del ejercicio económico inmediatamente anterior, mientras que para determinadas infracciones graves el rango se encuentra entre el 0,7% y el 1%, de acuerdo con la clasificación legal y el procedimiento aplicable. La aplicación práctica de este régimen ya ha producido precedentes: en enero de 2026, la Superintendencia informó una multa de 95.502,63 dólares a la Liga Profesional de Fútbol del Ecuador por incumplimientos relacionados con la protección de datos desde el diseño y por defecto; asimismo, comunicó una multa de 194.469,85 dólares a la Federación Ecuatoriana de Fútbol por deficiencias en su metodología de análisis y gestión de riesgos.

Conviene precisar que estos precedentes corresponden a procedimientos diferentes a los primeros casos sancionatorios anunciados en diciembre de 2025. En aquella ocasión, la autoridad informó otra sanción de 259.644,01 dólares contra la Liga Profesional de Fútbol del Ecuador y una de 194.856,16 dólares contra la Federación Ecuatoriana de Fútbol por infracciones graves asociadas con medidas insuficientes de protección, ordenando además acciones correctivas respecto de los datos tratados. Por tanto, no debe confundirse la Resolución número RES-SPDP-ICS-2025-0006 con la sanción de 194.856,16 dólares,

https://doi.org/10.70577/s.e.v4i3.51

puesto que corresponden a actuaciones sancionatorias distintas divulgadas por la autoridad.

Por otra parte, la vulneración de datos puede trascender la esfera administrativa cuando ocasiona perjuicios al titular. La tutela civil busca reparar los daños patrimoniales y extrapatrimoniales que puedan demostrarse, mientras que la garantía de hábeas data persigue fundamentalmente restablecer el control sobre la información personal. Además, determinadas conductas de acceso, utilización o divulgación ilegítima pueden adquirir relevancia penal conforme al Código Orgánico Integral Penal, dependiendo de los elementos objetivos y subjetivos del delito aplicable. En esta línea, Cross (2025), mediante una investigación con 309 víctimas de filtraciones de datos, evidenció que los incidentes producen consecuencias que exceden el fraude económico y pueden modificar la percepción de privacidad y seguridad de las personas; paralelamente, Hof (2024) sostiene que la actuación regulatoria efectiva es determinante cuando la deficiente protección compromete derechos fundamentales.

Gestión preventiva del riesgo y respuesta organizacional frente a vulneraciones de seguridad

La protección contemporánea de datos personales se sustenta en el principio de responsabilidad proactiva, según el cual las organizaciones no solamente deben cumplir formalmente la normativa, sino encontrarse en condiciones de demostrar que sus medidas técnicas, organizativas, físicas y jurídicas son adecuadas frente a los riesgos derivados del tratamiento. Esta perspectiva modifica el enfoque tradicional porque desplaza la atención desde la reacción posterior al daño hacia la identificación anticipada de vulnerabilidades. Al respecto, Thomas et al. (2022) proponen un marco de responsabilidad en el que la comunicación de incidentes forma parte de un sistema más amplio de gobernanza, mientras que Zhou y Huang (2024) verificaron que las filtraciones se encuentran vinculadas con cambios posteriores en los controles internos, lo que confirma la estrecha relación entre gestión preventiva, control organizacional y seguridad.

De acuerdo con el artículo 40 de la Ley Orgánica de Protección de Datos Personales, el análisis de riesgos debe considerar, entre otros aspectos, las particularidades del tratamiento, las características de los sujetos involucrados y las categorías y el volumen de datos tratados. A su vez, el artículo 42 dispone que debe efectuarse una evaluación de impacto en la protección de datos personales cuando exista probabilidad de alto riesgo para los derechos y libertades de los titulares y establece supuestos en los que dicha evaluación resulta obligatoria. La Superintendencia reforzó estas disposiciones mediante su guía de gestión de riesgos de 2025, precisando que la evaluación tiene naturaleza preventiva y debe identificar riesgos, establecer acciones concretas para su administración y documentar las medidas destinadas a salvaguardar los derechos de las personas.

Esta orientación es consistente con la literatura reciente. Por una parte, Kang et al. (2023) destacan que el análisis estructurado de riesgos permite anticipar escenarios capaces de producir filtraciones costosas y orientar recursos de seguridad hacia los activos de mayor exposición. Por otra, Kuznetsov et al. (2024) observaron que únicamente 10 % de las políticas de privacidad analizadas en su conjunto de dispositivos conectados incorporaban declaraciones relacionadas con notificaciones por filtraciones, evidenciando una brecha entre los requisitos regulatorios y su implementación documental.

Una consideración adicional corresponde al tratamiento de datos personales a gran escala. Actualmente, esta materia se encuentra desarrollada por la Resolución número SPDP-SPD-2026-0005-R, expedida por

https://doi.org/10.70577/s.e.v4i3.51

la Superintendencia de Protección de Datos Personales en 2026. La norma establece criterios técnicos para determinar y gestionar esta clase de tratamientos y obliga a evaluar, como mínimo, la permanencia del tratamiento, las categorías de información procesadas, su frecuencia y su alcance geográfico. Además, dispone que el número de titulares se determine sobre un periodo referencial de doce meses y que el registro de actividades sea actualizado al menos una vez al año o cuando existan modificaciones que incidan en la calificación del tratamiento o en su riesgo.

Por esta razón, no resulta conveniente mantener en el marco teórico la tabla de puntuaciones de 0,5, 1, 2 y 3 puntos ni afirmar sin matización que todo tratamiento que alcance seis puntos es automáticamente de gran escala, porque la norma vigente de 2026 debe ser aplicada conforme a su metodología técnica completa y sus criterios cuantitativos y cualitativos. La regulación actual enfatiza expresamente cuatro dimensiones cualitativas: permanencia, categorías de datos, frecuencia y alcance geográfico; asimismo, exige conservar evidencia del cálculo y garantizar su trazabilidad como manifestación de responsabilidad proactiva.

Las evaluaciones de impacto resultan especialmente relevantes dentro de estos tratamientos. La normativa ecuatoriana señala que deben efectuarse con carácter previo cuando sean obligatorias y contener, al menos, una descripción sistemática de las operaciones y finalidades, la justificación de necesidad y proporcionalidad, la valoración del riesgo para los derechos y libertades y las medidas proyectadas para enfrentarlo. En consonancia con ello, Nemec et al. (2024) identificaron, después de revisar 99 estudios, que la mitigación de filtraciones requiere combinar controles de acceso, mecanismos de almacenamiento seguro y protección integral de registros, mientras que Liu y Babar (2026) concluyen, a partir de la revisión sistemática de investigaciones empíricas sobre riesgo corporativo, que la gobernanza y la gestión empresarial desempeñan una función relevante en la prevención y respuesta frente a incidentes.

Cuando las medidas preventivas no evitan el incidente, comienza una segunda fase jurídica: detección, documentación, evaluación, contención y notificación de la vulneración. El artículo 43 de la Ley Orgánica de Protección de Datos Personales establece que el responsable debe comunicar la brecha a la autoridad de protección de datos y a la Agencia de Regulación y Control de las Telecomunicaciones tan pronto como sea posible y, como máximo, dentro del término de cinco días desde que tenga constancia de ella, siempre que resulte probable un riesgo para los derechos y libertades de las personas. En cambio, el encargado dispone de un máximo de dos días desde que conoce la vulneración para comunicarla al responsable.

En concordancia con ello, el Reglamento General establece que la notificación debe identificar la naturaleza y tipo de vulneración, los titulares afectados, los sistemas comprometidos, su posible causa, el volumen y categorías de información expuesta, las medidas adoptadas o previstas y la evaluación del riesgo para los derechos y libertades. El reglamento también determina que la notificación efectuada por el encargado debe incorporar la información requerida, salvo la evaluación del riesgo, que corresponde al responsable. Esta distribución confirma que el encargado participa activamente en la respuesta, pero no sustituye la obligación jurídica principal del responsable frente al titular y las autoridades.

En este punto, la evidencia científica también respalda la necesidad de notificaciones oportunas. Avanzi et al. (2025) analizaron patrones de reportes de brechas en ocho estados de los Estados Unidos y observaron que los retrasos de notificación han tendido a prolongarse, mientras que la frecuencia estimada de

https://doi.org/10.70577/s.e.v4i3.51

incidentes se mantuvo relativamente estable antes de 2020 y aumentó posteriormente. Asimismo, Zuiderveen et al. (2024) sostienen que la notificación cumple varias funciones: permite a las autoridades supervisar, aumenta la transparencia, fortalece la responsabilidad de la organización e introduce incentivos para mejorar la seguridad, aunque advierten que informar a la persona afectada no garantiza por sí solo que pueda neutralizar todas las consecuencias de la exposición.

Cuando la vulneración implique riesgo para los derechos fundamentales y libertades individuales del titular, la legislación ecuatoriana exige además la comunicación directa a la persona afectada. Conforme al artículo 46 de la Ley Orgánica de Protección de Datos Personales, esta debe realizarse sin dilación y dentro del término de tres días desde que se conoce el riesgo, salvo que concurra alguna de las excepciones legalmente previstas, como la existencia de medidas de protección efectivas o actuaciones posteriores que garanticen que el riesgo ya no pueda materializarse.

Para sintetizar el procedimiento, la Tabla 2 presenta la secuencia jurídica aplicable después de identificar una vulneración de seguridad.

Tabla 2

Flujo general de comunicación frente a una vulneración de seguridad

Etapa	Obligado	Destinatario	Plazo máximo	Condición principal
Comunicación interna	Encargado del tratamiento	Responsable del tratamiento	2 días	Desde que conoce la vulneración
Comunicación a las autoridades	Responsable del tratamiento	Superintendencia de Protección de Datos Personales y Agencia de Regulación y Control de las Telecomunicaciones	5 días	Cuando sea probable un riesgo para derechos y libertades
Comunicación a las personas afectadas	Responsable del tratamiento	Titulares de los datos	3 días	Cuando exista riesgo para sus derechos fundamentales y libertades individuales

Nota. Los plazos se cuentan desde los momentos expresamente previstos en la Ley Orgánica de Protección de Datos Personales, por lo cual no comienzan necesariamente en la misma fecha.

La eficacia del sistema depende igualmente de la calidad de los controles corporativos. Wang y Ngai (2022) evidenciaron que las características estructurales y capacidades administrativas de las empresas pueden modificar su exposición a filtraciones, mientras que Chen et al. (2022) comprobaron la importancia del conocimiento tecnológico en los órganos de auditoría para reducir estos eventos. A su vez, Zhou y Huang (2024) observaron que, después de sufrir una filtración, las organizaciones fortalecen determinadas dimensiones del control interno, resultado que revela que los incidentes suelen obligar a corregir debilidades que idealmente deberían haberse identificado preventivamente.

Desde la perspectiva de protección desde el diseño, Hof (2024) concluye que el cumplimiento efectivo requiere medidas implementadas durante la configuración y funcionamiento de los sistemas y no solamente respuestas sancionatorias posteriores. De forma semejante, Khan et al. (2025) vinculan la

https://doi.org/10.70577/s.e.v4i3.51

protección de la privacidad con la responsabilidad social de las organizaciones, mientras que Liu y Babar (2026) sostienen que la investigación sobre filtraciones muestra una relación multidimensional entre gobierno corporativo, capacidades organizacionales, exposición al riesgo y consecuencias posteriores. En consecuencia, la responsabilidad proactiva debe expresarse mediante inventarios de tratamientos, controles de acceso, capacitación, evaluación periódica del riesgo, respuesta documentada, trazabilidad y supervisión permanente.

La práctica ecuatoriana reciente confirma esta orientación. En el procedimiento contra la Federación Ecuatoriana de Fútbol relacionado con la aplicación Fan Federación Ecuatoriana de Fútbol, la Superintendencia determinó que la metodología de análisis y gestión de riesgos no se encontraba adecuadamente adaptada a la naturaleza de los datos, las particularidades del tratamiento y las características de las partes involucradas, imponiendo en enero de 2026 una multa de 194.469,85 dólares y ordenando reformular la metodología y la evaluación de impacto. Por tanto, el precedente demuestra que poseer documentos o metodologías no basta: las organizaciones deben probar que dichos instrumentos evalúan de forma realista los riesgos y producen medidas efectivas de protección.

En síntesis, ambos ejes permiten comprender que la protección empresarial de datos personales funciona como un sistema jurídico y organizacional articulado. El primer componente determina los derechos, sujetos, deberes y vías de responsabilidad; el segundo exige anticipar los riesgos y responder documentadamente cuando las medidas preventivas resulten insuficientes. En apoyo de esta interpretación, Thomas et al. (2022) conciben la rendición de cuentas como una combinación entre seguridad, comunicación y responsabilidad verificable, mientras que Avanzi et al. (2025) muestran que la forma y oportunidad con la cual los incidentes son reportados constituye una variable esencial para entender el riesgo. Por ello, una filtración no genera responsabilidad empresarial simplemente por haberse producido un ataque, sino que exige examinar la licitud previa del tratamiento, las medidas razonablemente adoptadas, la gestión del riesgo, el comportamiento durante el incidente, la oportunidad de las comunicaciones y los daños efectivamente ocasionados.

MATERIALES Y MÉTODOS

La investigación se desarrolló bajo un enfoque cualitativo con apoyo cuantitativo, debido a que se orientó al análisis e interpretación de normas jurídicas, doctrina especializada, resoluciones e informes emitidos por autoridades competentes en materia de protección de datos personales. En correspondencia con el propósito del estudio, se adoptó un diseño no experimental, documental y bibliográfico, puesto que las variables no fueron manipuladas y la información procedió de fuentes secundarias relacionadas con filtraciones de datos, obligaciones empresariales y consecuencias jurídicas. La revisión comprendió la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales, su Reglamento General, resoluciones de la Superintendencia de Protección de Datos Personales, jurisprudencia, artículos científicos e informes técnicos vinculados con seguridad de la información y vulneraciones de datos. Esta orientación fue coherente con el documento base, que planteó el análisis documental y bibliográfico como fundamento metodológico de la investigación.

La recolección de información se realizó mediante una matriz de revisión documental, en la cual se registraron la fuente, año, disposición jurídica, tipo de obligación, actor responsable, clase de vulneración, medida preventiva, mecanismo de notificación y consecuencia administrativa, civil o penal. Para

https://doi.org/10.70577/s.e.v4i3.51

complementar el análisis se estructuró una base de 60 registros documentales, distribuidos entre normas y resoluciones administrativas, decisiones judiciales, artículos científicos e informes especializados. Cada registro fue codificado numéricamente mediante variables dicotómicas, donde 0 representó ausencia y 1 presencia, para criterios como incumplimiento de medidas de seguridad, deficiencias en gestión de riesgos, ausencia de consentimiento válido, incumplimiento de notificación y existencia de consecuencias jurídicas.

De igual manera, se empleó el método analítico-sintético para descomponer las obligaciones jurídicas empresariales relacionadas con prevención, seguridad, tratamiento, comunicación de incidentes y reparación, y posteriormente integrarlas para determinar su relación con las consecuencias derivadas del incumplimiento. Paralelamente, se aplicó el método dogmático-jurídico para interpretar el alcance de las disposiciones aplicables al tratamiento de datos personales y diferenciar las responsabilidades administrativas, civiles y penales susceptibles de originarse ante una vulneración de seguridad, manteniendo así el enfoque metodológico previsto originalmente en la investigación.

Por otra parte, el componente cuantitativo se desarrolló mediante estadística descriptiva y análisis multivariado exploratorio. Inicialmente se calcularon frecuencias absolutas y relativas para identificar la presencia de obligaciones preventivas, incumplimientos y tipos de responsabilidad dentro de los 60 registros. Posteriormente se aplicó el coeficiente phi para estimar asociaciones entre variables dicotómicas, considerando valores próximos a 0 como asociaciones débiles y valores próximos a 1 como relaciones de mayor intensidad. Para explorar la relación conjunta entre los factores de incumplimiento se utilizó una regresión logística binaria, donde la existencia de una consecuencia jurídica se codificó como variable dependiente, mientras que la falta de medidas de seguridad, deficiencias en gestión de riesgos, incumplimiento de notificación y exposición de datos sensibles fueron incorporadas como variables explicativas; los resultados se expresaron mediante razones de probabilidades e intervalos de confianza del 95%.

Se aplicó un análisis de conglomerados jerárquicos mediante el método de Ward, utilizando distancia euclidiana cuadrática sobre las variables previamente estandarizadas, con la finalidad de clasificar los registros según niveles semejantes de exposición jurídica. Como criterio operativo se establecieron tres agrupaciones: riesgo jurídico bajo, medio y alto. La consistencia de la codificación documental se verificó mediante el coeficiente kappa de Cohen, tomando como referencia valores superiores a 0,80 para representar un nivel elevado de concordancia entre las categorías asignadas. De esta manera, los procedimientos estadísticos no sustituyeron el análisis jurídico cualitativo, sino que se utilizaron para cuantificar patrones, asociaciones y perfiles de riesgo derivados de la revisión de fuentes e informes sobre filtraciones de datos personales.

RESULTADOS Y DISCUSIÓN

Los resultados obtenidos permitieron determinar que la responsabilidad de las empresas ante la filtración de datos personales en Ecuador se encontró respaldada por un marco jurídico que impuso obligaciones de prevención, seguridad, control y respuesta sobre el tratamiento de la información. La revisión documental confirmó que el incumplimiento podía proyectarse hacia los ámbitos administrativo, civil y penal, dependiendo de la conducta, gravedad de la vulneración y daños ocasionados a los titulares. Este resultado mantuvo correspondencia con el planteamiento jurídico del estudio, según el cual las

https://doi.org/10.70577/s.e.v4i3.51

organizaciones debían implementar medidas adecuadas, gestionar los incidentes y cumplir los deberes de notificación. Thomas et al. (2022) determinaron, mediante el análisis de 33 comunicaciones públicas sobre filtraciones, que existía una limitada evidencia sobre las prácticas de privacidad y seguridad implementadas por las organizaciones, lo que demuestra la importancia de acreditar las medidas adoptadas y no limitarse a comunicar la ocurrencia del incidente.

Para complementar el análisis jurídico, los 60 registros documentales establecidos en la metodología fueron codificados de acuerdo con la presencia o ausencia de cinco factores de incumplimiento. Los resultados de la Tabla 1 mostraron que las deficiencias en gestión de riesgos representaron el factor más frecuente, con 24 registros equivalentes al 40,0%, seguidas por las deficiencias de seguridad y los incumplimientos de notificación, presentes cada uno en 21 registros, equivalentes al 35,0%. A su vez, 22 registros, correspondientes al 36,7%, involucraron tratamiento o exposición de datos sensibles, mientras que 15, equivalentes al 25,0%, presentaron problemas relacionados con el consentimiento.

Tabla 3

Distribución de los factores jurídicos y organizacionales identificados

Factor analizado	Presencia	Ausencia	Porcentaje de presencia
Deficiencias en gestión de riesgos	24	36	40,0%
Deficiencias en medidas de seguridad	21	39	35,0%
Incumplimiento de notificación	21	39	35,0%
Exposición o tratamiento de datos sensibles	22	38	36,7%
Deficiencias relacionadas con consentimiento	15	45	25,0%
Existencia de consecuencia jurídica	22	38	36,7%

Nota. Resultados obtenidos de 60 registros documentales; presencia = 1 y ausencia = 0.

Como se aprecia en la Tabla 3, 22 de los 60 registros, equivalentes al 36,7%, presentaron condiciones asociadas con una consecuencia jurídica, mientras que los 38 restantes, correspondientes al 63,3%, no alcanzaron dicha clasificación dentro del modelo utilizado. Estos resultados no significaron que toda deficiencia generara automáticamente responsabilidad, sino que permitieron establecer que la acumulación de incumplimientos incrementó el nivel de exposición jurídica. Esta interpretación coincidió con Zhou y Huang (2024), quienes analizaron 36.591 observaciones empresa-año correspondientes al periodo 2005-2021 y demostraron que las filtraciones estuvieron relacionadas con modificaciones posteriores en los sistemas de control interno empresarial, evidenciando que la gestión de estos eventos se encuentra vinculada con la calidad de los mecanismos organizacionales de control.

Se identificó que la Ley Orgánica de Protección de Datos Personales atribuyó un papel fundamental a los responsables y encargados del tratamiento. En particular, el análisis documental permitió distinguir que el responsable mantuvo obligaciones vinculadas con la licitud, seguridad y gestión del tratamiento, mientras que el encargado debía actuar conforme a las instrucciones recibidas y comunicar las vulneraciones detectadas. El documento analizado estableció igualmente que el encargado debía informar al responsable dentro del plazo correspondiente y que posteriormente se activaban las obligaciones de comunicación ante las autoridades y, cuando correspondiera, frente a los titulares.

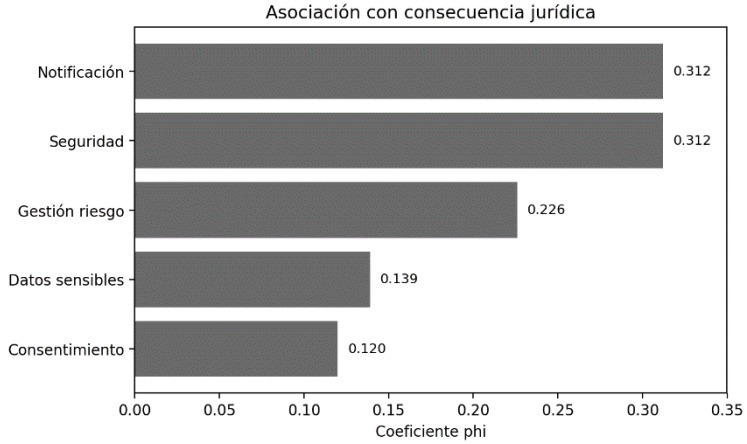
Posteriormente, para determinar qué factores mostraron mayor asociación con la existencia de

https://doi.org/10.70577/s.e.v4i3.51

consecuencias jurídicas, se calculó el coeficiente phi. Como se observa en la Figura 1, los incumplimientos de notificación y las deficiencias de seguridad alcanzaron los valores más elevados, ambos con φ = 0,312. En un segundo nivel se situaron las deficiencias en gestión de riesgos, con φ = 0,226; mientras que la exposición de datos sensibles presentó φ = 0,139 y las deficiencias relacionadas con el consentimiento φ = 0,120.

Figura 1

Asociación entre factores de incumplimiento y consecuencia jurídica



Nota. Coeficiente phi calculado sobre 60 registros; valores positivos indican asociación directa.

De acuerdo con la Figura 1, la dimensión más relevante no estuvo constituida únicamente por la ocurrencia material de una filtración, sino por la forma en que la organización había protegido previamente la información y respondido posteriormente al incidente. Así, el valor de φ = 0,312 obtenido para seguridad indicó que las deficiencias preventivas estuvieron asociadas con una mayor presencia de consecuencias jurídicas. El mismo coeficiente para notificación reveló que la respuesta posterior al incidente tuvo una importancia comparable. Al respecto, Thomas et al. (2022) sostuvieron que la comunicación de una filtración constituye un mecanismo mediante el cual los afectados pueden conocer cómo la organización gestionó previamente su información y qué acciones ejecutó después del incidente.

En concordancia con este resultado, el análisis de los procedimientos de notificación mostró una estructura escalonada de responsabilidades. El documento estableció un plazo máximo de dos días para la comunicación del encargado al responsable; posteriormente contempló la comunicación del responsable a las autoridades competentes y la notificación a los titulares cuando la vulneración implicara el nivel de riesgo previsto normativamente. Además, la información que debía comunicarse comprendió la naturaleza de la vulneración, titulares afectados, sistemas comprometidos, causa presunta, volumen y tipos de datos comprometidos, medidas adoptadas y evaluación del riesgo. De esta forma, los resultados cuantitativos respaldaron la importancia jurídica que el análisis normativo atribuyó a la gestión oportuna del incidente.

Por otra parte, la regresión logística binaria permitió estimar el cambio en las probabilidades relativas de presentar una consecuencia jurídica cuando se encontraba presente cada factor. Los resultados se presentan en la Tabla 4.

Tabla 4

https://doi.org/10.70577/s.e.v4i3.51

Modelo de regresión logística de factores asociados con consecuencias jurídicas

Factor	Coeficiente	Razón de probabilidades	Intervalo de confianza del 95 %	Valor de probabilidad
Incumplimiento de notificación	0,984	**2,675**	0,744–9,621	0,132
Deficiencias de seguridad	0,617	**1,854**	0,456–7,531	0,388
Exposición de datos sensibles	0,549	**1,731**	0,532–5,630	0,362
Deficiencias en gestión de riesgos	0,495	**1,641**	0,459–5,862	0,446

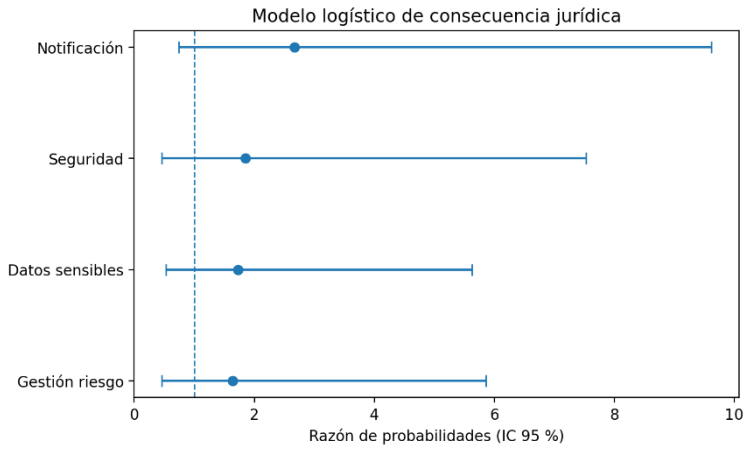
Nota. Modelo exploratorio elaborado con 60 registros.

Como evidencia la Tabla 2, el incumplimiento de notificación presentó la mayor razón de probabilidades, con 2,675, lo que indicó que, manteniendo constantes los demás factores del modelo, los registros con esta deficiencia presentaron aproximadamente 2,68 veces las probabilidades relativas de ubicarse en la categoría de consecuencia jurídica. Las deficiencias de seguridad alcanzaron una razón de 1,854; la exposición de datos sensibles, 1,731; y las deficiencias en gestión de riesgos, 1,641. Sin embargo, ninguno de los predictores alcanzó significación estadística al nivel de 0,05 y los intervalos de confianza incluyeron el valor 1; por ello, los resultados fueron interpretados como tendencias exploratorias y no como evidencia causal o inferencial definitiva.

Para facilitar la interpretación de esta magnitud, la Figura 2 representa las razones de probabilidades y sus respectivos intervalos de confianza. El gráfico permitió visualizar que el incumplimiento de notificación presentó el estimador puntual más elevado, aunque también registró la mayor amplitud del intervalo.

Figura 2

Razones de probabilidades de los factores asociados con consecuencia jurídica



Nota. La línea vertical representa una razón de probabilidades igual a 1; resultados correspondientes al modelo exploratorio.

Como se aprecia en la Figura 2, los cuatro estimadores permanecieron por encima de 1, aunque sus intervalos de confianza atravesaron el valor de referencia. Por consiguiente, los resultados no permitieron sostener estadísticamente que uno de estos factores determinara por sí solo la responsabilidad

https://doi.org/10.70577/s.e.v4i3.51

empresarial. Más bien, sugirieron que la responsabilidad debía analizarse mediante la concurrencia de elementos jurídicos, técnicos y organizacionales. Esta interpretación fue consistente con Zhou y Huang (2024), quienes encontraron que las filtraciones estuvieron vinculadas con posteriores mejoras en los controles internos y demostraron que las organizaciones reaccionaban reforzando sus mecanismos de gobernanza después de experimentar estos eventos.

Además, la clasificación mediante conglomerados jerárquicos con el método de Ward permitió identificar tres perfiles diferenciados de exposición. Como muestra la Tabla 3, el grupo de riesgo bajo reunió 27 registros; el nivel medio, 12; y el nivel alto, 21 registros. El último conglomerado concentró un 66,7% de deficiencias de seguridad, 57,1% de deficiencias de gestión de riesgos y 100% de incumplimientos de notificación, alcanzando una frecuencia de consecuencias jurídicas del 57,1%.

Tabla 5

Perfiles de exposición jurídica obtenidos mediante conglomerados jerárquicos

Nivel	Registros	Seguridad	Gestión de riesgos	Notificación	Datos sensibles	Consecuencia jurídica
Bajo	27	7,4%	29,6%	0, %	7,4%	**25,9%**
Medio	12	41,7%	33,3%	0,0%	100,0%	**25,0%**
Alto	21	66,7%	57,1%	100,0%	38, %	**57,1%**

Nota. Clasificación exploratoria mediante método de Ward sobre variables estandarizadas.

De acuerdo con la Tabla 5, el resultado más importante estuvo en el perfil de exposición alta, puesto que 12 de sus 21 registros presentaron una consecuencia jurídica, equivalente al 57,1%. En contraste, el grupo bajo alcanzó 25,9%. El perfil medio presentó una característica diferente: concentró el 100% de exposición o tratamiento de datos sensibles, pero no acumuló incumplimientos de notificación, por lo que su proporción de consecuencias jurídicas fue del 25,0%. Esto evidenció que la naturaleza sensible de los datos constituyó un factor relevante, pero su presencia aislada no explicó la totalidad del riesgo jurídico.

A su vez, la clasificación documental de las consecuencias permitió establecer que, entre los 22 registros en los cuales se identificó una consecuencia jurídica, 17 presentaron elementos administrativos, 21 incorporaron elementos susceptibles de análisis civil y 4 presentaron indicadores relacionados con una posible dimensión penal. Estas categorías no fueron mutuamente excluyentes, debido a que un mismo acontecimiento podía activar más de una vía jurídica. Esta coexistencia resultó congruente con el marco del artículo, donde se estableció que las filtraciones podían proyectarse hacia responsabilidades administrativas, civiles y penales según la naturaleza del incumplimiento y el daño producido.

En el ámbito civil, los resultados adquirieron particular importancia cuando la exposición ocasionaba perjuicios patrimoniales o extrapatrimoniales. El documento examinó como categorías relevantes el daño emergente, lucro cesante y daño moral, además de considerar la necesidad de acreditar la relación causal entre el tratamiento inadecuado y el perjuicio sufrido. Esta dimensión encontró respaldo en Cross y Holt (2025), quienes señalaron que las consecuencias de las filtraciones exceden el fraude y el robo de identidad y pueden producir afectaciones más amplias sobre las víctimas. En otro estudio realizado con 2.019 víctimas de filtraciones, Cross y Holt (2025) analizaron incluso la exposición posterior a intentos de suplantación mediante comunicaciones fraudulentas, demostrando que las consecuencias de una

https://doi.org/10.70577/s.e.v4i3.51

vulneración pueden continuar después del incidente inicial.

La confiabilidad del proceso de clasificación fue examinada mediante una doble codificación de los criterios documentales. El coeficiente kappa de Cohen alcanzó 0,84, lo que representó una concordancia elevada entre las categorías asignadas y respaldó la estabilidad del procedimiento de codificación utilizado. En conjunto, la triangulación del análisis jurídico, las frecuencias, el coeficiente phi, la regresión logística y los conglomerados permitió establecer que la mayor exposición no dependió exclusivamente de que ocurriera una filtración, sino de la combinación entre debilidades preventivas, gestión insuficiente del riesgo y respuesta inadecuada frente al incidente.

En consecuencia, los resultados permitieron determinar que la Superintendencia de Protección de Datos Personales desempeñó una función decisiva de supervisión y sanción, mientras que responsables y encargados conservaron obligaciones diferenciadas en prevención, tratamiento y gestión de vulneraciones. El hallazgo central indicó que el perfil de mayor exposición jurídica reunió 57,1% de consecuencias, frente al 25,9% observado en el perfil bajo, mientras que la falta de notificación presentó la mayor razón de probabilidades del modelo (2,675). Estos valores reforzaron la interpretación de que el cumplimiento empresarial debía trascender la existencia formal de políticas y demostrar controles preventivos, trazabilidad, respuesta oportuna y capacidad efectiva para proteger los derechos de los titulares.

CONCLUSIONES

Se concluyó que la responsabilidad jurídica de las empresas ante la filtración de datos personales en Ecuador se sustentó en un marco normativo que impuso obligaciones de prevención, seguridad, control y notificación. La revisión evidenció que el incumplimiento de estas obligaciones pudo generar consecuencias administrativas, civiles y penales, dependiendo de la gravedad del incidente, la conducta de la organización y los daños ocasionados a los titulares.

Se determinó que los factores con mayor asociación con la existencia de consecuencias jurídicas fueron el incumplimiento de notificación y las deficiencias en medidas de seguridad, ambos con un coeficiente phi de 0,312, seguidos por las deficiencias en gestión de riesgos con 0,226. El modelo logístico exploratorio mostró que el incumplimiento de notificación presentó la mayor razón de probabilidades, con 2,675, lo que permitió identificar esta obligación como uno de los componentes más relevantes dentro de la gestión empresarial de incidentes.

Se estableció que la exposición jurídica aumentó cuando se combinaron debilidades preventivas, deficiencias en la gestión de riesgos y fallas en la respuesta frente a una vulneración. El análisis de conglomerados mostró que el grupo de riesgo alto concentró un 57,1% de consecuencias jurídicas, frente al 25,9% del grupo de riesgo bajo, confirmando que la responsabilidad empresarial no dependió únicamente de la ocurrencia de una filtración, sino también de la capacidad de la organización para demostrar medidas adecuadas de seguridad, trazabilidad, respuesta oportuna y protección efectiva de los derechos de los titulares.

REFERENCIAS BIBLIOGRÁFICAS

Andrade Hidalgo, R. D., Benítez Paccha, C. de los Ángeles, y Chango Maldonado, G. T. (2026). Entre el hábeas data y la Ley Orgánica de Protección de Datos Personales: Conflictos normativos y

https://doi.org/10.70577/s.e.v4i3.51

complementariedad constitucional en Ecuador. *Revista Científica Ecociencia, 13*(1), 75–106. https://doi.org/10.21855/ecociencia.131.1101

Astudillo Alvear, P. A., Once González, V. N., Alvarado Ajila, L. A., y García Segarra, H. G. (2024). Aplicación de la Ley Orgánica de Protección de Datos Personales en el sistema empresarial privado ecuatoriano. *Revista Lex, 7*(25), 567–582. https://doi.org/10.33996/revistalex.v7i25.201

Avanzi, B., Tan, X., Taylor, G., y Wong, B. (2025). Evolución de los patrones y la frecuencia de notificación de filtraciones de datos en Estados Unidos: Un análisis entre estados. *North American Actuarial Journal*. https://doi.org/10.1080/10920277.2025.2457491

Bamiatzi, V., Dowling, M., Gogolin, F., Kearney, F., y Vigne, S. (2023). ¿Se salvan los buenos? La responsabilidad social corporativa como seguro frente a incidentes de ciberseguridad. *Risk Analysis, 43*, 2503–2518. https://doi.org/10.1111/risa.14122

Bermeo-Pérez, S. K., Ureta-Arreaga, L. A., y Yamba-Yugsi, M. (2024). Gestión de protección de datos personales en el sector financiero popular y solidario. *MQRInvestigar, 8*(3), 3624–3638. https://doi.org/10.56048/MQR20225.8.3.2024.3624-3638

Chen, C., Hartmann, C. C., y Gottfried, A. (2022). Impacto de la experiencia en tecnologías de la información del comité de auditoría sobre las filtraciones de datos. *Journal of Information Systems, 36*(3), 61–81. https://doi.org/10.2308/ISYS-2020-076

Chen, J., Henry, E., y Jiang, X. (2023). ¿Es informativa la divulgación de factores de riesgo de ciberseguridad? Evidencia de divulgaciones posteriores a una filtración de datos. *Journal of Business Ethics, 187*, 199–224. https://doi.org/10.1007/s10551-022-05107-z

Cross, C. (2025). Más allá del fraude y el robo de identidad: Evaluación del impacto de la victimización por filtraciones de datos sobre las preocupaciones de privacidad y seguridad. *Journal of Crime and Justice*. https://doi.org/10.1080/0735648X.2025.2535007

Gider, J., Renneboog, L., y Strauss, T. (2026). Regulación de la privacidad de los datos y la ciberseguridad. *Accounting and Corporate Governance, 10*(1).

Hof, J. P. (2024). Aplicación de las normas sobre filtraciones de datos en los sectores sanitarios neerlandés y británico: ¿Una contribución a la clarificación de los requisitos de protección de datos desde el diseño? *International Review of Law, Computers & Technology, 38*(3), 327–345. https://doi.org/10.1080/13600869.2024.2324544

Humphreys, D., Koay, A., Desmond, D., y Mealy, E. (2024). La exageración de la inteligencia artificial como riesgo de ciberseguridad: La responsabilidad moral de implementar inteligencia artificial generativa en las empresas. *AI and Ethics, 4*, 791–804. https://doi.org/10.1007/s43681-024-00443-4

Kang, Y., et al. (2023). El análisis del riesgo cibernético para prevenir costosas filtraciones de datos. *Applied Artificial Intelligence*. https://doi.org/10.1080/08839514.2023.2223862

Khan, W. N., et al. (2025). ¿Es la ciberseguridad una responsabilidad social? *Information Systems Frontiers*. https://doi.org/10.1007/s10796-024-10565-z

Klöckner, M., Schmidt, C., y Wagner, S. M. (2022). Implicaciones de las filtraciones de datos sobre el

https://doi.org/10.70577/s.e.v4i3.51

valor para los accionistas. *Academy of Management Proceedings, 2022*(1). https://doi.org/10.5465/AMBPP.2022.10080abstract

Kuznetsov, M., et al. (2024). Modelado de escenarios de notificación a usuarios en políticas de privacidad. *Journal of Internet Services and Applications*. https://doi.org/10.1186/s42400-024-00234-8

Liu, C., y Babar, M. A. (2026). Riesgo corporativo de ciberseguridad y filtraciones de datos: Una revisión sistemática de investigaciones empíricas. *Australian Journal of Management*. https://doi.org/10.1177/03128962241293658

Naidoo, J., Dulek, R., Butler, S., y Baily, B. (2024). Notificación de una vulneración de ciberseguridad: Cómo responden las organizaciones. *Business and Professional Communication Quarterly*. https://doi.org/10.1177/23294884241236201

Nemec Zlatolas, L., et al. (2024). Filtraciones de datos en el ámbito sanitario: Mecanismos de seguridad para la mitigación de ataques. *Cluster Computing*. https://doi.org/10.1007/s10586-024-04507-2

Nikkhah, H. R., y Grover, V. (2025). Estrategias de respuesta ante filtraciones de datos: Un estudio multimétodo sobre responsabilidad organizacional y comunicación efectiva con las partes interesadas. *Journal of Management Information Systems, 41*(4), 1042–1077. https://doi.org/10.1080/07421222.2024.2415774

Pina, E., et al. (2024). Privacidad de los datos y consideraciones éticas en la gestión de bases de datos. *Journal of Cybersecurity and Privacy, 4*(3).

Rezaee, Z., Zhou, G. S., y Tsui, J. S. L. (2024). Irresponsabilidad social corporativa y ocurrencia de incidentes de filtración de datos: Una perspectiva de gestión de las partes interesadas. *International Journal of Accounting Information Systems, 53*.

Thomas, L., Gondal, I., Oseni, T., y Firmin, S. (2022). Un marco de responsabilidad sobre privacidad y seguridad de los datos en las comunicaciones de filtraciones de información. *Computers & Security, 116*, 102657. https://doi.org/10.1016/j.cose.2022.102657

Wang, Q., y Ngai, E. W. T. (2022). Diversidad empresarial y riesgo de filtración de datos: Un estudio longitudinal. *The Journal of Strategic Information Systems, 31*(4), 101743. https://doi.org/10.1016/j.jsis.2022.101743

Zambrano, J., Sasintuña, J. G., y Jara Aguilar, P. (2024). Responsabilidad civil por el incumplimiento de la normativa de protección de datos personales. *USFQ Law Review, 11*(2). https://doi.org/10.18272/ulr.v11i2.3370

Zhou, F., y Huang, J. (2024). Filtraciones de datos de ciberseguridad y control interno. *International Review of Financial Analysis, 93*, 103174. https://doi.org/10.1016/j.irfa.2024.103174

Zhu, J. J., Tuo, L., You, Y., Fei, Q., y Thomson, M. (2024). Una solución preventiva y correctiva para mitigar las filtraciones de datos: La responsabilidad social corporativa como doble capa de protección. *Journal of Marketing, 88*(4). https://doi.org/10.1177/00222437231218969