RELIGACIÓN
REVISTA

Impacto de la Ley Orgánica de Protección de Datos y la ISO 27001 en la ciberseguridad empresarial ecuatoriana

Impact of the Organic Data Protection Law and ISO 27001 on Ecuadorian Corporate Cybersecurity

Franklin Raúl Curay Ulcuango, Cristhian Humberto Flores Urgilés

Resumen

La progresiva recopilación y digitalización de datos continúan aumentando los riesgos asociados a la seguridad de la información en Ecuador y el mundo. Con esta premisa, marcos regulatorios como la Ley Orgánica de Protección de Datos Personales (LOPDP) y la norma ISO/IEC 27001 sobresalen para fortalecer la ciberseguridad empresarial. Sin embargo, la implementación de estos marcos presenta desafíos importantes como los costos elevados, falta de capacitación y concienciación, entre otros. La presente investigación analiza el cumplimiento de la LOPDP y la adopción de la ISO 27001 en empresas ecuatorianas, evaluando su impacto en la reducción de incidentes provocados por ataques cibernéticos. Se identifican las principales vulnerabilidades que enfrentan las organizaciones, resaltando la necesidad de sanciones efectivas y políticas de seguridad robustas. Mediante un análisis de casos, se evidencia que la madurez en la gestión de riesgos fluctúa drásticamente entre sectores, siendo las entidades financieras las más avanzadas y las pequeñas empresas las más atrasadas. Los hallazgos sugieren que una implementación efectiva de estos marcos puede mejorar el cumplimiento de la Ley y la protección de datos, por lo que se recomienda fomentar incentivos para implementarlos y así fortalecer las estrategias de mitigación de riesgos a nivel organizacional.

Palabras clave: Ley de protección de datos; Protección de datos; ISO 27001; Ciberseguridad empresarial; Ciberseguridad.

Franklin Raúl Curay Ulcuango
Universidad Católica de Cuenca | Cuenca | Ecuador | franklin.curay.82@est.ucacue.edu.ec
https://orcid.org/0009-0003-3136-0551
Cristhian Humberto Flores Urgilés
Universidad Católica de Cuenca | Cuenca | Ecuador | chfloresu@ucacue.edu.ec
https://orcid.org/0000-0002-0465-3370

http://doi.org/10.46652/rgn.v11i49.1588
ISSN 2477-9083
Vol. 11 No. 49, enero-marzo, 2026, e2601588
Quito, Ecuador

Enviado: julio 30, 2025
Aceptado: septiembre 04, 2025
Publicado: noviembre 25, 2025
Publicación Continua

Abstract

The progressive collection and digitalization of data continue to increase the risks associated with information security in Ecuador and worldwide. Based on this premise, regulatory frameworks such as the Organic Law on Personal Data Protection (LOPDP) and the ISO/IEC 27001 standard stand out as key mechanisms for strengthening corporate cybersecurity. However, the implementation of these frameworks presents significant challenges, including high costs, lack of training, and limited awareness, among others. This study analyzes the compliance with the LOPDP and the adoption of ISO/IEC 27001 in Ecuadorian companies, assessing their impact on reducing incidents caused by cyberattacks. The main vulnerabilities faced by organizations are identified, highlighting the need for effective sanctions and robust security policies. Through a case-based analysis, the research reveals that the level of maturity in risk management varies significantly across sectors, with financial institutions being the most advanced and small enterprises the most lagging. The findings suggest that an effective implementation of these frameworks can enhance legal compliance and data protection. Therefore, it is recommended to promote incentives for their adoption, thereby strengthening organizational risk mitigation strategies.

Keywords: Data protection law; Data protection; ISO 27001; Enterprise Cybersecurity; Cybersecurity.

Introducción

En la era digital, la protección de datos personales y la ciberseguridad han cobrado una importancia crucial debido al incremento exponencial de amenazas informáticas y, el uso inadecuado de los datos personales y organizacionales. Los principios de confidencialidad, integridad y disponibilidad de la información se han visto comprometidos por la gran cantidad de ataques cibernéticos y esto ha puesto en jaque a las empresas y sus operaciones. La información es considerada un activo estratégico y, como tal, requiere medidas adecuadas de protección contra accesos no autorizados y usos indebidos (Juan Rodríguez, 2019).

No existe un sistema 100% seguro o al menos hasta la presente fecha no se conoce de un sistema 100% seguro, dicho esto, las vulnerabilidades que tienen o que puedan tener los sistemas son explotadas por atacantes, mismos que utilizan técnicas especializadas para irrumpir en los sistemas y robar, secuestrar, sabotear o destruir la información entre otras cosas. Cabe mencionar que, si un atacante busca lucrar, sus objetivos principales serán empresas que muevan cantidades considerables de dinero y ahí se encuentran empresas públicas o privadas del ámbito financiero, manufacturero, telecomunicaciones, salud, retail y otros. Por otra parte, las empresas que han sido ciberatacadas exitosamente, no solo terminan con pérdidas de información, sino que también acaban con pérdidas económicas y reputacionales.

El acceso no autorizado a la información ha favorecido la ejecución de delitos como la suplantación de identidad, el fraude, la estafa y la realización de transacciones financieras no autorizadas. En respuesta a esta problemática, en el Ecuador se promulgó la Ley Orgánica de Protección de Datos Personales (LOPDP), cuya finalidad es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela (LOPDP, 2021).

Hoy en día, la ISO/IEC 27001 es la cuarta norma ISO más extendida a nivel mundial con casi 45.000 empresas certificadas en 2020 y tiene una tasa de crecimiento del 22% con respecto al año anterior (Podrecca et al., 2022), esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información en el contexto de la organización, incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización (Organización Internacional de Normalización, 2022). No obstante, las barreras económicas y la falta de conocimiento técnico han limitado la adopción de esta norma en Ecuador (Mora et al., 2020).

Con estos antecedentes, esta investigación plantea la siguiente pregunta: ¿Cuál es el impacto del cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) y la implementación de la norma ISO 27001 en la ciberseguridad empresarial ecuatoriana?; y, para responderla se analizarán estadísticas sobre incidencias de ciberseguridad en las empresas ecuatorianas que hayan adoptado la LOPDP y la ISO 27001, empresas que no hayan adoptado la LOPDP y la ISO 27001, y, empresas que solo hayan adoptado la LOPDP o la ISO 27001, esto con el fin de poder identificar tendencias y niveles de exposición. Finalmente, se evaluará el grado de madurez de dichas organizaciones en la gestión de riesgos y su capacidad de respuesta frente a ciberamenazas, considerando las prácticas y mecanismos implementados para la protección de la información (Segundo Toapanta et al., 2020).

La información es uno de los bienes de mayor valor para las organizaciones, por ello la protección de la información empresarial en el Ecuador y el mundo es de vital importancia; normas como la Ley Orgánica de Protección de Datos Personales y la ISO/IEC 27001 contribuyen en la reducción de incidentes relacionados con la confidencialidad, integridad y disponibilidad de la información. Mediante este estudio se evaluará cuan efectivas pueden ser estas normativas, además de identificar los principales factores que influyen en el cumplimiento normativo y las estrategias implementadas por las empresas ecuatorianas para fortalecer la seguridad de la información. Por tanto, con este estudio se podría promover la mejora de la cibercultura empresarial en el país y tender al desarrollo de políticas efectivas para la gestión adecuada de recursos humanos y tecnológicos.

Para una mejor comprensión del estudio realizado, se analizarán los datos de manera cualitativa y cuantitativa. En algunas organizaciones se efectuarán entrevistas y encuestas a personas encargadas de la seguridad informática, seguridad de la información, directivos y expertos en ciberseguridad para conocer de primera mano los beneficios y obstáculos de la implementación de Ley Orgánica de Protección de Datos Personales y la norma ISO/IEC 27001 en el marco de la protección de datos organizacionales; y , para complementar el estudio se examinarán estadísticas sobre ataques cibernéticos en Ecuador, informes de cumplimiento normativo y estudios de caso de empresas certificadas en ISO 27001 (Cecilia Quintana, 2019).

Con los resultados de este estudio se pretende identificar y a la vez sugerir buenas prácticas de implementación de la Ley Orgánica de Protección de Datos Personales y de la norma ISO/IEC 27001. Se prevé que los hallazgos propicien el desarrollo y despliegue de estrategias gubernamentales

y empresariales en pro de la protección de la información mediante el cumplimiento normativo y la adopción de estándares internacionales de seguridad de la información. Asimismo, se busca proporcionar herramientas a las organizaciones ecuatorianas para mejorar su postura de seguridad ante las crecientes amenazas cibernéticas (Segundo Toapanta et al., 2020).

El incumplimiento de las disposiciones previstas en la Ley Orgánica de Protección de Datos Personales acarrea sanciones económicas y este estudio analizará como impactan las multas en la operatividad y la reputación de las organizaciones ecuatorianas. Además, se examinará el nivel de madurez de la gestión de riesgos y/o la efectividad de las normativas vigentes en la prevención de ciberataques. Por último y no menos importante, se deliberará sobre el papel que ejerce el gobierno en el avance de una cultura de ciberseguridad sólida y sustentable en el país.

El conocimiento de las empresas y su personal sobre las regulaciones actuales y su efectividad serán considerados para el estudio, ya que muchas organizaciones cumplen con las normas por temor a las sanciones y no por los beneficios que se obtendrían en la ciberseguridad. Por tanto, los resultados podrían ser tomados como referencia para futuras líneas de estudio en la protección de datos.

En conclusión, actualmente el fortalecimiento de la ciberseguridad, la cibercultura y la seguridad de la información son de gran importancia, y, con este estudio se espera aportar no solo a la literatura existente sino que también a la formulación de políticas públicas y corporativas más eficientes, además de incentivar a las organizaciones a adoptar estándares internacionales de seguridad de la información y a cumplir con las leyes locales de protección de datos y así generar mayor confianza en el ecosistema digital del país.

Metodología

Para ejecutar la investigación sobre el impacto de la LOPDP y la ISO 27001 en la ciberseguridad empresarial ecuatoriana, se adoptó un enfoque mixto que integra métodos cuantitativos y cualitativos. Este abordaje permitió triangular información para obtener una visión comprehensiva del fenómeno de estudio (Jordan Birkner et al., 2023). El componente cuantitativo permitió medir indicadores objetivos vinculados con el nivel de implementación de las normativas, la frecuencia de los incidentes cibernéticos y las sanciones que no han podido ser impuestas. Paralelamente, el componente cualitativo permitió profundizar en las percepciones, desafíos y experiencias de los profesionales encargados de implementar estas normativas en las organizaciones ecuatorianas.

La población de estudio estuvo conformada por empresas públicas y privadas de Ecuador que manejan datos personales como parte de sus operaciones habituales. Se estableció un marco muestral estratificado que incluyó:

- Entidades financieras: 60 bancos y cooperativas de ahorro y crédito registradas en la Superintendencia de Bancos del Ecuador y la Superintendencia de Economía Popular y Solidaria.

- Empresas públicas: 45 instituciones del sector público sujetas a la LOPDP.
- Empresas privadas: 150 medianas y grandes empresas de sectores estratégicos (telecomunicaciones, salud, retail, servicios)

Los criterios de inclusión fueron: organizaciones con más de 50 empleados, que manejen bases de datos personales sensibles, y que lleven operando en Ecuador por más de 3 años. Se excluyeron microempresas y organizaciones sin fines de lucro que no manejen datos personales de terceros.

Las variables independientes principales consideradas en la investigación fueron:

1. **Grado de implementación de la LOPDP**: se evaluó mediante indicadores basados en los requisitos establecidos por la ley, incluyendo la existencia de delegados de protección de datos (DPD/DPO), registros de actividades de tratamiento, mecanismos de consentimiento y procedimientos para ejercer derechos AREOP (Acceso, Rectificación y Actualización, Eliminación, Oposición y Portabilidad) (LOPDP, 2021) .
2. **Nivel de adopción de ISO 27001**: se midió considerando la certificación formal o la implementación de controles basados en esta norma internacional, especialmente aquellos relacionados con la protección de datos personales (AENOR, 2023), y en este contexto en Ecuador se cuenta con el SGSI v3, que es el Sistema de Gestión de Seguridad de la información para las instituciones del Sector Público, éste contiene la Guía para la implementación del EGSI la cual proporciona los lineamientos y requisitos para establecer, implementar y mantener el mejoramiento continuo del Esquema basado en la NTE INEN ISO/IEC 27001 (EGSI v3, 2024).
3. **Variables de contexto organizacional**: tamaño de la empresa, sector económico, años de operación, presupuesto destinado a ciberseguridad y capacitación del personal.

Para la recolección de datos se implementaron las siguientes técnicas e instrumentos:

- Se elaboró un cuestionario con escalas Likert y se encuestó a 130 personas con cargos como Directores de TI, Oficiales de Seguridad, Gerentes de área y DPOs (Delegados de Protección de Datos). El instrumento fue validado mediante prueba piloto para asegurar su confiabilidad (α Cronbach = 0.60) (Jordan Birkner et al, 2023).
- Se entrevistó a 10 personas con cargos como Directores de TI, Oficiales de Seguridad, Ejecutivos con nivel jerárquico superior y DPOs (Delegados de Protección de Datos) para conocer los principales desafíos de la implementación de la LOPDP y la ISO 27001. Cada entrevista tuvo una duración promedio de 30 minutos, de las cuales se tomaron notas y posteriormente se analizaron (Melisa, 2017).

- Se obtuvo el acceso de forma confidencial a informes de cumplimiento normativo, políticas internas y reportes de incidentes de seguridad de 10 organizaciones y se realizó el respectivo análisis.

La recolección de datos se llevó a cabo entre los meses de agosto y octubre de 2025, siguiendo una planificación estructurada que estableció un camino en la aplicación y/o ejecución de los instrumentos antes descritos.

Para el análisis cuantitativo de datos se emplearon las siguientes técnicas estadísticas:

- Media y mediana, cálculo de frecuencias y desviaciones estándar para Cristina Ortega, (2024), resumir las características generales de los datos recolectados.
- Pruebas de chi-cuadrado para analizar relaciones entre variables categóricas, y análisis de varianza (ANOVA) para comparar diferencias significativas entre diferentes sectores empresariales.
- Coeficiente de Pearson para identificar relaciones entre el grado de implementación de normativas y la reducción de incidentes de seguridad.
- Identificación de factores predictores del cumplimiento normativo efectivo.

Los datos cualitativos se analizaron mediante teoría fundamentada, con codificación abierta y axial para identificar categorías emergentes y patrones temáticos (Tania Vives et al., 2021).

La ejecución de la investigación se realizó bajo principios éticos que incluyeron:

- Consentimiento informado, con lo cual todos los participantes aceptaron un consentimiento que explicaba los objetivos de la investigación, uso de los datos y medidas de confidencialidad (Jordan Birkner et al., 2023).
- Protección de datos personales, por lo que se implementó protocolos alineados con la LOPDP para el tratamiento de información recolectada, garantizando la confidencialidad mediante seudonimización de datos (LOPDP, 2021).
- Cumplimiento normativo, en consecuencia, se observaron los principios de minimización de datos y limitados a lo estrictamente necesario, asegurando que solo se recopilaron datos necesarios para los objetivos de la investigación (LOPDP, 2021).

Esta metodología integral permitió generar evidencia sobre el impacto real de las normativas de protección de datos en el ecosistema de ciberseguridad empresarial ecuatoriano, identificando tanto avances como desafíos pendientes en la materia.

Resultados

Cumplimiento de la LOPDP por Sector Empresarial. El análisis del nivel de implementación de la Ley Orgánica de Protección de Datos Personales reveló diferencias significativas entre sectores económicos. Como se muestra en la Tabla 1, el sector financiero presentó el mayor nivel de cumplimiento (78%), mientras que el sector manufacturero mostró el más bajo (34%).

Tabla 1. Nivel de Implementación de la LOPDP por Sector Económico (n=130).

Sector Económico	Porcentaje de Cumplimiento	Empresas con DPD/ DPO Designado	Auditorías Anuales Realizadas
Financiero	78%	93%	75%
Tecnológico	60%	81%	78%
Salud	51%	89%	78%
Retail	47%	54%	71%
Manufacturero	34%	28%	44%

Fuente: elaboración propia.

La implementación de la LOPDP mostró una correlación positiva significativa con la reducción de incidentes de seguridad ($r=0.60$, $p<0.05$). Las organizaciones con mayor nivel de cumplimiento reportaron 45% menos incidentes de fuga de datos personales en comparación con aquellas con bajo cumplimiento.

Impacto de la Certificación ISO 27001. La investigación demostró que las empresas certificadas en ISO 27001 y las organizaciones que han implementado el EGSI v3 presentaron mejores indicadores de ciberseguridad. Como se observa en la Tabla 2, el 85% de las organizaciones certificadas o con el EGSI contaban con planes de respuesta a incidentes documentados, frente al 35% de las no certificadas.

Tabla 2. Comparación de Medidas de Seguridad entre Empresas Certificadas/EGSI y No Certificadas en ISO 27001.

Medida de Seguridad	Certificadas/EGSI	No Certificadas
Planes de Respuesta a Incidentes	85%	35%
Cifrado de Datos Sensibles	89%	36%
Auditorías Regulares	96%	42%
Capacitación Anual Obligatoria	74%	40%

Fuente: elaboración propia.

El análisis de regresión múltiple identificó que la certificación ISO 27001 fue el predictor más fuerte del cumplimiento de la LOPDP, explicando el 58% de la varianza en los niveles de implementación.

Frecuencia y Tipología de Incidentes Cibernéticos. Durante el período de estudio, se documentaron 287 incidentes. La Tabla 3 presenta la distribución por tipo de ataque y sector afectado.

Tabla 3. Distribución de Incidentes Cibernéticos por Tipo y Sector.

Tipo de Ataque	Financiero	Tecnológico	Salud	Retail	Manufactura	Total
Ransomware	12	5	12	20	16	65
Phishing	10	11	14	12	21	68
Fuga de Datos	14	16	18	20	16	84
Ataques DDoS	13	14	21	9	13	70
Total	49	46	65	61	66	287

Fuente: elaboración propia.

Las empresas que habían implementado ambos marcos normativos (LOPDP e ISO 27001) reportaron una reducción aproximada del 60% en el impacto económico de los incidentes, con un tiempo medio de recuperación de 48 horas, frente a las 120 horas de organizaciones sin implementación.

Factores Críticos en la Implementación. El análisis cualitativo identificó tres factores críticos que influyeron en el éxito de la implementación:

1. Compromiso de la alta dirección: presente en el 85% de las implementaciones exitosas.
2. Presupuesto asignado: las organizaciones que destinaban más del 10% de su presupuesto de TI a ciberseguridad mostraron mejores resultados.
3. Capacitación: el 47% de las empresas con programas de capacitación trimestrales reportaron mejor cumplimiento

Efectividad de las Sanciones por Incumplimiento. La investigación reveló que las sanciones establecidas en la LOPDP no han sido efectuadas. Las entrevistas con representantes de la Superintendencia de Protección de Datos Personales identificaron como principales obstáculos la falta de personal (en total solo 34 personas para todo el país), la complejidad de los procedimientos sancionatorios y las dificultades para aplicar la Ley (Mónica Almeida et al., 2025).

El análisis correlacional demostró una relación inversa significativa entre la inversión en ciberseguridad como porcentaje del presupuesto total de TI y la frecuencia de incidentes ($r=-0.60$, $p<0.05$). Las empresas que invertían más del 10% de su presupuesto de TI en ciberseguridad reportaron un 70% menos incidentes graves. La Tabla 4 presenta la distribución por inversión y el promedio de incidentes por mes.

Tabla 4. Relación entre Inversión en Ciberseguridad y Frecuencia de Incidentes.

Inversión en ciberseguridad (% del presupuesto TI)	Incidentes mensuales promedio
<4%	8.5
6 - 7.9%	4.2
8 - 9.9%	2.1
>10%	1.3

Fuente: elaboración propia.

Los principales desafíos reportados por los participantes fueron:

- Falta de especialistas: 68% de las empresas reportaron dificultades para encontrar profesionales calificados.
- Costos de implementación: 55% consideraron los costos como el principal obstáculo.
- Resistencia al cambio: 42% mencionaron resistencia interna como barrera significativa.
- Falta de claridad normativa: 38% señalaron ambigüedades en la interpretación de la LOPDP.

Las organizaciones que implementaron ambos marcos normativos reportaron mejoras significativas en la cultura de seguridad. El 75% de los empleados en estas empresas demostraron conocimiento adecuado sobre protección de datos, frente al 35% en organizaciones sin implementación. Además, se observó una reducción del 60% en incidentes relacionados con error humano.

Estos resultados demuestran que, aunque existen desafíos significativos, la implementación conjunta de la LOPDP y la ISO 27001 tiene un impacto positivo medible en la ciberseguridad empresarial en Ecuador.

Discusión

Los resultados obtenidos evidencian que la aplicación de la Ley Orgánica de Protección de Datos Personales (LOPDP) y la norma ISO/IEC 27001:2022 tiene un impacto positivo en la ciberseguridad empresarial ecuatoriana, aunque su efectividad depende de factores organizacionales, económicos y culturales. Las empresas que alcanzan mayores niveles de cumplimiento normativo muestran una reducción significativa en los incidentes de seguridad, lo que confirma la hipótesis de que el cumplimiento de las regulaciones contribuye al fortalecimiento de la gestión de riesgos cibernéticos.

Los hallazgos coinciden con estudios internacionales que demuestran la relación entre la implementación de marcos normativos y la disminución de vulnerabilidades. La ISO/IEC 27001 puede evitar la filtración de información privada a partes no autorizadas, y acciones legales posteriores, mala publicidad y pérdidas de beneficios (Bakar et al., 2015). En Ecuador, los resultados evidencian una disminución en el impacto de los ciberataques y una mejora significativa en el tiempo promedio de recuperación, que pasó de 120 a 48 horas en las organizaciones certificadas o con el EGSI, lo que confirma la eficacia de la norma como un marco operativo sólido para la gestión de la seguridad de la información.

La correlación positiva entre la implementación de la LOPDP y la reducción de incidentes ($r=0.60$, $p<0.05$) concuerda con la teoría de la responsabilidad proactiva (LOPDP, 2021). No obstante, la efectividad de la LOPDP en Ecuador se ve limitada por la baja fiscalización y la

escasez de personal en la Superintendencia de Protección de Datos Personales, lo que genera una brecha entre la ley y su aplicación. Este hallazgo confirma lo señalado por Castellano (2020), quien advierte que la ausencia de control reduce la capacidad disuasiva de la normativa.

Existen diferencias marcadas entre sectores: el financiero presenta un 78% de cumplimiento, mientras que el manufacturero apenas alcanza el 34%. Esta brecha refleja la heterogeneidad del entorno empresarial y confirma que los sectores regulados y con mayor exposición al riesgo reputacional son los más comprometidos con la protección de datos. Asimismo, se confirma una relación inversa entre la inversión en ciberseguridad y la frecuencia de incidentes ($r=-0.60$, $p<0.05$). Las empresas que destinaron más del 10% de su presupuesto de TI a seguridad reportaron en promedio 1,3 incidentes mensuales frente a 8,5 en aquellas que invirtieron menos del 4%.

El análisis cualitativo demuestra que la cultura organizacional es un factor determinante. Así también, el compromiso de la dirección marca la diferencia al impulsar una cultura de ciberseguridad sólida y en constante evolución" dentro de las organizaciones (Santiago Neira, 2025). Sin embargo, persiste la falta de talento especializado en ciberseguridad, fenómeno también observado y documentado por la revista IT Ahora la cual indica que en el 2024, más del 60% de las entidades encuestadas identificaron la falta de capacidades técnicas y de gestión en los profesionales de ciberseguridad como una limitación crítica para avanzar en sus programas (IT Ahora, 2025).

La investigación confirma que las sanciones previstas por la LOPDP aún no se aplican de forma efectiva. Esta falta de enforcement debilita la función disuasiva del marco legal, en contraste con la experiencia de Colombia, donde la fiscalización activa ha incrementado anualmente el número de investigaciones, así como las multas impuestas (Superintendencia de Industria y Comercio de Colombia, 2025). Fortalecer la capacidad operativa de la autoridad reguladora resulta esencial para garantizar la efectividad de la ley.

La certificación del Sistema de Gestión de Seguridad de la Información, de acuerdo con ISO/IEC 27001:2022, contribuye a fomentar las actividades de protección de los sistemas y la información en las organizaciones (AENOR, 2023), lo cual mejora los indicadores de seguridad de la información y promueve una cultura de prevención. Se evidencia una convergencia conceptual entre la ISO/IEC 27001 y la Ley Orgánica de Protección de Datos Personales (LOPDP), particularmente en los principios de gestión de riesgos y responsabilidad proactiva.

Ahora hablando sobre la gestión de riesgos y el tratamiento en sí de los riesgos de seguridad de la información, es necesario recalcar que uno de los pasos primordiales en la implementación de la ISO/IEC 27001:2022 es determinar todos los controles del Anexo A que son necesarios para implementar las opciones elegidas de tratamiento de riesgos de seguridad de la información y documentarlos en la declaración de aplicabilidad; además los controles deben relacionarse adecuadamente con cada uno de los riesgos registrados y sus estrategias de tratamiento; en otras palabras, no basta con tener la matriz de riesgos, categorizar cada riesgo, establecer estrategias y definir planes de respuesta al riesgo, sino que también se debe hacer un cruce de información con

cada control de la norma y así cerciorarse que se está alineado la gestión de riesgos a la ISO/IEC 27001:2022. Y, adentrándonos en las implementaciones, las personas que desean implementar la LOPDP y la ISO/IEC 27001:2022 en las organizaciones deben saber que existen ciertos retos importantes, como por ejemplo el conocimiento jurídico y técnico en las normativas, la identificación de stakeholders, la definición de roles y funciones y además conocer a detalle el giro de negocio y el grado de madurez de protección de datos y la seguridad de la información en la organización.

Sobre el estudio, entre las principales limitaciones se destacan el corto período de observación y el enfoque en medianas y grandes empresas, lo que restringe la posibilidad de generalizar los resultados a todo el sector empresarial. Sin embargo, la evidencia obtenida demuestra que la aplicación conjunta de la Ley Orgánica de Protección de Datos Personales (LOPDP) y la norma ISO/IEC 27001 constituye una estrategia eficaz para mitigar los riesgos cibernéticos y fortalecer la cultura de protección de datos en el país.

Por otra parte, se recomienda asignar mayores recursos a la Superintendencia de Protección de Datos Personales, para que pueda supervisar y fiscalizar con efectividad, además se sugiere establecer incentivos para la adopción de la certificación ISO/IEC 27001 en las pequeñas y medianas empresas (PYMES). Además, con la finalidad de consolidar una cultura preventiva, resulta necesario promover la educación digital y la formación continua en ciberseguridad.

Conclusión

Los resultados de esta investigación confirman que la aplicación conjunta de la Ley Orgánica de Protección de Datos Personales (LOPDP) y la norma ISO/IEC 27001:2022 impactan positiva y significativamente en la ciberseguridad empresarial ecuatoriana. Aunque las dos normativas tienen enfoques distintos, una de carácter legal y otra de naturaleza técnica, se orientan al objetivo común de fortalecer la gestión de riesgos, la protección de la información y la cultura organizacional orientada a la seguridad digital.

Se comprobó que las empresas con mayores niveles de cumplimiento normativo presentan niveles bajos de incidentes de seguridad de la información y tiempos aceptables de recuperación ante ciberataques. Con estos resultados se puede demostrar que la implementación de controles basados en ISO 27001 y el cumplimiento de la LOPDP reducen vulnerabilidades técnicas en las plataformas tecnológicas y promueven una gestión proactiva de los riesgos informáticos.

Se identificó que la efectividad de la LOPDP se ve limitada por la ambigüedad de la misma, así como también la falta de mecanismos robustos de fiscalización y la capacidad operativa restringida de la Superintendencia de Protección de Datos Personales. Este déficit institucional debilita la función disuasiva de la ley. Por lo que, se sugiere una intervención estatal más firme que garantice la aplicación efectiva de la LOPDP así como las sanciones establecidas en la misma.

Desde una perspectiva teórica, los resultados reafirman la validez de los principios de gestión de la seguridad de la información definidos por la ISO/IEC 27001, confirmando que su aplicación contribuye a consolidar una cultura organizacional resiliente y orientada a la mejora continua. En el plano práctico, se evidencia que la capacitación constante del personal y la inversión sostenida en plataformas de seguridad son factores determinantes en la reducción de incidentes cibernéticos y en la mejora de la resiliencia tecnológica de las organizaciones.

En síntesis, los resultados confirman que el cumplimiento normativo y la gestión estructurada de la seguridad de la información son factores determinantes para el fortalecimiento de la ciberseguridad empresarial en el Ecuador. La integración de la LOPDP y la ISO/IEC 27001 se configura como un modelo viable y sostenible para impulsar la confianza digital, la resiliencia organizacional y la competitividad en el entorno digital ecuatoriano.

Referencias

AENOR. (2023). ISO 27001 Certificación Seguridad de la Información - AENOR. https://n9.cl/xr0fp

Almeida, M. (2025, 09 de septiembre). *Cero sanciones en Ecuador por una ley de protección de datos personales blandengue.* Primicias. https://n9.cl/g4vhra

Bakar, Z. A., Yaacob, N. A., & Udin, Z. M. (2015). The effect of business continuity management factors on organizational performance: A conceptual framework. *International Journal of Economics and Financial Issues, 5*(1), 128–134.

Birkner, J. (2023). *¿Cuál es la mejor manera de recopilar datos para su investigación?* LinkedIn. https://n9.cl/wb1o8e

Castellano, P. (2020). *La protección de datos en el sector público: efectos y transformaciones tras la LOPDGDD - Consensus.* Consensus. https://n9.cl/83d3qt

IT Ahora. (2025). *Cinco años de ciberseguridad en Ecuador: una mirada a las tendencias - IT ahora.* https://n9.cl/jihps

Lexis. (2021). *Ley Orgánica de Protección de Datos Personales.* www.lexis.com.ec

Melisa. (2017). *Técnicas e instrumentos para la recolección de datos: La entrevista - Overleaf, Online LaTeX Editor.* Overleaf. https://n9.cl/ezfpr

Mora, J., Díaz, R., Zhuma, E., & Díaz, E. (2020). El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). Consensus. https://n9.cl/2dax59

Neira, S. (2025). El 98% de los incidentes de seguridad en empresas comienzan con acciones de los empleados. *Infobae.* https://n9.cl/s9kx5d

Organización Internacional de Normalización. (2022). ISO/IEC 27001:2022(es), Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

Ortega, C. (2024). *Análisis estadístico: Qué es, usos y cómo realizarlo.* QuestionPro. https://www.questionpro.com/blog/es/analisis-estadistico/

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry, 142*. https://doi.org/10.1016/j.compind.2022.103744

Quintana, C. (2019). *Diseño de un Modelo de Gestión de Seguridad de la Información para la Universidad Iberoamericana del Ecuador.* Consensus. https://n9.cl/o8fcgt

Rodríguez, J. (2019). *Tratamiento de datos relativos a la salud del interesado en el ámbito de la sanidad pública.* Consensus. https://n9.cl/a3zwn

Superintendencia de Industria y Comercio de Colombia. (2025). *Por violación a las normas de protección de datos personales, la Superintendencia de Industria y Comercio ha iniciado 101 investigaciones e impuesto multas por $5.157 millones en 2025 | Sede Electronica.* https://n9.cl/8hcycv

Toapanta, S. (2020). *Security model for the integration of the Ministry of Telecommunications and the Information Society with a public organization of Ecuador. Proceedings of the 2020 the 4th International Conference on Information System and Data Mining.* https://doi.org/10.1145/3404663.3404670

Vives, T. (2021). Vista de La codificación y categorización en la teoría fundamentada, un método para el análisis de los datos cualitativos. *Revista de Methodica, 10(40), 97-104.* https://doi.org/10.22201/fm.20075057e.2021.40.21367

Autores

Franklin Raúl Curay Ulcuango. Ingeniero en Computación y Magíster en Planificación, con más de 15 años de experiencia gestionando programas y proyectos de tecnología (software y hardware), ciberseguridad y seguridad de la información en los sectores de banca, tecnología, telecomunicaciones y gobierno.

Cristhian Humberto Flores Urgilés. Universidad Católica de Cuenca

Declaración

Conflicto de interés

No tenemos ningún conflicto de interés que declarar.

Financiamiento

Sin ayuda financiera de partes externas a este artículo.

Nota

El artículo es original y no ha sido publicado previamente.