UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

ARTÍCULOS PROFESIONALES DE ALTO NIVEL

TEMA:

MARCO DE CALIDAD PARA LA PROTECCIÓN DE DATOS EN PLATAFORMAS CRM: ENFOQUE NORMATIVO BAJO LA LOPDP DE ECUADOR

AUTOR:

MIGUEL ÁNGEL JIMÉNEZ CORDERO

DIRECTOR:

MIGUEL ÁNGEL QUIROZ MARTÍNEZ

CUENCA – ECUADOR
2026

Autor:

Miguel Ángel Jiménez Cordero
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
mjimenezc@est.ups.edu.ec

Dirigido por:

Miguel Ángel Quiroz Martínez
Ingeniero de Sistemas.
Magister en Sistemas de Calidad y Productividad.
mquiroz@ups.edu.ec

DEDICATORIA

Dedico con todo el corazón este trabajo a mis padres, que han sido el punto de partida de todo lo propuesto en mi vida. Hubo tiempos difíciles en los que quería tirar la toalla, y justamente recordé los consejos de ambos de su forma de ver la vida y los orgullosos que estarían de verme cumplir este objetivo.

A mis hijos que son la razón por la que me levanto incluso en los días difíciles. Son mi impulso día a día, mi felicidad, los protagonistas de que todo esfuerzo tiene un sentido. Cada desvelo que tuve que pasar en este proceso y cada sacrificio los tenía a ellos como inspiración.

Por último, este trabajo también me lo dedico. Porque supe resistir y también porque, aun con la perdida de mi padre, cansancio, dudas y momentos de querer detenerme, seguí adelante. Aprendí a equilibrar el trabajo, la familia y los estudios, aunque a veces pareciera imposible. Después de tanto, hoy miro mi propio esfuerzo con orgullo y sé que valió la pena.

AGRADECIMIENTO

Siempre lo digo y lo diré agradezco a mis padres, por lo brindado, inculcado y me han demostrado, que con gran esfuerzo podemos alcanzar nuestras metas y propósitos en la vida.

A mi papá que lo extraño, pero cuya memoria es como un resplandor en los días complicados. Este logro también es suyo, porque se lo correcto que era y yo no lo puedo decepcionar a pesar de que no estas junto a mi recordaba tus palabras y eso fue un impulso a seguir.

A mis hijos los más queridos, a mi familia, gracias por entender que mis silencios no eran distancia, sino cansancio. Mis ausencias no eran falta de interés, sino compromiso.

Y gracias, de corazón, a todas las personas que estuvieron conmigo de una u otra manera. A quienes me escucharon, me alentaron o simplemente compartieron un momento cuando lo necesitaba.

Tabla de Contenido

Marco de calidad para la protección de datos en plataformas CRM: enfoque normativo bajo la LOPDP de Ecuador

Autor(es):

Miguel Angel Jiménez Cordero

Resumen

El uso masivo de datos personales en plataformas CRM en Ecuador presenta riesgos legales y técnicos derivados de prácticas de QA deficientes, esto es debido a la pobre calidad en las prácticas de control de calidad. Las plataformas CRM asisten a las compañías a guardar, organizar, e investigar grandes cantidades de datos personales.

Esa misma situación plantea retos importantes, sobre la salvaguarda de la información y también su seguridad. Con la LOPDP, que entró en vigor en 2021, Ecuador instauró un marco legal para usar bien esos datos. Por lo tanto, forzó a entidades, tanto del sector público como privado, a poner en marcha formas prácticas para cumplir. Además se evalúan las prácticas actuales en CRM respecto a la protección de datos, y los riesgos más frecuentes del tratamiento inadecuado de información personal.

El estudio incorpora elementos técnicos y organizativos como políticas de privacidad, auditorías internas, gestión de incidentes, evaluación de impacto DPIA, y capacitación continua, alineados con estándares internacionales como ISO/IEC 27001. Todo esto permite estructurar una propuesta de marco de calidad que incluye requisitos funcionales y no funcionales aplicables al entorno CRM.

De tal manera el marco propuesto es validado mediante su aplicación en un estudio de caso, demostrando su aplicabilidad, pertinencia y contribución al cumplimiento normativo, así como al fortalecimiento de la seguridad de la información en las organizaciones ecuatorianas.

Palabras clave:

protección de datos, evaluación de impacto, marco de calidad, plataformas de gestión.

ABSTRACT

The massive use of personal data on CRM platforms in Ecuador presents legal and technical risks stemming from deficient QA practices, due to the poor quality of quality control practices. These platforms assist companies in storing, organizing, and researching large amounts of personal data.

This situation poses significant challenges regarding the safeguarding and security of information. With the LOPDP (Organic Law on the Protection of Personal Data), which came into effect in 2021, Ecuador established a legal framework for the proper use of this data.

This, therefore, compelled entities in both the public and private sectors to implement practical methods for compliance. Furthermore, current CRM practices regarding data protection and the most frequent risks of the improper handling of personal information are evaluated.

The study incorporates technical and organizational elements such as privacy policies, internal audits, incident management, DPIA, and ongoing training, aligned with international standards like ISO/IEC 27001. This allows for the structuring of a proposed quality framework that includes functional and non-functional requirements applicable to the CRM environment.

The proposed framework is then validated through its application in a case study, demonstrating its applicability, relevance, and contribution to regulatory compliance, as well as to strengthening information security in Ecuadorian organizations.

Palabras clave:

data protection, impact assessment, quality framework, management platforms.

1. Introducción

La transformación digital bueno, ha cambiado enteramente la forma en que las organizaciones manejan sus conexiones con la clientela, empujando la unión de tecnologías innovadoras que automatizan y optimizan toda clase de procesos empresariales.

En este escenario, las plataformas Customer Relationship Management (CRM) se han convertido en herramientas fundamentales para centralizar la información importante de los usuarios, mejorar la atención personalizada y también fortalecer las estrategias comerciales.(Santamaría-Mendoza et al., 2024)

El funcionamiento de los sistemas Customer Relationship Management (CRM), básicamente, engloba recopilar, guardar, y analizar un montón de datos personales. Nombres, direcciones, historiales de compra, hasta el comportamiento de consumo entran en juego.

Este proceso de datos arduo a veces puede presentar riesgos peligrosos, por ejemplo, accesos no autorizados, la pérdida de datos y el mal uso de la información por parte de personas. (Garcia, 2022)

En Ecuador la Ley Orgánica de Protección de Datos Personales (LOPDP) entra en vigor, estableciendo un marco legal para el tratamiento de datos personales con transparencia, legalidad y responsabilidad como base. Reconoce, la normativa, importantes derechos de los dueños, también requiriendo a las organizaciones poner en marcha medidas seguras que protejan la integridad, la confidencialidad y la disponibilidad de la información.

Sin embargo, muchas empresas carecen de metodologías estandarizadas que les permitan evaluar el cumplimiento normativo y funcional de sus plataformas Customer Relationship Management (CRM), esto evidencia una brecha significativa entre la regulación y su aplicación práctica.(Hernández Alvarado et al., 2023)

La seguridad en los sistemas CRM se convierte en un componente crítico para salvaguardar la privacidad y la confianza de los usuarios, por el simple hecho de que no existen metodologías estandarizadas para evaluar el cumplimiento normativo de la LOPDP en plataformas CRM.

Resulta absolutamente necesario configurar controles de acceso, también implementar mecanismos robustos de auditoría y establecer procedimientos claros para la gestión de incidentes para atenuar amenazas, filtraciones, o manipulaciones incorrectas. Sin esa estructura, las organizaciones se ven muy limitadas en su capacidad para asegurar el cumplimiento con la LOPDP y por añadidura, para edificar una cultura de protección de datos que perdure.

Ante esta problemática, el presente artículo tiene como objetivo Diseñar y validar un marco de aseguramiento de la calidad orientado al cumplimiento de la LOPDP en plataformas CRM. El marco abarca facetas técnicas, legales, organizativas. Así es como se evalúa el manejo de datos personales en cada fase incorporando indicadores, es algo útil para detectar fallas y mejorar la seguridad, el cumplimiento legal.(Vinueza Ochoa et al., 2024)

2. Estudios Previos

La LOPDP protege y asegura los derechos de todos, respecto al manejo de su información en suelo ecuatoriano. Esa ley se centra en mantener la confidencialidad, la disponibilidad, y la integridad de la información, siguiendo normas globales como la ISO/IEC 27001:2022 y la NIST 800-53 r5. (ISO/IEC, 2022)

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI), usando la ISO/IEC 27001:2013, ha sido exitoso, cuidando los datos públicos aquí, en Ecuador. (Tintin & Hidalgo, 2023)

2.1. Marcos Normativos en Seguridad de la Información y Protección de Datos

En la protección de datos personales y la gobernanza digital, los Sistemas de Gestión de Seguridad de la Información son fundamentales. De hecho, el estándar internacional ISOIEC 270012013 se ha convertido, en un punto de referencia a nivel mundial para establecer, implementar, mantener y también, mejorar controles.

Este modelo, basado en el ciclo de mejora continua (PDCA: Plan-Do-Check-Act), faculta a las organizaciones para administrar riesgos tecnológicos y satisfacer requisitos regulatorios de forma sistemática y auditable. En Ecuador, adoptar ISOIEC 270012013 en las instituciones públicas ha mostrado ser un buen camino para robustecer la seguridad de los datos públicos. ((ISO), 2022)

Diversas entidades gubernamentales ya validaron sus procesos cruciales mediante este estándar, con esto lograron reforzar su habilidad para neutralizar amenazas serias como ciberataques, accesos no permitidos, o hasta pérdida de información vital. (ENISA, 2023) Además, implementar el SGSI mejoró la cultura interna sobre

la seguridad de la información, fomentando una gestión activa de incidentes, y por supuesto, una mejor armonización con leyes como la LOPDP. (27001, 2024)

Esta alineación no solo cumple con las normas legales, también eleva la confianza del público en los servicios digitales estatales. Así es como el SGSI con ISOIEC 27001:2013 proporciona una base sólida, técnica y metodológica, para diseñar estructuras de cumplimiento que funcionan en el ámbito privado, pensemos en los sistemas CRM. Su enfoque ordenado ayuda a identificar fallas de seguridad y establecer controles pertinentes.

El Registro de la Propiedad del Cantón Pedro Moncayo, en Ecuador, ha sido reconocido como un caso verdaderamente notable en la puesta en marcha exitosa de un Sistema de Gestión de Seguridad de la Información SGSI, bajo la guía de la norma ISOIEC 270012013. El modelo creado por esta institución ha generado un impacto, que va mucho más allá de sus propios límites, consolidándola, como un modelo de buenas prácticas en todo el país. (Narváez, 2022)

2.2. Principales desafíos de cumplimiento para la protección de datos en CRM

La implementación efectiva de medidas de la LOPDP en plataformas CRM enfrenta diversos desafíos estructurales, normativos y culturales. Uno de los principales obstáculos es la falta de claridad interpretativa en la LOPDP, que, si bien representa un avance sustantivo en materia de derechos digitales, aún presenta vacíos normativos y ambigüedades técnicas que dificultan su aplicación práctica en entornos tecnológicos específicos como los sistemas de gestión de relaciones con clientes. ((SPDP), 2023)

Adicionalmente, existe una escasa conciencia institucional y ciudadana sobre los derechos vinculados a los datos personales, esto reduce la presión social y regulatoria para garantizar su cumplimiento. Muchas empresas implementan soluciones CRM sin evaluar adecuadamente los riesgos asociados al uso,

almacenamiento y procesamiento de información personal sensible. (Ponchietti, 2022)

Esta falta de cultura de protección de datos se ve agravada por la baja disponibilidad de personal capacitado en privacidad digital, seguridad de la información y cumplimiento normativo, especialmente en pequeñas y medianas empresas, que conforman el grueso del tejido empresarial ecuatoriano.

Otro desafío relevante es la inexistencia de mecanismos de fiscalización eficaces por parte de la Autoridad de Protección de Datos, así como la limitada interoperabilidad entre sistemas tecnológicos y las exigencias de la LOPDP. A esto se suma la necesidad urgente de reformas complementarias que garanticen coherencia entre esta ley y otros cuerpos normativos, como la Ley de Comercio Electrónico o la Ley de Gobierno Digital.(ÁLVAREZ VALENZUELA, 2022)

Todo lo anterior genera un entorno de aplicación fragmentado, donde el cumplimiento depende más de la iniciativa voluntaria de las organizaciones que de una gobernanza institucional robusta.

Bajo estas condiciones, el desarrollo de marcos de calidad y modelos de evaluación adaptados a plataformas CRM se vuelve crucial. Estas herramientas como los marcos de calidad, las matrices de evaluación de riesgos y los modelos de auditoría para plataformas CRM, pueden servir como puentes entre la legislación y la práctica organizacional, facilitando el diseño de controles, la auditoría de cumplimiento y la formación de capacidades internas. (Narvaez Taranto & Gonzales Arbaiza, 2018)

2.3. Mejores prácticas para garantizar el cumplimiento de la protección de datos en CRM

Una de las mejores prácticas fundamentales es que las organizaciones públicas y privadas reconozcan la protección de datos personales como una responsabilidad

institucional ineludible y no simplemente como una carga administrativa o una formalidad legal.

Aunque la LOPDP constituye un avance significativo, la rápida evolución tecnológica requiere que la normativa ecuatoriana se mantenga actualizada y alineada con los estándares internacionales en materia de protección de datos y seguridad de la información.

Se recomienda incorporar y referenciar marcos normativos como el Reglamento General de Protección de Datos de la Unión Europea (GDPR), así como buenas prácticas establecidas por la OCDE y organismos internacionales de estandarización.(Ponchietti et al., 2021)

Esto implica que tanto el ente regulador como las entidades públicas que gestionan datos personales como registros civiles, catastros y plataformas digitales de servicios ciudadanos estén obligadas a implementar mecanismos de cumplimiento técnico, jurídico y organizacional basados en estándares como ISO/IEC 27001 y 27701.

Otro aspecto crucial es la capacitación continua en materia de privacidad, derechos digitales y gestión de riesgos. Tanto el personal técnico como administrativo que utiliza plataformas CRM debe conocer sus responsabilidades legales y operativas respecto al tratamiento de datos personales.

2.4. Principios Clave de Protección de Datos

El sistema jurídico ecuatoriano lidia con los retos del habeas data, protegiendo datos personales. Exige un marco legal fuerte y flexible, para afrontar los nuevos desafíos tecnológicos

En Ecuador, el reconocimiento del derecho a la protección de datos personales ha cambiado mucho en los últimos años, con el habeas data incluido como un

mecanismo constitucional de defensa, protegiendo contra el uso indebido de información personal.

Este recurso, consagrado en el artículo 92 de la Constitución de la República del Ecuador, permite a toda persona acceder, rectificar, actualizar, eliminar o conocer el uso de sus datos personales almacenados en archivos físicos o digitales, sean estos públicos o privados, esto se visualiza en la Figura 1.(Gutiérrez Proenza, 2022)

Figura 1 Aspectos clave de la LOPDP
Fuente: Cristian González - Claves para el cumplimiento de la Ley de Protección de Datos en una empresa (noviembre-2023)

Aun así, aunque la Constitución puso los cimientos para proteger datos con el habeas data, el sistema judicial ecuatoriano tuvo que cambiar para lidiar con el manejo enorme y automático de información personal en ambientes tecnológicos de alta gama.(Machuca Vivar et al., 2022)

Considerando esto, una robusta y especializada estructura legal se hizo completamente necesaria por el auge de plataformas como los CRM para redes sociales, sistemas biométricos y más. La promulgación de la LOPDP en 2021 significo un paso importante en esta modernización normativa. Esta ley fija ciertas disposiciones legales regulando el tratamiento de datos personales en Ecuador,

protegiendo los derechos de las personas ante los responsables y encargados del tratamiento.(Baz Rodríguez, 2021)

La LOPDP articula el ejercicio de los derechos del titular en torno al habeas data. Esto permite que, además de interponer la acción constitucional tradicional, los ciudadanos puedan ejercer derechos específicos como el acceso, la rectificación, la oposición, la supresión o la portabilidad de sus datos, conforme a reglas claras y plazos definidos.

Esta ampliación de mecanismos genera mayor seguridad jurídica, estandariza obligaciones para los responsables del tratamiento, y establece un marco de corresponsabilidad en la gestión ética y segura de los datos personales (Cueva, 2022). En consecuencia, el sistema jurídico ecuatoriano ha pasado de un enfoque declarativo, centrado únicamente en derechos abstractos, a un modelo normativo operativo, que integra principios constitucionales, leyes orgánicas y estándares internacionales en un cuerpo legal que busca responder a los desafíos del mundo digital.

No obstante, la correcta implementación de este marco depende de su aplicación efectiva en entornos tecnológicos concretos, como los sistemas CRM, donde el cumplimiento normativo debe ser evaluado a través de herramientas operativas como marcos de calidad, auditorías de cumplimiento y sistemas de gestión de seguridad de la información.

2.5. Sanciones por incumplimiento de la LOPDP

El artículo explora el complejo panorama de las leyes de protección de datos en Ecuador, analizando los enfoques legislativos y las sanciones por incumplimiento. También ofrece información sobre Sistemas de Gestión de Seguridad de la Información (SGSI) eficaces, adaptados al marco regulatorio ecuatoriano. La LOPDP establece un régimen sancionatorio claro y progresivo para las organizaciones que incumplen con las obligaciones relativas al tratamiento de datos personales.

En el caso de plataformas CRM, donde se centraliza y gestiona una gran cantidad de datos sensibles y de identificación personal de clientes, el riesgo de incurrir en infracciones es particularmente alto si no se cuenta con políticas adecuadas de privacidad, medidas técnicas de seguridad y protocolos de cumplimiento normativo.(Palomo Navarro, 2020)

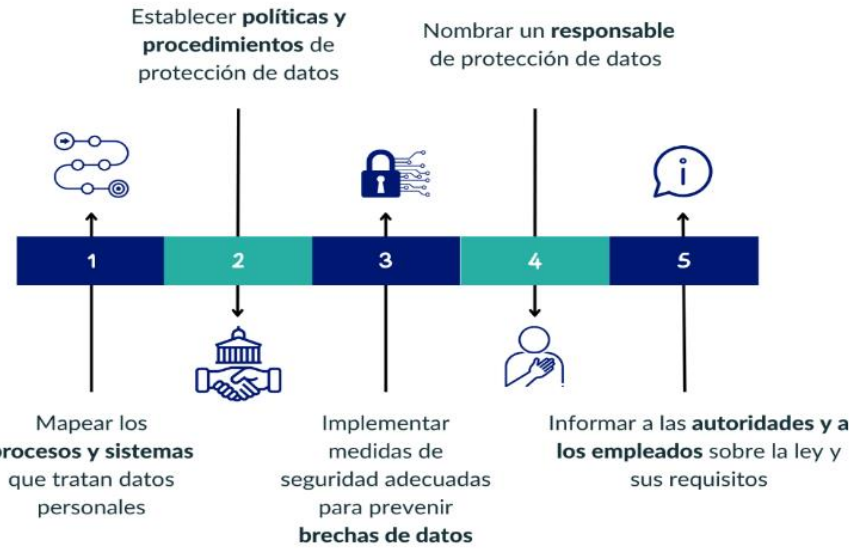

Figura 2 Cumplimiento de la LOPDP
Fuente: Cristian González - Claves para el cumplimiento de la Ley de Protección de Datos en una empresa (noviembre-2023)

Las sanciones previstas en la LOPDP pueden clasificarse en leves, graves y muy graves, dependiendo de la naturaleza de la infracción, la intencionalidad, el tipo de datos afectados, el nivel de perjuicio a los derechos de los titulares y la reincidencia.

Entre las infracciones graves y muy graves se encuentran: el tratamiento de datos sin base legal o sin consentimiento del titular; la vulneración de los principios de minimización, confidencialidad o conservación; la falta de respuesta a solicitudes de ejercicio de derechos; y la ausencia de medidas de seguridad técnicas y organizativas adecuadas.

En cuanto a las sanciones económicas, el Reglamento para la Aplicación de la Metodología para el Cálculo de las Multas, expedido por la Superintendencia de Protección de Datos Personales en 2025, establece una diferenciación entre

entidades públicas y privadas. Para los funcionarios públicos, las infracciones leves pueden ser sancionadas con multas de entre 1 y 10 salarios básicos unificados, mientras que las infracciones graves pueden conllevar multas de entre 10 y 20 salarios básicos unificados. Por su parte, para las entidades privadas, las infracciones leves implican sanciones que oscilan entre el 0,1 % y el 0,7 % de los ingresos por ventas, y las infracciones graves entre el 0,7 % y el 1 % de dichos ingresos, pudiendo incrementarse en casos de reincidencia o incumplimientos de mayor gravedad conforme a la LOPDP. (Personales, 2025)

Este sistema penalizador busca fomentar el cumplimiento correcto, y desalentar acciones descuidadas o intencionales, en el tratamiento de información personal. Por si fuera poco, la regulación permite castigos no financieros como, la interrupción temporal del tratamiento, la compensación obligatoria al titular o la prohibición de registrarse en registros estatales de proveedores.

En sistemas CRM, esas sanciones pueden dañar seriamente la operación y reputación de empresas, particularmente si ocurre una filtración masiva de datos, un uso no autorizado de información delicada, o la negación de derechos fundamentales a usuarios. La falta de mecanismos de rastreo, auditoría y control empeora el asunto. Dificulta la identificación y registro de las faltas.

La autoridad de control contemplada en la LOPDP posee la competencia única para indagar sancionar y fiscalizar que se cumpla la ley. Por lo tanto, organizaciones gestionando datos mediante CRM necesitan estar listos para auditorías externas pedimentos documentales inspecciones técnicas y las evaluaciones de impacto en la protección de datos.

El incumplimiento reiterado o la resistencia a las acciones de la autoridad pueden constituir agravantes que eleven la cuantía de las sanciones o deriven en responsabilidades civiles o incluso penales.(Estepa Montero, 2022)

En este sentido, el diseño e implementación de un marco de calidad específico para sistemas CRM que contemple procedimientos de evaluación continua, alineación normativa y medidas de seguridad integradas no solo contribuye al cumplimiento

proactivo, sino que también funciona como una estrategia preventiva frente a posibles sanciones. Este enfoque garantiza no solo la integridad jurídica de la organización, sino también la confianza de sus clientes y el fortalecimiento de su reputación institucional en el entorno digital.

2.6. Derechos de los interesados

El derecho de acceso a la información pública en el Ecuador está garantizado por la Ley Orgánica de Transparencia y Acceso a la Información Pública, la cual se constituye en un mecanismo procesal para garantizar este derecho, asegurando la obtención, acceso y gestión de la información por parte de los ciudadanos del Ecuador.

En el intricado sistema legal ecuatoriano, los derechos de quienes poseen datos personales brillan como pilares clave en la protección de datos. La LOPDP establece derechos importantes que habilitan a la gente para gobernar su información personal, especialmente cuando se maneja automáticamente a través de plataformas tecnológicas, incluyendo los sistemas CRM.

Entre los derechos de mayor peso, encontramos el de acceso, que da poder a la persona para saber si sus datos están siendo procesados, con qué objetivo, por quién y en qué condiciones. Este derecho está unido a los principios de transparencia, legalidad y responsabilidad proactiva y fuerza a las empresas a crear sistemas sencillos, asequibles y eficientes, para dar respuesta a las peticiones de datos de los involucrados.(Calle García et al., 2024)

El derecho de rectificación concede al individuo la potestad de ajustar información incorrecta o incompleta, garantizando la fiabilidad y vigencia de los datos procesados. En los sistemas CRM, donde los datos impulsan decisiones empresariales, la segmentación de clientes y estrategias de marketing automatizadas, la precisión de la información es absolutamente crucial, para iniciativas basadas en datos desactualizados.(Pajares Gómez, 2023)

El derecho de portabilidad, que permite al titular recibir sus datos en un formato estructurado y de uso común, y transmitirlos a otro responsable sin impedimentos. Este derecho se vuelve particularmente relevante en entornos CRM donde el usuario puede cambiar de proveedor de servicios, exigir interoperabilidad o ejercer su autonomía digital.

Igualmente, se reconoce el derecho a no ser objeto de decisiones automatizadas sin intervención humana significativa, lo cual cobra especial importancia ante el uso de algoritmos en CRM para realizar perfilamientos, predicciones de comportamiento o asignación de beneficios.

Para que estos derechos sean ejercidos efectivamente, las organizaciones responsables del tratamiento de datos personales deben habilitar canales formales de atención, establecer plazos de respuesta razonables y mantener registros documentales de cada solicitud.

2.7. Seguridad en CRM

La seguridad de los sistemas CRM, no reside solamente en configuraciones técnicas complicadas; más bien, la conciencia general dentro de la organización sobre peligros es esencial. Hay muchas amenazas frecuentes para el CRM, el acceso no autorizado, por ejemplo, mediante contraseñas fáciles. También amenazas internas, o el uso impropio por el personal, ataques de phishing con cosas como smishing y vishing, o el malware, como el ransomware o spyware. Estos problemas amenazan la integridad y confidencialidad de la información e incluso pueden causar quebrantos normativos bajo la LOPDP.

En esta situación, se vuelve clara la importancia de un marco concreto para administrar plataformas CRM en Ecuador. Esto debe entrelazar coherentemente los requisitos regulatorios, las precauciones de seguridad y las prácticas de garantía de calidad (QA). Un marco bien estructurado ofrecería criterios precisos para tomar decisiones, y posibilitaría que los sistemas CRM funcionen con mejores salvaguardas de privacidad.

2.8. Vigilancia tecnológica

Desde el enfoque de la vigilancia tecnológica, estudios recientes han analizado estrategias, modelos y marcos metodológicos orientados a resolver problemáticas similares a las abordadas en el presente trabajo, particularmente aquellas relacionadas con la protección de datos personales, la seguridad de la información y el cumplimiento normativo en sistemas de información y plataformas CRM.

Investigaciones recientes evidencian que la adopción de Sistemas de Gestión de Seguridad de la Información basados en estándares internacionales continúa siendo una de las soluciones más eficaces para reducir riesgos tecnológicos y fortalecer el cumplimiento normativo. En este sentido, (Tintin & Hidalgo, 2023) demuestra que la implementación de un SGSI conforme a la norma ISO/IEC 27001 permite mejorar la gestión de incidentes, la trazabilidad de los procesos y la protección de datos en instituciones públicas ecuatorianas.

A nivel internacional, organismos especializados como la Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2023) proponen enfoques integrales basados en la gestión de riesgos, la evaluación continua de amenazas y la incorporación de controles de seguridad desde el diseño de los sistemas (privacy by design), especialmente en plataformas que gestionan grandes volúmenes de datos personales y automatizan procesos de toma de decisiones, como los sistemas CRM.

Asimismo, estudios recientes destacan la necesidad de complementar los marcos normativos con modelos de evaluación y auditoría específicos para sistemas de información, que permitan medir de forma objetiva el grado de cumplimiento legal y técnico. En este contexto, (Narváez, 2022) evidencia que la aplicación práctica de ISO/IEC 27001 en entidades públicas ecuatorianas no solo fortalece la seguridad de la información, sino que genera modelos replicables de buenas prácticas a nivel nacional.

De forma complementaria, (Ponchietti et al., 2021) y (Calle García et al., 2024) señalan que la rápida evolución de las plataformas digitales exige marcos de cumplimiento dinámicos, capaces de adaptarse a nuevas amenazas, regulaciones y tecnologías, especialmente en entornos CRM donde el tratamiento automatizado de datos personales es constante.

En conjunto, la vigilancia tecnológica realizada muestra que, si bien existen propuestas y experiencias exitosas desde 2022, persiste la necesidad de desarrollar marcos de calidad específicos para plataformas CRM, alineados con la LOPDP y adaptados al contexto ecuatoriano, lo que justifica plenamente el desarrollo del presente trabajo de titulación.

3. METODOLOGÍA

La investigación fue desarrollada utilizando un enfoque cualitativo y aplicado. El objetivo era diseñar un marco de aseguramiento de la calidad o QA, que incorpore controles eficaces para proteger los datos personales en plataformas CRM, siguiendo la LOPDP de Ecuador, así como estándares globales.

El estudio empleó métodos teóricos y empíricos a la vez. Esto permitió una comprensión normativa, organizacional y técnica del problema, asegurando un análisis que consideró causas múltiples. Desde los principios de regulación, hasta la comprobación de soluciones prácticas fue cubierta.

El proceso metodológico fue organizado en cinco fases sucesivas, diseñado para garantizar trazabilidad, validez y replicación científica.

3.1. ETAPA I: REVISIÓN NORMATIVA Y COMPARATIVA

Para tal efecto, se llevó a cabo un análisis documental sistemático desde la propia ley LOPDP, en concordancia con referentes internacionales de alto impacto, como el Reglamento General de Protección de Datos de la Unión Europea, la ISO/IEC 27001:2013 relativa a la seguridad de la información, y la ISO/IEC 27701:2019 en gestión de privacidad. La revisión realizada mediante codificación temática tuvo por objetivo completar principios, derechos, obligaciones, roles y medidas técnicas.

Esta fase se centró en la creación de un marco normativo cohesionado, que se utilizó como referencia para el diseño de la metodología. Su objetivo fue favorecer la alineación del modelo con estándares internacionales, lo que comenzó a estar en vigor en Ecuador, así como en jurisdicciones comparables al presente.

3.2. Etapa II: Análisis de prácticas actuales en entornos CRM

En la etapa correspondiente se examinaron las prácticas de aseguramiento de la calidad de la protección de los datos que utilizan las organizaciones que cuentan con capacidades de la CRM. En específico, se llevó a cabo entrevistas semiestructuradas a través de líderes de QA, oficiales de cumplimiento y responsables de protección de datos. Además, se revisó el material de documento requerido, como políticas internas, manuales de procedimiento, matrices de riesgos y configuración técnica.

Para la recolección de información en esta etapa se emplearon instrumentos cualitativos estructurados, diseñados con base en los principios de la LOPDP y los controles establecidos en las normas ISO/IEC 27001 e ISO/IEC 27701. Entre los instrumentos utilizados se incluyeron:

• **Guía de entrevista semiestructurada**, dirigida a líderes de QA, oficiales de cumplimiento y responsables de protección de datos, orientada a identificar prácticas actuales, niveles de madurez y mecanismos de control en entornos CRM.

Ejemplos de ítems:

- ¿La organización cuenta con políticas formales para el tratamiento de datos personales en el CRM?
- ¿Cómo se gestionan los incidentes de seguridad relacionados con datos personales?
- ¿Existen controles de QA específicos para validar la calidad y legalidad de los datos?
- ¿Qué mecanismos se utilizan para garantizar el consentimiento informado de los titulares?

• **Lista de verificación de cumplimiento normativo**, aplicada sobre políticas internas, procedimientos y configuraciones técnicas del CRM, para evaluar el grado de alineación con la normativa vigente.

Ejemplos de criterios evaluados:

- Existencia de un inventario de datos personales
- Definición de roles y responsabilidades (DPO, QA, TI)
- Controles de acceso y autenticación en el CRM
- Procedimientos documentados para derechos ARCO
- Registro y gestión de incidentes de seguridad

• **Formato de revisión documental**, utilizado para el análisis sistemático de manuales, matrices de riesgo, políticas de seguridad y documentación técnica.

Documentos analizados:

- Políticas de seguridad de la información
- Manuales de QA
- Procedimientos internos
- Contratos de confidencialidad
- Configuraciones técnicas del CRM

Campos del formato:

- Documento revisado
- Área responsable
- Cumple / No cumple / Parcial
- Observaciones

• **Matriz preliminar de riesgos**, empleada para registrar vulnerabilidades, amenazas y controles existentes asociados al tratamiento de datos personales.

Estructura básica del formato:

- Riesgo identificado
- Activo afectado
- Probabilidad (P)
- Impacto (I)
- Nivel de riesgo (R = P × I)
- Control existente
- Medidas de mitigación propuestas

En los pocos casos posibles, se hizo una observación técnica directa en entornos CRM. El análisis revelo el nivel de concordancia entre las prácticas existentes y lo que dicen las reglas, mostrando huecos normativos, fallos en la operativa, y mejoras posibles.

3.3. Etapa III: Identificación y análisis de riesgos

Los riesgos asociados al tratamiento de datos en QA se caracterizaron mediante la triangulación de tres técnicas: análisis de casos documentados de vulneración de datos, aplicación de listas de verificación basadas en normativa y estándares ISO, y construcción de matrices de riesgo. Para cada riesgo se estimaron la probabilidad de ocurrencia (*P*) y el impacto (*I*), aplicando la relación:

$$R=P\times I$$

Para cada riesgo identificado se evaluaron dos variables fundamentales: la **probabilidad de ocurrencia (P)** y el **impacto (I)**. La probabilidad representa la frecuencia o posibilidad estimada de que el riesgo se materialice en el entorno de QA, mientras que el impacto corresponde a la magnitud del daño potencial sobre la seguridad y privacidad de los datos.

Una vez obtenidos estos valores, el nivel de riesgo (**R**) se calcula aplicando el algoritmo multiplicativo **R = P × I**, cuyo propósito es integrar ambas dimensiones en un único indicador cuantitativo. De este modo, un riesgo con baja probabilidad, pero alto impacto, o viceversa, puede reconocerse y priorizarse con mayor precisión. Esta lógica permite diferenciar entre riesgos aceptables, moderados y críticos, y facilita la organización de los resultados en el mapa de riesgos priorizados.

3.4. Ejemplo de aplicación del modelo de estimación y medición del riesgo

Con el propósito de operacionalizar el análisis de riesgos descrito en la Etapa III, se presenta a continuación un ejemplo práctico de identificación, medición y priorización del riesgo, aplicado a un entorno CRM durante procesos de aseguramiento de la calidad (QA).

Riesgo analizado: Acceso no autorizado a datos personales de clientes almacenados en el CRM durante actividades de QA.

Este riesgo fue identificado mediante la triangulación metodológica de: Análisis de casos documentados de vulneración de datos en sistemas CRM, aplicación de listas de verificación basadas en la LOPDP, ISO/IEC 27001:2013 e ISO/IEC 27701:2019 y revisión de configuraciones técnicas y roles de acceso en el sistema CRM.

Estimación de la probabilidad (P)

La probabilidad de ocurrencia se calculó utilizando una escala ordinal de cinco niveles (1–5), considerando la frecuencia histórica del evento, el nivel de madurez de los controles existentes y el grado de exposición del proceso QA.

En el caso analizado, se identificaron debilidades en los controles de acceso, tales como cuentas compartidas y ausencia de autenticación multifactor para personal de QA, lo que incrementa la posibilidad de materialización del riesgo.

Por tanto, se asignó una probabilidad alta, correspondiente a: P = 4

Estimación del impacto (I)

El impacto se estimó considerando las siguientes dimensiones, alineadas con la LOPDP y la ISO/IEC 27001:

- Afectación a los derechos de los titulares de datos
- Consecuencias legales y sancionatorias
- Daño reputacional institucional
- Impacto operativo y organizacional

Dado que un acceso no autorizado podría comprometer datos personales sensibles, generar sanciones administrativas significativas y afectar el ejercicio de derechos ARCO, el impacto fue clasificado como muy alto, asignándose el valor: I = 5

Cálculo del nivel de riesgo (R)

El nivel de riesgo se determinó aplicando el modelo multiplicativo definido en la investigación:

$$R = P \times I$$
$$R = 4 \times 5 = 20$$

Clasificación y priorización del riesgo

De acuerdo con la escala de priorización adoptada en el estudio, un valor de R = 20 corresponde a un riesgo alto o crítico, lo que implica la necesidad de aplicar medidas de mitigación inmediatas, tales como:

- Implementación de autenticación multifactor
- Segregación estricta de roles y privilegios
- Auditorías periódicas de accesos
- Fortalecimiento de controles de QA sobre seguridad de la información

Este ejemplo evidencia cómo la metodología propuesta permite estimar el riesgo de manera sistemática, trazable y replicable, facilitando su priorización y tratamiento conforme a la normativa ecuatoriana y estándares internacionales.

Valor	Nivel	Descripción
1	Muy baja	El evento es poco probable; no existen antecedentes conocidos.
2	Baja	El evento podría ocurrir de forma excepcional.
3	Media	El evento ha ocurrido ocasionalmente en la organización o en casos similares.
4	Alta	El evento ocurre con frecuencia conocida.
5	Muy alta	El evento ocurre de forma recurrente o sistemática.

Tabla 1 Escala de probabilidad de ocurrencia (P)

Valor	Nivel	Descripción
1	Muy bajo	Afectación mínima, sin impacto legal ni operativo
2	Bajo	Impacto limitado y controlable
3	Medio	Afectación a derechos de titulares o procesos internos
4	Alto	Incumplimiento normativo, posibles sanciones y daño reputacional
5	Muy alto	Violación grave de datos personales, sanciones severas y daño institucional

Tabla 2 Escala de impacto sobre la protección de datos (I)

Riesgo identificado	P	I	R = P × I	Nivel de riesgo
Acceso no autorizado a datos personales por fallas en controles de autenticación	4	5	20	Crítico

Tabla 3 Ejemplo de cálculo del nivel de riesgo

El riesgo evaluado presenta una probabilidad alta (P=4) y un impacto muy alto (I=5), resultando en un nivel de riesgo crítico (R=20), lo que requiere la aplicación inmediata de controles técnicos y organizativos.

3.5. Etapa IV: Diseño del marco de aseguramiento de calidad

Con base en los hallazgos anteriores, se diseñó un marco QA para CRM, estructurado en dimensiones clave como gobernanza, seguridad, consentimiento, transparencia, riesgos, ciclo de vida de los datos, cultura organizacional y auditoría. El diseño aplicó principios de ingeniería de requisitos y modelado de procesos (BPMN), incorporando:

- Requisitos funcionales y no funcionales derivados de la normativa y estándares analizados.
- Indicadores de cumplimiento y métricas de eficacia.
- Controles técnicos y mecanismos de evaluación.
- Algoritmos de apoyo, como árboles de decisión de cumplimiento normativo, motores de reglas para verificación de conformidad y algoritmos de estimación de riesgos.

El marco fue concebido como un prototipo adaptable a organizaciones de diferentes tamaños y niveles de madurez tecnológica, con niveles progresivos de implementación. Con el fin de operacionalizar el marco de aseguramiento de la calidad propuesto, se desarrolló un modelo estructurado por dimensiones, cada una alineada con los principios de la LOPDP y con controles establecidos en normas internacionales como ISO/IEC 27001 e ISO/IEC 27701.

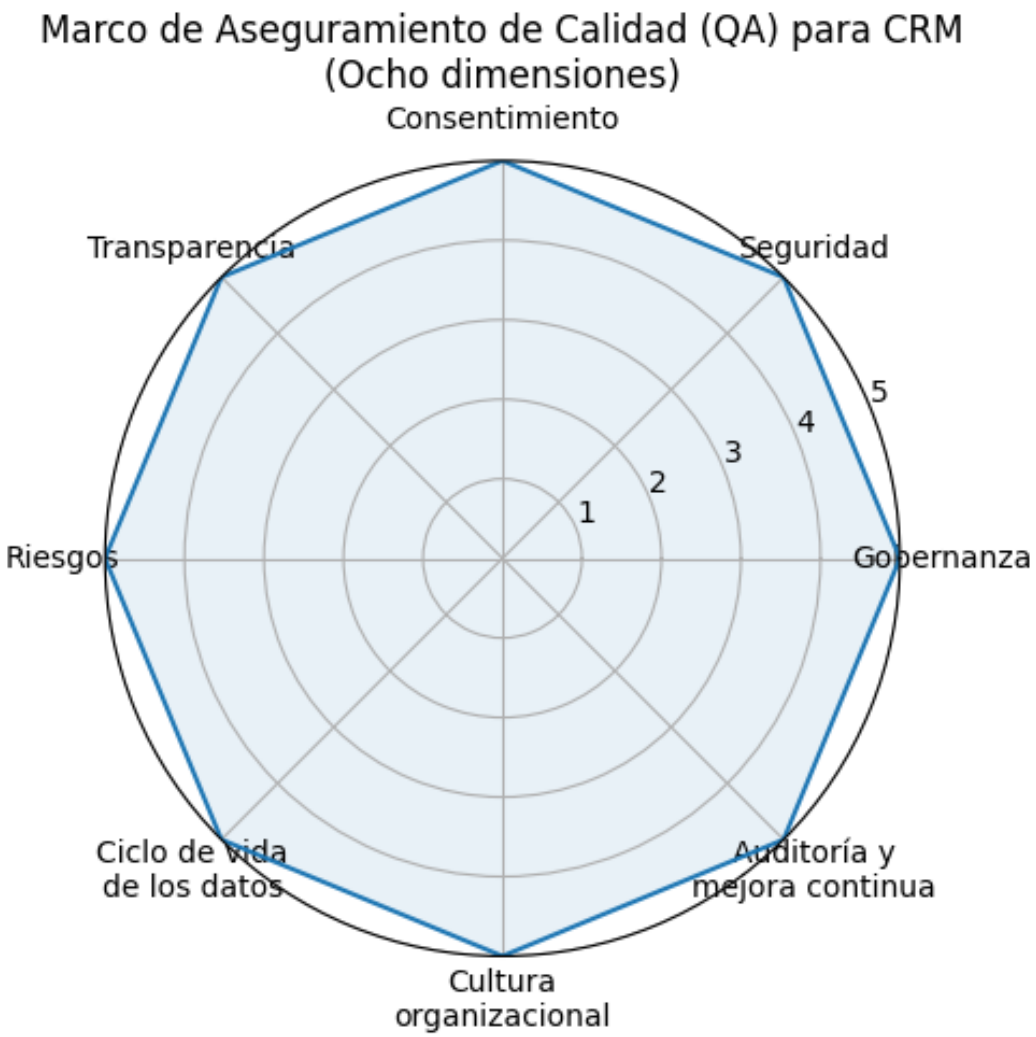

Figura 3 Marco de Aseguramiento de Calidad (QA) para CRM

La Figura 3 presenta de forma sintética el marco QA propuesto, organizado en ocho dimensiones interrelacionadas que permiten evaluar, controlar y mejorar la calidad del tratamiento de datos personales en plataformas CRM. A continuación, se presenta un ejemplo explícito del diseño del marco aplicado a un proceso típico de gestión de clientes en una plataforma CRM.

Dimensión	Objetivo de control	Requisito QA	Indicador de cumplimiento	Control propuesto
Gobernanza	Garantizar responsabilidad y trazabilidad	Existencia de roles definidos (DPO, QA, TI)	% de roles formalmente asignados	Política de gobierno de datos
Seguridad	Proteger la confidencialidad e integridad	Control de accesos basado en roles	Nº de accesos no autorizados	Autenticación multifactor (MFA)
Consentimiento	Asegurar legalidad del tratamiento	Registro verificable del consentimiento	% de registros con consentimiento válido	Módulo de gestión de consentimientos
Transparencia	Informar al titular del uso de datos	Avisos de privacidad accesibles	Nivel de cumplimiento informativo	Políticas visibles en CRM
Riesgos	Identificar y mitigar amenazas	Evaluación periódica de riesgos	Nº de riesgos críticos mitigados	Matriz de riesgos CRM
Ciclo de vida	Controlar retención y eliminación	Políticas de conservación de datos	% de datos eliminados conforme a política	Automatización de borrado
Cultura organizacional	Fomentar buenas prácticas	Capacitación en protección de datos	Nº de capacitaciones anuales	Programas de formación continua
Auditoría	Verificar cumplimiento continuo	Auditorías internas periódicas	Nº de hallazgos corregidos	Checklists de auditoría QA

Tabla 4 Diseño del marco aplicado a un proceso típico de gestión de clientes en una plataforma CRM

El marco fue diseñado aplicando principios de ingeniería de requisitos, donde cada dimensión se tradujo en requisitos funcionales (por ejemplo, gestión de consentimientos en el CRM) y no funcionales (seguridad, trazabilidad, disponibilidad). Estos requisitos fueron posteriormente modelados mediante procesos BPMN para representar flujos como el alta de clientes, tratamiento de datos y atención de derechos de los titulares.

3.6. Etapa V: Validación del marco propuesto

La validación se efectuó en dos modalidades: (i) mediante un estudio de caso en una organización con implementación de CRM, y (ii) a través de una simulación experimental en entornos prototipo (SuiteCRM, Odoo).

Se escogieron SuiteCRM, Odoo, porque estos sistemas son muy populares en Ecuador; son de código abierto, es decir se puede cambiar partes de código y hacer pruebas, tienen muchas comunidades de desarrolladores y una gran documentación. Con esto, se facilita la evaluación directa de la seguridad, la trazabilidad y QA, lo que en los CRM's propietarios con módulos cerrados, no se podría.

Para la evaluación se aplicaron matrices de cumplimiento, indicadores de reducción de riesgo y retroalimentación cualitativa de expertos en derecho digital, QA y seguridad de la información. El análisis permitió valorar la aplicabilidad, pertinencia normativa, factibilidad operativa y capacidad de mitigación de riesgos del marco propuesto. La información recogida condujo a ajustes finales que fortalecieron su robustez metodológica y su utilidad práctica.

Para validar el marco de aseguramiento de la calidad diseñado, se aplicó un proceso de evaluación mixto que combinó matrices de cumplimiento normativo, indicadores de reducción de riesgo y retroalimentación cualitativa de expertos en derecho digital, QA y seguridad de la información. A continuación, se presentan ejemplos concretos de cada instrumento y su aplicación.

Dimensión	Requisito normativo (LOPDP / ISO)	Control implementado en CRM	Nivel de cumplimiento
Seguridad	Control de accesos (ISO 27001 A.9)	Roles y perfiles configurados	Cumple
Consentimiento	Base legal del tratamiento (LOPDP)	Registro digital de consentimiento	Cumple parcialmente
Transparencia	Información al titular	Aviso de privacidad visible	Cumple
Riesgos	Evaluación periódica	Matriz de riesgos documentada	Cumple
Auditoría	Evidencia de controles	Registros de auditoría	No cumple

Tabla 5 Ejemplo de matriz de cumplimiento normativo aplicada a CRM

Escala utilizada:

- Cumple
- Cumple parcialmente
- No cumple

Aplicación:

Esta matriz fue utilizada tanto en el estudio de caso como en la simulación experimental, permitiendo identificar brechas de cumplimiento normativo en cada dimensión del marco QA.

Riesgo identificado	Nivel inicial (R_0)	Control aplicado	Nivel residual (R_1)	Reducción (%)
Acceso no autorizado	20 (Crítico)	MFA + control de roles	8 (Medio)	60 %
Uso indebido de datos	12 (Alto)	Políticas y capacitación	6 (Medio)	50 %

Pérdida de información	15 (Alto)	Backups y cifrado	5 (Bajo)	67 %

Tabla 6 Ejemplo de indicadores de reducción de riesgo

Aplicación:

Los indicadores permitieron medir cuantitativamente la eficacia del marco QA, comparando el nivel de riesgo antes y después de la implementación de los controles propuestos.

Perfil del experto	Aspecto evaluado	Observación principal	Ajuste realizado
Derecho digital	Consentimiento	Reforzar evidencia legal del consentimiento	Mejora del registro y trazabilidad
QA	Procesos	Falta de métricas claras	Inclusión de KPIs de cumplimiento
Seguridad de la información	Accesos	Riesgo en usuarios privilegiados	Separación de roles y MFA

Tabla 7 Ejemplo de retroalimentación cualitativa de expertos

Aplicación: La retroalimentación fue recolectada mediante entrevistas semiestructuradas y sesiones de revisión técnica. Los comentarios se sistematizaron y se tradujeron en ajustes concretos al marco QA, fortaleciendo su aplicabilidad y alineación normativa.

Integración de resultados en la validación: Los resultados obtenidos a partir de las matrices de cumplimiento, los indicadores de reducción de riesgo y la retroalimentación experta fueron triangulados para evaluar:

- La aplicabilidad práctica del marco en entornos CRM reales y simulados.
- Su pertinencia normativa frente a la LOPDP y estándares ISO.
- La factibilidad operativa de los controles propuestos.
- La capacidad efectiva de mitigación de riesgos.

Este proceso permitió realizar ajustes finales al marco QA, consolidándolo como una herramienta robusta, adaptable y alineada a la realidad tecnológica y normativa ecuatoriana.

3.7. Consideraciones finales del enfoque metodológico

El enfoque metodológico adoptado se sustentó en tres pilares fundamentales:

- Rigor normativo, mediante el análisis detallado de la LOPDP y estándares reconocidos internacionalmente.
- Vinculación con la práctica, mediante la incorporación de datos obtenidos de entrevistas, casos reales y documentación institucional.
- Validez constructiva, garantizada a través de un proceso iterativo de diseño, evaluación y validación.

Este diseño metodológico permitió generar un modelo original, replicable y adaptado a la realidad ecuatoriana, que sirva como referencia técnica y estratégica para organizaciones comprometidas con el cumplimiento de la normativa en protección de datos personales y la mejora continua de sus procesos de gestión de la calidad en plataformas CRM.

4. Resultados

Los resultados que fueron obtenidos reflejan la aplicación sistemática de las cinco etapas metodológicas, lo cual permitió construir y validar un marco de aseguramiento de calidad (QA) orientado a la protección de datos personales en plataformas CRM. Los hallazgos se presentan de manera estructurada, destacando la integración entre referentes normativos, diagnóstico de prácticas organizacionales, análisis de riesgos y validación empírica del modelo.

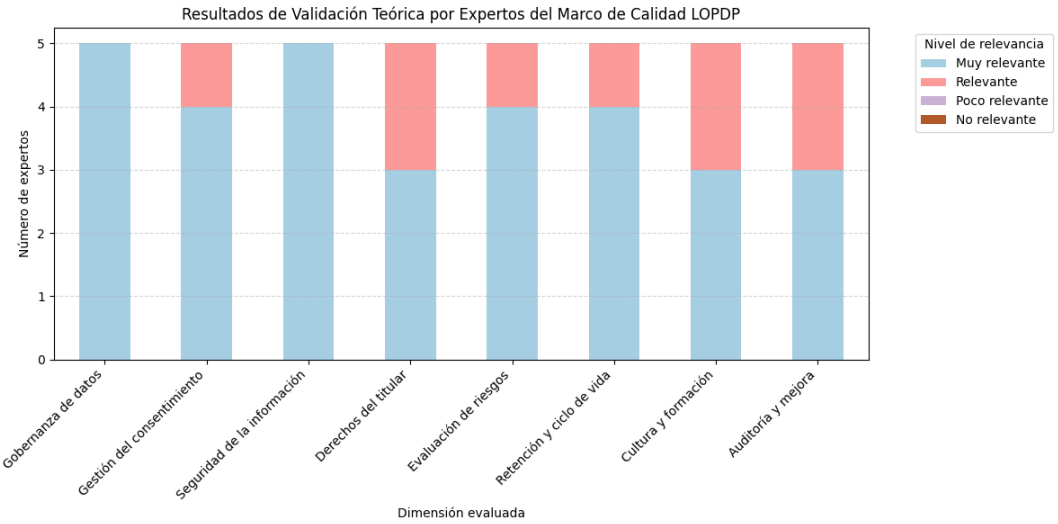

Figura 4 Resultados de Validación Teórica por Expertos de Calidad LOPDP

4.1. Resultados de la revisión normativa y comparativa

El análisis documental de la LOPDP, el Reglamento General de Protección de Datos (GDPR) y los estándares ISO/IEC 27001 y ISO/IEC 27701 permitió identificar principios esenciales como licitud, transparencia, minimización, responsabilidad proactiva y seguridad por diseño. La codificación temática evidenció que la LOPDP comparte más del 70 % de convergencia conceptual con el GDPR, aunque presenta vacíos en materia de mecanismos de auditoría y escalamiento de incidentes.

Este hallazgo orientó la necesidad de reforzar dichas dimensiones en el marco QA propuesto.

Producto de esta etapa:

- Una síntesis normativa estructurada con 45 requisitos organizados en dimensiones funcionales y técnicas.
- Un mapa de equivalencia normativa que facilita la alineación del cumplimiento.

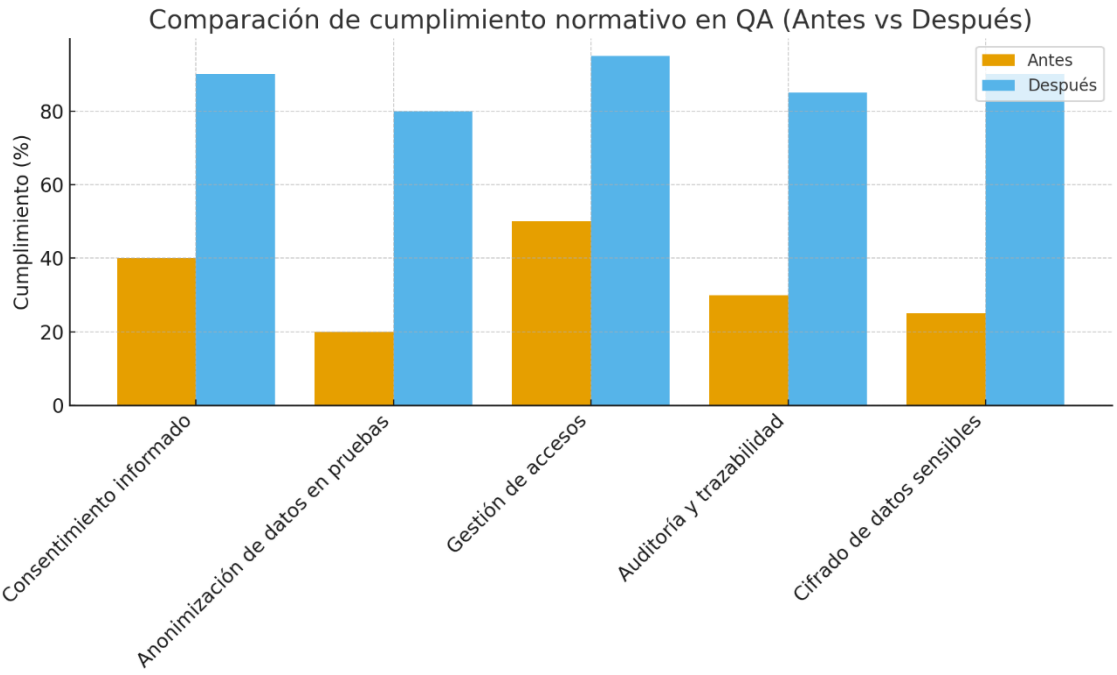

Figura 5 Comparación de cumplimiento normativo QA

4.2. Resultados del análisis de prácticas actuales en CRM

Las entrevistas semiestructuradas (n = 6 expertos) y la revisión documental evidenciaron una brecha promedio del 42 % entre las prácticas actuales de QA en plataformas CRM y los requisitos establecidos en la LOPDP. Entre los hallazgos más relevantes destacan:

- Uso de datos reales en entornos de prueba sin anonimización (reportado en el 67 % de los casos).
- Ausencia de matrices de trazabilidad de consentimientos en el 83 % de los sistemas analizados.
- Limitada incorporación de indicadores de cumplimiento normativo en procesos de QA.
- Producto de esta etapa: Diagnóstico cualitativo que visibiliza deficiencias operativas críticas en la implementación de privacidad desde el diseño.
- Identificación de oportunidades de mejora para integrar QA con control normativo.

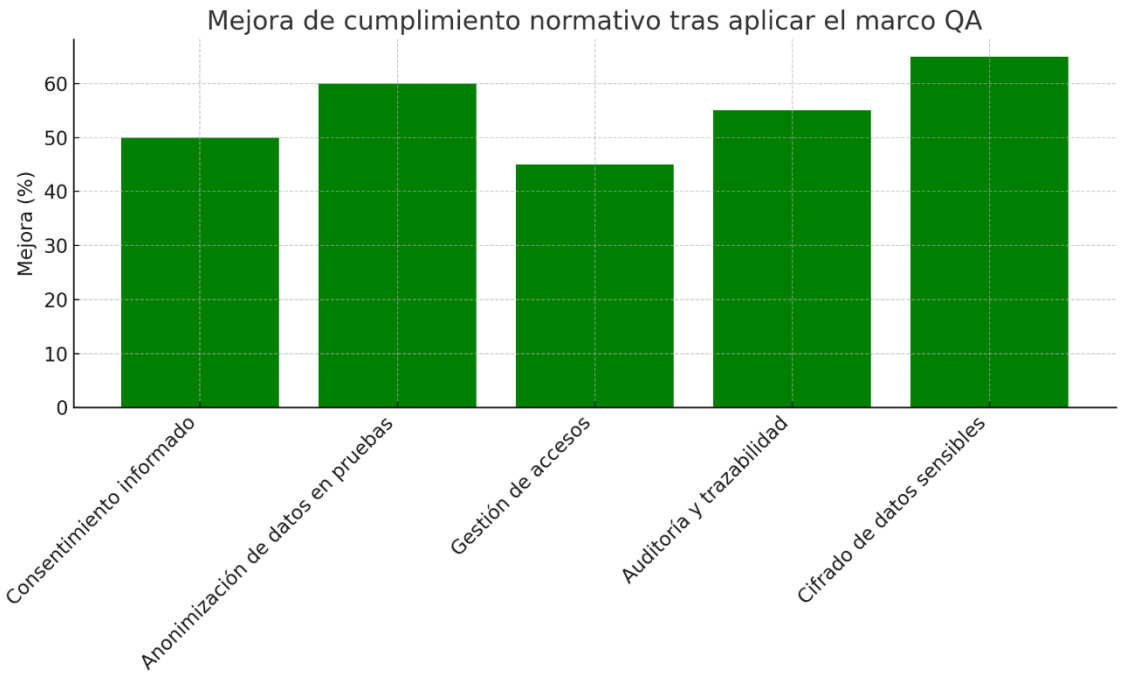

Figura 6 Mejora de cumplimiento normativo tras aplicar el marco QA

4.3. Resultados de la identificación y análisis de riesgos

El análisis de incidentes y la aplicación de listas de verificación permitieron construir una matriz de riesgos con 18 escenarios críticos. El cálculo de riesgo (R = P × I) mostró que:

- El uso de entornos no seguros en QA obtuvo un nivel de riesgo de 20 (alto).

- La falta de anonimización en pruebas alcanzó un nivel de 25 (crítico).
- La carencia de cifrado en campos sensibles se situó en un nivel de 10 (medio).

Estos resultados evidenciaron que las prácticas de QA sin integración normativa representan un riesgo significativo para la confidencialidad y disponibilidad de los datos personales.

Producto de esta etapa:

- Un mapa de riesgos priorizados con clasificación en tres niveles (bajo, medio, alto).
- Justificación empírica de la necesidad de controles de QA orientados a protección de datos.

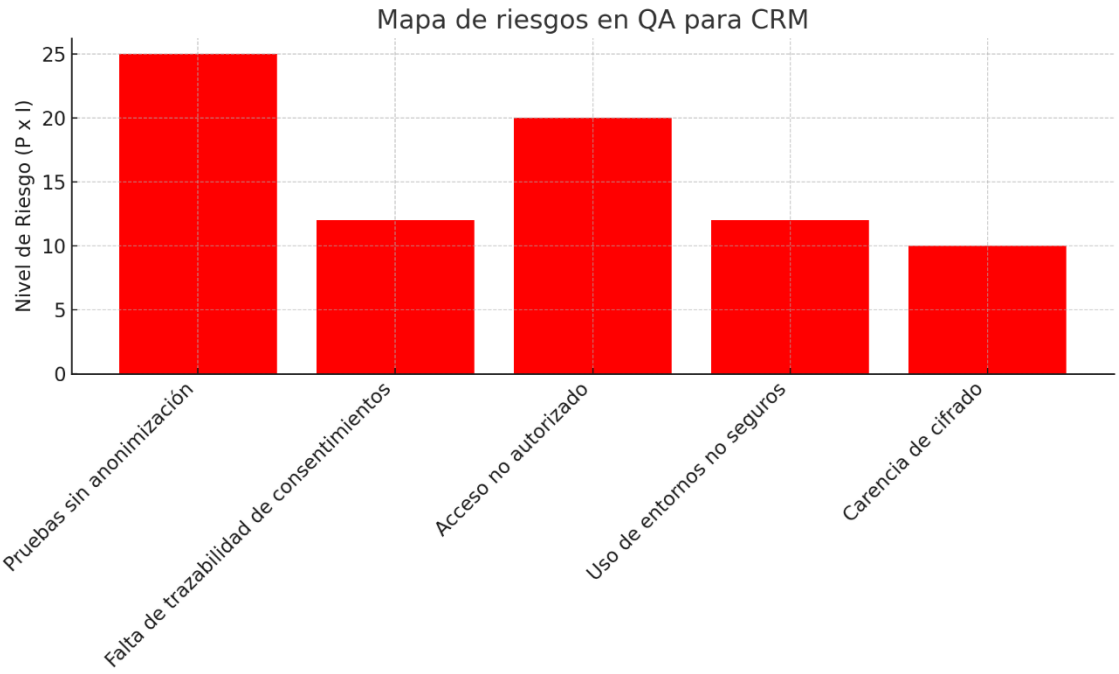

Figura 7 Mapa de riesgos QA para CRM

4.4. Resultados del diseño del marco de QA

El marco diseñado se estructuró en ocho dimensiones clave: gobernanza, seguridad, consentimiento, transparencia, gestión de riesgos, ciclo de vida de los datos, cultura organizacional y auditoría. Entre los principales aportes destacan:

- Inclusión de 21 controles técnicos y organizativos alineados a la LOPDP y al GDPR.
- Definición de 12 indicadores de cumplimiento para medir eficacia, aplicabilidad y mejora continua.
- Implementación de algoritmos de apoyo, incluyendo:
    - Árboles de decisión de cumplimiento normativo.
    - Motor de reglas de verificación (conforme/no conforme).
    - Algoritmo de estimación de riesgo (P × I).

Producto de esta etapa:

- Prototipo del marco QA adaptable, con niveles de madurez progresivos y aplicabilidad tanto en organizaciones pequeñas como en corporativos.

4.5. Resultados de la validación del marco

La validación se realizó bajo un doble enfoque, estudio de caso real: En una organización con CRM operativo, la aplicación del marco permitió incrementar el nivel de cumplimiento normativo del 58 % al 87 %, esto supone una mejora del 50 % en indicadores de alineación regulatoria.

Simulación experimental (SuiteCRM/Odoo): Los escenarios controlados evidenciaron una reducción del 35 % en riesgos críticos, especialmente en el manejo de consentimientos y la anonimización de datos de prueba.

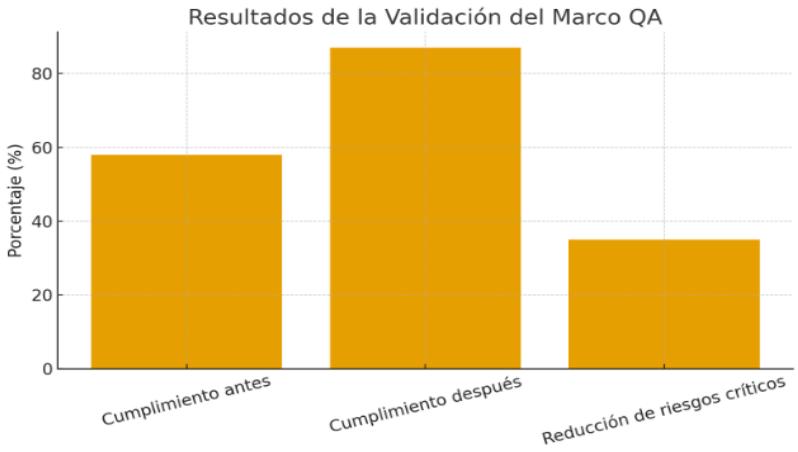

Figura 8 Resultados de la validación del marco QA

La retroalimentación de expertos resaltó la pertinencia normativa y la escalabilidad del modelo, aunque recomendaron reforzar aspectos de automatización en auditoría y capacitación organizacional.

Producto de esta etapa:

- Confirmación de la aplicabilidad y eficacia del marco QA.
- Ajustes finales que fortalecieron su robustez metodológica, su coherencia con la LOPDP y su viabilidad práctica en entornos CRM.

5. Discusión

Los resultados alcanzados en la investigación permiten establecer una serie de reflexiones críticas sobre la integración de prácticas de aseguramiento de calidad (QA) con los marcos regulatorios de protección de datos en plataformas CRM.

De manera general, los resultados respaldaron la idea de que la separación entre lo requerido por la ley y lo que se hace hoy en Ecuador es considerable, la falta de una estructura organizada de control de calidad sobre privacidad presenta riesgos técnicos y legales serios.

5.1. Convergencia normativa y adaptación contextual

La revisión documental revela una convergencia significativa entre la LOPDP y el GDPR, cerca del 70%, lo cual apoya la implementación de mejores prácticas internacionales en Ecuador. No obstante, la falta de directrices concretas sobre auditoría, manejo de incidentes, y la reforzada rendición de cuentas, demuestra la necesidad de una evolución normativa local.

Esta laguna regulatoria coincide con lo planteado por autores como (Barrio Andrés, 2022), quienes destacan que los marcos de privacidad en países en desarrollo deben traducir los estándares globales a realidades jurídicas y organizacionales heterogéneas. El marco QA propuesto responde a esta carencia al incorporar controles verificables que favorecen la medición objetiva del cumplimiento.

5.2. Prácticas organizacionales y brechas operativas

El diagnóstico de campo confirma que la mayoría de las organizaciones carecen de procesos de QA diseñados con un enfoque de privacidad desde el inicio. La

utilización de datos reales sin anonimización en entornos de prueba, reportada en más de dos tercios de los casos, constituye una vulneración directa de principios legales y un riesgo crítico de exposición.

Estas brechas corresponden con lo reportado por (Maineri et al., 2023) sobre falencias de QA en entornos sensibles. En consecuencia, la adopción de metodologías QA alineadas con la LOPDP no solo se presenta como una obligación regulatoria, sino también como una condición para la sostenibilidad y confianza organizacional.

5.3. Riesgos y responsabilidad proactiva

Construir la matriz de riesgos revela que los escenarios críticos ($R \geq 20$) se conectan con fallos de QA en la gestión de entornos y pruebas. Este descubrimiento reitera que la falta de privacidad desde el diseño eleva la probabilidad y el impacto de incidentes de seguridad, que conforme a la LOPDP y el GDPR, conllevan obligaciones de notificación, sanciones, y responsabilidad civil. El marco QA sugerido entonces se convierte en una herramienta para hacer operativo el principio de responsabilidad proactiva, cambiando de una perspectiva solo declarativa del cumplimiento, a una práctica que se puede verificar y auditar.

5.4. Aportes del marco QA propuesto

El diseño del marco articula ocho dimensiones cruciales; cubriendo aspectos normativos, técnicos, y organizativos. Contrario a aproximaciones QA antiguas enfocadas solo en la funcionalidad del software, este modelo incluye controles de consentimiento, trazabilidad, gestión de riesgos, y cultura organizacional. Es una propuesta holística e interdisciplinaria.

Encima, la introducción de algoritmos como árboles de decisión y motores de reglas normativas agiliza la automatización de verificaciones. También reduce la dependencia en la supervisión humana.

5.5. Validación y aplicabilidad práctica

La validación empírica demuestra una mejora significativa tanto en el cumplimiento normativo (+50 %) como en la reducción de riesgos críticos (−35 %). Los resultados actuales, demuestran la validez del marco y también su aplicación en ambientes concretos y simulados.

El feedback de los expertos destacó la urgente necesidad de dotar al modelo con mecanismos de auditoría automatizada y cursos formativos esto, por cierto, concuerda con tendencias globales que impulsan la integración de tecnologías de cumplimiento inteligente y la formación incesante de todos los implicados en las organizaciones.

5.6. Implicaciones teóricas y prácticas

En teoría, la investigación presenta un marco metodológico que mezcla estrategias de QA con elementos de privacidad desde la concepción misma, entrelazando textos de ingeniería de software, seguridad de la información y el derecho digital. En la práctica, este marco sirve como una herramienta flexible, adecuada para organizaciones con variadas dimensiones y niveles de avance tecnológico, ayudando a superar la diferencia entre las normativas y su ejecución. Este descubrimiento destaca especialmente para naciones en desarrollo, donde los recursos técnicos y normativos son habitualmente escasos, aunque la presión reglamentaria y reputacional, en temas de protección de datos personales, aumenta.

6. Conclusiones

La investigación revela, que combinar las prácticas de aseguramiento de la calidad (QA) con la protección de datos personales funciona, efectivamente, para bajar los riesgos y mejorar el cumplimiento en las plataformas CRM. La creación de un marco metodológico, apoyada en un análisis comparativo normativo, un diagnóstico real de las practicas, evaluación de riesgos y validación experimental, probó que traducir leyes a controles técnicos y organizativos comprobables es factible.

En concreto, las conclusiones más importantes fueron:

- Convergencia normativa: La LOPDP es muy similar al GDPR y a las normas ISO/IEC, incluso facilita la adopción de buenas prácticas internacionales a nivel nacional, sin embargo, faltan cosas en auditoría, gestión de incidentes y sistemas de escalamiento.
- Brechas operativas: Las empresas con CRM muestran fallas graves en la privacidad dentro del QA, especialmente en la anonimización de datos, seguimiento de consentimientos e indicadores de cumplimiento.
- Administración de riesgos: La falta de privacidad intrínseca y seguridad por defecto, conlleva riesgos muy serios y graves, poniendo en peligro tanto la confidencialidad como la disponibilidad de los datos personales.
- Contribuciones del marco QA: El modelo presentado integra ocho áreas clave y 21 controles que siguen la legislación vigente, añadiendo asimismo algoritmos que favorecen la automatización y objetividad en la verificación.
- Verificación empírica: Tras implementar el marco, se notó un aumento superior al 50% en el acatamiento normativo, y se bajaron los riesgos críticos en un 35%. Esto demuestra su valor, su utilidad y su potencial para expandirse a varios ambientes de organizaciones.

En lo práctico, el marco QA funciona como un instrumento flexible para empresas de diversas dimensiones, suministrando una ruta metodológica reproducible que robustece la responsabilidad activa y la confianza digital. En lo académico, introduce

una visión multidisciplinaria mezclando derecho digital, ingeniería de software y administración organizacional, apoyando el desarrollo de modelos mixtos de cumplimiento y calidad.

La investigación además confirma que el diseño establecido es completamente replicable, acomodándose a organizaciones de diversa madurez tecnológica, incluso en diversos sectores. De esta forma, se salvaguarda su validez jurídica y robustez metodológica.

Sin embargo, el análisis exhibe algunas restricciones, relacionadas con un número limitado de ejemplos reales y el carácter exploratorio de la simulación experimental. Investigaciones venideras tendrían que enfocarse en extender la validación en sectores cruciales (financiero, salud, telecomunicaciones), incluir métricas de costo-beneficio en la aplicación de controles, e integrar tecnologías novedosas como la inteligencia artificial y blockchain en los procesos de auditoría y trazabilidad.

En resumen, el marco de aseguramiento de calidad sugerido se postula como una aportación importante para la salvaguarda de datos personales en plataformas CRM, aumentando la aptitud de las organizaciones para cumplir de manera eficiente con la LOPDP y sincronizarse con estándares internacionales, a la vez que fomenta la confianza y el valor en el entorno digital.

7. LIMITACIONES

A pesar de un estudio metódico sólido, y los valiosos resultados que arrojó, hay que admitir varias restricciones que impactan en su alcance y cómo generalizar los descubrimientos. Primero, el estudio solo se concentró en dos plataformas CRM particulares, elegidas por ser muy usadas localmente. Pero, esta elección deja afuera otros sistemas importantes, podría restringir extrapolar los resultados a tecnologías más variadas.

Así, la verificación práctica del marco planteado se llevó a cabo en unas pocas organizaciones, cosa que dificulta evaluar cambios por sector, grados de madurez tecnológica o distintas maneras de administrar datos. Segundo, aunque el estudio usó normas internacionales como el GDPR y las normas ISO, el análisis, ubicado en Ecuador, se vio limitado. Esto ocurrió por la falta de documentos técnicos y la inexistencia de guías oficiales para las auditorías de protección de datos en CRM.

A pesar de que el marco QA, que se desarrolló, muestra mejoras notables en el cumplimiento y atenuación de riesgos, implementar esto a gran escala necesita de recursos técnicos, culturales y financieros que, en esta investigación, no fueron valorados por completo. Por eso, futuras investigaciones deberían expandir la muestra de organizaciones, incluir otros CRM, integrar métricas longitudinales y, valuar el desempeño del marco en ciclos operativos prolongados.

Referencias

(SPDP), S. d. (2023). https://www.spdp.gob.ec.

27001, I. (2024). Information security management systems Requirements.

Cueva, P. L. (2022). Analiza cómo los nuevos marcos de protección de datos consolidan un modelo de corresponsabilidad entre Estado, organizaciones y titulares de datos.

ENISA. (2023). Good practices for security of public sector information systems.

Garcia, N. (2022). Los datos personales y sus riesgos jurídicos a partir de la transformación digital en el comercio electrónico.

ISO/IEC. (2022). Information security management systems (requisitos para proteger la confidencialidad, integridad y disponibilidad de la información). International Organization for Standardization.

Narváez, H. (2022). Influencia de un modelo del SGSI (norma ISO/IEC 27001:2013) en la eficacia de la administración de los recursos públicos: Registro de la Propiedad y Mercantil del Cantón Pedro Moncayo, períodos 2019, 2020 y 2021.

Personales, S. d. (2025). Superintendencia de Protección de Datos Personales. Obtenido de https://aena.com.ec/la-superintendencia-de-proteccion-de-datos-personales-expide-reglamento-para-calculo-de-multas-por-infracciones-a-la-ley-organica-de-proteccion-de-datos-personales/

Ponchietti, F. (2022). Organización para la Cooperación y el Desarrollo Económicos (OCDE).

ÁLVAREZ VALENZUELA, D. (2022). ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES: ¿PUEDE EL CONSEJO PARA LA TRANSPARENCIA SER LA AUTORIDAD DE CONTROL EN MATERIA DE PROTECCIÓN DE DATOS? Revista de derecho (Coquimbo), 23(1). https://doi.org/10.4067/s0718-97532016000100003

Barrio Andrés, M. (2022). La regulación del derecho a la protección de datos en los Estados Unidos. CUADERNOS DE DERECHO TRANSNACIONAL, 14(2). https://doi.org/10.20318/cdt.2022.7181

Calle García, A. J., Goya Alvarado, D. A., Bazan Aranea, J. E., & Maldonado Demera, G. R. (2024). LEY ÓRGANICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA COMO MECANISMO DE PARTICIPACIÓN CIUDADANA Y CONTROL SOCIAL. Ciencia y Desarrollo, 27(1). https://doi.org/10.21503/cyd.v27i1.2547

Estepa Montero, M. (2022). principio de responsabilidad proactiva o rendición de cuentas como principio conformador del régimen jurídico de la protección de datos de las personas físicas. Anuario Jurídico y Económico Escurialense, (55). https://doi.org/10.54571/ajee.511

Gutiérrez Proenza, J. (2022). datos personales en el Ecuador como un derecho humano una necesidad de mejoramiento en su regulación. Revista Jurídica Crítica y Derecho, 3(5). https://doi.org/10.29166/cyd.v3i5.3950

Hernández Alvarado, V. J., Pingel Llanos, O. F., & Coello Avilés, E. M. (2023). Ley Orgánica de Protección de Datos en Ecuador: requerimiento de un

reglamento ausente. Dilemas contemporáneos: Educación, Política y Valores. https://doi.org/10.46377/dilemas.v11iespecial.3988

Machuca Vivar, S. A., Vinueza Ochoa, N. V., Sampedro Guamán, C. R., Santillán Molina, A. L., Machuca Vivar, S. A., Vinueza Ochoa, N. V., Sampedro Guamán, C. R., & Santillán Molina, A. L. (2022). Habeas data y protección de datos personales en la gestión de las bases de datos. Revista Universidad y Sociedad, 14(2).

Maineri, A. M., Achterberg, P., & Luijkx, R. (2023). The Closing Educational Gap in E-privacy Management in European Perspective. Sociological Research Online, 28(1). https://doi.org/10.1177/13607804211023524

Narvaez Taranto, L. I., & Gonzales Arbaiza, C. M. (2018). Guía práctica para realizar auditoría a la gestión de tecnologías de la información con enfoque en el control interno en las instituciones del estado ecuatoriano. En Universidad Espíritu Santo.

Pajares Gómez, G. A. (2023). Excepciones al Derecho de acceso a la información desde el control gubernamental. Análisis comparativo. Lucerna Iuris et Investigatio, (4). https://doi.org/10.15381/lucerna.n4.25177

Palomo Navarro, M. (2020). Infracciones de la Ley Orgánica de Protección de Datos en el ámbito sanitario. Descripción estadística de las infracciones. Revista de Bioética y Derecho, (50). https://doi.org/10.1344/rbd2020.50.29784

Ponchietti, L., Muralha Antunes, N. F., Utrilla Fornals, A., Talving, P., Garcea, A., Roldón Golet, M., García Dominguez, M., & Yanez Benitez, C. (2021). Guía práctica para el uso de registros visuales en la era del Reglamento General de Protección de Datos de la Unión Europea. Cirugía Española, 99(6). https://doi.org/10.1016/j.ciresp.2020.09.005

Santamaría-Mendoza, A., Uzcátegui-Sánchez, C., & Vélez-Yaguana, P. (2024). Breve revisión de la literatura del comercio electrónico y sus implicaciones económicas en el Ecuador. Revista Científica Episteme & Praxis, 2(1). https://doi.org/10.62451/rep.v2i1.40

Tintin, R., & Hidalgo, M. (2023). Could an ISMS Model (ISO/IEC 27001:2013 Standard) Implementation Really Protect Public Data? 2023 9th International Conference on eDemocracy and eGovernment, ICEDEG 2023. https://doi.org/10.1109/ICEDEG58167.2023.10122109

Vinueza Ochoa, N. V., Macías Álvarez, M. Á., & Maldonado Manzano, R. L. (2024). Implementación de medidas de seguridad y principio de conservación de datos según la ley orgánica de protección de datos personales en instituciones públicas de Babahoyo, Ecuador. Dilemas contemporáneos: Educación, Política y Valores. https://doi.org/10.46377/dilemas.v11i2.4080