UNIVERSIDAD LAICA VICENTE ROCAFUERTE DE GUAYAQUIL

FACULTAD DE ADMINISTRACIÓN

CARRERA DE CONTABILIDAD Y AUDITORIA

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

LICENCIADO EN CONTABILIDAD Y AUDITORÍA

TEMA

EL CONTROL INTERNO EN EL ÁREA COMERCIAL PARA GARANTIZAR EL CUMPLIMIENTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES.

TUTOR

Mgtr. GISELLA PATRICIA HUREL FRANCO

AUTORES

JUAN ANDRES VALENCIA ALBAN

HECTOR DIEGO VILLENA FALCONES

GUAYAQUIL

2025

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA	
FICHA DE REGISTRO DE TESIS	
TÍTULO Y SUBTÍTULO: El control interno en el área comercial para garantizar el cumplimiento de la Ley de Protección de Datos Personales.	
AUTOR/ES: Valencia Alban Juan Andrés Villena Falcones Héctor Diego	**TUTOR:** Hurel Franco Gisella Patricia
INSTITUCIÓN: **Universidad Laica Vicente Rocafuerte de Guayaquil**	**Grado obtenido:** Licenciado(a) Contabilidad y Auditoria
FACULTAD: ADMINISTRACIÓN	**CARRERA:** CONTABILIDAD Y AUDITORIA
	N. DE PÁGS: 99
ÁREAS TEMÁTICAS: Educación comercial y administración	
PALABRAS CLAVE: Auditoria de gestión - Protección de datos - Norma jurídica – Ecuador	

RESUMEN:

Con la Ley Orgánica de Protección de Datos Personales LOPDP (2021) el área comercial quedó bajo lupa; este estudio explora cómo el control interno viabiliza cumplimiento, confianza del cliente y continuidad operativa. Objetivo general: Analizar el control interno del área comercial para garantizar el cumplimiento de la Ley de Protección de Datos Personales. Metodología: Enfoque cualitativo, exploratorio-descriptivo; entrevistas semiestructuradas a Jefe Comercial, Sistemas y Control Interno; revisión documental y diagnóstico; checklist LOPDP y DPIA; muestreo intencionado y triangulación de evidencias. Resultado principal: El diagnóstico ubicó el cumplimiento promedio en ~70 %; se observaron fortalezas en cifrado, registros de acceso y políticas, junto con brechas críticas en actualización de consentimientos, seguridad móvil por ausencia de MDM, contratos con terceros y visibilidad de canales ARCO; el plan prioriza la designación del DPD, la automatización del consentimiento y bloqueos en CRM, la implementación de MDM/MFA, la actualización de la DPIA con terceros, un calendario de conservación y un tablero de KPIs con auditorías trimestrales. Se concluyo que un control interno específico y transversal para el frente comercial,

<table>
<tr><td colspan="3">alineado a los principios de la LOPDP, transforma prácticas reactivas en responsabilidad proactiva, reduce la exposición a sanciones, mejora la trazabilidad y eleva la confianza, siempre que se sostenga en una gobernanza clara (Comité y DPD), procesos maduros (RAT, ARCO), tecnología adecuada (MDM, MFA), gestión rigurosa de terceros (contratos y verificación) y monitoreo continuo (KPIs y auditorías).</td></tr>
<tr><td>N. DE REGISTRO (en base de datos):</td><td colspan="2">N. DE CLASIFICACIÓN:</td></tr>
<tr><td colspan="3">DIRECCIÓN URL (Web):</td></tr>
<tr><td>ADJUNTO PDF:</td><td>SI [x]</td><td>NO [ ]</td></tr>
<tr><td>CONTACTO CON AUTOR/ES:
Valencia Alban Juan Andrés
Villena Falcones Héctor Diego</td><td>Teléfono:
0991717605
096 897 2029</td><td>E-mail:
jvalenciaal@ulvr.edu.ec
hvillenafa@ulvr.edu.ec</td></tr>
<tr><td>CONTACTO EN LA INSTITUCIÓN:</td><td colspan="2">Mgtr. Jéssica Julieta Aroca Clavijo (Decano)
Teléfono: 2 596500 Ext. 201
E-mail: jarocac@ulvr.edu.ec
Mgtr. Martha Beatriz Hernández Armendáriz
(Director de Carrera)
Teléfono: 2 596500 Ext. 271
E-mail: mhernandeza@ulvr.edu.ec</td></tr>
</table>

CERTIFICADO DE SIMILITUD

CERTIFICADO DE ANÁLISIS
magister

TT-ULVR-FADM-A25 VALENCIA ALBAN Y VILLENA FALCONES

15% Textos sospechosos

8% Similitudes
< 1 % similitudes entre comillas
0 % entre las fuentes mencionadas
4% Idiomas no reconocidos (ignorado)
8% Textos potencialmente generados por la IA

Nombre del documento: TT-ULVR-FADM-A25 VALENCIA ALBAN Y VILLENA FALCONES.docx
ID del documento: 75d2b16dc7115576baaa785db4aaa26a743fc74e
Tamaño del documento original: 260,34 kB

Depositante: Gisella Hurel Franco
Fecha de depósito: 17/8/2025
Tipo de carga: interface
fecha de fin de análisis: 17/8/2025

Número de palabras: 21.364
Número de caracteres: 145.454

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.finanzaspopulares.gob.ec https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_protecc... 78 fuentes similares	9%		Palabras idénticas: 9% (2043 palabras)
2	www.anacse.org.ec http://www.anacse.org.ec/uploads/content/2021/06/file_1624574647_1624574681.pdf 51 fuentes similares	7%		Palabras idénticas: 7% (1661 palabras)
3	openaccess.uoc.edu | La regulación de la protección de datos personales en la le... https://openaccess.uoc.edu/bitstream/10609/128046/6/edisonperezvacaTFM0121memoria.pdf 52 fuentes similares	4%		Palabras idénticas: 4% (920 palabras)
4	spdp.gob.ec | CONSULTAS https://spdp.gob.ec/consultasatendidas/ 56 fuentes similares	3%		Palabras idénticas: 3% (726 palabras)
5	Documento de otro usuario #c717bd Viene de de otro grupo 22 fuentes similares	3%		Palabras idénticas: 3% (674 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.tecniseguros.com.ec | Tecniseguros » LA CONTINUIDAD DEL NEGOCIO AN... https://www.tecniseguros.com.ec/la-continuidad-del-negocio-ante-una-catastrofe/	< 1%		Palabras idénticas: < 1% (33 palabras)
2	nmslaw.com.ec | Se expide el Reglamento a la Ley de Protección de Datos Perso... https://nmslaw.com.ec/blog/2023/11/08/ecuador-reglamento-lopdp-2023/	< 1%		Palabras idénticas: < 1% (29 palabras)
3	iurenovum.com | Gestión de Datos Personales: ¿Quién Decide y Quién Ejecuta? - ... https://iurenovum.com/gestion-de-datos-personales-quien-decide-y-quien-ejecuta/	< 1%		Palabras idénticas: < 1% (26 palabras)
4	insolidumabogados.com | Violación de Datos Personales y Responsabilidad en e... https://insolidumabogados.com/violacion-de-datos-personales-y-responsabilidad-en-ambito-j...	< 1%		Palabras idénticas: < 1% (20 palabras)
5	hdl.handle.net | Transparencia administrativa, acceso a la información y protecci... http://hdl.handle.net/10486/682966	< 1%		Palabras idénticas: < 1% (23 palabras)

Gisella Patricia Hurel Franco
Time Stamping Security Data

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS PATRIMONIALES

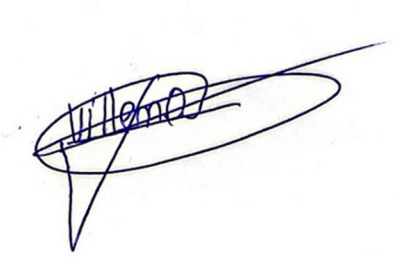
El(Los) estudiante(s) egresado(s) Valencia Alban Juan Andrés y Villena Falcones Héctor Diego, declara (mos) bajo juramento, que la autoría del presente Trabajo de Titulación, “El control interno en el área comercial para garantizar el cumplimiento de la Ley de Protección de Datos Personales”, corresponde totalmente a el(los) suscrito(s) y me (nos) responsabilizo (amos) con los criterios y opiniones científicas que en el mismo se declaran, como producto de la investigación realizada.

De la misma forma, cedo (emos) los derechos patrimoniales y de titularidad a la Universidad Laica VICENTE ROCAFUERTE de Guayaquil, según lo establece la normativa vigente.

Autor(es)

Valencia Alban Juan Andrés

C.I. 0925579070



Villena Falcones Héctor Diego

C.I. 0922683180

CERTIFICACIÓN DE ACEPTACIÓN DEL DOCENTE TUTOR

En mi calidad de docente Tutor del Trabajo de “El control interno en el área comercial para garantizar el cumplimiento de la Ley de Protección de Datos Personales”, designado(a) por el Consejo Directivo de la Facultad de Administración de la Universidad Laica VICENTE ROCAFUERTE de Guayaquil.

CERTIFICO:

Haber dirigido, revisado y aprobado en todas sus partes el Trabajo de Titulación, titulado: “El control interno en el área comercial para garantizar el cumplimiento de la Ley de Protección de Datos Personales”, presentado por el (los) estudiante (s) Valencia Alban Juan Andrés y Villena Falcones Héctor Diego como requisito previo, para optar al Título de Licenciado(a) Contabilidad y Auditoria, encontrándose apto para su sustentación.

Firma: 

Mgtr. Gisella Patricia Hurel Franco

C.C. 0916615487

AGRADECIMIENTO

A mi papá Héctor Villena, por ser mi mayor ejemplo de perseverancia y dedicación. Gracias por enseñarme que todo esfuerzo tiene su recompensa, por tu apoyo incondicional y por estar siempre a mi lado en cada paso de mi vida académica y personal.

A mi mamá Jacqueline Falcones, por su amor infinito, por ser mi guía y fortaleza, y por brindarme palabras de aliento en los momentos más difíciles. Tu cariño y comprensión han sido el motor que me impulsó a seguir adelante.
A mi tío Manuel Villena, por su constante apoyo, por creer en mis capacidades y por motivarme a alcanzar mis metas. Su confianza en mí ha sido un pilar fundamental en este camino.

A Dios, por darme la vida, la salud y la fortaleza necesarias para superar cada reto y por iluminar mi camino hacia esta meta tan importante.
A la máster Hurel Franco, mi tutora, por su paciencia, orientación y compromiso durante el desarrollo de esta investigación. Sus valiosos consejos y dedicación fueron clave para la culminación de este trabajo.

A mis compañeros y amigos, por su apoyo, por los momentos compartidos y por ser parte de esta etapa que siempre recordaré con cariño.

Este logro no me pertenece únicamente a mí, sino también a todas las personas que, con su amor, confianza y generosidad, hicieron posible que hoy culmine esta etapa de mi vida. A todos ustedes, mi más profundo y sincero agradecimiento.

Villena Falcones Héctor Diego

Expreso mi más sincero agradecimiento a Dios, por concederme la fortaleza y sabiduría necesarias para culminar este proyecto. De manera especial, agradezco a mis padres, Maritza Alban y Juan Eduardo Valencia, por su amor incondicional, sacrificio y apoyo constante, que han sido el pilar fundamental para alcanzar esta meta. También agradezco a todas las personas que me quieren, por su respaldo y aliento durante todo este proceso. Sin su confianza y compañía, la realización de esta tesis no hubiera sido posible.

Valencia Alban Juan Andrés

DEDICATORIA

A mi amado papá, Héctor Villena, cuya perseverancia ha sido la brújula que orientó mi camino. Gracias por enseñarme que los sueños se conquistan con disciplina y que cada esfuerzo deja huellas imborrables en el corazón.

A mi querida mamá, Jacqueline Falcones, faro de amor y ternura, por ser mi refugio en las tormentas y mi impulso en los días claros. Tu fe en mí me sostuvo cuando mis fuerzas flaqueaban.

A mi tío, Manuel Villena, por su apoyo incondicional y por recordarme siempre que no hay meta demasiado alta cuando el corazón late con determinación.

A Dios, fuente de vida, luz y esperanza, por regalarme cada amanecer y la fortaleza para seguir, aun cuando el camino parecía incierto.

A la máster Hurel Franco, mi tutora, por su orientación sabia, su paciencia infinita y su compromiso sincero en cada etapa de esta investigación.

Dedico estas páginas a todos los que, con un gesto, una palabra o una mirada, hicieron más liviana la carga y más dulce la meta. Este logro es un pedacito de cada uno de ustedes y una promesa cumplida para mí mismo.

Villena Falcones Héctor Diego

Dedico esta tesis a mi padre, Juan Eduardo Valencia, por ser un ejemplo de esfuerzo, perseverancia y compromiso. Su apoyo constante y sus enseñanzas han sido fundamentales para alcanzar esta meta.

Valencia Alban Juan Andrés

RESUMEN

Con la Ley Orgánica de Protección de Datos Personales LOPDP (2021) el área comercial quedó bajo lupa; este estudio explora cómo el control interno viabiliza cumplimiento, confianza del cliente y continuidad operativa. Objetivo general: Analizar el control interno del área comercial para garantizar el cumplimiento de la Ley de Protección de Datos Personales. Metodología: Enfoque cualitativo, exploratorio-descriptivo; entrevistas semiestructuradas a Jefe Comercial, Sistemas y Control Interno; revisión documental y diagnóstico; checklist LOPDP y DPIA; muestreo intencionado y triangulación de evidencias. Resultado principal: El diagnóstico ubicó el cumplimiento promedio en ~70 %; se observaron fortalezas en cifrado, registros de acceso y políticas, junto con brechas críticas en actualización de consentimientos, seguridad móvil por ausencia de MDM, contratos con terceros y visibilidad de canales ARCO; el plan prioriza la designación del DPD, la automatización del consentimiento y bloqueos en CRM, la implementación de MDM/MFA, la actualización de la DPIA con terceros, un calendario de conservación y un tablero de KPIs con auditorías trimestrales. Se concluyo que un control interno específico y transversal para el frente comercial, alineado a los principios de la LOPDP, transforma prácticas reactivas en responsabilidad proactiva, reduce la exposición a sanciones, mejora la trazabilidad y eleva la confianza, siempre que se sostenga en una gobernanza clara (Comité y DPD), procesos maduros (RAT, ARCO), tecnología adecuada (MDM, MFA), gestión rigurosa de terceros (contratos y verificación) y monitoreo continuo (KPIs y auditorías).

Palabras clave : Auditoria de gestión - Protección de datos - Norma jurídica – Ecuador

ABSTRACT

With the 2021 Personal Data Protection Law (LOPDP), the commercial area came under scrutiny; this study explores how internal control enables compliance, customer trust, and operational continuity. General objective: To analyze the internal control of the commercial area to ensure compliance with the Personal Data Protection Law. Methodology: A qualitative, exploratory-descriptive approach was adopted; semi-structured interviews were conducted with the head of Commercial, Systems, and Internal Control; documentation review and diagnosis were performed; a LOPDP checklist and a DPIA (Data Protection Impact Assessment) were applied; purposive sampling and triangulation of evidence were used. Main result: The diagnosis placed average compliance at approximately 70 %; strengths were observed in encryption, access logs, and policies, alongside critical gaps in the updating of consents, mobile security due to the absence of Mobile Device Management (MDM), contracts with third parties, and visibility of ARCO channels; the plan prioritizes the appointment of the Data Protection Officer (DPO), automation of consent and CRM lockouts, implementation of MDM/MFA, updating of the DPIA regarding third parties, a retention schedule, and a KPI dashboard with quarterly audits. Main conclusion: A specific and cross-functional internal control for the commercial front, aligned with the principles of the LOPDP, transforms reactive practices into proactive responsibility, reduces exposure to sanctions, improves traceability, and enhances trust, provided it is supported by clear governance (Committee and DPO), mature processes (Records of Activities of Treatment, ARCO), adequate technology (MDM, MFA), rigorous third-party management (contracts and verification), and continuous monitoring (KPIs and audits).

Keywords : Management Audit - Data Protection - Legal Regulation - Ecuador

ÍNDICE GENERAL

..... 1
CERTIFICADO DE SIMILITUD iv
DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS PATRIMONIALES v
CERTIFICACIÓN DE ACEPTACIÓN DEL DOCENTE TUTOR vi
AGRADECIMIENTO vii
DEDICATORIA viii
RESUMEN ix
ABSTRACT x
ÍNDICE GENERAL xi
ÍNDICE DE TABLAS xiv
ÍNDICE DE FIGURAS xiv
INTRODUCCIÓN 1
CAPÍTULO I 3
ENFOQUE DE LA PROPUESTA 3
1.1 Tema: 3
1.2 Planteamiento del Problema: 3
1.3 Formulación del Problema: 6
1.4 Objetivo General 6
1.5 Objetivos Específicos 6
1.6 Idea a Defender 7
CAPÍTULO II 8
MARCO REFERENCIAL 8
2.1 Antecedentes 8
2.2 Marco Teórico: 9
2.2.1. Fundamentos del Control Interno 9

2.2.2. Control Interno en el Área Comercial 13
2.2.3. Protección de Datos Personales en el Ecuador 17
2.2.4. Cumplimiento Normativo y Control Interno 21
2.2.5. Seguridad de la Información y Gestión de Riesgos 24
CAPÍTULO III 36
MARCO METODOLÓGICO 36
3.1 Enfoque de investigación 36
3.2 Alcance de la investigación 36
3.3 Técnicas e Instrumentos 37
3.4 Población y Muestra 39
3.5 Tipo de muestreo 40
CAPÍTULO IV 42
PROPUESTA O INFORME 42
4.1 Presentación y análisis de resultados 42
4.2 Diagnostico de control interno 53
4.3 Checklist de cumplimiento - Ley Orgánica de Protección de Datos Personales (ECUADOR) 57
4.4 Propuesta integral de fortalecimiento del control interno en el área comercial para garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) 63
4.4.1. Arquitectura de gobernanza y roles 64
4.4.2. Mapa de procesos y Registro de Actividades de Tratamiento (RAT) 64
4.4.3. Gestión de consentimiento 360° 65
4.4.4. Derechos de titulares y portal ARCO 67
4.4.5. Seguridad por diseño y por defecto 70
4.4.6. Gestión de terceros y transferencias 74
4.4.7. Evaluación de Impacto (DPIA) y gestión de riesgos 74
4.4.8. Calendario de conservación y minimización 75

4.4.9. Monitoreo e indicadores (KPI/KRI) 76
4.4.10. Plan de acción y cronograma 77
4.4.11. Auditoría y mejora continua 78
4.4.12. Gráficos de soporte 78
CONCLUSIONES 79
RECOMENDACIONES 80
REFERENCIAS BIBLIOGRÁFICAS 81
ANEXOS 84

ÍNDICE DE TABLAS

Tabla 1 Ambiente de control 53

Tabla 2 Evaluación de Riesgos..... 54

Tabla 3 Actividades de Control 54

Tabla 4 Información y Comunicación 55

Tabla 5 Supervisión y Monitoreo..... 56

Tabla 6 Matriz de Riesgos..... 60

Tabla 7 Matriz de acciones 62

Tabla 8 Campos mínimos sugeridos para el RAT..... 64

Tabla 9 Matriz de riesgos priorizados:..... 75

Tabla 10 Indicadores..... 76

Tabla 11 Cronograma 766

ÍNDICE DE FIGURAS

Figura 1 Cumplimiento por componente (ítems 1–15).....78

Figura 2. Cronograma de implementación (Gantt simplificado).....78

INTRODUCCIÓN

En los últimos años, la protección de los datos personales dejó de ser un tema meramente técnico o legal para convertirse en un asunto profundamente humano. En Ecuador, este cambio de paradigma se consolidó con la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en mayo de 2021, una normativa que no solo trajo consigo nuevas obligaciones para las organizaciones, sino que también despertó una mayor conciencia sobre el valor —y la vulnerabilidad— de la información personal (Registro Oficial Suplemento No. 459, 2021).

Dentro de ese nuevo escenario normativo, el área comercial de las empresas quedó bajo una lupa particularmente exigente. Y no era para menos: se trata de la zona donde se recopilan, gestionan y, muchas veces, se comparten grandes volúmenes de datos personales con fines estratégicos. Desde formularios de contacto hasta bases de clientes segmentadas, pasando por promociones personalizadas, canales de atención o sistemas CRM, la actividad comercial implica —en cada paso— un tratamiento de datos que puede rozar, sin darse cuenta, los límites de la legalidad. La presión por cumplir metas de ventas, la velocidad con la que se ejecutan campañas, y el uso de herramientas digitales a gran escala, con frecuencia desbordaron las capacidades tradicionales de control y supervisión.

Fue precisamente en este contexto que el control interno adquirió una relevancia decisiva. Más allá de los clásicos procedimientos administrativos, se hizo evidente la necesidad de establecer mecanismos que aseguren, de forma proactiva, el cumplimiento de la LOPDP. Este control interno no se limitó a detectar fallos, sino que pasó a desempeñar un papel de guía, acompañando a las áreas comerciales en su transición hacia prácticas más responsables. Incluyó desde auditorías internas periódicas y revisiones de protocolos de consentimiento, hasta la capacitación constante de personal en temas de privacidad, seguridad y ética comercial.

Y es que, como bien lo establece la LOPDP, el tratamiento de datos personales debe regirse por principios como la legalidad, la minimización, la finalidad específica y el consentimiento informado (LOPDP, art. 7). Estos principios, aunque parezcan lógicos sobre papel, son complicados difícilmente aplicables, porque un clic erróneo,

una omisión en la política de privacidad, o manejo malicioso de una lista de clientes puede dar lugar a consecuencias legales, de reputación y emocionales.

La realidad es que hacer cumplir esa ley tampoco se puede dejar solos para departamentos legales escalonados o para tecnologías de última generación. Las empresas necesitan tener suficientemente bien definida una red interna, donde cada persona que forma parte de la cadena de comercio sepa su propia función en la protección de la privacidad del consumidor. Por ello, este estudio se planteó explorar cómo el diseño y aplicación efectiva del control interno en el área comercial permite no solo cumplir con lo dispuesto por la ley, sino también fortalecer la confianza del cliente, prevenir incidentes y, en última instancia, promover una cultura organizacional más ética y sostenible.

CAPÍTULO I

ENFOQUE DE LA PROPUESTA

1.1 Tema:

El control interno en el área comercial para garantizar el cumplimiento de la Ley de Protección de Datos Personales.

1.2 Planteamiento del Problema:

La Ley Orgánica de Protección de Datos Personales (LOPDP), vigente en Ecuador, establece un marco jurídico riguroso para la protección de la información personal, otorgando derechos específicos a los titulares de datos e imponiendo obligaciones significativas a las organizaciones que los tratan.

Las áreas comerciales en el centro mismo de las empresas tendrían un efecto motor impulsando todo el proceso y es en este lugar donde el manejo de datos personales se convierte en crucial y permanente. Desde que se identifican los primeros prospectos hasta que se le vuelve a utilizar, cada paso tiene relación con tratamientos muy sensibles de información. Se referimos a consejos como no ponernos nombres, no poner números de identificación, no añadir direcciones, no meter teléfonos, no poner correos, ni datos de cuando hablamos por teléfono, o incluso horas y lugares específicos donde están y todas aquellas cosas sobre nuestras compras o gustos personales. Todo esto, desde el registro de sus intereses hasta la atención al cliente, está en juego, y es que en cada campaña de marketing directo, la confianza de los consumidores depende de cómo se maneje esta valiosa información.

Justamente, se comprobó que la Autoridad de Protección de Datos Personales en Ecuador empezó, desde mayo de 2023, a aplicar sanciones administrativas sobre entidades privadas por incumplimientos diversos, como no inscribir bases de datos, no notificar incidentes de seguridad o no implementar medidas desde el diseño.

Además, estudios legales y académicos evidenciaron que si bien la Constitución ecuatoriana (art. 66.19) reconocía el derecho a la protección de datos desde 2008, solo con la LOPDP se estableció un marco sólido; hasta entonces, las

normas sectoriales eran dispersas y contradictorias, lo que generó un vacío normativo que dificultó la protección efectiva de los ciudadanos (Naranjo, 2023).

Por otra parte, se observó que muchas compañías ecuatorianas no diseñaron, ni implementaron, sistemas de control interno específicos vinculados al cumplimiento normativo en el área comercial. Estudios sobre control interno en empresas nacientes revelaron que colaboradores desconocían si existía ese sistema y que dependían de controles empíricos poco formales, lo que generó riesgos operativos y de cumplimiento (Rivas, 2022)

El problema central radica en que, a pesar de la obligatoriedad de la LOPDP, muchas organizaciones no cuentan con un sistema de control interno robusto y adaptado que garantice su cumplimiento efectivo en las operaciones comerciales. Esto se manifiesta en varias deficiencias críticas:

Algunos aspectos como la falta de concienciación y capacitación: El personal del área comercial, a menudo, carece del conocimiento profundo sobre la LOPDP, sus principios (licitud, finalidad, proporcionalidad, lealtad, transparencia) y los derechos de los titulares. Esto puede llevar a prácticas inadecuadas en la recolección, uso y almacenamiento de datos.

Uno de los factores más delicados en el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) dentro del área comercial ha sido, sin duda, la gestión inadecuada del consentimiento. En varias ocasiones, no se logró obtener un consentimiento claro, verificable y realmente informado de los titulares de los datos. Es decir, algo que fuera realmente expreso y sin lugar a duda. Esto se hizo aún más crítico cuando se trataba de actividades de marketing o cuando los datos se compartían con terceros, lo que dejó a las empresas vulnerables a riesgos legales bastante serios.

Además, las fallas en la seguridad de la información se convirtieron en otro gran dolor de cabeza. Muchos sistemas donde se almacenaban o procesaban datos personales, como los CRM o las bases de datos de clientes, no contaban con las protecciones adecuadas para evitar accesos no autorizados o, peor aún, pérdidas y filtraciones. Y es que, aunque algunas plataformas parecían ser seguras a simple

vista, bastaba con una configuración incorrecta o un usuario distraído para que toda esa valiosa información quedara al alcance de cualquiera.

Otro punto en contra fue la ausencia de procedimientos de los protocolos. En muchas organizaciones, carecían los protocolos formales y claramente definidos para manejar los datos personales a lo largo durante del ciclo comercial. Desde el primer contacto con un posible cliente hasta el fin de la relación y borradura de la información, debía establecerse cada paso. Pero en efecto que estas situaciones prácticas se realizaban con criterios poco claros, con incongruencia muy grande y con posibilidad de errores o forma de fallas involuntarias.

Además, se encontró infografía de los derechos del titular. Las empresas, en su mayoría, no contaban con canales efectivos ni mecanismos claros para que las personas pudieran ejercer sus derechos ARCO (acceso, rectificación, cancelación y oposición), así como los de portabilidad y suspensión del tratamiento.

La carencia de protección adecuada no solamente generaba enfado a los usuarios, sino que además, permitía a terceros hacer reclamos o denuncias ante las autoridades correspondientes. Y la verdad es eso no solo conducía a riesgos legales sino que también era un golpe directo a la imagen y los fondos de la sociedad. No solo eso el incumplimiento de la LOPDP lo que llevaba a estrés eran las multas que la Superintendencia de Protección de Datos Personales podría conceder. El daño más profundo era otro: el de perder la confianza de los clientes. Porque a la pérdida puesta en el comercio de la información es fiada no sólo legal, sino también una consecuencia de una pérdida financiera. Es mucho más personal, emocional y relacional. Afecta directamente la estabilidad y credibilidad del área comercial.

En sectores como la administración de fondos, donde manejar datos sensibles es parte fundamental del día a día, estos riesgos adquieren una dimensión aún mayor, ya que la confianza del cliente es lo que impulsa todo. Estos datos incluyen información financiera, historial crediticio, datos de contacto y otra información personal que permite la gestión eficiente de contratos, la evaluación de riesgos y el otorgamiento de créditos.

Sin embargo por su naturaleza sensible, estos datos deben ser protegidos muy mucho. Por lo que resulta necesario estudiar el control interno implantado en área

comercial, a fin de identificar si en efecto realiza cumplimiento normativo y reduce los riesgos de tratamiento de datos personales.

El mal manejo o manejo incorrecto de esta información puede provocar una serie de consecuencias graves desde pérdidas económicas hasta sanciones legales que pueden arruinar la imagen de la empresa. Como bien dice el documental, la transparencia será el nuevo componente fundamental, y la verdad es que, en un sector donde la confianza dependerá de todo, una gestión incorrecta de los datos personales, comenzará a debilitar esa relación tan esencial como es la entre cliente y empresa. Esto a su vez coloca en riesgo la sostenibilidad y crecimiento a mediano y largo plazo empresarial.

Por eso hacer que se garantice la integridad, la confidencialidad y la disponibilidad de los datos personales no es solo cuestión de cumplir la legalidad. Se encuentra en el centro de la estrategia de mantener la competitividad y seguir siendo una institución que logre seguir ganando la confianza de sus clientes, especialmente en el mundo financiero, en el que la confianza es todo.

1.3 Formulación del Problema:

¿De qué manera el control interno en el area comercial garantiza el cumplimiento de la ley de protección de datos personales?

1.4 Objetivo General

Analizar el control interno en el área comercial para asegurar el cumplimiento efectivo de la ley de protección de datos personales.

1.5 Objetivos Específicos

- Determinar los aspectos normativos y teóricos de la Ley Orgánica de Protección de Datos Personales, explorando su relación con los sistemas de control interno dentro de los procesos comerciales.

- Realizar un diagnóstico detallado del sistema de control interno vigente en la administradora de fondos, con el objetivo de verificar que se cumpla a cabalidad la normativa de protección de datos personales.

- Proponer acciones de mejora diseñadas para fortalecer el control interno, garantizando el cumplimiento de la legislación en lo que respecta a la protección de la información personal de los clientes.

1.6 Idea a Defender

El control interno en el área comercial de la administradora de fondos para garantizar el cumplimiento de la Ley de Protección de Datos Personales

1.7 Línea de Investigación Institucional / Facultad.

Desarrollo estratégico empresarial y emprendimientos sustentables.

CAPÍTULO II

MARCO REFERENCIAL

2.1 Antecedentes

Sevilla Moncayo, Amanda Edith. (“2023”). Impacto de la LOPDP en el control interno y fiscalización de las compañías privadas ecuatorianas. Este estudio buscó explorar cómo la LOPDP impactó la estructura y prácticas del control interno en las empresas privadas del país. Utilizó una metodología cualitativa a través de la revisión de documentos y análisis de estudios de casos empresariales actuales. Los hallazgos mostraron que varias organizaciones no habían actualizado sus sistemas de control interno para cumplir con las regulaciones, lo que dificultó la supervisión efectiva. Las conclusiones subrayaron la necesidad de mejorar los marcos de políticas internas y la capacitación, así como fortalecer la vinculación del control interno con el cumplimiento de las regulaciones.

Nevardo (2020). Situación de la protección de datos personales en Ecuador. El objetivo del estudio fue analizar el desarrollo constitucional desde la constitución hasta la LOPDP y su aplicación práctica en el país. Empleó una metodología de análisis histórico-normativo. El estudio tuvo como resultados concluyentes que antes del año 2021 existía un ecosistema legal fragmentado y contradictorio que creaba vacíos regulatorios. El estudio subrayó que la promulgación de la LOPDP proporcionaba un marco holístico muy necesario, aunque se señaló que su aplicación efectiva dependía de marcos operativos bien desarrollados.y marcos legales internacionales más sofisticados.

La organización y diseño del marco normativo de ordenación de protección de datos en Ecuador se basó en la ley general de protección de datos de la Unión Europea, así como otras legislaciones latinoamericanas y de países Ajmember, destacando la ley 25 de Uruguay en 2008. Se especializa en la Ley Orgánica de Protección de Datos Personales y su aplicación en la empresa ecuatoriana. En una investigación descriptiva, mediante encuestas y entrevistas, constató la falta de privacy by design en el sistema de gestión de datos, además de un marco regulacional completamente en la sombra. Como hallazgos intérpretes adicionales, el modelo de

encuadre letífesto dio un sentido de empresa elopista en la gestión de su imagen ante terceros, pues no se tenían protocolos escalonados de atención a incidentes.

Los hallazgos que emergían del análisis de datos se pueden catalogar en la concepción que se tiene del marketing en empresas ecuatorianas, buscándolo exclusivamente como convertir a las personas en consumidores. En el marketing, no se considera que el propósito de una empresa no debería ser hacer consumidores, sino satisfacer las necesidades humanas. Como conclusión, el énfasis recayó en que estos sistemas proporcionan un nivel adecuado de seguridad, optimizan el control financiero y también refuerzan el cumplimiento normativo asociado.

Hernández y Vázquez . (2023), en su investigación sobre la ley de protección de datos personales en Ecuador y España, se propusieron analizar ambas normativas con el propósito de detectar buenas políticas y elementos que requieran un mayor nivel de optimización. Adoptaron un método – jurídico comparativo – que les permitió profundizar en las dimensiones que resultaban más relevantes en la normatividad de ambos sistemas. Los resultados hallados mostraron contrastes significativos, sobre todo en lo que respecta a la evaluación de impacto, así como las obligaciones que el delegado de datos debía cumplir. Su principal conclusión es que Ecuador tendría la posibilidad de beneficiarse en gran medida si adoptara un mayor número de mecanismos avanzados, por medio de políticas comparativas con otras legislaciones para fortalecer y modernizar su normativa.

2.2 Marco Teórico:

2.2.1. Fundamentos del Control Interno

El control interno no son solamente un grupo de normas fijas; constituye el engranaje que mueve la organización. Es el núcleo que permite el manejo eficiente de los recursos, la prevención de riesgos, y el aseguramiento del cumplimiento normativo. En aquellos sectores donde el manejo de la información, la protección de los activos y la transparencia son cruciales, su adopción resulta imperativa ya que asegura la sostenibilidad en el tiempo. En escenarios tan dinámicos y regulados como el financiero o los comerciales, no solo se supervisa, también se controla. Es un sistema que se transforma en un recurso estratégico por el solo hecho de no limitarse al control y en su lugar, dirigirse a la mejora continua.

Definición y objetivos del control interno: El control interno ha sido definido por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO) como un proceso integrado, efectuado por la dirección y el personal de una entidad, diseñado para proporcionar una seguridad razonable en la consecución de objetivos vinculados a la operación, la información financiera y el cumplimiento de leyes y regulaciones aplicables (COSO, 2013). En su esencia, el control interno no busca eliminar todos los riesgos, en cambio, intenta gestionar aquellos riesgos que amenazan el logro de los objetivos estratégicos de la organización.

El control interno tiene como objetivo salvaguardar los activos de la empresa, mantener registros financieros precisos, mejorar la eficiencia operativa y garantizar el cumplimiento de las leyes y regulaciones aplicables. Además, el control interno no es solo operativo. Promueve una cultura organizacional que valora la ética, la transparencia y la responsabilidad. En última instancia, no se trata solo de cumplimiento; se trata de construir confianza e integridad en toda la organización.

Componentes del control interno según COSO

El marco COSO, ampliamente adoptado a nivel internacional, establece cinco componentes interrelacionados que conforman la estructura del control interno. El primero es el ambiente de control**,** que incluye los valores éticos, la estructura organizativa, la asignación de autoridad y responsabilidad, así como el compromiso con la competencia. Este componente representa la base sobre la cual se construye todo el sistema (COSO, 2013).

En segundo lugar, la evaluación de riesgos permite identificar, analizar y gestionar los riesgos que pueden impedir el logro de los objetivos empresariales. Luego, se implementan actividades de control, como autorizaciones, verificaciones, conciliaciones o revisiones operativas, con el fin de reducir esos riesgos a niveles que se consideren aceptables.

El cuarto componente, la información y comunicación, juega un papel clave al asegurar que todas las personas involucradas tengan acceso a la información necesaria, en el momento justo, para cumplir con sus responsabilidades. Y es que, al final, no basta con tener la información; debe llegar a las personas adecuadas cuando

más la necesitan. Finalmente, la supervisión o monitoreo continuo es esencial para que el sistema de control no quede obsoleto. Este componente asegura que se mantenga actualizado, se adapte a los cambios y se corrijan cualquier fallo o desajuste que surja.

Estos cinco elementos no actúan de manera aislada, sino que se retroalimentan y fortalecen mutuamente, generando un marco dinámico de gobernanza interna.

Control interno en empresas del sector financiero y comercial: En el contexto del sector financiero y comercial, el control interno adquiere una dimensión aún más sensible. Estas organizaciones manejan grandes volúmenes de información confidencial, recursos económicos y relaciones contractuales con terceros. Por tanto, requieren sistemas de control robustos que no solo aseguren la precisión de sus registros contables, sino que también protejan los datos de sus clientes, supervisen las operaciones de crédito y mitiguen riesgos como el fraude o el lavado de activos (Mendoza-Zamora et al., 2018).

En empresas comerciales, por ejemplo, el control interno es clave para gestionar las ventas a crédito, controlar las cuentas por cobrar, evitar pérdidas por devoluciones fraudulentas o monitorear el cumplimiento de políticas comerciales. En las entidades financieras, por otro lado, la estructura de control se enfoca en la evaluación del riesgo crediticio, la transparencia de las operaciones y el cumplimiento regulatorio exigido por los entes de supervisión, como la Superintendencia de Bancos del Ecuador.

Además, estas empresas están sujetas a la Ley Orgánica de Protección de Datos Personales (2021), lo que obliga a integrar en sus sistemas de control mecanismos que aseguren la trazabilidad, la confidencialidad y la integridad de los datos tratados. Un sistema de control interno bien implementado permite, en este caso, no solo cumplir con lo legal, sino también generar confianza en los clientes y fortalecer la reputación organizacional.

Evolución histórica del control interno: Hablar de control interno es casi como recorrer un mapa que ha ido transformándose con el paso del tiempo. En sus

inicios, allá por los años noventa, el Informe COSO I (1992) apareció como una brújula necesaria para las organizaciones que buscaban orden y seguridad en sus operaciones. No era solo un documento técnico: representaba la primera vez que se entendía al control interno como un sistema integral, compuesto por políticas, prácticas y valores que impregnaban toda la cultura de una empresa (COSO, 2013).

Años después, en 2004, llegó COSO II, conocido como el Enterprise Risk Management (ERM). Este modelo no solo afinó los engranajes del anterior, sino que puso el acento en la gestión del riesgo como núcleo de la toma de decisiones. En un mundo empresarial donde la incertidumbre era la regla, COSO II ofreció un marco más amplio y dinámico, permitiendo que las organizaciones se anticiparan a escenarios complejos, en lugar de limitarse a reaccionar.

Finalmente, con la actualización de COSO 2013, el discurso cambió otra vez. El marco se adaptó a los nuevos desafíos de la globalización y la tecnología, subrayando la importancia de la información confiable y la rendición de cuentas. La visión moderna ya no habla de un control rígido, casi policial, sino de un proceso flexible, orientado a riesgos, que acompaña a la estrategia del negocio. Y es que, hoy en día, el control interno no se concibe como un simple “mecanismo de freno”, sino como un verdadero acelerador de confianza y sostenibilidad organizacional.

En definitiva, este recorrido histórico muestra cómo el control interno ha dejado de ser una herramienta estática para convertirse en un compañero de ruta que evoluciona con las necesidades y vulnerabilidades del entorno empresarial.

Modelos internacionales de control interno: Cuando se habla de modelos internacionales, dos nombres aparecen siempre en la conversación: COSO y COBIT. Ambos han marcado pautas distintas, pero complementarias, para entender cómo se deben vigilar y encauzar los procesos de una organización.

Por un lado, el marco COSO se enfoca en la visión estratégica y global de la empresa. Su fuerza radica en integrar aspectos como el ambiente de control, la evaluación de riesgos, las actividades de supervisión y la comunicación interna. Es decir, se preocupa de que la organización, en su conjunto, tenga una cultura de cumplimiento, ética y eficiencia (COSO, 2013).

El modelo COBIT (Control Objectives for Information and Related Technology), en cambio, nació en el mundo de las tecnologías de la información. Si COSO es como el mapa general, COBIT sería el manual detallado que explica cómo alinear la gestión de TI con los objetivos de negocio, asegurando que la información esté protegida, disponible y confiable (Mendoza-Zamora et al., 2018). COBIT se convirtió en un referente indispensable en empresas donde los sistemas digitales no son solo una herramienta, sino el corazón mismo de la operación.

La diferencia, entonces, es clara: COSO abraza el todo; COBIT, la parte tecnológica. Pero en la práctica, muchas organizaciones optan por combinarlos. Y es que, en una época en la que lo digital atraviesa cada rincón del negocio, no basta con un marco general; se necesita también la lupa técnica que proporciona COBIT.

2.2.2. Control Interno en el Área Comercial

Cuentas por cobrar y gestión de clientes: En Ecuador, el control interno aplicado a cuentas por cobrar tuvo una relevancia particular en empresas comerciales, ya que permitió mejorar la liquidez y reducir la morosidad. Por ejemplo, un estudio sobre la empresa Barzam S.A. (periodo 2020-2021) analizó cómo el control interno en el área de cobranza incidió directamente en la liquidez de la organización. Se usó un enfoque descriptivo y evaluación documental para medir la efectividad del sistema, estableciendo indicadores como días de mora y comportamientos de pago.

Los resultados evidenciaron que procesos más estructurados (conciliaciones puntuales, seguimiento sistemático y roles definidos para el personal) generaron aumentos significativos en la recuperación financiera antes del vencimiento (Barzola & Zambrano 2021) De este modo, se concluyó que una gestión de clientes con controles internos rigurosos fomentó no solo eficiencia contable, sino también confianza en los usuarios.

Otro caso revelador fue el de la Junta de Agua Potable de Chipe-Hamburgo (La Maná, 2023), donde se aplicó un estudio mixto (encuestas, entrevistas y análisis financiero-documental). Allí se detectaron factores como falta de seguimiento, capacitación y procedimientos claros, lo que se tradujo en un alto índice de morosidad (más del 60 %). Se concluyó que sin una estructura definida (con políticas de

cobranza y roles precisos la institución enfrentó graves consecuencias operativas y financieras (Patrón et al., 2024).

Prevención de riesgos operativos y financieros: El control interno también desempeñó un rol central en la mitigación de riesgos operativos y financieros dentro del área comercial. Un reporte reciente reconoció que esta herramienta estructurada permitió reducir pérdidas, fraudes y errores administrativos mediante políticas internas, segregación de funciones y monitoreo (Cumbicos et al., 2023).

Asimismo, un estudio focalizado en cooperativas de ahorro en Cuenca (2024) adoptó un enfoque mixto para evaluar la implementación de buenas prácticas internas. El hallazgo más notable fue que en aquellos casos donde hubo un verdadero compromiso por parte de la alta dirección y donde la tecnología se utilizaba de manera efectiva, hubo una menor exposición tanto a riesgos operativos como financieros (Ávila et al., 2024) rperspectivasinvestigativas.org. La lógica sugiere que estos resultados mostraron que el control interno no solo tenía como objetivo salvaguardar los activos, sino que también ayudaba a la organización a mejorar su resiliencia ante desafíos inesperados. De alguna manera, actuó como una póliza de seguros: protegiendo a la organización no solo en activos tangibles, sino preparándola para lo imprevisto.

Rol del control interno frente a la protección de datos personales: Con la promulgación de la Ley Orgánica de Protección de Datos Personales o LOPDP en 2021 en Ecuador, hubo un cambio en la estructura organizacional de las empresas, particularmente en el tratamiento sensible con el sector comercial. La nueva normativa fortaleció el control interno como una herramienta organizacional no solo para cumplir con la ley, sino también para fomentar una cultura de cumplimiento que valore la responsabilidad, la transparencia y la privacidad.

Desde el punto de vista en el ámbito operativo, el control interno ha permitido implementar políticas específicas sobre la gestión de la información personal, desde su recolección hasta su eliminación o archivo. Por citar un ejemplo, el control de acceso a las bases de datos, la recolección documentada y controlada de los consentimientos informados, las auditorías internas periódicas, y el monitoreo de la información compartida, entre otras, han surgido como medidas irrenunciables para la salvaguarda de posibles perjuicios. Estas acciones, además de ejercer y resguardar

la privacidad, también facilitaron el fortalecimiento de la confianza de las organizaciones y sus clientes. La Asamblea Nacional del Ecuador, analiza y sugiere en su documento del 2021 que, ante la ausencia de medidas técnicas y organizativas de resguardo como la soberanía y la justicia, sumadas a la protección de la trazabilidad de la información, eso podrá conllevar a una falta y un incumplimiento y restricción de la soberanía y la justicia.

Asimismo, estudios recientes evidenciaron que aquellas empresas que contaban con un sistema de control interno robusto estaban en mejores condiciones para adaptarse a los principios rectores de la LOPDP, como la minimización, la finalidad específica y la confidencialidad (VisualCom Publications, 2023). Esto se tradujo en una mayor capacidad para prevenir filtraciones, errores humanos o accesos no autorizados, todos ellos considerados riesgos operacionales críticos. Por otro lado, el control interno también facilitó la inclusión de nuevas figuras exigidas por la ley, como el Delegado de Protección de Datos Personales (DPD), quien actúa como garante del cumplimiento normativo dentro de la organización (Registro Oficial Suplemento No. 459, 2021).

Riesgos específicos en procesos comerciales: Cuando se habla del área comercial, muchos piensan en ventas, metas y campañas llamativas. Pero detrás de esa fachada vibrante, se esconden riesgos que pueden golpear muy duro a una organización si no se gestionan a tiempo. Uno de los más frecuentes aparece en la captación de clientes. Basta con un formulario mal diseñado o un asesor apresurado para que se recojan datos sin el consentimiento adecuado. Y es que, en un escenario donde la confianza es oro, un error tan pequeño puede desencadenar sanciones legales o, peor aún, la pérdida de credibilidad frente a los propios clientes (Álvarez, 2023).

Otro riesgo crítico es la fuga de información en los CRM. Estos sistemas, que se han convertido en el corazón del área comercial, concentran datos valiosísimos: números de identificación, historiales de compra, preferencias financieras. Un acceso indebido —quizás un descuido con la contraseña o la ausencia de controles en dispositivos móviles— puede terminar exponiendo todo. Tal como advierte Rivas Macías (2022), la falta de controles formales abre la puerta a vulneraciones que ponen en jaque tanto la reputación como la estabilidad operativa.

A esto se suma un riesgo silencioso, pero muy común: los incumplimientos en marketing. Correos electrónicos enviados sin permiso, llamadas no autorizadas o campañas invasivas pueden violar directamente la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021). Y la verdad es que, más allá de las multas, la consecuencia más dura es perder la confianza del consumidor. Porque un cliente que se siente invadido difícilmente vuelve.

Buenas prácticas internacionales en control comercial: Aunque los riesgos son reales, también existen faros que iluminan el camino: las buenas prácticas internacionales. En el sector retail, por ejemplo, cadenas globales han aprendido a segmentar campañas publicitarias únicamente con datos previamente autorizados, utilizando sistemas que bloquean automáticamente cualquier contacto si no existe un consentimiento válido. Esto no solo reduce riesgos legales, sino que genera una experiencia de compra más respetuosa y cercana (VisualCom, 2023).

En la banca, los avances son todavía más notables. Muchas entidades implementan protocolos de doble autenticación y cifrado extremo a extremo en sus plataformas comerciales, asegurando que los datos de clientes nunca viajen desprotegidos (Mendoza-Zamora et al., 2018). Además, han creado portales donde los usuarios pueden ejercer sus derechos ARCO en cuestión de minutos, lo que refuerza la transparencia y fortalece la relación de confianza.

El sector de telecomunicaciones tampoco se queda atrás. Empresas líderes han desarrollado programas de control interno que incluyen auditorías trimestrales sobre el uso de datos en campañas masivas, asegurando que cada acción de marketing esté alineada con las normas de protección de datos. Incluso han incorporado mecanismos de “opt-in” renovables, donde los clientes deciden periódicamente si quieren seguir recibiendo información. Un pequeño gesto que, sin embargo, marca una gran diferencia en la percepción de respeto hacia el consumidor (Sevilla, 2023).

Rol de la cultura organizacional en el cumplimiento: Al final, por más controles tecnológicos o marcos legales que existan, todo se sostiene en un pilar mucho más humano: la cultura organizacional. Y es que, cuando el personal entiende

que proteger los datos de los clientes es tan importante como lograr una venta, el control interno deja de ser una carga y se convierte en un hábito natural.

La ética corporativa juega aquí un papel decisivo. Una empresa que premia la transparencia, que no tolera atajos ni prácticas dudosas, termina construyendo un ambiente donde cada colaborador actúa como guardián de la información. Como señalan Hernández y Vázquez (2023), el aprendizaje de experiencias internacionales evidencia que la cultura de cumplimiento es el verdadero motor que sostiene la aplicación de las leyes.

Pero no basta con buenas intenciones. La formación continua es la herramienta que transforma la cultura en acción. Capacitar a los equipos de ventas sobre la LOPDP, simular casos reales de manejo de consentimientos o explicar las consecuencias de un error en el trato de datos son pasos que marcan la diferencia. Además, estas iniciativas transmiten un mensaje poderoso: “cuidar la información del cliente es cuidar la propia vida de la empresa”.

En definitiva, una cultura organizacional sólida, cimentada en ética y capacitación, no solo garantiza el cumplimiento de la normativa, sino que refuerza la confianza de los clientes y convierte al área comercial en un espacio donde la legalidad y la responsabilidad caminan de la mano.

2.2.3. Protección de Datos Personales en el Ecuador

La protección de los datos personales en Ecuador experimentó una transformación importante desde su reconocimiento constitucional hasta la aprobación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en 2021. Este apartado exploró ese recorrido jurídico, los principios rectores de la Ley, los derechos que confiere a los titulares y el papel central del consentimiento informado en el tratamiento legítimo.

Evolución legal: de la Constitución a la LOPDP (2021): El derecho a la protección de datos personales fue reconocido por primera vez en la Constitución ecuatoriana de 2008, en su artículo 66, numeral 19, lo que otorgó un estatus constitucional al derecho a la privacidad y el manejo informado de información personal (Registro de la República del Ecuador, 2008).

Sin embargo, ese reconocimiento no incluyó mecanismos específicos para su aplicación práctica, lo cual generó lagunas regulatorias. Ante esta realidad, el país promulgó el 26 de mayo de 2021 la LOPDP (publicada en el Registro Oficial Suplemento 459) con el propósito de establecer principios, obligaciones y derechos claros para el tratamiento de datos personales tanto en el sector público como privado (Ley Orgánica de Protección de Datos Personales, 2021)

Principios de la Ley Orgánica de Protección de Datos Personales: La LOPDP consagró una serie de principios que guiaron todo tratamiento de datos personales. Entre estos se incluyeron los principios de legalidad, lealtad, transparencia, finalidad específica, minimización, exactitud, proporcionalidad e integridad y confidencialidad. Además, incorporó la responsabilidad proactiva, que obliga a demostrar cumplimiento normativo mediante medidas técnicas y organizativas adecuadas (Játiva y Yánez, 2021). Estos principios aseguraron que las entidades solo procesaran datos cuando existiera una base legítima y formal, evitando usos indebidos o excesivos.

Derechos ARCO y obligaciones del responsable del tratamiento

La normativa también estableció un conjunto de derechos para los titulares, conocidos como derechos ARCO: Acceso, Rectificación, Cancelación y Oposición, así como otros derechos adicionales como portabilidad y suspensión del tratamiento (SEPS, 2023).

Las organizaciones quedaron obligadas a habilitar mecanismos accesibles (como plataformas digitales o líneas de atención) para atender estas solicitudes en plazos establecidos (p. e., quince días). Además, el responsable del tratamiento debía registrar activamente sus bases de datos, realizar evaluaciones de impacto y adoptar medidas preventivas frente a incidentes y vulneraciones (Reglamento general, 2021).

El consentimiento como eje del tratamiento legítimo: El consentimiento del titular se erigió como fundamento del tratamiento legal de datos personales. La LOPDP definió que este debía ser libre, específico, informado e inequívoco, y requirió que se registrara formalmente cada manifestación de voluntad del titular (Ley Orgánica de Protección de Datos Personales, art. …). Esto resultó fundamental, especialmente cuando se cedían datos a terceros o se empleaban para marketing

(PwC Ecuador, 2023; Reglamento, 2021). Si no se cumplían esos requisitos, el tratamiento se volvía ilegítimo y podía acarrear sanciones o reclamaciones por parte del titular.

1. Comparación con la normativa internacional (GDPR, Ley mexicana, Ley argentina)

Comparar la LOPDP con marcos internacionales no es un juego de diferencias por deporte; es, más bien, una forma de entender hacia dónde empuja el mundo el estándar de privacidad. Con el GDPR como faro, la LOPDP converge en principios esenciales: licitud, transparencia, finalidad específica, minimización y seguridad, además de reconocer derechos del titular que van desde los ARCO hasta la portabilidad. Esta sintonía no es casual: Ecuador abrazó, con matices propios, la lógica europea de la responsabilidad proactiva, la privacidad desde el diseño y la evaluación de impacto cuando el riesgo es alto (Asamblea Nacional del Ecuador, 2021; Presidencia de la República del Ecuador, 2023).

Ahora bien, hay diferencias que conviene mirar con lupa. En la LOPDP, la designación del Delegado de Protección de Datos (DPD) es obligatoria en ciertos contextos —tratamientos masivos o categorías especiales—, mientras que en el esquema europeo la figura del DPO suele tener umbrales más amplios. También varían los plazos y formalidades de notificación de brechas: el texto ecuatoriano fija ventanas específicas para responsables y encargados, reflejando una apuesta por la trazabilidad y la reacción temprana (arts. 39–43 LOPDP). En conjunto, el marco nacional se alinea con Europa, pero conserva decisiones de diseño normativo propias del entorno institucional ecuatoriano (Hernández & Vázquez, 2023; Asamblea Nacional del Ecuador, 2021).

Si miramos a México y Argentina, encontramos una base común muy marcada en consentimiento informado y derechos ARCO, herencia de una tradición regional que priorizó el control del titular sobre su información. La LOPDP, sin embargo, se acerca más al estándar europeo en algo clave: exige demostrar cumplimiento, no solo declararlo, y empuja a las organizaciones a institucionalizar herramientas como la DPIA, registros de tratamiento y controles verificables. En otras palabras, la región comparte el corazón (ARCO y consentimiento), pero Ecuador da un paso extra hacia

la evidencia y la gobernanza del dato, algo que los análisis comparados y las guías técnicas recomiendan desde hace tiempo (Nevardo, 2020).

Principio de responsabilidad proactiva: La responsabilidad proactiva cambia las reglas del juego: no basta con "cumplir", hay que poder probarlo. Y es que, en la práctica, la autoridad no se conforma con políticas bonitas en un archivador; necesita evidencias: registros de actividades de tratamiento, consentimientos con trazabilidad, DPIA actualizadas, contratos con encargados, bitácoras de incidentes y, por supuesto, controles técnicos que funcionen de verdad. La LOPDP y su Reglamento lo dicen sin rodeos: medidas técnicas y organizativas adecuadas, de forma permanente y acorde al riesgo (Asamblea Nacional del Ecuador, 2021; Presidencia de la República del Ecuador, 2023).

Una forma sencilla de entenderlo es con una analogía: no alcanza con ponerse el cinturón; hay que mostrar la ficha técnica del auto y el historial de mantenimiento. En términos corporativos, eso se traduce en KPIs de cumplimiento, auditorías periódicas y evidencia de que los hallazgos se cierran a tiempo. La designación del DPD —con independencia funcional y perfil acreditado— no es un "adorno" normativo, sino el pivote que articula asesoría, supervisión y diálogo con la autoridad (Resolución SPDP-SPD-2025-0004). Para muchas empresas, incorporar ISO/IEC 27701 como extensión de 27001 ha sido el atajo más ordenado para materializar esa responsabilidad proactiva en procesos, métricas y controles auditables (ISO, 2024).

Casos de sanciones y precedentes recientes en Ecuador y Latinoamérica: La teoría suena bien, pero lo que endereza conductas son los precedentes. En Ecuador, desde mayo de 2023 la autoridad empezó a imponer sanciones administrativas, con un régimen que clasifica infracciones leves, graves y muy graves, y con multas que pueden alcanzar hasta el 1 % del volumen de negocio. El mensaje es claro: quien trata datos debe hacerlo con rigor y demostrarlo con evidencias (Asamblea Nacional del Ecuador, 2021; Presidencia de la República del Ecuador, 2023).

¿Qué conductas se han observado en la región? Tres patrones se repiten: marketing sin consentimiento (o con consentimientos ambiguos), no notificar incidentes a tiempo y relaciones con terceros sin contratos de encargo que definan

medidas y responsabilidades. Son fallos que parecen “operativos”, sí, pero que dejan un rastro jurídico difícil de sostener ante una auditoría o una investigación. La literatura reciente en Ecuador lo ha retratado con honestidad: dificultades para inscribir bases, notificar brechas y adoptar controles técnicos adecuados, lo que revela que el mayor riesgo no es técnico, sino de gobernanza (Álvarez, 2023).

La lección, aunque suene obvia, es poderosa: quien no mide, no controla; y quien no controla, se arriesga. Por eso, más que temer a la sanción, conviene verla como un recordatorio de que la confianza del cliente —ese activo que no aparece en el balance— depende de prácticas verificables: consentimientos auditables, DPIA vivas, contratos con encargados bien amarrados y una resiliencia tecnológica que soporte el día a día y, cuando toque, responda rápido ante un incidente (ISO/IEC, 2022).

2.2.4. Cumplimiento Normativo y Control Interno

Este segmento exploró de manera más profunda cómo el cumplimiento de la LOPDP en Ecuador exigió la articulación de normas legales, políticas propias de privacidad y la figura del Delegado de Protección de Datos, todo enmarcado dentro de un sistema de control interno eficaz.

Normas legales aplicables al sector empresarial: La aprobación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en mayo de 2021 marcó un hito regulatorio para Ecuador, estableciendo líneas claras sobre el uso, registro y gestión de datos personales por parte del sector público y privado (LOPDP, art. 47-49)

El Reglamento General añadió directrices específicas: registro de bases de datos, evaluaciones de impacto, medidas organizativas y técnicas, y un régimen sancionador categorizado en infracciones leves, graves y muy graves con multas de hasta el 1 % del volumen de negocio (Reglamento, cap. II y XI). La Superintendencia de Protección de Datos Personales (SPDP) se constituyó como autoridad autónoma con capacidad sancionadora y facultades para dictar directrices vinculantes, supervisar el cumplimiento y autorizar auditorías (Resolución SPDP 2025-2026).

Diseño de políticas internas y auditorías: Las empresas emprendieron procesos internos para adecuarse a la normativa mediante políticas de privacidad que

incluyeron registros de tratamiento, protocolos de consentimiento y procedimientos de evaluación de impacto. Las auditorías internas se convirtieron en pilares del control interno, con revisiones documentales, inspecciones tecnológicas y encuestas de cumplimiento para detectar fallos antes de sanciones formales (Consulting Systems, 2024).

Estudios en cooperativas en Cuenca mostraron que aquellas entidades que integraron auditorías periódicas y mecanismos de supervisión redujeron significativamente incidencias operacionales y de seguridad de datos (Ávila et al., 2024). Estas prácticas no solo garantizaron cumplimiento, sino que también funcionaron como freno a la negligencia y como herramienta de mejora continua.

Delegado de Protección de Datos Personales (DPD) y mecanismos de supervisión

La LOPDP exigió la designación de un Delegado de Protección de Datos Personales cuando el tratamiento fuese masivo o implicara datos sensibles (art. 48). Este profesional asumió la responsabilidad de asesorar a la alta dirección, supervisar el cumplimiento normativo, coordinar análisis de riesgos y evaluaciones de impacto, y actuar como enlace con la SPDP (Viteri, 2025).

Además, la resolución SPDP-SPD-2025-0004 estableció requisitos estrictos: formación en Derecho o TIC, experiencia mínima de cinco años y protección frente a destitución injustificada para preservar su independencia (SPDP, 2025). La integración de esta figura dentro del control interno fortaleció no solo la vigilancia del cumplimiento, sino también la confianza del titular y la respuesta ágil ante incidentes o infracciones (Baclaw, 2025)

El Delegado de Protección de Datos (DPD): funciones y desafíos: El DPD no es un “policía del no”, sino la voz que anticipa incendios y acompaña al negocio para que avance sin quemarse. Su misión es estratégica: asesorar a la alta dirección, supervisar el cumplimiento de la LOPDP y su Reglamento, coordinar evaluaciones de impacto (DPIA), articular respuestas ante incidentes y servir de enlace con la autoridad. Además, impulsa la formación continua y vigila evidencias clave: registros de tratamiento, contratos con encargados, bitácoras de incidentes y trazabilidad del

consentimiento (Asamblea Nacional del Ecuador, 2021; Presidencia de la República del Ecuador, 2023).

La ley ecuatoriana exige designarlo cuando el tratamiento es masivo o involucra categorías sensibles; y, para que el rol funcione, demanda independencia funcional y un perfil técnico-jurídico sólido. La SPDP ha detallado requisitos y salvaguardas para evitar destituciones arbitrarias, reforzando su autonomía frente a presiones operativas (Resolución SPDP-SPD-2025-0004). En la práctica, el DPD sostiene una conversación incómoda pero necesaria: ¿qué riesgos asumimos?, ¿qué controles faltan?, ¿cómo probamos que cumplimos? (Hernández & Vázquez, 2023).

Ahora, la verdad es que en Ecuador el rol todavía luce débil. Hay escasez de perfiles con experiencia, confusiones entre funciones de Cumplimiento, TI y Auditoría, y, a veces, presupuestos insuficientes para operar con dignidad. El reto es doble: blindar su independencia (acceso a Comité, agenda propia, canales directos con la gerencia) y aterrizar su impacto en métricas: tiempo medio de respuesta ARCO, porcentaje de consentimientos vigentes, DPIA actualizadas, hallazgos cerrados en plazo y verificación de terceros críticos. Y es que sin indicadores el DPD se queda en discurso, justo cuando la LOPDP prevé sanciones que pueden alcanzar hasta el 1 % del volumen de negocio en infracciones muy graves (Asamblea Nacional del Ecuador, 2021; PwC Ecuador, 2023).

En organizaciones comerciales —por ejemplo, una administradora de fondos— el DPD se vuelve la bisagra entre ventas y prudencia: acompaña el diseño de campañas desde el principio, valida bases de licitud y consentimientos, y negocia con TI controles como MFA/MDM o bloqueos en CRM cuando falte evidencia. No frena el negocio; lo ordena para que crezca sin sorpresas regulatorias (VisualCom Publications, 2023).

Auditorías de cumplimiento y certificaciones internacionales: Cumplir no es un acto de fe; se demuestra. Por eso, las auditorías de cumplimiento son el pulso del programa: revisan políticas, contrastan evidencias, prueban configuraciones y dejan trazabilidad de lo que funciona… y de lo que aún duele. Bajo marcos de control como COSO, la auditoría conecta gobierno, riesgos y actividades de control; y cuando

el dato personal entra en juego, esa visión se complementa con estándares de seguridad y privacidad (COSO, 2013).

Aquí destaca ISO/IEC 27701, la extensión de ISO/IEC 27001 para privacidad. No es un sello decorativo: agrega un PIMS (Privacy Information Management System) sobre el SGSI, con controles específicos para gobernanza del dato, consentimiento, relaciones con encargados y gestión de derechos. En castellano llano: aterriza la responsabilidad proactiva en procedimientos, roles, registros y métricas que pueden auditarse (ISO/IEC, 2022).

Adoptar 27001+27701 facilita el mapeo contra la LOPDP: inventarios y RAT, criterios de minimización y conservación, DPIA para tratamientos de alto riesgo, respuesta a incidentes dentro de plazo, controles técnicos (cifrado, MFA/MDM), y cláusulas con encargados que resistan el escrutinio. Además, habilita ciclos PDCA con planes de acción y cierres verificables, justo lo que la autoridad —y los clientes— esperan ver (Presidencia de la República del Ecuador, 2023).

Un buen programa define qué auditar (consentimientos, ARCO, terceros, seguridad, campañas), cómo medirlo (KPI/KRI realistas) y cuándo corregir (plazos y responsables). Y es que, sin ese triángulo, la auditoría se vuelve un ritual anual sin consecuencias. Con él, en cambio, se transforma en motor de mejora continua y en el mejor argumento para demostrar, con serenidad y papeles en mano, que la organización no solo dice cumplir: lo prueba (VisualCom Publications, 2023).

2.2.5. Seguridad de la Información y Gestión de Riesgos

Este bloque abordó cómo las organizaciones ecuatorianas integraron sistemas de gestión de seguridad con un enfoque de control interno robusto, buscando proteger sus activos informáticos y mitigar riesgos operativos vinculados al tratamiento de datos personales.

Sistemas de Gestión de Seguridad de la Información (SGSI): Se comprobó que muchas empresas en Ecuador implementaron Sistemas de Gestión de Seguridad de la Información (SGSI), inspirados en normas internacionales, como la ISO/IEC 27001. Este enfoque permitió gestionar de manera estructurada la confidencialidad, integridad y disponibilidad de los activos informáticos, siguiendo el ciclo PDCA

(Planificar-Hacer-Verificar-Actuar) para promover la mejora continua (ISO/IEC 27001, 2022).

Mediante este sistema, se definieron políticas claras de seguridad, inventarios de activos, análisis de riesgos y controles formales, lo cual reforzó la protección desde el diseño mismo del tratamiento.

Normas internacionales aplicables (ISO 27001, etc.): La adopción de la ISO 27001 se complementó con la aplicación de extensiones como la ISO 27701, que añade controles de privacidad alineados con estándares como la GDPR, aportando evidencia jurídica-técnica adecuada para conformidad con la LOPDP ecuatoriana (ISO/IEC 27701, 2019). Estudios en entidades privadas demostraron que esta integración facilitó la responsabilidad proactiva, dotó de trazabilidad al tratamiento de datos y fortaleció la gobernanza de la información (Inforc, 2024).

Gestión del riesgo y control de accesos: La gestión de riesgos se institucionalizó como una práctica clave. En particular, un estudio : centrado en una organización de mujeres en la provincia de El Oro identificó que los datos sensibles –sociales, legales, psicológicos– eran altamente vulnerables. Por ello, se propusieron controles como cifrado, segmentación de accesos, políticas de contraseñas y revisiones periódicas con clasificación de datos (Alvear et al., 2024). Esto permitió mitigar riesgos operativos y fortalecer la confiabilidad del tratamiento de información personal.

Auditoría informática y trazabilidad de los datos: La auditoría informática, como componente del control interno, evaluó los sistemas tecnológicos, procesos y controles para garantizar la integridad y seguridad de la información. Fue usada para verificar la conformidad con la LOPDP y otros estándares, identificar vulnerabilidades y proponer mejoras técnico-operativas (Imbaquingo et al., 2020).

Asimismo, se enfatizó la trazabilidad de los datos mediante registros de acceso, bitácoras y reportes, permitiendo auditar el ciclo completo, desde la recolección hasta la supresión, incluyendo cesiones o transferencias de datos.

El enfoque de “Seguridad por diseño y por defecto”

Pensar la seguridad *por diseño y por defecto* es pasar de los remiendos a la arquitectura. El art. 39 de la LOPDP exige incorporar la protección de datos desde las primeras fases del proyecto y, además, garantizar que por defecto solo se trate lo estrictamente necesario para cada finalidad. Es decir, nada de casillas premarcadas, nada de recopilaciones “por si acaso”, nada de retenciones eternas. La ley pide previsión, mesura y evidencias de que esas decisiones se tomaron con cabeza fría (Asamblea Nacional del Ecuador, 2021).

Este enfoque se complementa con la obligación de analizar riesgos, amenazas y vulnerabilidades, y de determinar medidas técnicas y organizativas acordes al nivel de exposición (arts. 40–41). En la práctica, esto significa mapear el ciclo del dato, clasificar información, definir controles de acceso y probar que funcionan antes de salir a producción. La verdad es que, cuando estas decisiones se toman tarde, se paga caro: corregir en marcha es más costoso y, muchas veces, insuficiente (Presidencia de la República del Ecuador, 2023).

Para aterrizarlo, marcos como ISO/IEC 27001 y su extensión ISO/IEC 27701 ayudan a convertir el principio legal en procesos repetibles: políticas claras, inventarios de activos, análisis de riesgos, controles para privacidad y seguridad, y evidencia auditables del “cómo” y el “cuándo” (Inforc, 2024). Un ejemplo sencillo: si tu formulario de captación solo pide lo indispensable, el CRM bloquea cualquier uso no previsto y, por defecto, los accesos están segmentados y cifrados, estás honrando el espíritu del art. 39 sin frenar la operación.

Evaluación de Impacto a la Privacidad (DPIA) como herramienta de control: La DPIA es el “ensayo general” antes del estreno. El art. 42 de la LOPDP la vuelve obligatoria cuando el tratamiento, por su naturaleza o contexto, pueda generar alto riesgo para los derechos de las personas. Y es que la DPIA obliga a hacer preguntas incómodas (pero necesarias): ¿para qué tratamos estos datos?, ¿con qué base de licitud?, ¿qué puede salir mal?, ¿qué controles necesitamos para evitarlo? (Asamblea Nacional del Ecuador, 2021).

En clave operativa, una DPIA sólida mapea flujos, identifica categorías de datos y destinatarios, evalúa probabilidad e impacto, y prioriza medidas de mitigación

con responsables y plazos. Además, se documenta: nada de “cumplimos porque sí”. La guía práctica que se promueve en el país apunta justo a eso: evidencias que resistan auditoría, con criterios de proporcionalidad y minimización (Presidencia de la República del Ecuador, 2023; PwC Ecuador, 2023; VisualCom Publications, 2023).

Integrar la DPIA al SGSI (27001) y al PIMS (27701) evita que quede en un informe “bonito” sin consecuencias: activa planes de acción, revisiones periódicas y cierres verificables de hallazgos. Y, cuando hay terceros, exige revisar contratos y controles de punta a punta. De hecho, diagnósticos recientes muestran que omitir transferencias a terceros en la DPIA es un talón de Aquiles frecuente… y costoso (ISO/IEC, 2019; Inforc, 2024).

Riesgos emergentes en la era digital: El tablero de riesgos se movió. Ciberataques cada vez más sofisticados (phishing dirigido, ransomware en cadena), uso despreocupado de IA generativa que termina filtrando datos en prompts, dispositivos móviles sin gestión centralizada y ese universo paralelo del shadow IT dibujan un escenario exigente. Aquí, la LOPDP aporta dos anclas: notificar vulneraciones a tiempo y demostrar medidas razonables antes de que ocurra lo peor (art. 43). Y es que, sin trazabilidad ni controles, la reacción llega tarde (Asamblea Nacional del Ecuador, 2021).

En lo técnico, reforzar cifrado, MFA y MDM, monitoreo con logs revisables, segmentación de accesos y planes de continuidad probados; en lo organizativo, auditoría informática periódica, políticas claras de uso de herramientas de IA y un catálogo de aplicaciones autorizadas para desterrar el shadow IT (ISO/IEC, 2022; Imbaquingo et al., 2020; Lucero, 2023). Además, la formación hace la diferencia: donde hay cultura de control y liderazgo comprometido, los incidentes caen y la respuesta mejora (Cumbicos et al., 2023).

En síntesis, no se trata de vivir con miedo, sino de jugar a la ofensiva: anticipar riesgos, probar controles y cerrar brechas con disciplina. La combinación de LOPDP + 27001/27701 + auditoría continua ofrece una ruta realista para navegar esta era digital sin sacrificar lo esencial: la confianza de las personas cuyos datos custodiamos (Inforc, 2024).

2.3 Marco Legal:

La jurisdicción es el tratado al compromiso, ya que la situación que amerite hacia las entidades generales como políticos, ley orgánica y régimen social, son partes importantes para el desarrollo característicos de eventos importantes que imponga un país. La ley en si ayuda que los procesos se lleven de una manera satisfactoria y con el hecho de potenciar la nación y sus cualidades hacia un buen y eficiente comercio. (Asamblea nacional del la republica del Ecuador, 2021)

1) Constitución de la República del Ecuador (2008)

Art. 66, núm. 19

El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley

Art. 66, núm. 20

El derecho a la intimidad personal y familiar.

Art. 66, núm. 21

El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.

Art. 92 (hábeas data).

Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su

finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.

2) Ley Orgánica de Protección de Datos Personales – LOPDP (2021)

Art. 1 (objeto y finalidad).

Objeto y finalidad.-El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla

principios, derechos, obligaciones y mecanismos de tutela.

(Ley Orgánica de Protección de Datos Personales [LOPDP], 2021, art. 1).

Art. 2 (ámbito material).

Ámbito de aplicación material.-La presente ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior. La ley no será aplicable a:

a) Personas naturales que utilicen estos datos en la realización de actividades familiares o domésticas;

b) Personas fallecidas, sin perjuicio de lo establecido en el artículo 28 de la presente Ley;

c) Datos anonimizados, en tanto no sea posible identificar a su titular. Tan pronto los datos dejen de estar disociados o de ser anónimos, su tratamiento estará sujeto al cumplimiento de las obligaciones de esta ley, especialmente la de contar con una base de licitud para continuar tratando los datos de manera no anonimizada o disociada;

d) Actividades periodísticas y otros contenidos editoriales;

e) Datos personales cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía en materia de gestión de riesgos por desastres naturales; y, seguridad y defensa del Estado, en cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad;

f) Datos o bases de datos establecidos para la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, llevado a cabo por los organismos estatales competentes en cumplimiento de sus funciones legales. En cualquiera de estos casos

deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad; y

g) Datos que identifican o hacen identificable a personas jurídicas.
Son accesibles al público y susceptibles de tratamiento los datos personales referentes al contacto de profesionales y los datos de comerciantes, representantes y socios y accionistas de personas jurídicas y servidores públicos, siempre y cuando se refieran al ejercicio de su profesión, oficio, giro

de negocio, competencias, facultades, atribuciones o cargo y se trate de nombres y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, y, número de teléfono profesional. En el caso de los servidores públicos, además serán de acceso público y susceptibles de tratamiento de datos, el histórico y vigente de la declaración patrimonial y de su remuneración.

(LOPDP, 2021, art. 2).

Art. 3 (ámbito territorial).

Ámbito de aplicación territorial.-Sin perjuicio de la normativa establecida en los instrumentos internacionales ratificados por el Estado ecuatoriano que versen sobre esta materia, se aplicará la presente Ley cuando:

1. El tratamiento de datos personales se realice en cualquier parte del territorio nacional;

2. El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional;

3. Se realice tratamiento de datos personales de titulares que residan en el Ecuador por parte de un responsable o encargado no establecido en el Ecuador, cuando las actividades del tratamiento estén relacionadas con: 1) La oferta de bienes o servicios a dichos titulares, independientemente de si a estos se les requiere su pago, o, 2) del control de su comportamiento, en la medida en que este tenga lugar en el Ecuador; y,

4. Al responsable o encargado del tratamiento de datos personales, no domiciliado en el territorio nacional, le resulte aplicable la legislación nacional en virtud de un contrato o de las regulaciones vigentes del derecho internacional público.**(LOPDP, 2021, art. 3)**.

Art. 7 (bases de licitud).

Tratamiento legítimo de datos personas.-El tratamiento será legítimo y lícito si se cumple con alguna de las siguientes condiciones:

1) Por consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades especificas;

2) Que sea realizado por el responsable del tratamiento en cumplimiento de una obligación legal;

3) Que sea realizado por el responsable del tratamiento, por orden judicial, debiendo observarse los principios de la presente ley;

4) Que el tratamiento de datos personales se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad;

5) Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado; 6) Para proteger intereses vitales del interesado o de otra persona natural, como su vida, salud o integridad;

7) Para tratamiento de datos personales que consten en bases de datos de acceso público; u,

8) Para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma.**(LOPDP, 2021, art. 7)**.

Art. 8 (consentimiento).

Consentimiento.-Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea:

1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento;

2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento;

3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia,

4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular. El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento. El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste que dicho consentimiento se otorga para todas ellas **(LOPDP, 2021, art. 8)**.

Arts. 39–43

Art. 39.-Protección de datos personales desde el diseño y por defecto.-Se entiende a la protección de datos desde el diseño como el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al

estado de la técnica, naturaleza y fines del tratamiento, para lo cual, implementará las medidas técnicas, organizativas y de cualquier otra índole, con miras a garantizar el cumplimiento de las obligaciones en materia de protección de datos, en los términos del reglamento. La protección de datos por defecto hace referencia a que el responsable debe aplicar las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos del reglamento.

Art. 40.-Análisis de riesgo, amenazas y vulnerabilidades.-Para el análisis de riesgos, amenazas y vulnerabilidades, el responsable y el encargado del tratamiento de los datos personales deberán

utilizar una metodología que considere, entre otras:

1) Las particularidades del tratamiento;

2) Las particularidades de las partes involucradas; y,

3) Las categorías y el volumen de datos personales objeto de tratamiento.

Art. 41.-Determinación de medidas de seguridad aplicables.-Para determinar las medidas de seguridad, aceptadas por el estado de la técnica, a las que están obligadas el responsable y el encargado del tratamiento de los datos personales, se deberán tomar en consideración, entre otros:

1) Los resultados del análisis de riesgos, amenazas y vulnerabilidades;

2) La naturaleza de los datos personales;

3) Las características de las partes involucradas; y,

4) Los antecedentes de destrucción de datos personales, la pérdida, alteración, divulgación o impedimento de acceso a los mismos por parte del titular, sean accidentales e intencionales, por acción u omisión, así como los antecedentes de transferencia, comunicación o de acceso no autorizado o exceso de autorización de tales datos.

El responsable y el encargado del tratamiento de datos personales deberán tomar las medidas adecuadas y necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conlleven un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa que emita la Autoridad de Protección de Datos Personales.

Art. 42.-Evaluación de impacto del tratamiento de datos personales.-El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera.

La evaluación de impacto relativa a la protección de los datos será de carácter obligatoria en caso de:

a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de

perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales;

b) Tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales, o
c) Observación sistemática a gran escala de una zona de acceso público.

La Autoridad de Protección de Datos Personales establecerá otros tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos.

La evaluación de impacto deberá efectuarse previo al inicio del tratamiento de datos personales.

Art. 43.-Notificación de vulneración de seguridad.-El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que

sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación.

El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella.**(LOPDP, 2021, arts. 39–43)**.

CAPÍTULO III

MARCO METODOLÓGICO

La presente investigación se desarrolló bajo un enfoque cualitativo, con un alcance exploratorio y descriptivo, atendiendo a la necesidad de comprender en profundidad la forma en que las empresas, específicamente en su área comercial, integraron el control interno para cumplir con la Ley Orgánica de Protección de Datos Personales (LOPDP) en el contexto ecuatoriano.

3.1 Enfoque de investigación

Se optó por un enfoque cualitativo, debido a que este permitió mirar más allá de los aspectos técnicos o normativos, centrándose en las vivencias, prácticas y percepciones reales de los actores involucrados en la gestión de datos personales dentro del entorno comercial. Esta perspectiva aportó profundidad interpretativa, ya que no se trató únicamente de verificar si se cumplía con la ley, sino de entender cómo se la interpretaba, qué prácticas nacían del control interno y qué tensiones o vacíos emergían en su aplicación diaria.

Además, el enfoque cualitativo facilitó el diseño de recomendaciones contextualizadas, pues permitió recuperar no solo experiencias institucionales, sino también el sentido que las personas (administradores, colaboradores, responsables de tratamiento) otorgaban a la normativa y sus implicaciones. De este modo, el análisis se orientó hacia una comprensión situada y sensible a la realidad organizacional.

3.2 Alcance de la investigación

El estudio tuvo un alcance exploratorio y descriptivo, lo cual permitió abordar la problemática desde dos planos complementarios:

- **Exploratorio**, La vinculación que existe entre el control interno, el área de ventas, y el cumplimiento de la LOPDP en Ecuador aún no ha sido objeto de estudio profundo, particularmente desde el enfoque holístico que integre lo normativo y lo práctico. En este trabajo no se formularon supuestos conclusivos; en cambio, se intentó formular preguntas, reconocer

secuencias que emergieran y clarificar situaciones que no habían sido tan sistematizadas.. La verdad es que, al ser la LOPDP una normativa reciente (2021) y encontrarse aún en proceso de consolidación en varios sectores, se necesitaba un enfoque flexible para captar los cambios, los vacíos y las buenas prácticas que pudieran estar emergiendo.

- **Descriptivo**, es una investigación descriptiva porque trata de explicar cómo se lleva a cabo la implementación de los mecanismos de control interno en el área comercial, particularmente en el tema de cómo se protege la información personal. Esto implicó revisar políticas internas, flujos de información, procesos de consentimiento, datos relacionados con el control de información personal y la gestión de incidentes. Este enfoque descriptivo contribuyó en mayor medida a aclarar la situación que se documentó e informó sobre el cumplimiento y destacó los logros y limitaciones en los procesos del sistema corporativo en la República del Ecuador.

La combinación de un enfoque cualitativo con alcance exploratorio y descriptivo fue especialmente adecuada en este caso, porque la temática (protección de datos personales en el área comercial) se encuentra atravesada por dimensiones técnicas, jurídicas, humanas y organizacionales. Se trató de una problemática compleja y en transformación, marcada por la evolución tecnológica, las nuevas regulaciones, los cambios en los hábitos de consumo y las tensiones entre innovación comercial y responsabilidad ética.

En ese sentido, esta metodología permitió no solo mapear la realidad actual, sino también dar voz a los actores, comprender las barreras para el cumplimiento y construir propuestas que partan de las condiciones concretas de las empresas ecuatorianas, sin idealizaciones ni simplificaciones normativas.

3.3 Técnicas e Instrumentos

Para la presente investigación titulada “El control interno en el área comercial para garantizar el cumplimiento de la Ley de Protección de Datos Personales en una administradora privada de fondos”, se emplearán técnicas e instrumentos pertinentes al enfoque cualitativo y descriptivo, con el objetivo de obtener información precisa, contextualizada y aplicable al análisis del sistema de control interno vigente.

Técnicas empleadas:

Entrevista semiestructurada a profesionales clave

Se realizarán tres entrevistas dirigidas a actores estratégicos dentro de la empresa:

Jefe del Área Comercial

Encargado del Área de Sistemas

Encargado del Área de Control Interno

Estas entrevistas permitirán explorar, desde diferentes perspectivas, la implementación de los controles internos relacionados con la protección de datos personales, identificar brechas prácticas en el cumplimiento de la normativa vigente (LOPDP), y obtener insumos directos sobre las percepciones, desafíos y propuestas de mejora.

Análisis documental y diagnóstico interno

Paralelamente, se aplicará una técnica de revisión documental que incluirá políticas internas, procedimientos, registros de auditoría y protocolos de tratamiento de datos personales. Sobre la base de dicha documentación, se desarrollará un diagnóstico detallado del control interno, que servirá como evidencia objetiva para la evaluación.

Instrumentos de recolección:

Guías de entrevista personalizadas

Elaboradas conforme al rol de cada profesional entrevistado, estas guías contienen preguntas abiertas que permitirán profundizar en los procesos específicos de cada área y su relación con la protección de datos. Las entrevistas han sido diseñadas con base en los criterios de la Ley Orgánica de Protección de Datos Personales (Ecuador) y los principios del control interno según el modelo COSO.

Checklist de cumplimiento normativo (LOPDP)

Instrumento basado en los requisitos legales establecidos en la LOPDP, estructurado en secciones que evalúan gobernanza, principios de tratamiento, consentimiento, seguridad de la información y relación con terceros. Permite identificar el grado de cumplimiento y las obligaciones pendientes por parte de la empresa.

Matriz de riesgos de tratamiento de datos personales

Herramienta que permitirá identificar y clasificar los riesgos inherentes al tratamiento de datos en el área comercial, evaluando la probabilidad de ocurrencia y el impacto potencial, así como estableciendo medidas de mitigación recomendadas. Esta matriz se elaborará con enfoque preventivo, en función de los hallazgos de las entrevistas y documentos revisados.

Evaluación de Impacto a la Privacidad (DPIA)

Instrumento requerido por la LOPDP cuando existe tratamiento intensivo o sensible de datos personales. La DPIA permitirá realizar un análisis sistemático de los riesgos para los derechos y libertades de los titulares, la proporcionalidad del tratamiento, y las medidas técnicas u organizativas que se deben adoptar.

3.4 Población y Muestra

En el contexto de la investigación cualitativa, la definición de población no se orienta hacia la representatividad estadística, sino hacia la pertinencia conceptual y la profundidad del caso de estudio. Por ello, la población fue definida de forma estratégica, considerando a los actores con experiencia directa en la implementación y supervisión del control interno, específicamente en relación con el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP), dentro de los procesos comerciales de organizaciones del sector financiero.

La población objetivo de esta investigación fueron los profesionales responsables de gestionar, supervisar o monitorear los procesos para asegurar que la recolección de datos relacionados con los clientes, especialmente en actividades comerciales que requieren interacción y manejo de información, sea gestionada

adecuadamente. Más particularmente, se dirigió el enfoque hacia las personas a cargo del área comercial, los supervisores de sistemas (tecnología) y los supervisores de control interno de una administradora de fondos privada. Esto se debe a que su papel es crítico para el cumplimiento de la legislación existente, ya que participan en procesos clave para el marco de protección de los datos.

Desde este límite, se llevó a cabo un muestreo no probabilístico intencionado, en el cual se seleccionaron informantes clave cuya experiencia y conocimiento experto eran pertinentes para el fenómeno en investigación. Esta muestra incluyó tres perfiles profesionales que estaban directamente relacionados con el asunto en estudio:

Jefe del Área Comercial, por su rol en la recolección, uso y resguardo de datos de clientes.

Encargado de Sistemas, responsable de la infraestructura tecnológica que soporta la protección de datos.

Encargado de Control Interno, experto en normativa, auditoría y gestión de riesgos relacionados con el tratamiento de información personal.

Este enfoque metodológico permitió un abordaje profundo de la problemática, privilegiando la riqueza del discurso, la experiencia vivida y la documentación interna de procesos, más allá de una aproximación cuantitativa generalizable. Asimismo, facilitó una comprensión crítica, situada y contextualizada del nivel de cumplimiento de la LOPDP dentro de un entorno organizacional específico, sin comprometer los criterios de rigurosidad científica y validez interna propios de la investigación cualitativa.

2.2.6. Tipo de muestreo

Muestreo intencionado o por conveniencia (no probabilístico)

El muestreo intencionado (también conocido como muestreo deliberado o dirigido) es una técnica propia de investigaciones cualitativas en la cual se seleccionan los participantes de manera consciente y deliberada, con base en

criterios específicos de experiencia, conocimiento o participación directa en el fenómeno estudiado.

Se decidió utilizar esta modalidad dado que el propósito del estudio no es lograr una representatividad estadística, sino acceder a informantes clave que ofrezcan información procesada, relevante y contextualizada sobre la aplicación del control interno en relación con la Ley Orgánica de Protección de Datos Personales (LOPDP).

El método de muestreo intencional está bien defendido en este caso porque los entrevistados fueron elegidos en función de una estructura corporativa y su relación directa con las actividades fundamentales de recolección, procesamiento y salvaguarda de datos, lo que proporciona una comprensión profunda y matizada del tema de estudio.

● **Tipo específico utilizado dentro del muestreo intencionado:**

- **Muestreo por expertos o informantes clave:** Se eligió a profesionales con experiencia específica en el área comercial, tecnológica y de control interno.
- **Muestreo por conveniencia:** Adicionalmente, se aplicó este enfoque debido a la accesibilidad real a dichos informantes dentro de la organización estudiada, garantizando la viabilidad del trabajo de campo.

CAPÍTULO IV

PROPUESTA O INFORME

4.1 Presentación y análisis de resultados

Análisis de las entrevistas

1. Entrevista al Jefe del Área Comercial

Nombre simulado: Ing. Carlos M. Espinoza

Cargo: Jefe del Área Comercial

Lugar: Oficinas corporativas, Guayaquil

1. ¿Cuáles son los principales tipos de datos personales que gestiona el área comercial en su actividad diaria?

R: Principalmente manejamos información de identificación básica como nombres completos, cédulas, direcciones, correos electrónicos y teléfonos. También gestionamos datos financieros vinculados a los productos que ofrecemos, como saldos de cuenta, historial de aportes y preferencias de inversión. Todo esto entra dentro de lo que la ley cataloga como datos personales, y algunos incluso pueden considerarse sensibles.

2. ¿Qué procedimientos internos se aplican actualmente para garantizar la confidencialidad y seguridad de estos datos?

R: Tenemos protocolos muy claros, tanto en el ámbito físico como digital, que están diseñados para proteger la información. Por ejemplo, los asesores comerciales solo tienen acceso a los datos que realmente necesitan para cumplir con sus funciones. Además, hemos implementado políticas como la de escritorio limpio, el uso obligatorio de contraseñas fuertes y la regla de bloquear los equipos cuando alguien se ausenta de su puesto de trabajo. Y es que, todo el manejo de las bases de datos se realiza exclusivamente dentro de los sistemas internos de la empresa; está estrictamente prohibido copiar cualquier información fuera de este entorno.

3. ¿Qué controles específicos existen para evitar el uso indebido o la fuga de información por parte del personal comercial?

R: Se realizan auditorías internas de acceso a la información, donde se verifica qué usuario accedió a qué dato y en qué momento. También existe una política de sanciones internas que va desde llamados de atención hasta desvinculación, dependiendo de la gravedad. De todos modos, apostamos más a la prevención a través de la formación que a la sanción.

4. ¿Cómo se capacita al equipo comercial respecto a la Ley de Protección de Datos Personales y a las políticas internas de protección de datos?

R: Realizamos capacitaciones obligatorias cada seis meses. Además, al momento de ingresar, cada colaborador firma un acuerdo de confidencialidad y recibe una inducción específica sobre tratamiento de datos. Procuramos que las capacitaciones sean prácticas y basadas en casos reales que se pueden dar en la interacción con clientes.

5. ¿Qué herramientas digitales o manuales se utilizan en el área para la gestión de la información sensible?

R: Todo se gestiona a través de un CRM corporativo que tiene niveles de acceso personalizados. No trabajamos con archivos físicos, salvo formularios que luego se digitalizan y se archivan en condiciones seguras. Los reportes se generan automáticamente dentro del sistema y cualquier exportación de datos requiere autorización previa.

6. ¿Cómo se documentan y supervisan los procesos de consentimiento de los clientes respecto al uso de sus datos?

R: Cada cliente firma un formulario de consentimiento informado, ya sea en formato físico o digital, y ese documento se guarda cuidadosamente en su expediente. Además, nuestro CRM tiene una función que nos obliga a verificar que el consentimiento esté registrado antes de realizar cualquier acción comercial. Si no está disponible, simplemente bloquea la operación, lo que asegura que no se hagan movimientos sin el visto bueno del cliente.

7. ¿Qué tan alineadas considera que están las prácticas comerciales actuales con los lineamientos legales de protección de datos?

R: Creo que estamos bastante alineados, aunque siempre hay espacio para mejorar. En los últimos años, hemos implementado varias mejoras para asegurarnos de cumplir con la Ley Orgánica de Protección de Datos Personales de Ecuador. La verdad es que trabajamos de la mano con el área de cumplimiento y control interno, ajustando nuestras prácticas conforme a lo que dicta la normativa, lo que nos da la tranquilidad de estar en el camino correcto.

8. ¿Ha tenido el área comercial auditorías internas o externas respecto al cumplimiento de la Ley de Protección de Datos? ¿Qué hallazgos se identificaron?

R: Sí, hace unos meses tuvimos una auditoría interna. El principal hallazgo fue que algunos asesores no estaban actualizando los consentimientos de forma oportuna. Desde entonces, hemos reforzado ese punto con recordatorios automáticos y controles adicionales.

9. En términos de riesgos, ¿qué desafíos enfrenta el área comercial al implementar sistemas de control interno sin comprometer la eficiencia operativa o la experiencia del cliente?

R: Los desafíos en encontrar el equilibrio adecuado entre salvaguardar la información privada del cliente mientras se sigue brindando velocidad y eficiencia en el servicio al cliente. Obtener consentimiento es, de hecho, un requisito en ciertas situaciones. Por lo tanto, tratamos de gestionar el proceso de una manera amigable y sencilla, para que el cliente racionalice lo que se hace y no se sienta incómodo. El objetivo es que el cliente disfrute, mientras se le comprende y el proceso es eficiente.

10. Desde su perspectiva, ¿qué mejoras podrían implementarse para fortalecer el cumplimiento normativo en protección de datos desde lo comercial?

R: Mejorar la integración de sistemas y automatizar más procesos ayudaría mucho. También sería útil contar con campañas internas más frecuentes sobre la importancia de la protección de datos, para que no se vea como una carga, sino como parte natural de nuestro trabajo.

Analisis:

La entrevista al Jefe del Área Comercial, Ing. Carlos M. Espinoza, revela que tú gestionas datos personales como nombres, cédulas, direcciones, correos, teléfonos y datos financieros, como saldos e historial de aportes, en un CRM con accesos restringidos. Implementas protocolos como escritorio limpio, contraseñas robustas y bloqueo de equipos, además de auditorías de acceso y capacitaciones semestrales. Los clientes firman consentimientos que el sistema verifica antes de acciones comerciales.

Sin embargo, algunos asesores no actualizan consentimientos a tiempo, lo que genera riesgos legales, y los procesos de consentimiento ralentizan la atención al cliente. Como fortalezas, los protocolos y auditorías reducen fugas de información, y el CRM asegura accesos limitados. Para mejorar, automatiza la verificación de consentimientos con alertas en el CRM, usa guiones breves para explicar consentimientos a clientes en 30 segundos, refuerza capacitaciones con simulaciones mensuales y crea un tablero de control para monitorear el cumplimiento por asesor.

2. Entrevista al Encargado de Sistemas (TI)

Nombre simulado: Lic. Daniel L. Cárdenas

Cargo: Jefe de Tecnología y Seguridad de la Información

Lugar: Oficina de TI, Guayaquil

1. ¿Qué sistemas informáticos se usan en su empresa para almacenar y procesar datos personales de los clientes?

R: Se usan sistemas centralizados que integra un CRM con una base de datos segura y servidores internos, la información se maneja mediante una red privada virtual (VPN), lo que nos permite mantener la seguridad, mientras que los accesos se controlan mediante políticas de roles bien definidas.

2. ¿Qué medidas de seguridad se han implementado a nivel de infraestructura tecnológica para salvaguardar esos datos?

R: Tenemos cortafuegos activos, cifrado de datos durante la transmisión y cuando están almacenados, y autenticación multifactor como algunas de las medidas tecnológicas en vigor para controlar el acceso a la información y minimizar enormemente no solo la filtración de datos, sino también al personal autorizado para acceder a ella. Además, con la implementación de un sistema de detección de intrusiones y esquemas de seguridad en múltiples capas, el riesgo general se mitiga en gran medida.

3. ¿Qué medidas existen para restringir el acceso del personal comercial a las bases de datos de clientes y qué nivel de acceso tienen?

R: El acceso se gestiona de manera altamente granular y compartimentada, el personal comercial tiene acceso a toda la información pertinente a sus funciones, además se les impide realizar cualquier modificación a datos sensibles. También

quedan registrados los accesos, lo que permite a la institución controlar fácilmente la información y las interacciones que la rodean.

4. ¿Existe un sistema de trazabilidad o una auditoría que registre quién accedió a los datos personales y el tiempo de acceso?

R: Sí, tenemos un sistema de logs que graba cada acción que se realiza dentro de la plataforma, como accesos, modificaciones o descargas de información, los registros son revisados de forma periódica para garantizar que todo esté controlado y conforme a nuestras políticas de seguridad.

5. ¿Qué mecanismos de encriptación o resguardo se utilizan para proteger la información sensible durante la transmisión o almacenamiento?

R: Usamos protocolos de encriptación tipo SSL/TLS para transmisión y cifrado AES-256 para almacenamiento. La base de datos también tiene respaldo automatizado diario.

6. ¿Qué protocolos están en marcha para manejar incidentes de seguridad como filtraciones de datos y accesos no autorizados?

R: Tenemos un protocolo de respuesta a incidentes con múltiples pasos críticos que van desde la contención inmediata hasta forenses exhaustivos, se contactaron a las autoridades correspondientes cuando fue necesario y se realizo las brechas de seguridad, también para estar completamente preparados, simulamos incidentes periódicamente para evaluar nuestra respuesta a una variedad de escenarios.

7. Usando la protección de datos personales como referencia, ¿cómo trabaja el departamento de sistemas con el área comercial para hacer cumplir las políticas internas que garantizan el cumplimiento de la ley?

R: Colaboramos en detalle en la definición de procesos, se validó los flujos de datos, modificamos las interfaces del sistema para alinearlas con las demandas comerciales y, lo más importante, no comprometemos la seguridad. Verdaderamente, la colaboración de ambas partes es esencial para equilibrar la agilidad empresarial con el cumplimiento regulatorio.

8. ¿Se realizan evaluaciones de vulnerabilidad o auditorías tecnológicas de manera periódica? ¿Quién realiza estas evaluaciones?

R: Sí, se realizan evaluaciones internas de forma semestral y contratamos auditores externos anualmente para asegurarnos de estar al día.

9. ¿Cómo se asegura la integridad y disponibilidad de los datos personales ante fallos o desastres informáticos?

R: Tenemos un plan de recuperación ante desastres, servidores redundantes y respaldo fuera del sitio. La disponibilidad está garantizada al 99.9%.

10. ¿Qué desafíos tecnológicos ha identificado para reforzar los controles internos en el manejo de datos por parte del área comercial?

R: Uno de los mayores desafíos es lidiar con la resistencia al cambio, especialmente cuando introducimos nuevas restricciones o validaciones. A veces, los equipos sienten que estos ajustes ralentizan su trabajo, pero sabemos que son necesarios. Además, otro reto importante es garantizar que los dispositivos móviles, que muchos asesores usan, también estén adecuadamente protegidos. Esto se vuelve aún más crítico porque los dispositivos móviles son una puerta de entrada potencial a riesgos de seguridad.

Análisis:

En la entrevista con el Encargado de Sistemas, Lic. Daniel L. Cárdenas, nos explica que utilizan un CRM respaldado por una base de datos segura en servidores internos y una red privada virtual (VPN). Para mantener todo bajo control, aplican medidas como cortafuegos, encriptación AES-256, autenticación multifactor y un sistema de detección de intrusos. Además, todos los accesos, ediciones y descargas quedan registrados en logs detallados. El equipo realiza pruebas de vulnerabilidad internas cada seis meses y externas anualmente, respaldos diarios y cuentan con un plan de recuperación con una disponibilidad del 99.9%.

Aunque las fortalezas son claras, como la robusta encriptación y los logs detallados, los retos continúan, sobre todo con la resistencia al cambio y la protección de los dispositivos móviles de los asesores. Para fortalecer aún más el sistema, se está implementando software de gestión de dispositivos móviles (MDM) que cifrará los datos, ofreciendo además incentivos para quienes adopten las nuevas restricciones. También se han programado actualizaciones automáticas mensuales de software y simulaciones trimestrales de incidentes, que ahora incluyen dispositivos móviles, para asegurar que todo esté cubierto ante cualquier eventualidad.

3. Entrevista al Encargado de Control Interno

Nombre simulado: Abg. Lorena V. Ruiz

Cargo: Responsable de Control Interno y Cumplimiento Normativo

Lugar: Oficina de Auditoría Interna, Guayaquil

1. ¿Cuál es el enfoque general del sistema de control interno de la empresa en relación con la protección de datos personales?

R: Nuestro enfoque es preventivo y correctivo. Es decir, buscamos anticiparnos a los riesgos y actuar de inmediato si algo sale mal. Nos apoyamos en un conjunto de políticas, procedimientos y controles diseñados para reducir al máximo el riesgo de no cumplir con las normativas. Además, todo esto está respaldado por una fuerte cultura de cumplimiento que fomentamos constantemente dentro de la empresa.

2. ¿Qué tipos específicos de controles internos se han diseñado para el área comercial en este contexto?

R: Hemos implementado varios controles clave, como los controles de acceso, que aseguran que solo las personas autorizadas puedan ver información sensible. También revisamos de manera activa toda la información de los clientes, validamos sus permisos de acceso a la información y auditamos sus actividades de manera regular. Asimismo, mantenemos control de versiones sobre nuestras políticas de control de datos para asegurarnos de que estén vigentes y sean normativamente concordantes.

3. ¿Existen matrices de riesgo en relación con el manejo de información personal en el área comercial? ¿Cómo se gestionan estos riesgos?

R: Sí, tenemos una matriz de riesgo que estamos actualizando anualmente. Este sistema nos permite detectar y categorizar riesgos y, posteriormente, mitigarlos con planes de acción definidos. Realizamos un seguimiento mensual para asegurarnos de que los riesgos se estén gestionando como estaba planeado y que haya medidas mitigantes oportunas para manejar circunstancias imprevistas.

4. ¿Qué herramientas o metodologías utiliza el área de control interno para evaluar el cumplimiento de la Ley de Protección de Datos Personales?

R: Auditorías internas, revisiones documentales, entrevistas y análisis de indicadores de cumplimiento. Utilizamos listas de chequeo basadas en la normativa vigente.

5. ¿Se han identificado brechas o hallazgos recurrentes en auditorías relacionadas al manejo de datos personales por parte del área comercial?

R: Sí, hemos identificado retrasos en la recolección de consentimientos y en ocasiones, errores en el registro de los mismos. Esto ya está siendo corregido.

6. ¿Qué pasos se toman para monitorizar y asegurar la mejora de los controles internos en relación con el manejo de información sensible?

R: Hacemos esto a través de comités internos con las funciones relevantes de la empresa, donde revisamos los KPI relevantes de manera trimestral, así como con las actualizaciones regulatorias pertinentes de la empresa. Estas actualizaciones regulatorias se traducen en ajustes significativos a los controles que nos permiten mantenernos alineados con las mejores prácticas de la industria y abordando cualquier desafío que surja de manera oportuna. Este es un proceso constante, y además de proporcionarnos la capacidad de adaptarnos, también mejora nuestras capacidades en protección de datos.

7. ¿Cuál es el papel del control interno en la formación de concienciación sobre la protección de datos para los empleados?

R: El área de control interno está muy comprometida en la formación ya que tenemos tanto, diseñar como evaluar su implementación, adaptando si es necesario. También se aseguró de que llegara al corazón de la concienciación sobre la protección de datos de los empleados. Además, producimos boletines internos así como alertas sobre cualquier problema emergente, de esta manera, todos están informados y actualizados activamente sobre cualquier problema de protección de datos y, por lo tanto, están listos para enfrentar cualquier problema de protección de datos que surja.

8. ¿Hay coordinación con el departamento de TI y el área comercial para mejorar los sistemas de control interno? ¿Cómo funciona esa relación?

R: Sí, trabajamos de manera transversal. Cualquier decisión que cambie la gestión operativa de datos requiere aprobación conjunta.

9. En su experiencia, ¿cuáles son las principales debilidades que enfrentan las empresas de protección de datos en el sector?

R: Una de las principales debilidades es la falta de actualización de los sistemas tecnológicos de protección. A menudo, las empresas carecen de las herramientas tecnológicas más actuales, lo que las pone en desventaja. Además, hay una cultura de protección de datos que aún no se ha abrazado completamente en todos los niveles de la organización. Además de eso, tenemos desafíos legales porque hay nuevas normas con requisitos que hacen que el negocio esté en un estado constante de cambio.

10. ¿Qué recomendaciones estratégicas propondría para mejorar el control interno en el área comercial con miras a una mayor protección y cumplimiento normativo?

R: Creo que lo primero sería invertir en tecnología que ayude a automatizar los controles. Esto no solo hace los procesos más ágiles, sino que también reduce el margen de error. Además, es clave seguir reforzando la formación continua de todo el equipo, porque solo así se mantiene el compromiso con la protección de datos. También recomendaría establecer métricas claras de cumplimiento, para poder medir el progreso de manera objetiva. Y, por supuesto, fomentar la responsabilidad individual de cada miembro de la organización en cuanto al uso adecuado de los datos personales.

Análisis:

La entrevista con Abg. Lorena V. Ruiz, la Jefa de Control Interno, muestra que la empresa sigue tanto estrategias preventivas como correctivas, con medidas como acceso restringido, supervisión de la interacción con clientes del IC y validación de consentimientos. Sus matrices de riesgo se actualizan anualmente, junto con auditorías internas, listas de verificación y comités trimestrales orientados a la refinación de procesos. Sin embargo, señalaron la persistente debilidad de los retrasos en la obtención de consentimientos.

Integrarse con los sistemas y las áreas comerciales es, de hecho, valioso; sin embargo, luchan con tecnología obsoleta y una cultura de privacidad de datos subdesarrollada. Las fortalezas incluyen la matriz de riesgos y la colaboración

cruzada. Aún mejor, la propuesta sugiere establecer alertas automáticas en el CRM para retrasos en la concesión del consentimiento. Otras sugerencias incluyen la compra de herramientas de monitoreo automatizado y campañas trimestrales que presenten ejemplos reales de sanciones impuestas a otras empresas. Además, sería vital organizar reuniones mensuales con los equipos de Sistemas y Comerciales para abordar los cuellos de botella y diseñar estrategias de respuesta ágiles.

4.2 Diagnostico de control interno

Componentes del diagnóstico

1. Ambiente de Control

Tabla 1

Ambiente de control

Aspecto Evaluado	Evidencia / Observación	Nivel de Cumplimiento	Riesgo Asociado	Recomendación
Políticas de protección de datos	Existen políticas internas de confidencialidad y escritorio limpio, firmadas por el personal.	80%	Falta de un Delegado de Protección de Datos (DPD).	Designa un DPD con experiencia en LOPDP antes de diciembre de 2025.
Capacitación del personal	Capacitaciones semestrales sobre LOPDP, pero no todos los asesores las completan.	60%	Errores por desconocimiento de la normativa.	Implementa capacitaciones mensuales con simulaciones prácticas.
Aspecto Evaluado	**Evidencia / Observación**	**Nivel de Cumplimiento**	**Riesgo Asociado**	**Recomendación**
Cultura de cumplimiento	Acuerdos de confidencialidad firmados, pero baja concienciación en algunos niveles.	65%	Uso indebido de datos por falta de cultura.	Lanza campañas trimestrales con ejemplos de sanciones reales.

Elaborado por: Valencia y Villena (2025)

2. Evaluación de Riesgos

Tabla 2

Evaluación de Riesgos

Aspecto Evaluado	Evidencia / Observación	Nivel de Cumplimiento	Riesgo Asociado	Recomendación
Matriz de riesgos	Matriz actualizada anualmente, identifica retrasos en consentimientos y riesgos en móviles.	75%	Sanciones por in-cumplimiento de LOPDP.	Actualiza la matriz semestralmente con evaluación de nuevos riesgos.
Identificación de vulneraciones	Sistema de logs registra accesos, pero no detecta riesgos en dispositivos móviles.	70%	Fugas de datos por accesos no autorizados.	Implementa software MDM para dispositivos móviles en seis meses.
Evaluación de impacto (DPIA)	DPIA realizada, pero no incluye transferencias a terceros.	65%	Riesgo legal por transferencias sin protocolos.	Incluye análisis de terceros en la DPIA antes de 2026.

Elaborado por: Valencia y Villena (2025)

Tabla 3

Actividades de Control

3. Actividades de Control

Aspecto Evaluado	Evidencia / Observación	Nivel de Cumplimiento	Riesgo Asociado	Recomendación
Gestión de consentimientos	Consentimientos firmados, pero retrasos en actualizaciones detectados en auditoría.	60%	Incumpli del principio de consentimiento informado.	ıientoAutomatiza la verificación de consentimientos en el CRM.
Aspecto Evaluado	**Evidencia / Observación**	**Nivel de Cumplimiento**	**Riesgo Asociado**	**Recomendación**

Controles de acceso	CRM con accesos restringidos y logs de actividad.	85%	Riesgo en dispositivos móviles no protegidos.	Aplica autenticación multifactor en todos los dispositivos.
Seguridad tecnológica	Encriptación AES256 y SSL/TLS implementadas.	80%	Configuraciones débiles en algunos sistemas.	Realiza auditorías externas anuales para validar configuraciones.

Elaborado por: Valencia y Villena (2025)

4. Información y Comunicación

Tabla 4

Información y Comunicación

Aspecto Evaluado	Evidencia / Observación	Nivel de Cumplimiento	Riesgo Asociado	Recomendación
Canales de comunicación interna	Boletines internos y comités trimestrales existen, pero no todos los asesores los leen.	70%	Falta de concienciación por comunicación ineficaz.	Usa alertas digitales semanales para reforzar políticas.
Comunicación con Clientes	Formularios de consentimiento claros, pero explicaciones lentas afectan la experiencia.	65%	Insatisfaccion del cliente por procesos burocráticos.	iDiseña guiones de 30 segundos para explicar consentimientos.
Gestión de derechos ARCO	Canales para derechos ARCO existen, pero no son ampliamente conocidos.	60%	Reclamos por dificultad para ejercer derechos.	Publica un portal web para solicitudes ARCO antes de 2026.

Elaborado por: Valencia y Villena (2025)

5. Supervisión y Monitoreo

Tabla 5

Supervisión y Monitoreo

Aspecto Evaluado	Evidencia / Observación	Nivel de Cumplimiento	Riesgo Asociado	Recomendación
Auditorías internas	Auditorías internas semestrales detectan retrasos en consentimientos.	75%	Brechas no detectadas por auditorías poco frecuentes.	Realiza auditorías trimestrales con enfoque en consentimientos.
Monitoreo en tiempo real	Logs registran accesos, pero no hay tableros de control dinámicos.	60%	Retrasos en la detec-ción de incumplimientos.	Implementa un tablero de control en tiempo real en 2026.
Respuesta a incidentes	Protocolo de respuesta existe, pero no se simula con frecuencia.	65%	Respuesta lenta a vulneraciones de seguridad.	Simula incidentes trimestralmente para entrenar al equipo.

Elaborado por: Valencia y Villena (2025)

La empresa cuenta con fortalezas como encriptación robusta (AES-256, SSL/TLS), logs de acceso y políticas de confidencialidad, logrando un cumplimiento promedio del 70% con la LOPDP. Sin embargo, enfrentas debilidades críticas: retrasos en la actualización de consentimientos (60% de cumplimiento en actividades de control), riesgos en dispositivos móviles (70% en evaluación de riesgos) y baja concienciación en algunos niveles (65% en ambiente de control). La falta de un Delegado de Protección de Datos (DPD) y la gestión manual de procesos aumentan el riesgo de sanciones, que pueden alcanzar el 1% del volumen de negocio anual. La comunicación con clientes y la supervisión necesitan mejoras para garantizar agilidad y cumplimiento.

4.3 Checklist de cumplimiento - Ley Orgánica de Protección de Datos Personales (ECUADOR)

Checklist de cumplimiento LOPDP

1. Gobernanza y Responsabilidad

[ ] ¿La empresa ha designado un Responsable de Protección de Datos (DPO)?

Observación: No se ha designado un Delegado de Protección de Datos (DPD), incumpliendo el artículo 48 de la LOPDP.

[X] ¿Existe una política interna de protección de datos personales?

Observación: Existen políticas de confidencialidad y escritorio limpio, firmadas por el personal, según el Jefe del Área Comercial.

[X] ¿Se han asignado responsabilidades claras a cada área que trata datos personales?

Observación: Las áreas comercial, de sistemas y de control interno tienen roles definidos, según las entrevistas.

2. Principios de Tratamiento

[ ] ¿Se recolectan únicamente los datos necesarios para la finalidad declarada (principio de minimización)?

Observación: La retención indefinida de datos inactivos incumple el principio de minimización, según la DPIA.

[X] ¿Se informa al titular sobre la finalidad, plazo y responsable del tratamiento?

Observación: Los formularios de consentimiento informan la finalidad, pero no siempre el plazo, según el Jefe del Área Comercial.

[X] ¿Se respetan los principios de licitud, transparencia y lealtad?

Observación: La empresa aplica licitud y transparencia, pero la gestión manual de datos limita la consistencia, según el diagnóstico.

3. Consentimiento y Derechos del Titular

[X] ¿Se obtiene consentimiento explícito del titular antes de tratar datos?

Observación: Los clientes firman consentimientos físicos o digitales, pero hay retrasos en su actualización, según auditorías internas.

[X] ¿Se permite al titular ejercer sus derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)?

Observación: Existen canales para derechos ARCO, pero no son ampliamente conocidos, según el Encargado de Control Interno.

[ ] ¿Se documentan las solicitudes de los titulares y su atención dentro del plazo legal?

Observación: No hay evidencia de un registro sistemático de solicitudes ARCO, incumpliendo el artículo 19 de la LOPDP.

4. Medidas de Seguridad

[X] ¿Existen medidas técnicas y organizativas adecuadas para proteger los datos personales?

Observación: Se implementan encriptación AES-256, SSL/TLS, autenticación multifactor y logs, pero hay riesgos en dispositivos móviles, según el Encargado de Sistemas.

[X] ¿Se realizan pruebas de seguridad periódicas (auditorías, pruebas de penetración)?

Observación: Se realizan auditorías internas semestrales y externas anuales, según el Encargado de Sistemas.

[X] ¿Se ha documentado un protocolo para la gestión de incidentes de seguridad?

Observación: Existe un protocolo de respuesta a incidentes, pero no se simula con frecuencia, según el Encargado de Sistemas.

5. Relación con Terceros (Encargados)

[ ] ¿Existen contratos con encargados de tratamiento que incluyan cláusulas de protección de datos?

Observación: No hay contratos específicos con terceros, incumpliendo el artículo 36 de la LOPDP, según el Encargado de Control Interno.

[ ] ¿Se verifica que los proveedores cumplan con la LOPDP?

Observación: No se realizan auditorías de cumplimiento a proveedores, según el diagnóstico.

[ ] ¿Se lleva un registro actualizado de encargados y actividades delegadas?

Observación: No existe un registro formal de encargados, según la DPIA.

6. Registro y Evaluación de Riesgos

[X] ¿Se lleva un registro de actividades de tratamiento (art. 34 LOPDP)?

Observación: La matriz de riesgos identifica actividades de tratamiento, pero no está completamente documentada, según el Encargado de Control Interno.

[X] ¿Se realiza Evaluación de Impacto a la Privacidad (DPIA) cuando corresponde?

Observación: Se realizó una DPIA, pero omite transferencias a terceros, según el diagnóstico.

[X] ¿Se actualiza periódicamente la matriz de riesgos de tratamiento de datos?

Observación: La matriz se actualiza anualmente, pero se recomienda hacerlo semestralmente, según el diagnóstico.

EVALUACIÓNDEIMPACTOALAPRIVACIDAD(DPIA)

Tú realizas esta Evaluación de Impacto a la Privacidad (DPIA) para la empresa, una administradora de fondos en Ecuador, con el objetivo de identificar riesgos en el tratamiento de datos personales en el área comercial, evaluar la proporcionalidad y necesidad de los procesos, y proponer medidas para cumplir con la Ley Orgánica de Protección de Datos Personales (LOPDP). La DPIA se basa en entrevistas a tres

profesionales clave (Jefe del Área Comercial, Encargado de Sistemas, Encargado de Control Interno), revisión de políticas internas, auditorías y el diagnóstico de control interno. La empresa gestiona datos sensibles, como nombres, cédulas, direcciones, correos, teléfonos y datos financieros (saldos, historial de aportes), a través de un CRM. Esta evaluación es obligatoria debido al tratamiento masivo de datos sensibles, según el artículo 25 de la LOPDP.

Identificación y Evaluación de Riesgos

Tú identificas cuatro riesgos principales en el tratamiento de datos personales, basándote en las entrevistas, el checklist de cumplimiento y la matriz de riesgos del diagnóstico. La tabla siguiente detalla cada riesgo, su probabilidad, impacto, medidas actuales y observaciones.

Tabla 6

Matriz de Riesgos

Riesgo	Descripción	Probabilidad	Impacto	Medidas Actuales
Retrasos en consentimientos	Algunos asesores no actualizan los consentimientos a tiempo, detectado en auditorías internas.	70%	Alto (sanciones hasta 1% del volumen de negocio, pérdida de confianza).	Formularios físicos y digitales en el CRM, con verificación manual.
Accesos no autorizados en móviles	Los asesores acceden a datos desde móviles sin software de gestión.	50%	Alto (fugas de datos, sanciones, daño reputacional).	CRM con accesos restringidos y logs, sin controles para móviles.

Riesgo	Descripción	Probabilidad	Impacto	Medidas Actuales
Transferencias a terceros	La empresa comparte datos con proveedores sin contratos de confidencialidad.	60%	Alto (incumplimiento legal, uso indebido por terceros).	Ningún protocolo formal documentado.

Baja conci enciación	Algunos asesores desconocen la LOPDP debido a capacitaciones semestrales insuficientes.	60%	Medio (errores operativos, recla- mos de clientes).	Capacitaciones semestrales y acuerdos de confidencialidad al ingreso.

Elaborado por: Valencia y Villena (2025)

Observaciones: La gestión manual de consentimientos causa errores, incumpliendo el artículo 7 de la LOPDP. La falta de software MDM expone datos sensibles. La ausencia de contratos con terceros viola el artículo 36. La formación poco frecuente genera riesgos operativos.

Evaluación de Proporcionalidad y Necesidad

Tú evalúas si el tratamiento de datos en el área comercial cumple con los principios de finalidad, necesidad y proporcionalidad de la LOPDP (art. 7).

- Propósito del Tratamiento: La empresa recopila datos de clientes con la intención de ofrecer productos y servicios financieros, mantener relaciones con los clientes y cumplir con obligaciones legales. Este propósito es legítimo y se basa en el consentimiento y contratos de administración. Esto fue explicado por el Gerente Comercial del Área.

- Necesidad: La empresa ofrece productos y servicios recopilando nombres, números de identificación, direcciones, correos electrónicos, números de teléfono y datos financieros para personalizar ofertas y verificar la identidad del cliente. Sin embargo, mantener datos de usuarios inactivos por un período indefinido de tiempo no es necesario y viola el principio de minimización de datos como se señala en la Evaluación de Impacto y Riesgo de Protección de Datos (DPIA).

- Proporcionalidad: Se considera que el sistema CRM que emplea cifrado AES-256, SSL/TLS y acceso restringido es adecuado y proporcional al riesgo. Sin embargo, según el Oficial de Control Interno, el manejo manual de la gestión de consentimientos y la falta de protocolos definidos para el intercambio de datos con organizaciones de terceros introduce un riesgo indebido.

- Alternativas: Los riesgos asociados a tener el consentimiento verificado manualmente pueden ser mitigados automatizando el proceso de verificación de consentimientos, implementando software de Gestión de Dispositivos Móviles (MDM) y restringiendo la retención de datos a un máximo de cinco años. Todas estas opciones presentan menores riesgos y no impactan la funcionalidad de la organización. Estas opciones son viables según la opinión del Gerente de Sistemas.

El procesamiento de datos en el departamento comercial presenta riesgos serios, particularmente debido a retrasos en la obtención de consentimientos (70% de riesgo), acceso no autorizado a dispositivos móviles (50%), protocolos de transferencia de datos comerciales poco claros (60%) y falta de conocimiento del personal (60%).

Las medidas actuales, como el cifrado de datos, los registros de actividad y las auditorías internas, aseguran solo un 65% de cumplimiento con la Orgánica Ley de Protección de Datos Personales (LOPDP) basado en la lista de verificación de cumplimiento.

La ausencia de un Delegado de Protección de Datos (DPD), la gestión manual de los consentimientos y la falta de contratos con terceros incrementan el riesgo de sanciones legales (que podrían alcanzar hasta el 1% del volumen de negocio) y dañar la reputación de la empresa.

La retención indefinida de datos inactivos y la falta de canales claros para derechos ARCO agravan la vulnerabilidad.

Tabla 7

Matriz de acciones

Acción	Descripción	Responsable	Plazo	Indicador
Automatizar consentimientos	Configura alertas en el CRM para bloquear operaciones sin consentimientos actualizados.	Área de Sistemas	Junio 2026	100% de consentimientos actualizados.
Implementar MDM	Instala software MDM en móviles para cifrar datos y restringir accesos.	Área de Sistemas	Marzo 2026	100% de dispositivos protegidos.

Establecer contratos con terceros	Firma contratos de confidencialidad con auditorías anuales.	Área de Control Interno	Diciembre 2025	100% de terceros con contratos.
Capacitar al personal	Realiza capacitaciones mensuales con simulaciones de casos ARCO.	Área de Control Interno	Mensual desde enero 2026	90% de asistencia del personal.
Designar DPD	Contrata un DPD con experiencia en LOPDP.	Gerencia General	Diciembre 2025	DPD designado y registrado.
Limitar retención de datos	Elimina datos inactivos tras cinco años en el CRM.	Área de Sistemas	Junio 2026	0% de datos inactivos retenidos.

Elaborado por: Valencia y Villena (2025)

Estas medidas fortalecerán la protección de datos, reducirán riesgos legales y mejorarán la confianza de los clientes, alineándose con la LOPDP.

4.4 Propuesta integral de fortalecimiento del control interno en el área comercial para garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP)

Esta propuesta se diseña para cerrar brechas de cumplimiento y elevar el estándar de control interno en el área comercial, integrando gobierno, procesos, tecnología, cultura e indicadores bajo el principio de responsabilidad proactiva y con enfoque humano; se sustenta en los objetivos y resultados del diagnóstico, en las entrevistas y en el checklist de cumplimiento, y articula medidas que conectan las obligaciones de la LOPDP con la operación cotidiana, priorizando la experiencia del cliente, la trazabilidad y la mejora continua; el documento incluye un mapa de procesos, un registro de actividades de tratamiento, un esquema de gobierno con Delegado de Protección de Datos, un plan de gestión de consentimientos, un portal para los derechos ARCO, controles técnicos como MDM y MFA, un plan de gestión de incidentes, un programa de auditoría, un cronograma de implementación y un

tablero de KPIs que permitirán demostrar, de modo verificable, el cumplimiento normativo y la madurez del sistema.

4.4.1. Arquitectura de gobernanza y roles

Se establece un Comité de Privacidad y Cumplimiento Comercial presidido por Gerencia e integrado por el Delegado de Protección de Datos, Comercial, Sistemas, Control Interno y Asesoría Legal, con sesiones mensuales y extraordinarias ante incidentes; se adopta una matriz RACI donde Gerencia es responsable del programa, el DPD es responsable de la asesoría y supervisión, Comercial y Sistemas ejecutan controles operativos, Control Interno audita y Legal valida contratos con terceros; se formaliza la designación del DPD con independencia funcional, perfil documentado y acta de nombramiento, y se promueve la cultura de privacidad mediante comunicaciones internas, micromódulos mensuales y coaching en terreno.

4.4.2. Mapa de procesos y Registro de Actividades de Tratamiento (RAT)

Se levanta el flujo extremo a extremo del dato en captación, evaluación, oferta, contratación, posventa, campañas y reclamaciones, identificando titulares, categorías, finalidades, bases jurídicas, sistemas, encargados, destinatarios y plazos de conservación; se consolida un Registro de Actividades de Tratamiento con campos mínimos, se asocia cada actividad a riesgos y controles, y se alinea con la DPIA para que cualquier cambio relevante dispare revisión de riesgos y actualización de medidas.

Tabla 8

Campos mínimos sugeridos para el RAT

Proceso	**Finalidad**	**Base jurídica**	**Categorías de datos/titulares**	**Sistemas/Ubicación**	**Encargados/Destinatarios**	**Conservación**	**Riesgos/Controles**
Captación de leads	Contacto y oferta de productos	Consentimiento	Identificación y contacto; potencia	Web/CRM on-prem	Call center; email marketing	12 meses inactivos	Consentimiento; minimización; MDM/MFA

			les clientes				
Onboarding contractual	Formalización y verificación	Contrato; obligación legal	Identificación, financieros	Core + CRM	Proveedor validación identidad	Vigencia contractual + 5 años	Segregación de funciones; cifrado; backups

Elaborado por: Valencia y Villena (2025)

4.4.3. Gestión de consentimiento 360°

Propósito. Lograr que cada tratamiento comercial se apoye en un consentimiento libre, específico, informado e inequívoco, con evidencia verificable, vigencia controlada y uso estrictamente ligado a la finalidad declarada. La LOPDP exige estas condiciones y, además, pide seguridad "por diseño y por defecto", con análisis de riesgos y medidas organizativas y técnicas acordes (arts. 7, 8 y 39–41).

a) Información previa clara (antes del "sí")

- **Avisos por capas.** Una capa breve y humana ("¿Para qué usaremos tu correo?") y otra ampliada con finalidades, bases de licitud, plazos de conservación y canales ARCO. Menos jerga, más claridad.
- **Versionado de textos.** Cada aviso y cláusula tiene ID de versión y fecha de vigencia. Así, cuando alguien consiente, sabemos exactamente qué leyó y cuándo lo aceptó.
- **Ejemplo de redacción:** "Te pedimos tu correo solo para enviarte novedades del producto X. Puedes darte de baja en cualquier momento. No lo compartiremos con terceros sin tu permiso." (alineado a licitud, minimización y transparencia).

b) Captura multicanal con evidencia

- **Canales admitidos:** web y app (doble opt-in), presencial en tablet, call center (grabación + transcripción) y mensajería corporativa registrada. como objeto auditable en

- **Granularidad por finalidad.** Se solicitan consentimientos separados para marketing, profiling, cesión a terceros y comunicaciones comerciales. Nada de "todo incluido" por defecto.
- **Evidencia probatoria:**
    - **Hash** de la aceptación (p. ej., SHA-256 del payload),
    - **Marca de tiempo** confiable,
    - **Usuario/asesor** y **origen** (IP, deviceID),
    - **Prueba de doble opt-in** cuando aplique (token de confirmación). Todo se guarda el CRM/MA: titular, finalidad, versión informativa, base legal, evidencia, timestamp y estado (vigente/expirado/revocado).

c) Renovación automatizada y caducidad

- **Política de vigencia.** Define plazos por finalidad (p. ej., 24 meses para marketing sin interacción). El sistema notifica T-30/T-7; si no hay respuesta, expira y dispara supresión o anonimización según el calendario de conservación. La revocación debe ser tan fácil como consentir (botón de baja).
- **Gobierno de finalidades.** Un **catálogo corporativo** define para qué sirve cada consentimiento y qué usos "compatibles" caben sin pedir otro. Si la finalidad cambia de manera sustantiva, se recolecta uno nuevo.

d) Bloqueo de campañas ante vencimiento (consent gate)

- **Regla dura:** si consent.estado != vigente → no-enviar. Se valida en CRM/MA y también al exportar listas (se registra quién exporta, cuándo y para qué).
- **Pruebas de control.** Antes de cada campaña, una seed list verifica que el motor de audiencias excluye consentimientos vencidos o revocados. Control Interno revisa muestras y deja rastro en la bitácora.

e) Guiones para asesores (30–45 segundos)

- **Script sugerido:** “Con tu permiso, registraremos tu correo para enviarte información del producto Ahorro+. Solo la usaremos para eso. Podrás darte de baja en un clic. ¿Te parece bien?”
- **Micro-capacitaciones mensuales.** Objeciones frecuentes (“no quiero spam”, “¿qué pasa con mis datos?”) y role-play para ganar naturalidad.

f) Indicadores y tablero por canal/segmento

- **Consentimientos vigentes (campañas activas):** ≥ **98 %**.
- **Consentimientos expirados:** ≤ **1 %**.
- **Tiempo medio de renovación:** ≤ **3 días**.
- **Revocaciones atendidas:** < **24 h**.
- **Hallazgos críticos en auditoría de consentimientos:** 0. Estos KPIs se muestran por canal (web, app, call center, presencial) y segmento (prospectos/clientes), con alertas automáticas a DPD y Comité de Privacidad.

Resultado esperado. Campañas más limpias, rastros sólidos ante auditoría y, sobre todo, confianza: cuando la persona entiende y controla su consentimiento, participa sin reservas. (LOPDP; ISO/IEC 27701).

4.4.4. Derechos de titulares y portal ARCO

Propósito. Habilitar un portal unificado para recibir, autenticar, gestionar y cerrar solicitudes de Acceso, Rectificación, Eliminación, Oposición, Portabilidad y Suspensión, con SLA internos más exigentes que los legales, bitácora única y respuestas modelo consistentes. Así se cumple con la LOPDP y se materializa la responsabilidad proactiva con evidencias.

a) Autenticación y canales

- **Autenticación proporcional al riesgo.**
    - Acceso/Portabilidad → validación reforzada (documento + OTP).

- Rectificación/Eliminación → verificación de identidad + evidencia del dato correcto.

- **Omnicanal.** Web/app (preferente), presencial y call center; todos alimentan **el mismo workflow** y la **misma bitácora**.
- **Accesibilidad real.** Lenguaje llano, ayudas contextuales ("¿Qué derecho necesito?"), soporte móvil y trazabilidad visible para el titular.

b) Flujo operativo (de punta a punta)

1. **Radicación** (ticket único): derecho invocado, identidad verificada, alcance, adjuntos, **timestamp**.
2. **Clasificación** automática por reglas:
   - Rectificación → solicitar evidencia y proponer campos editables.
   - Portabilidad → preparar **exportación segura** y formato interoperable.
3. **Enrutamiento RACI**: Comercial (datos de cliente), Sistemas (extracciones/logs), Legal/DPD (criterios y excepciones).
4. **Respuesta** con **plantillas modelo**: tono empático, base legal citada, aclaración de alcances y límites.
5. **Cierre** con confirmación al titular y **encuesta de satisfacción**.
6. **Bitácora central**: cada paso queda registrado (usuario, acción, fecha, evidencia). Lista para auditoría.

c) SLA internos y control de plazos

- **Objetivo interno:** cerrar solicitudes en **≤ 10 días** naturales (más exigente que la práctica de 15 días mencionada en la literatura). Alertas T-5, T-2 y T-0 con **escalamiento** automático a DPD.
- **Calidad de respuesta.** Checklist de completitud (datos, base legal, anexos), tono y confirmación de cierre en sistemas fuente (CRM/ERP/DMS).

d) Respuestas modelo (plantillas vivas)

- **Acceso.** Categorías de datos, finalidades, bases de licitud, fuentes, destinatarios, plazos de conservación y copia de datos en formato legible.
- **Rectificación.** Aceptación/denegación motivada y **prueba** de actualización en origen.
- **Eliminación.** Qué se suprime/anonimiza, qué se conserva por obligación legal y por cuánto tiempo.
- **Oposición.** Evaluación de interés legítimo y alternativas (limitación del tratamiento).
- **Portabilidad.** Entrega segura (enlace con token y ventana de tiempo).
- **Suspensión.** Congelamiento temporal del tratamiento hasta resolver disputa. Las plantillas se revisan trimestralmente por DPD/Legal para mantener consistencia y apego a la norma.

e) Simulacros y mejora continua

- **Table-top mensual.** Casos mixtos (p. ej., “rectificación + portabilidad simultáneas”) para medir tiempos y detectar cuellos de botella.
- **Auditoría interna trimestral.** Muestreo de expedientes ARCO, verificación de evidencias y **cierres de hallazgos** en ≤ 30 días.
- **Retroalimentación** al Comité de Privacidad y actualización de POE.

f) Integraciones y seguridad

- **Actualización en origen.** El portal ARCO **escribe** en los sistemas maestros (single source of truth), evitando desalineaciones.
- **Seguridad.** Cifrado en tránsito y reposo, **MFA** para operadores, registros **inmutables** (WORM) y segregación de funciones.
- **Retención de expedientes ARCO.** Plazo proporcional, alineado al calendario de conservación y a la trazabilidad exigida por la autoridad.

g) Indicadores clave

- **ARCO a tiempo: ≥ 95 %**.
- **Tiempo medio de resolución: ≤ 10 días**.
- **Satisfacción del titular: ≥ 90 %**.
- **Reaperturas: ≤ 3 %**.
- **Incidentes por gestión ARCO: 0**.

  Se visualizan en un tablero unificado y se reportan al Comité y al DPD para decisiones informadas.

Impacto esperado. Menos riesgo regulatorio, menos fricción con clientes y —sobre todo— más confianza. Un portal que escucha, responde y demuestra, en papel y en práctica, que la organización toma en serio los derechos de las personas.

4.4.5. Seguridad por diseño y por defecto

La seguridad no es un candado al final del camino; es el plano de la casa. Diseñar y configurar por defecto con criterios de privacidad y control reduce fricciones, evita sustos y, sobre todo, te deja evidencia sólida para demostrar cumplimiento. La LOPDP lo exige (art. 39–41) y los marcos ISO/IEC lo vuelven operable con procedimientos repetibles. La verdad es que, si se piensa tarde, se paga caro; por eso aquí se refuerza la defensa en profundidad con controles técnicos y organizativos que conviven con el día a día comercial. (Asamblea Nacional del Ecuador, 2021; ISO/IEC, 2022; ISO/IEC, 2019).

a) Principios operativos (cómo se ve "por diseño y por defecto")

- **Minimización desde el inicio:** solo se solicitan y almacenan los datos indispensables para la finalidad declarada; cualquier campo "de relleno" se elimina del formulario y del CRM.
- **Configuraciones seguras por defecto:** cifrado activado, exportaciones restringidas, alertas prendidas, perfiles con privilegio mínimo y registros (logs) siempre encendidos.

- **Trazabilidad obligatoria:** todo acceso, exportación o cambio relevante deja rastro con **usuario, fecha/hora y contexto**.
- **Ciclo de vida del dato** mapeado: creación → uso → transferencia → conservación → supresión/anonimización con evidencia.
  Estas reglas aterrizan el art. 39 de la LOPDP y se integran al SGSI/PIMS (ISO/IEC 27001/27701).

b) Controles técnicos prioritarios (lo imprescindible que debe estar prendido)

1. **MDM en dispositivos** (100 % del parque comercial): cifrado forzado, bloqueo automático, borrado remoto, listas blancas de apps y verificación de parches. Si el dispositivo no cumple, no entra.
2. **MFA en accesos** (al menos para todo acceso remoto y cuentas privilegiadas): sin segundo factor, no hay sesión.
3. **Cifrado robusto**: **en tránsito** (TLS moderno) y **en reposo** (AES-256 o equivalente) para bases, respaldos y exportaciones temporales.
4. **Registro inmutable**: bitácoras WORM o mecanismos equivalentes para accesos y **todas** las exportaciones del CRM.
5. **EDR/antimalware** con monitoreo centralizado y respuesta ante incidentes.
6. **Segmentación y firewall/IPS** entre servicios críticos (CRM, DWH, correo, almacenamiento).
7. **Gestión de secretos** (rotación de llaves/API, bóvedas seguras) y **KMS** con rotación periódica.
8. **DLP** en correo y puntos de salida para evitar fugas accidentales (o maliciosas).
   Estos controles anclan la defensa en capas y se auditan de forma periódica. (ISO/IEC, 2022; Imbaquingo et al., 2020).

c) Segregación de funciones en el CRM (SoD que se siente)

- **Roles diferenciados:** *asesor comercial* (consulta/actualización mínima), *supervisor* (revisión), *marketing* (campañas sin ver datos sensibles), *control interno* (auditoría de logs), *TI* (configuración), *DPD* (supervisión).
- **Exportaciones con freno de mano:** solo perfiles autorizados, con **justificación obligatoria**, **aprobación** y **registro inmutable**.
- **Gates de cumplimiento:** si **no hay consentimiento vigente** o el dato está "caducado", el propio CRM **bloquea** campañas y descargas masivas. Esto evita tratamientos acéfalos o incompatibles, y facilita demostrar responsabilidad proactiva. (Asamblea Nacional del Ecuador, 2021).

d) Monitoreo y revisión semanal de eventos relevantes

- **Qué se revisa:** intentos fallidos de autenticación, accesos fuera de horario, exportaciones inusuales, cambios masivos en consentimientos, creaciones de usuarios, y actividad en dispositivos móviles no conformes.
- **Cómo se revisa:** tablero SIEM (o equivalente) con **reglas de correlación** y **alertas** al equipo de Seguridad/DPD; bitácora de revisiones firmada.
- **Qué se conserva:** logs de aplicación, sistema y red, con retención proporcional al riesgo y a obligaciones internas. Además de cumplir, esto **acorta tiempos de detección** y mejora la respuesta. (Lucero, 2023).

e) Continuidad del negocio: RTO/RPO que importan

- **RTO (tiempo objetivo de recuperación)** y **RPO (punto objetivo de recuperación)** definidos por proceso (p. ej., CRM crítico: RTO ≤ 8 h, RPO ≤ 1 h).
- **Regla 3-2-1** para respaldos: tres copias, dos medios, una **off-site** y, cuando aplique, offline.
- **Pruebas semestrales**: *table-top* + restauración real de una base crítica y simulacro de indisponibilidad parcial.

- **Evidencia**: actas, capturas, reportes de tiempos y acciones correctivas. Este “seguro de vida” técnico enlaza con el plan de continuidad y el art. 41 (medidas proporcionales al riesgo). (Presidencia de la República del Ecuador, 2023; ISO/IEC, 2022).

f) Gestión de configuraciones y cambios (lo que se documenta se defiende)

- **Base de configuración**: plantillas endurecidas (hardening) para servidores, CRM, bases y endpoints; **infraestructura como código** cuando sea posible.
- **Cambios con trazabilidad**: ticket, análisis de riesgo, aprobación, ventana, *rollback* y evidencia de resultados.
- **Parches**: críticos ≤ 7 días; altos ≤ 15 días; verificación posterior.
- **Vulnerabilidades**: escaneos periódicos y *pen tests* anuales con cierre de hallazgos.
- **Inventario vivo** de activos, certificados y dependencias. Todo esto convierte “seguridad” en prácticas medibles y auditables. (ISO/IEC, 2022; COSO, 2013).

g) KPIs/KRIs (para pilotear con datos, no con intuiciones)

- **Cobertura MDM** = **100 %** de dispositivos comerciales.
- **Cobertura MFA** = **100 %** remotos y privilegiados.
- **Cifrado en reposo** = **100 %** de bases y respaldos críticos.
- **Integridad de logs** (sin huecos) ≥ **99,9 %**.
- **Backups exitosos** ≥ **99 %** y **restauraciones probadas** en < **4 h** para CRM.
- **Parches críticos** dentro de SLA ≥ **95 %**.
- **Segregación efectiva** (intentos de exportación no autorizada) = **0**.

- **Incidentes críticos** = **0**; si ocurren, **notificación** y **cierre** en plazo. Estos indicadores se reportan al Comité y al DPD, con planes de acción cuando se enciende una alerta. (VisualCom Publications, 2023; PwC Ecuador, 2023).

h) Ejemplo práctico (cómo se ve en una semana corriente)

Una campaña de “Ahorro Plus” se alista en el CRM. El motor de audiencias excluye de forma automática a quien tenga consentimiento expirado. Marketing intenta exportar una lista; el sistema pide justificación, envía la solicitud a aprobación y registra el evento en el log inmutable. En paralelo, el SIEM detecta varios accesos fallidos fuera de horario: alerta al analista, bloqueo preventivo y verificación. El viernes, el equipo ejecuta el restauro de prueba de una base y documenta el tiempo de recuperación. Nada épico, pero así se construye confianza: con rutina y evidencia. (Diagnóstico y propuesta de la tesis; ISO/IEC, 2022).

Resultado esperado. Un entorno donde las decisiones técnicas respaldan la ley y los procesos comerciales fluyen con seguridad: menos superficie de ataque, menos errores humanos, menos sobresaltos regulatorios y más trazabilidad para auditorías internas y externas. En otras palabras, seguridad que no frena… sino que da permiso para crecer con cabeza. (Asamblea Nacional del Ecuador, 2021; ISO/IEC, 2019; ISO/IEC, 2022).

4.4.6. Gestión de terceros y transferencias

Se establece un registro de encargados y destinatarios, se suscriben contratos de encargo con instrucciones, confidencialidad, medidas de seguridad, subencargos, auditorías y finalización con supresión o devolución, y se gestionan transferencias internacionales o interorganizacionales con cláusulas adecuadas y registro de destinos, reforzando la conformidad legal y la trazabilidad.

4.4.7. Evaluación de Impacto (DPIA) y gestión de riesgos

Se consolida una DPIA viva que incorpora transferencias a terceros, observación sistemática cuando corresponda y escenarios de alto riesgo; se aplica una metodología de valoración por probabilidad e impacto, se construye un mapa de

calor y se ejecutan planes de tratamiento con responsables y plazos, con revisión semestral o al cambio significativo del tratamiento.

Tabla 9

Matriz de riesgos priorizados:

Riesgo	Descripción	Probabilidad	Impacto	Medidas actuales	Medidas propuestas
Retrasos en consentimientos	Actualización tardía o no verificada de consentimientos para campañas y operaciones	70%	90%	Consentimientos físicos/digitales con verificación manual en CRM	Automatizar verificación y bloqueo de operaciones; alertas en CRM; recolección multicanal con evidencia
Accesos no autorizados en móviles	Acceso a datos desde dispositivos sin MDM ni cifrado forzado	50%	90%	Acceso segmentado y logs; sin controles específicos en móviles	Implementar MDM; MFA obligatorio; borrado remoto; listas blancas de apps
Transferencias a terceros sin contrato	Cesiones de datos sin contratos de encargo ni auditorías de cumplimiento	60%	90%	Relaciones operativas sin contrato PD	Contratos de encargo; verificación anual; cláusulas de transferencia; registro de destinatarios
Baja concienciación del personal	Conocimiento insuficiente de LOPDP y procedimientos; errores operativos	60%	60%	Capacitaciones semestrales y acuerdos de confidencialidad	Micro-módulos mensuales; simulaciones; coaching; mystery compliance

Elaborado por: Valencia y Villena (2025)

4.4.8. Calendario de conservación y minimización

Se define un calendario por finalidad que fija plazos de retención, reglas de inactividad y borrado seguro; se habilita supresión o anonimización con bitácora y se alinea con las renovaciones de consentimiento y con obligaciones legales, previniendo retenciones indebidas y reduciendo exposición.

4.4.9. Monitoreo e indicadores (KPI/KRI)

Se construye un tablero con vistas por rol que contiene indicadores de consentimientos, derechos ARCO, seguridad, terceros, cultura y auditorías; se definen metas y frecuencia, se asignan fuentes de datos y se integran alertas para activar acciones correctivas tempranas.

Tabla 10

Indicadores

KPI	Definición	Meta	Fuente	Frecuencia
Consentimientos vigentes	Proporción de consentimientos válidos sobre universo de campañas activas	≥98%	CRM / Tablero	Mensual
Consentimientos expirados	Consentimientos vencidos respecto del total aplicable	≤1%	CRM / Tablero	Mensual
Tiempo medio ARCO	Promedio de días naturales por solicitud resuelta	≤10 días	Portal ARCO	Mensual
ARCO a tiempo	Porcentaje de solicitudes respondidas dentro del plazo máximo	≥95%	Portal ARCO	Mensual
Cobertura MDM	Dispositivos comerciales con MDM habilitado	100%	Consola MDM	Mensual
Cobertura MFA	Cuentas con MFA aplicado en accesos remotos y privilegiados	100%	IAM / SIEM	Mensual
Incidentes críticos	Número de incidentes de seguridad clasificados como críticos	0	Gestión de incidentes	Mensual
Contratos con terceros	Proveedores críticos con contrato de encargo y verificación anual	100%	Repositorio contratos	Trimestral
Capacitación efectiva	Porcentaje de colaboradores con evaluación ≥80/100	≥90%	LMS / Evaluaciones	Trimestral

Elaborado por: Valencia y Villena (2025)

4.4.10. Plan de acción y cronograma

El plan se organiza en tres fases con hitos definidos y responsables claros, integrando acciones de gobierno, tecnología, procesos y cultura; cada acción cuenta con un indicador verificable y una fecha objetivo, permitiendo seguimiento y toma de decisiones basada en evidencia.

Tabla 11

Cronograma

Acción	Descripción	Responsable	Plazo	Indicador
Designar DPD	Nombramiento formal con perfil, funciones e independencia; acta y registro	Gerencia General	Dic 2025	DPD designado y registrado
Automatizar consentimiento	Alertas y bloqueo en CRM; renovación y caducidad; evidencias de consentimiento	Área de Sistemas	Jun 2026	100% consentimientos vigentes en campañas
Implementar MDM	Cifrado forzado; borrado remoto; listas blancas; compliance de parches	Área de Sistemas	Mar 2026	100% dispositivos protegidos
Contratos con terceros	Acuerdos de encargo; auditorías; cláusulas de transferencia	Control Interno / Legal	Dic 2025	100% terceros críticos con contrato y verificación
Portal ARCO	Plataforma de recepción y seguimiento de solicitudes; autenticación adecuada; SLA	Área de Sistemas	Jun 2026	≥95% satisfacción; ≤10 días respuesta media
Tablero de cumplimiento	KPIs en tiempo real; alertas; vistas por rol; bitácora	Área de Sistemas / DPD	Mar 2026	Tablero v1 operativo; alertas activas
Auditorías trimestrales	Foco en consentimientos, accesos, terceros; cierre de hallazgos	Control Interno	Desde 2026	Cierre de hallazgos críticos ≤30 días
Revisión DPIA	Actualización semestral; inclusión de terceros y observación sistemática	DPD / Comité	Semestral	DPIA vigente con plan de tratamiento en ejecución
Calendario de conservación	Reglas por finalidad; supresión/anonimización; evidencia	DPD / Sistemas	Fase 1-2	0% retención indebida de inactivos

Elaborado por: Valencia y Villena (2025)

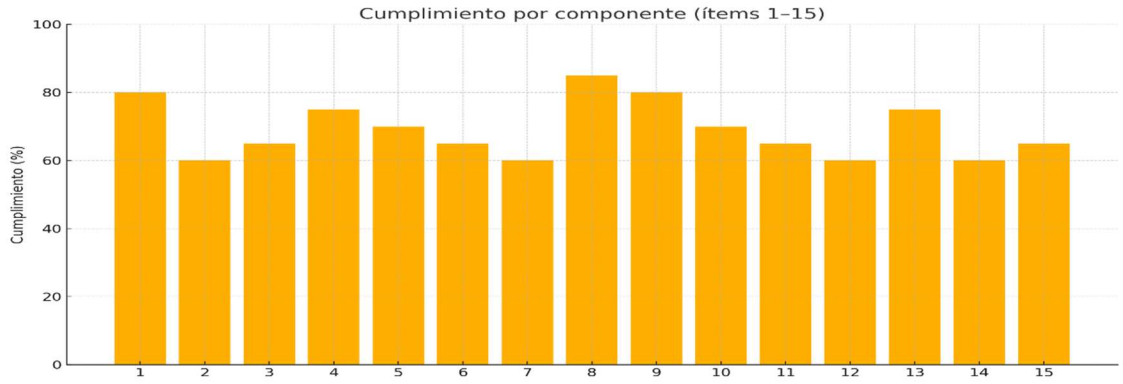
4.4.11. Auditoría y mejora continua

Control Interno realizará auditorías trimestrales focalizadas y una firma externa ejecutará pruebas anuales de configuración y penetración, con registro de evidencias, planes de acción y cierre de hallazgos en plazos definidos; se implementa un ciclo PDCA con retrospectivas posteriores a incidentes y auditorías, consolidando una cultura de aprendizaje continuo.

4.4.12. Gráficos de soporte

Figura 1

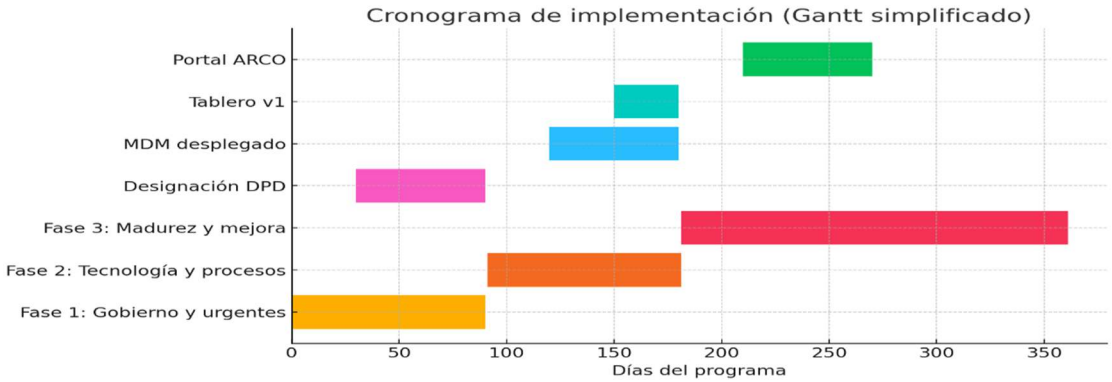
Cumplimiento por componente (ítems 1–15).



Elaborado por: Valencia y Villena (2025)

Figura 2.

Cronograma de implementación (Gantt simplificado).



Elaborado por: Valencia y Villena (2025)

CONCLUSIONES

El análisis integral del control interno en el área comercial evidencia que, si bien existe un marco de políticas, protocolos y medidas técnicas —como cifrado robusto, registro de accesos y roles definidos— que aportan a un 70 % de cumplimiento con la LOPDP, persisten debilidades críticas en la actualización de consentimientos, la seguridad en dispositivos móviles, la formalización de contratos con terceros y la divulgación de canales para derechos ARCO; dichas brechas, sumadas a la ausencia de un Delegado de Protección de Datos Personales (DPD), generan un riesgo real de sanciones legales y pérdida de confianza del cliente.

El examen de los fundamentos normativos y teóricos confirma que la LOPDP y la Constitución imponen obligaciones específicas al área comercial que solo se cumplen de manera parcial; aunque se han implementado principios como licitud, transparencia y confidencialidad, la gestión manual de consentimientos, la retención indefinida de datos inactivos y la falta de protocolos para transferencias a terceros contradicen los principios de minimización, finalidad y responsabilidad proactiva.

El diagnóstico interno revela que, pese a las fortalezas en seguridad tecnológica y control de accesos, las auditorías detectan hallazgos recurrentes en consentimientos desactualizados y deficiencias en la capacitación del personal; además, el sistema actual carece de mecanismos automatizados para verificar cumplimientos, monitorear riesgos en tiempo real y simular incidentes con la frecuencia necesaria.

La propuesta formulada —basada en un plan en tres fases— es viable, coherente y suficiente para cerrar las brechas detectadas; contempla la designación del DPD, la automatización de consentimientos, la implementación de MDM y MFA, el desarrollo de un portal ARCO, el establecimiento de contratos con terceros y la instalación de un tablero de indicadores, priorizando la experiencia del cliente y la evidencia documentada del cumplimiento.

RECOMENDACIONES

Implementar de manera inmediata la estructura de gobernanza propuesta, con la creación del Comité de Privacidad y la designación del DPD antes de diciembre de 2025; asignar presupuesto y recursos para ejecutar el plan de acción completo, y establecer revisiones mensuales con base en un tablero de indicadores que integre métricas de cumplimiento legal, satisfacción del cliente y gestión de riesgos.

Actualizar el corpus documental para alinearlo plenamente con la LOPDP y su Reglamento: políticas de privacidad y consentimiento con finalidades granulares y plazos claros, registro formal de actividades de tratamiento, protocolos de transferencia de datos y de notificación de incidentes; incorporar controles técnicos que bloqueen cualquier operación sin consentimiento válido y limitar la retención de datos inactivos a un periodo máximo de cinco años.

Automatizar la verificación de consentimientos y la detección de riesgos en dispositivos móviles mediante software MDM; implementar alertas en el CRM para bloquear operaciones fuera de norma; fortalecer la cultura de cumplimiento con capacitaciones mensuales, simulaciones de casos reales y campañas internas; establecer auditorías trimestrales con foco en consentimientos, ARCO y accesos privilegiados, incluyendo simulacros de incidentes.

Ejecutar la propuesta en tres fases sin aplazamientos: Fase 1: Gobierno y urgencias (DPD, RAT inicial, política de consentimientos, calendario de conservación, plan de capacitación). Fase 2: Tecnología y procesos (MDM, MFA, tablero v1, contratos con terceros, DPIA actualizada). Fase 3: Madurez (portal ARCO, tablero v2 con analítica, auditorías trimestrales, revisión semestral de la DPIA). Asegurar que cada acción tenga un responsable, un plazo definido y un indicador verificable.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, M. (2023). Aplicación de la Ley Orgánica de Protección de Datos Personales en el sistema empresarial ecuatoriano. *Revista Jurídica Ecuador*, 15(2), 45–62. https://doi.org/10.32719/ejuridica.2023.15

Alvear, M., et al. (2024). Gestión de riesgos y control de accesos en organizaciones sociales. *Revista de Seguridad Informática y Sociedad*, 2(1), 14–28.

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento N.º 459. https://www.registrooficial.gob.ec

Asamblea nacional del la republica del Ecuador. (2021). *Ley organica de proteccion de datos personales.* Quito, 21 de mayo de 2021: Registro Oficial Suplemento 459. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Barzola Torres, P., & Zambrano Ormaza, A. (2021). Control interno y liquidez en empresas comerciales: Caso Barzam S.A. *Revista Contaduría y Auditoría*, 5(2), 110–125.

Chuquizuta Vera, K. R., & Oncoy Cordova, M. A. (2017). INCIDENCIA DEL SISTEMA DE CONTROL INTERNO EN LAS CUENTAS POR COBRAR DE LA UBICADA EN EL DISTRITO DE LOS OLIVOS, AÑO 2013. *[Tesis de pregrado]*. Lima : Universidad de Ciencias y Humanidades .

Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO). (2013). *Marco Integrado de Control Interno*. COSO.

Cumbicos, L., et al. (2023). Control interno como herramienta de mitigación de riesgos operativos y financieros. *Revista de Administración Empresarial*, 10(3), 201–219.

García Guerra , J. I. (09 de Diciembre de 2024). Revisión crítica a los riesgos financieros y productos estructurados en Ecuador. *[Revista cientifica], Vol. 10 (2)*, pp. 89 - 99 . doi:http://doi.org/10.48190/cumbres.v10n2a6

Gaspar Barrios , D. A. (Junio de 2024). Educación financiera en jovenes de educación superior. *[Revista cientifica], Vol. 20 (1)*, pp. 37 - 50 . doi:http://doi.org/10.18004/riics.2024.junio.37

Hernández, N. B., & Vázquez, M. Y. L. (2023). Análisis comparado de la Ley de Protección de Datos Personales de Ecuador y España. *Revista Iberoamericana de Derecho Comparado*, 5(2), 89–112.

Inforc. (2024). Implementación de ISO 27701 en empresas ecuatorianas: Retos y beneficios. *Informe Técnico Inforc*, 12(1), 1–15.

ISO/IEC. (2019). *ISO/IEC 27701:2019 — Extensión de la ISO/IEC 27001 para la gestión de la privacidad*. International Organization for Standardization.

ISO/IEC. (2022). *ISO/IEC 27001:2022 — Sistemas de gestión de seguridad de la información*. International Organization for Standardization.

Lucero, L. (01 de Julio de 2023). El rol de la auditoría informática en la era de la protección de datos personales en Ecuador. *[Revista cientifica], Vol. 2(2)*, pp. 1 - 14. doi:https://doi.org/10.55204/trj.v2i2.e17

Mendoza-Zamora, J., et al. (2018). Control interno y gestión de riesgos en el sector financiero ecuatoriano. *Revista de Ciencias Financieras*, 6(1), 87–104.

Miguel Perez, J. C. (2015). *Proteccion de datos y seguridad de la informacion .* RA-MA,S.A.Editorial y Publicaciones .

Miño-Castillo, A. C. (15 de Marzo de 2025). La inteligencia artificial y los efectos en la productividad de las empresas privadas del cantón de latacunga en el año 2024. Caso de estudio sector financiero. *[Revista cientifica], 9(1)*. doi:http://doi.org/10.56048/MQR20225.9.1.2025.e101

Nazarova, H. (Diciembre de 2023). La auditoría de estados financieros como componentes de la seguridad econónomica y financiera de una empresa bajo la ley marcial: enfoques y analisis. *[Revista cientifica]*.

Nevardo, P. (2020). Situación de la protección de datos personales en Ecuador. *Revista Latinoamericana de Derecho y Tecnología*, 8(1), 101–119.

Patrón Mera, M., et al. (2024). Gestión de cuentas por cobrar y control interno en juntas de agua potable. *Revista de Gestión Pública Local*, 4(1), 22–35.

Presidencia de la República del Ecuador. (2023). *Decreto Ejecutivo N.º 904. Reglamento General a la Ley Orgánica de Protección de Datos Personales*. Registro Oficial, Tercer Suplemento N.º 435. https://www.registrooficial.gob.ec

PwC Ecuador. (2023). *Guía de cumplimiento para la Ley Orgánica de Protección de Datos Personales en Ecuador*. PwC.

Rivas Macías, A. I. (2022). Control interno en empresas comerciales nacientes en Ecuador. *Revista de Negocios y Gestión*, 7(3), 55–70.

Sevilla Moncayo, A. E. (2023). Impacto de la LOPDP en el control interno y fiscalización de las compañías privadas ecuatorianas. *Revista de Administración y Derecho*, 12(1), 33–49.

Superintendencia de Protección de Datos Personales. (2025). *Resolución SPDP-SPD-2025-0004: Requisitos para Delegados de Protección de Datos*. Quito, Ecuador.

VisualCom Publications. (2023). *Buenas prácticas empresariales en la implementación de la LOPDP*. VisualCom.

ANEXOS

4.5 Anexo A. Diagnóstico de cumplimiento por componente

Ítem	Componente / Aspecto	Cumplimiento (%)	Observación breve
1	Ambiente de control - Políticas de protección de datos	80	Fortaleza
2	Ambiente de control - Capacitación del personal	60	Atención prioritaria
3	Ambiente de control - Cultura de cumplimiento	65	Atención prioritaria
4	Evaluación de riesgos - Matriz de riesgos	75	Mejora necesaria
5	Evaluación de riesgos - Identificación de vulneraciones	70	Mejora necesaria
6	Evaluación de riesgos - DPIA	65	Atención prioritaria
7	Actividades de control - Gestión de consentimientos	60	Atención prioritaria
8	Actividades de control - Controles de acceso	85	Fortaleza
9	Actividades de control - Seguridad tecnológica	80	Fortaleza
10	Información y comunicación - Canales internos	70	Mejora necesaria

11	Información y comunicación - Comunicación con clientes	65	Atención prioritaria
12	Información y comunicación - Gestión de derechos ARCO	60	Atención prioritaria
13	Supervisión y monitoreo - Auditorías internas	75	Mejora necesaria
14	Supervisión y monitoreo - Monitoreo en tiempo real	60	Atención prioritaria
15	Supervisión y monitoreo - Respuesta a incidentes	65	Atención prioritaria