

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

[DOI 10.35381/noesisin.v7i2.618](https://doi.org/10.35381/noesisin.v7i2.618)

Buenas prácticas para la protección de datos personales

Best practices for personal data protection

Sebastián Gonzalo Velasco-Urgilés

sebastianvu87@uniandes.edu.ec

Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador

<https://orcid.org/0009-0007-8997-3392>

Gladis Margo Proaño-Reyes

posgrado@uniandes.edu.ec

Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador

<https://orcid.org/0000-0003-1653-5889>

Fernando de Jesús Castro-Sánchez

fernandodcs.ainv@uniandes.edu.ec

Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador

<https://orcid.org/0000-0003-3937-8142>

Recibido: 15 de abril 2025
Revisado: 15 de mayo 2025
Aprobado: 15 de julio 2025
Publicado: 01 de agosto 2025

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

RESUMEN

Este artículo propone un conjunto de buenas prácticas en materia de protección de datos personales para aquellas que según la ley, no están obligadas a designar un Delegado de Protección de Datos (DPD). Aunque exentas de esta figura, la relevancia del tema, impulsada por la Ley Orgánica de Protección de Datos Personales, hace que estas organizaciones se vean llamadas a adoptar medidas en ese sentido. Mediante una metodología cualitativa y un diseño no experimental, se identifican deficiencias comunes sobre esta materia en el sector privado. Sobre la base de un análisis documental y la realización de entrevistas a expertos, se estructura una guía de buenas prácticas que resulta comprensible y accesible. Esta propuesta busca fortalecer el cumplimiento normativo y fomentar una cultura organizacional de protección de datos, demostrando que una gestión adecuada de la información personal es fundamental para generar confianza y seguridad en el ecosistema digital ecuatoriano.

Descriptores: Protección de datos; cumplimiento de la ley; buenas prácticas; seguridad de los datos; derecho a la privacidad; gestión de la información. (Tesauro UNESCO).

ABSTRACT

This article proposes a set of best practices in personal data protection for those who, according to the law, are not required to appoint a Data Protection Officer (DPO). Although exempt from this requirement, the relevance of the issue, driven by the Organic Law on Personal Data Protection, means that these organizations are called upon to adopt measures in this regard. Using a qualitative methodology and a non-experimental design, common deficiencies in this area in the private sector are identified. Based on a documentary analysis and interviews with experts, a guide to best practices is structured that is understandable and accessible. This proposal seeks to strengthen regulatory compliance and foster an organizational culture of data protection, demonstrating that proper management of personal information is essential to building trust and security in Ecuador's digital ecosystem.

Descriptors: Data protection; legal compliance; best practices; data security; right to privacy; information management. (UNESCO Thesaurus).

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

INTRODUCCIÓN

La protección de datos personales ha cobrado creciente relevancia en Ecuador, impulsada por el avance tecnológico y por la necesidad de perfeccionar el tratamiento a la información sensible. La Constitución garantiza este derecho en su artículo 66 y lo norma la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional 2008; 2021). También este aspecto es regulado por su reglamento, el Decreto Ejecutivo 904 de 2023. En estas normativas se establece un marco legal que regula el manejo de esta información en el sector público y en el privado. Los principios que se promueven son los de legalidad, transparencia, minimización de datos y responsabilidad anticipada, alineándose con estándares internacionales como el Reglamento de Protección de Datos de la Unión Europea.

Esta investigación se enfoca en organizaciones privadas que gestionan datos sensibles sin estar obligadas a designar un delegado de protección de datos. A través de un análisis normativo y casos específicos, se evidencia la deficiente aplicación de buenas prácticas, lo que a su vez se traduce en falta de claridad y transparencia en las medidas adoptadas. Con esto se elevan los riesgos de ocurrencia de hechos como accesos no autorizados o filtraciones de información

La protección de los datos personales no solo depende de un marco legal robusto, sino también de la implementación de buenas prácticas que minimicen los riesgos y garanticen el respeto de los derechos de los titulares. Autores como Rosas y Pila (2023) destacan la importancia de que las organizaciones adopten políticas claras de gestión de datos, asegurando la transparencia en su tratamiento, la seguridad en la custodia de la información y la responsabilidad en su manejo.

Los protocolos deben incluir auditorías regulares, formación continua para la persona encargada del manejo de datos, y también que la adopción de tecnologías que garanticen la confidencialidad e integridad de la información. Estas medidas son esenciales tanto para el cumplimiento normativo como para generar confianza en los

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

usuarios (Macías y Galarza, 2022).

El derecho a la intimidad es una parte esencial en cualquier sociedad democrática. Por tanto, proteger los datos personales debe entenderse como una extensión de este derecho, lo que implica una responsabilidad conjunta entre el Estado, las empresas y los individuos para asegurar una gestión adecuada de la información (Mendoza, 2021).

El Código Orgánico Integral Penal, contempla sanciones para conductas que comprometan la privacidad de la información, aunque estas no se relacionen exclusivamente en la protección de datos personales. Se penaliza el acceso no autorizado a sistemas informáticos, la violación de la intimidad incluyendo la divulgación indebida de los datos de las personas.

En este estudio se proponen buenas prácticas para las organizaciones privadas en Ecuador, con el fin de fortalecer la seguridad y el cumplimiento normativo. Se identifican, además deficiencias en la gestión de los datos y se analizan modelos de referencia internacionales efectivos. De esta forma se procura fomentar una cultura organizacional comprometida con la protección de los datos personales y con la privacidad.

MÉTODO

Por la modalidad o enfoque se trata de un estudio cualitativo, que conlleva a analizar y proponer buenas prácticas para la protección de los datos personales en entidades ecuatorianas que no están obligadas a designar un Delegado de Protección de Datos (DPD). Se abordó la problemática de la falta de claridad en la implementación de estas prácticas, desarrollando un marco de referencia basado en la normativa ecuatoriana.

El diseño de esta investigación es de carácter no experimental, centrado en la exploración y análisis de la legislación ecuatoriana vinculada a la protección de datos. Se revisaron documentos clave con el propósito de identificar áreas de mejora y proponer prácticas específicas que refuercen la seguridad y protección de la

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

información en organizaciones que no están obligadas a nombrar un delegado para la Protección de Datos.

En tanto que la investigación se enmarcó en un enfoque jurídico-administrativo, combinando el análisis legal con la gestión práctica. Se consideraron los siguientes aspectos descriptivo, para examinar y describir prácticas actuales; analítico, para descomponer y examinar la normativa y prácticas organizativas; evaluativo, para valorar la eficacia de las prácticas actuales; y propositivo, para desarrollar y sugerir prácticas específicas que las organizaciones puedan adoptar.

Se recurrió al método analítico-sintético con el que se examinó la normativa ecuatoriana y las prácticas organizativas actuales, integrando estos elementos en una síntesis para formular buenas prácticas coherentes; en tanto que el método inductivo-deductivo: A partir del estudio de casos específicos, se identificaron patrones y principios generales, que luego se aplicaron a situaciones particulares en otras organizaciones, asegurando la pertinencia de las recomendaciones.

Este trabajo se apoyó en técnicas e instrumentos de investigación como es el análisis documental exhaustivo de normativas, reglamentos y políticas de protección de datos en Ecuador, para identificar áreas donde la implementación de buenas prácticas era insuficiente o podía mejorar, enfocándose en organizaciones que no están obligadas a designar un DPD, para lo que se aplicó entrevistas a expertos y responsables de cumplimiento en Ecuador para recopilar información cualitativa sobre la implementación de buenas prácticas. También fue válido el estudio de casos de la literatura y de informes especializados, identificando patrones y desafíos en la adopción de buenas prácticas para formular recomendaciones aplicables.

En la población y muestra se consideró tanto la parte objetual, por los documentos normativos seleccionados y analizados, como la parte referida a los sujetos expertos incorporados a la investigación. Para la selección de expertos y responsables de cumplimiento en organizaciones del sector privado, se aplicaron criterios de inclusión

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

y exclusión basados en su experiencia directa con la protección de datos personales. En dicha selección, se presentó un grupo de organizaciones que, de acuerdo a su giro de negocia tratan grandes volúmenes de información o datos sensibles, enfocándose en aquellas que, aunque no están obligadas a designar un DPD, implementan o buscan implementar buenas prácticas en este ámbito. De un total de quince organizaciones identificadas, se incluyeron diez en el estudio, eligiendo solo las que cuentan con una experiencia superior a cinco años en la gestión de datos personales y un historial comprobado de cumplimiento normativo. Las otras cinco organizaciones fueron descartadas debido a su menor tiempo de operación o experiencia limitada en la aplicación de normativas de protección de datos.

RESULTADOS

Análisis de conceptos fundamentales

En la búsqueda de referentes sobre el tema, se considera que Arellano (2020), Aguilar et al. (2022) y Sánchez (2023) analizan el derecho a la protección de los datos personales como una garantía constitucional. Vinculan este aspecto a la privacidad, la autodeterminación de las personas a emitir información sobre aspectos personales y el Habeas data. Estos autores se enfocan en el marco legal ecuatoriano, su evolución hasta llegar a nuestros días y su alineación otras prácticas y estándares internacionales. Mientras Gil (2020), ofrece una mirada crítica sobre el impacto de tecnologías denominadas disruptivas como el Big Data en esa privacidad y reflexiona sobre los riesgos que surgen del tratamiento masivo de datos, y por tanto hacia la necesidad de concebir regulaciones adaptativas y flexibles para dar respuesta a esta problemática emergente.

Autores como Fernández (2023), Ávila (2024), o Martínez y Pincay (2024), centran su atención en específicamente en la protección de datos desde la gestión organizacional o empresarial. Ellos abordan temáticas como la seguridad en las instituciones públicas,

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

el manejo de datos abiertos y el empleo de códigos de ética como alternativas de autorregulación. Por su parte Contreras et al (2022) y Machuca et al. (2022) se centran en el análisis de casos judiciales y herramientas como el habeas data. Ellos tienen en común el destacar cómo se aplican los principios de la protección de datos, en la práctica jurídico, legal y administrativa.

El análisis de los conceptos fundamentales en la protección de los datos personales en Ecuador se enfocó en los principios clave establecidos por la Ley Orgánica de Protección de Datos Personales en su Registro Oficial No. 459 de 26 de mayo de 2021 y su reglamento. Estos principios, que están en consonancia con regulaciones internacionales como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, forman la base del marco legal en el país y son esenciales para garantizar la privacidad y seguridad de los datos personales que manejan las organizaciones.

Principios de Licitud, Lealtad y Transparencia

Licitud: El artículo 6 de la Ley Orgánica de Protección de Datos Personales, Todo manejo de datos personales debe ejecutarse de manera lícita, equitativa y transparente, garantizando que los datos sean gestionados conforme a las normativas legales, con justicia y claridad para las personas involucradas. Este principio obliga a las organizaciones a garantizar que los datos sean recolectados con un propósito legítimo y respaldados por la normativa válida, como la aprobación del titular de los datos o de la ejecución de una exigencia legal.

Lealtad y Transparencia: La ley obliga a las organizaciones a informar de manera clara y accesible a los dueños de los datos sobre cómo se gestionará sus datos. Sin embargo, el análisis reveló que, aunque muchas organizaciones del sector privado entienden este principio, su aplicación efectiva es frecuentemente deficiente. La falta de claridad en la comunicación con los titulares puede dar lugar a incumplimientos de este principio, exponiendo a las organizaciones a posibles sanciones.

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

El artículo 7 de la Ley Orgánica de Protección de Datos Personales establece que solo deben recolectarse aquellos datos que sean estrictamente necesarios para el propósito declarado. En la práctica, sin embargo, se encontró que muchas organizaciones recogen más datos de los necesarios, lo que no solo contraviene el principio de minimización sino que también incrementa los riesgos asociados al manejo de grandes volúmenes de información personal.

Recomendaciones basadas en normativas: La regulación recomienda que las organizaciones adopten como controles de acceso, cifrado de datos y auditorías periódicas para garantizar la integridad y confidencialidad de la información. La ausencia de medidas de estas medidas podría exponer a las organizaciones a riesgos considerables, no solo legales, sino también de reputación.

El análisis de los conceptos fundamentales revela que, aunque la normativa ecuatoriana proporciona un marco sólido referente a la protección de datos, la aplicación de estos principios en las organizaciones privadas sigue siendo irregular y, en muchos casos, insuficiente. La alineación con estándares internacionales, como los establecidos por el RGPD, podría mejorar la coherencia y efectividad en la aplicación de estos principios en Ecuador. Además, la implementación de políticas claras y la capacitación continua son esenciales para garantizar que las organizaciones no solo comprendan estos principios, sino que los apliquen de manera efectiva en sus operaciones diarias.

Resultados del análisis documental

En el marco de la presente investigación, se realizó un exhaustivo análisis documental centrado en las normativas y reglamentos ecuatorianos relacionados con la protección de datos personales, específicamente en cómo estas normativas se aplican en el sector privado. Este análisis permitió identificar tanto fortalezas como deficiencias en la implementación y cumplimiento de las normativas vigentes. Los hallazgos clave del análisis documental, con un enfoque particular en los fundamentos legales que

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

sustentan estos resultados.

Fortalezas del marco normativo ecuatoriano

La Ley Orgánica de Protección de Datos Personales, emitida el 26 de mayo de 2021 y publicada en el Suplemento No. 459 del Registro Oficial, es el principal marco legal que regula la protección de datos personales en Ecuador. Esta norma establece una base legal robusta y en gran parte en consonancia con los estándares internacionales, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Entre los aspectos más relevantes se destacan los siguientes:

Derechos que gozan los Titulares de los Datos: la Ley de protección de Datos Personales en el artículo 25 define con claridad todos los derechos que tiene de los dueños de la información, entre ellos están el derecho de acceso, rectificación, eliminación y oposición. Este marco jurídico garantiza que las personas mantengan el control de su información personal y requiere que las organizaciones respondan de forma rápida y adecuada a las peticiones relacionadas con

La normativa aplicable para el manejo de Datos: según el artículo 14, los datos personales tienen que estar justificado en una normativa valida, La autorización explícita del titular, el cumplimiento de un deber legal o el interés legítimo del encargado del tratamiento, entre otros. Esta regulación asegura que la gestión de datos personales se llevará a cabo dentro de un marco jurídico definido y con una justificación apropiada.

Deficiencias en la aplicación práctica de la normativa

A pesar del sólido marco legal, el análisis documental reveló varios desafíos en la implementación práctica de la Ley de Protección de Datos Personales en las empresas del sector privado ecuatoriano. Estos desafíos son especialmente evidentes en organizaciones que no están obligadas a designar un Delegado de Protección de Datos (DPD).

Las deficiencias más notables incluyen:

- Falta de directrices específicas para el sector privado: aunque la ley establece

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

principios claros para la protección de datos, se observó que existe una falta de directrices específicas que orienten a las organizaciones del sector privado, especialmente a aquellas pequeñas y medianas empresas (PYMES), sobre cómo implementar estos principios de manera efectiva. La ausencia de guías prácticas deja a muchas organizaciones sin un camino claro para cumplir con la ley, lo que incrementa el riesgo de incumplimientos.

- Capacitación y conocimiento limitados: la regulación exige que las entidades adopten acciones técnicas y administrativas adecuadas para garantizar la seguridad de los datos personales. (artículos 30 y 31). Sin embargo, el análisis mostró que muchas organizaciones carecen de los recursos necesarios para capacitar a su personal en estos aspectos, lo que resulta en una implementación deficiente de las medidas de seguridad requeridas. La ley menciona la necesidad de la capacitación continua (artículo 51), pero en la práctica, esta obligación no siempre se cumple, lo que deja a las organizaciones vulnerables a fallas en la protección de datos.
- Débil supervisión y monitoreo: si bien la ley establece la responsabilidad proactiva como un principio fundamental (artículo 11), que requiere que las organizaciones no solo respeten la normativa, sino que también sean capaces de evidenciar su cumplimiento, el análisis documental reveló una debilidad en la supervisión y monitoreo efectivos por parte de las autoridades competentes. La Superintendencia de control, creada para vigilar el cumplimiento de la normativa, aún enfrenta limitaciones en recursos y capacidades para realizar auditorías exhaustivas y sancionar incumplimientos de manera eficaz.

Áreas específicas de mejora identificadas

Realizando el análisis documental, se identificaron varias áreas clave donde la implementación de la Ley Orgánica de Protección de Datos Personales podría mejorarse para fortalecer la protección de datos personales en el sector privado:

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

- **Desarrollo de Guías de Cumplimiento para PYMES:** Es necesario que la Superintendencia de Protección de Datos Personales emita guías específicas que orienten a las PYMES en la implementación de buenas prácticas de protección de datos, adaptadas a sus capacidades y recursos. Estas guías deberían incluir ejemplos concretos de políticas de privacidad, medidas de seguridad, y procedimientos para manejar solicitudes de los titulares de datos.
- **Fortalecimiento de la Capacitación Obligatoria:** Se debería intensificar la exigencia de capacitación continua para los responsables del tratamiento de datos en las organizaciones, tal como lo establece el artículo 51. Además, el Estado podría considerar la creación de programas de capacitación accesibles, en colaboración con instituciones académicas, que ayuden a las organizaciones a cumplir con esta obligación.
- **Mejoras en la Supervisión y Sanciones:** La Superintendencia encargada de la protección de datos debe fortalecer su capacidad de supervisión mediante el desarrollo de un sistema más riguroso de auditorías y sanciones. Esto incluye la creación de un marco más detallado para la evaluación del cumplimiento normativo, así como la aplicación de sanciones proporcionales y disuasorias que incentiven a las organizaciones a cumplir con la normativa.

Comparación con normativas internacionales y recomendaciones

El análisis comparativo con normativas internacionales, como el RGPD, reveló que Ecuador ha adoptado varios de los principios fundamentales de protección de datos presentes en las normativas europeas. No obstante, para incrementar su efectividad, se sugiere lo siguiente:

- **Adopción de un Enfoque Proactivo en el Cumplimiento:** Siguiendo el modelo europeo, donde se incentiva a las organizaciones a adoptar una actitud proactiva en la protección de datos, Ecuador podría implementar incentivos para aquellas empresas que demuestren un cumplimiento destacado, como la reducción de

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

sanciones o la concesión de reconocimientos oficiales.

- Fortalecimiento del Rol del DPD en el Sector Privado: Aunque no todas las organizaciones están obligadas a nombrar un DPD, se podría promover la designación voluntaria a través de incentivos, además de proporcionar formación específica para estos roles, asegurando que los responsables cuenten con el conocimiento y la autoridad necesarios para desempeñar eficazmente sus funciones.

El marco normativo ecuatoriano en cuanto a protección de datos personales es sólido y está alineado con los estándares internacionales, pero su aplicación en el sector privado enfrenta importantes desafíos. Para superar estas brechas, se necesita un esfuerzo coordinado entre las autoridades reguladoras y las empresas privadas, centrado en la elaboración de directrices específicas, el fortalecimiento de la capacitación y la mejora de los mecanismos de supervisión. Solo con estas mejoras será posible asegurar una protección eficaz y coherente de los datos personales en Ecuador, cumpliendo con los altos estándares de la normativa vigente.

Resultados del diagnóstico situacional

Las entrevistas llevadas a cabo con expertos y responsables de cumplimiento en las organizaciones seleccionadas proporcionaron una visión cualitativa detallada sobre las prácticas actuales y los retos en la protección de datos personales. A continuación, se describen los aspectos clave tratados durante estas entrevistas:

- Cumplimiento normativo: Los entrevistados señalaron que, aunque son conscientes de los deberes establecidos por la Ley, su aplicación resulta a menudo compleja debido a la falta de recursos especializados y a la ambigüedad en algunas disposiciones legales. Esto lleva a una implementación parcial de las medidas necesarias para cumplir con la normativa, lo que expone a las organizaciones a posibles sanciones.
- Capacitación y conciencia: Un tema recurrente fue la necesidad de fortalecer la

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

capacitación y la concienciación dentro de las organizaciones. Los responsables de cumplimiento indicaron que, aunque se realizan esfuerzos por capacitar al personal en temas de protección de datos, estos resultan insuficientes para garantizar un conocimiento adecuado de las normativas y de las mejores prácticas internacionales. La carencia de formación especializada impacta directamente en la capacidad de las organizaciones para implementar y sostener prácticas efectivas de protección de datos.

- Responsabilidad proactiva: Otro aspecto central que se abordó fue el principio de responsabilidad proactiva. Los entrevistados reconocieron la relevancia de este principio, que exige no solo cumplir con la normativa, sino también evidenciar dicho cumplimiento mediante auditorías internas y una documentación exhaustiva. No obstante, señalaron que la implementación de mecanismos de auditoría y monitoreo es limitada, principalmente debido a restricciones presupuestarias y a la escasez de personal capacitado.
- Desafíos en la implementación de tecnologías: También se discutieron las dificultades relacionadas con la implementación de tecnologías avanzadas para el resguardo de datos., como el encriptado de extremo a extremo y la anonimización de datos. Los entrevistados coincidieron en que, si bien estas tecnologías son esenciales para garantizar la integridad y confidencialidad de los datos, su implementación exige inversiones significativas que no todas las organizaciones pueden permitirse.

En conclusión, la investigación muestra que, aunque Ecuador dispone de un marco normativo adecuado, su efectividad en el sector privado requiere mejoras significativas en términos de capacitación, supervisión y la adopción de buenas prácticas, alineadas con los estándares internacionales.

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

DISCUSIÓN

La investigación permitió analizar la implementación de la Ley Orgánica de protección de Datos Personales en el sector privado ecuatoriano, mostrando que aunque el marco legal tiene puntos en común con los estándares internacionales, su aplicación en la práctica no es homogénea. Las principales dificultades radican en las limitaciones de recursos especialidades, existencia de ambigüedades en la norma y la insuficiente adaptación de las directrices al contexto de las Pymes en Ecuador. Esto prueba la necesidad de potenciar no solo la infraestructura legal, sino también la formación técnica de los recursos humanos en las organizaciones sobre esta materia, con vistas a lograr una mayor comprensión y cumplimiento de las obligaciones en materia de protección de datos.

Al comparar el contexto ecuatoriano con otras jurisdicciones como Estados Unidos y la Unión Europea, se aprecia que el desarrollo eficaz de la implementación de estas legislaciones depende en gran medida del apoyo institucional del Estado. Su rol, esencialmente consistiría en el establecimiento de programas de capacitación accesibles y la erogación de recursos para estos fines. También se propone el fomento de las alianzas entre el sector privado, el público, la academia y los juristas para contribuir al logro de esa formación continua. Además, se debe evaluar el impacto esperado de la implementación de tecnologías como la anonimización y el cifrado de la información.

Propuestas para la elaboración de buenas prácticas para la protección de datos personales en el sector privado en Ecuador

En el contexto de la evolución normativa en cuanto a la protección de datos personales en Ecuador, la Ley Orgánica de Protección de Datos Personales establece una base jurídica robusta para asegurar la seguridad y confidencialidad de la información manejada por las organizaciones. Sin embargo, los resultados de esta investigación revelan que la aplicación de dicha normativa en el sector privado enfrenta importantes

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

desafíos, principalmente debido a la falta de pautas específicas, recursos limitados y una cultura que históricamente no ha priorizado la protección de los datos. se propone las siguientes medidas para optimizar las prácticas de protección de datos en el sector privado ecuatoriano.

Desarrollo de guías prácticas para la implementación de normativas

Se sugiere que la Superintendencia de Protección de Datos Personales elabore guías prácticas específicas para distintos tipos de organizaciones, particularmente para las medianas y pequeñas empresas, que expliquen cómo cumplir de manera efectiva con los requisitos de la Ley Orgánica de Protección de Datos Personales. Estas directrices deben incorporar ejemplos específicos de políticas de privacidad, procedimientos detallados para la recopilación, custodia y erradicación de datos personales, así como estrategias para implementar medidas de seguridad, como controles de acceso y cifrado. El propósito es ofrecer a las organizaciones herramientas claras y prácticas que simplifiquen el cumplimiento de las normativas, minimizando los riesgos relacionados con la gestión de datos personales.

Fomento de la capacitación continua y la concientización

La ausencia de capacitación es uno de los principales problemas para la correcta implementación de las normativas de protección de datos, se propone la creación de un programa nacional de capacitación continua dirigido a los responsables de cumplimiento y al personal operativo en las organizaciones privadas. Este programa, desarrollado en colaboración con universidades e instituciones especializadas, debería incluir cursos o capacitaciones sobre la Ley Orgánica de Protección de Datos Personales, talleres prácticos sobre el diseño e implementación de políticas de protección de datos, y certificaciones que avalen la competencia en protección de datos. La meta es asegurar que todas las organizaciones, independientemente de su tamaño, cuenten con el conocimiento y las habilidades necesarias para proteger eficazmente la información personal.

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

Incentivos para la adopción de tecnologías avanzadas de protección de datos

Para promover la adopción de tecnologías avanzadas de protección de datos, como el Encriptado de punta a punta y la desidentificación de datos, se recomienda la creación de incentivos económicos y fiscales. Estos incentivos podrían incluir deducciones fiscales por inversiones en tecnología de protección de datos, subsidio o préstamos con un mínimo interés en la compra de equipos de seguridad, y reconocimientos oficiales para organizaciones que implementen estas tecnologías de manera efectiva. La adopción de estas tecnologías es crucial para proteger la integridad y confidencialidad de los datos, y los incentivos económicos ayudarían a superar las barreras financieras que actualmente limitan su implementación en muchas organizaciones.

Fortalecimiento de la supervisión y el monitoreo

Es fundamental que, una vez creada, la Superintendencia de Protección de Datos Personales refuerce sus capacidades para llevar a cabo auditorías regulares y exhaustivas en las organizaciones, con un enfoque particular en aquellas que manejan grandes volúmenes de información o datos sensibles. Aunque esta entidad aún no ha sido establecida, es crucial que, al ser implementada, desarrolle un sistema de auditorías aleatorias que garantice el cumplimiento continuo de la normativa. Además, debería implementar un sistema de reportes obligatorios para incidentes de seguridad y aplicar sanciones proporcionales y disuasorias ajustadas a la gravedad de las violaciones. Un sistema de supervisión sólido es esencial para disuadir el incumplimiento y promover una cultura de responsabilidad proactiva dentro de las organizaciones, asegurando así una efectiva protección de los datos personales en Ecuador.

Promoción de la designación voluntaria de delegados de protección de datos

Aunque no todas las organizaciones están obligadas a designar un Delegado de Protección de Datos (DPD), se propone fomentar esta práctica a través de incentivos y apoyo técnico. Esto podría incluir beneficios fiscales, programas de formación

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

especializados para DPD, y acceso prioritario a recursos de la Superintendencia para organizaciones con un DPD designado. La designación de un DPD es crucial para garantizar que las organizaciones adopten un enfoque integral y coherente en la protección de datos, mejorando la gestión de la información personal y asegurando un cumplimiento normativo más riguroso.

CONCLUSIONES

La Ley Orgánica de Protección de Datos Personales en Ecuador establece un marco legal estable y alineado con estándares internacionales, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Sin embargo, su efectividad en el sector privado depende en gran medida de la correcta interpretación y aplicación de sus disposiciones, las cuales requieren un mayor esfuerzo en términos de claridad y adaptación a las realidades operativas de las organizaciones, especialmente las pequeñas y medianas empresas (PYMES).

Aunque la normativa proporciona un marco general para la protección de datos, existe una carencia notable de directrices prácticas específicas que orienten a las organizaciones, especialmente a las PYMES, en la implementación efectiva de las normativas. La ausencia de estas guías prácticas incrementa el riesgo de incumplimientos y deja a muchas organizaciones sin un camino claro para cumplir con las obligaciones legales, lo que subraya la necesidad urgente de desarrollar y difundir dichas directrices.

La carencia de formación adecuada y la poca concienciación sobre la relevancia de la protección de datos entre el personal de las organizaciones han sido identificadas como obstáculos importantes para el cumplimiento de la normativa. Se concluye que es fundamental implementar programas de capacitación continua que no solo eduquen sobre las normativas vigentes, sino que también promueven una cultura organizacional que valore y priorice la seguridad de la información personal.

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

La creación de un organismo de supervisión, como la Superintendencia de Protección de Datos Personales, es fundamental para asegurar el cumplimiento de la normativa. Un sistema de auditorías periódicas, junto con la aplicación de sanciones proporcionales y disuasorias, es clave para fomentar la responsabilidad anticipada dentro de las organizaciones y garantizar un cumplimiento normativo constante. Aunque esta entidad aún no ha sido creada, su futura implementación deberá estar acompañada de un enfoque consistente y efectivo en la supervisión y control.

En conclusión, para que la protección de datos personales en Ecuador sea efectiva y esté a la altura de los estándares internacionales, es necesario un enfoque multidimensional que incluya la creación de guías prácticas específicas, la mejora de la capacitación y concienciación en las organizaciones, la adopción de tecnologías avanzadas de seguridad, y el establecimiento de un sistema de supervisión sólido y eficiente. Solo a través de estas medidas se podrá asegurar que las organizaciones privadas en Ecuador cumplan con la normativa vigente y protejan adecuadamente los datos personales de los individuos.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A todos los actores sociales involucrados en el desarrollo de la investigación.

REFERENCIAS CONSULTADAS

- Aguilar, M., Paredes, J. A., Gordillo, D. P., y Burgos, G. P. (2022). La protección de datos personales en Ecuador. *Estudios del Desarrollo Social: Cuba y América Latina*, 10(especial 1). <https://acortar.link/W2t6fU>
- Arellano, C. A. (2020). El derecho de protección de datos personales. *Biolex*, 12(23), 163-174. <https://acortar.link/kAbiiZ>

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

- Asamblea Nacional. (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de Ecuador*. <https://acortar.link/GdolxE>
- Asamblea Nacional. (2008). *Constitución de la República del Ecuador*. <https://acortar.link/KTgFc>
- Asamblea Nacional. (2014). *Código Orgánico Integral Penal*. <https://acortar.link/3SxiCO>
- Asamblea Nacional. (2015). *Ley Orgánica de Telecomunicaciones de Ecuador*. <https://acortar.link/JdfML9>
- Asamblea Nacional. (2021). *Ley Orgánica de Protección de Datos Personales de Ecuador*. <https://acortar.link/nYmchL>
- Ávila, A. A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. *Journal of Economic and Social Science Research*, 4(2), 140-156. <https://acortar.link/almfx8>
- Contreras, P., Bordachar, M., y Ortiz, L. (2022). *Privacidad y protección de datos personales. Jurisprudencia seleccionada y comentada*. DER Ediciones. <https://acortar.link/iX1yoC>
- Fernández, M. F. (2023). El código ético como mecanismo de autorregulación empresarial en la protección de datos de sus empleados: Singularidades sobre su eficacia. *Lex Social: Revista de Derechos Sociales*, 13(2), 1-34. <https://doi.org/10.46661/lexsocial.8758>
- Gil, E. (2020). *Big Data, privacidad y protección de datos*. Editorial Casa del Libro. <https://acortar.link/HDWr5G>
- Machuca, S. A., Vinueza, N. V., Sampedro, C. R., y Santillán, A. L. (2022). Habeas data y protección de datos personales en la gestión de las bases de datos. *Revista Universidad y Sociedad*, 14(2), 244-251. <https://acortar.link/KRjlsz>
- Macías, A. D., y Galarza, M. D. (2022). Análisis de ciberataques sobre el uso de redes sociales en relación a la protección de datos personales en Ecuador. *Dominio de las Ciencias*, 8(1), 1070-1079. <https://acortar.link/wgclZg>
- Martínez, M. R., y Pincay, J. I. (2024). Buenas Prácticas de Seguridad para la Protección de la Privacidad con Datos Abiertos. *Revista Científica de*

Sebastián Gonzalo Velasco-Urgilés; Gladis Margot Proaño-Reyes; Fernando de Jesús Castro-Sánchez

Informática ENCRYPTAR, 7(14), 187-205. <https://acortar.link/6Ynonz>

Mendoza, O. A. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista Ius*, 15(48), 179-207. <https://doi.org/10.35487/rius.v15i48.2021.743>

Rosas, G., y Pila, G. (2023). La protección de datos personales en Ecuador: Una revisión histórica-normativa de este derecho fundamental en el país suramericano. *VISUAL REVIEW. International Visual Culture Review/Revista Internacional de Cultura Visual*, 13(2), 1-16. <https://acortar.link/fEf7wg>

Sánchez, M. F. (2023). El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo*, 10(1). <https://acortar.link/oQjC8Q>

Unión Europea (2016). *Reglamento General de Protección de Datos (RGPD) de la Unión Europea*. <https://gdpr-info.eu/>