

UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

DISEÑO DE UN SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA.

PPROYECTO DE INVESTIGACION PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

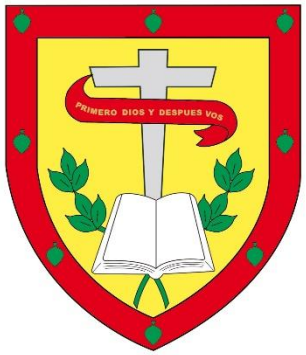
AUTOR: HENDRY ALFREDO SANCHEZ PAUCAR

DIRECTOR: CRISTINA MARIUXI FLORES URGILES

CAÑAR - ECUADOR

2026

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA}

CARRERA DE INGENIERIA EN SISTEMAS DE LA INFORMACIÓN

DISEÑO DE UN SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA.

PROYECTO DE INVESTIGACION PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

AUTOR: HENDRY ALFREDO SANCHEZ PAUCAR

DIRECTOR: CRISTINA MARIUXI FLORES URGILES

CAÑAR - ECUADOR

2026

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUDITORÍA Y RESPONSABILIDAD

Declaratoria de auditoría y responsabilidad **HENDRY ALFREDO SANCHEZ PAUCAR** portador de la cedula de ciudadanía N° 0350337853. Declaro ser el autor de la obra: **"DISEÑO DE UN SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA"** sobre la cual me hago responsable de las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.



HENDRY ALFREDO SANCHEZ PAUCAR

C.I. 0350337853

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el est. HENDRY ALFREDO SANCHEZ PAUCAR, bajo mi supervisión.



Ing. Cristina Flores Urgiles

DIRECTOR DEL TRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA EXTENSIÓN CAÑAR

DEDICATORIA

Dedico este trabajo de titulación, en primer lugar, a Dios, por ser mi guía y fortaleza en cada etapa de mi vida, por brindarme salud, sabiduría y perseverancia para superar los obstáculos que se presentaron durante este camino y permitirme alcanzar una de las metas más importantes de mi vida.

A mis padres, por su amor incondicional, sus sacrificios y su apoyo constante. Gracias por enseñarme el valor del esfuerzo, la responsabilidad y la perseverancia; por creer en mí incluso en los momentos difíciles y por ser el pilar fundamental que me ha impulsado a seguir adelante hasta cumplir este sueño. Este logro también es de ustedes, pues detrás de cada paso hay un sacrificio y una enseñanza que llevaré siempre en mi corazón.

A mis hermanas, por su cariño, compañía y palabras de aliento, por estar presentes en mi vida y motivarme a ser mejor cada día. Gracias por brindarme su apoyo y por compartir conmigo la alegría de alcanzar esta meta tan importante.

Finalmente, dedico este logro a mi familia, por ser mi mayor inspiración y mi motivo para no rendirme. Este triunfo representa no solo la culminación de una etapa académica, sino también el resultado del amor, la fe y el apoyo de quienes han estado a mi lado a lo largo de este camino.

Con todo mi amor y gratitud, les dedico este logro.

AGRADECIMIENTO

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por estar siempre presentes.

A la Universidad Católica de Cuenca, Extensión Cañar, y de manera particular a la Carrera de Ingeniería de Sistemas de Información, por los conocimientos, experiencias y valores adquiridos durante mi formación académica.

Al Ing. Jhovany Santacruz Espinoza, subdirector de la Carrera, por su gestión, apoyo y constante disposición para atender las necesidades de los estudiantes durante nuestro proceso formativo. Extiendo mi gratitud al cuerpo docente, que con su dedicación, profesionalismo y vocación compartió sus conocimientos y contribuyó a mi crecimiento académico y personal, así como al personal administrativo, por su amabilidad, colaboración y oportuna atención en cada uno de los trámites y requerimientos a lo largo de la carrera.

De manera especial, expreso mi agradecimiento a la Ing. Cristina Flores Urgiles, directora de este trabajo de investigación, por su orientación, acompañamiento, paciencia y rigurosidad académica. Sus valiosas observaciones y recomendaciones fueron fundamentales para el desarrollo y culminación de la presente investigación.

Resumen

La Cooperativa de Ahorro y Crédito Achik Inti Ltda. trata datos personales y crediticios de sus socios sin disponer de un sistema formal que garantice el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador. Esta investigación tuvo como objetivo diseñar un sistema de gestión de protección de datos personales para la entidad, articulando los requisitos de la LOPDP con los estándares ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27701 y con la metodología de análisis de riesgos MAGERIT versión 3. El estudio, de tipo aplicado y proyectivo, con diseño no experimental de corte transversal y enfoque mixto, desarrolló un diagnóstico mediante una encuesta estructurada de cincuenta y cinco ítems organizados en diez dominios de control, aplicada por censo a los responsables de las cuatro áreas técnicas (n = 4), y un inventario y valoración de veinticuatro activos de información. Los resultados revelaron un cumplimiento global del 62,7 %, con brechas críticas en la gestión de incidentes (16,7 %) y en el dominio de cumplimiento (25 %), además de trece activos de criticidad muy alta. Sobre esta evidencia se diseñó la propuesta: un manual de políticas, procedimientos, una matriz de roles encabezada por el Delegado de Protección de Datos, una matriz de riesgos con su plan de tratamiento y el registro de actividades de tratamiento, articulados bajo el ciclo PHVA. El sistema propuesto ofrece a la cooperativa una ruta verificable hacia la responsabilidad proactiva y demostrada que exige la normativa ecuatoriana.

Palabras clave: protección de datos personales; LOPDP; sistema de gestión; análisis de riesgos; cooperativa de ahorro y crédito

ABSTRACT

Achik Inti Ltda. Savings and Credit Cooperative processes personal and credit data of its members without having a formal system in place to guarantee compliance with Ecuador's Organic Law on Personal Data Protection (LOPDP, by its acronym in Spanish). This research aimed to design a personal data protection management system for the organization, aligning the requirements of the LOPDP with the ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27701 standards, as well as the MAGERIT version 3 risk analysis methodology. The study, of an applied and projective type with a non-experimental, cross-sectional design and a mixed approach, developed a diagnostic assessment using a structured survey consisting of fifty-five items organized into ten control domains, administered to all heads of the four technical areas (n = 4), as well as an inventory and evaluation of twenty-four information assets. The results revealed an overall compliance rate of 62.7%, with critical gaps in incident management (16.7%) and the compliance domain (25%), as well as thirteen assets with very high criticality. Based on this evidence, the proposal was designed: a manual of policies and procedures, a matrix of roles headed by the Data Protection Officer, a risk matrix with its treatment plan, and the record of processing activities, all structured according to the plan, do, check, act (PDCA) cycle. The proposed system offers the cooperative a verifiable path toward the proactive and demonstrated accountability required by Ecuadorian regulations.

***Keywords*:** personal data protection; LOPDP; management system; risk analysis; savings and credit cooperative

INDICE

Declaratoria de auditoría y responsabilidad II
CERTIFICACIÓN III
DEDICATORIA IV
AGRADECIMIENTO V
Resumen VI
ABSTRACT VII
INTRODUCCIÓN A VIII
CAPÍTULO I 13
1.1. Planteamiento del problema 13
1.1.1 Formulación del problema 14
1.2. Antecedentes de la Investigación 15
1.3. Justificación de la investigación 16
1.4. Objetivos 18
1.4.1 Objetivo General 18
1.4.2 Objetivos Específicos 18
1.5. Limitaciones 18
1.6. Delimitaciones 19
CAPÍTULO II 19
2. MARCO TEÓRICO 19
2.1. Protección de datos personales 19
2.1.1 Concepto de datos personales 20
2.1.2 Clasificación de los datos personales 20
2.1.3 Tratamiento de datos personales 21
2.1.4 Derechos de los titulares 22
2.2. Marco normativo de la protección de datos personales 22
2.2.1 Constitución de la República del Ecuador 22
2.2.2 Ley Orgánica de Protección de Datos Personales (LOPDP) 22
2.2.3 Reglamento a la Ley Orgánica de Protección de Datos Personales 23
2.2.4 Superintendencia de Protección de Datos Personales 23
2.2.5 El RGPD (Reglamento General de Protección de Datos) como referente internacional 23
2.2.6 Obligaciones del responsable y del encargado del tratamiento. 24
2.3. Estándares internacionales para la gestión de la privacidad 25
2.3.1 Familia de normas ISO/IEC 27000 25
2.3.2 Norma ISO/IEC 27001:2022 25

2.3.3 Norma ISO/IEC 27002:2022 Controles de seguridad de la información 26
2.3.4 Norma ISO/IEC 27701:2025 (PIMS) 26
2.3.5 Norma ISO/IEC 29100 Marco de privacidad 26
2.3.6 Norma ISO/IEC 29134:2023 Evaluación de Impacto en la Privacidad (PIA).....27
2.3.7 Encargados del tratamiento y servicios en la nube (ISO/IEC 27018:2025 e ISO/IEC 27036) 27
2.4. Seguridad de la información en el tratamiento de datos personales 28
2.4.1 Conceptos básicos de la seguridad de la información 28
2.4.2 Confidencialidad, integridad y disponibilidad de la información.....28
2.4.3 Relación entre seguridad de la información y privacidad.....29
2.4.4 Controles de seguridad y privacidad.....29
2.5. Sistemas de gestión y selección del enfoque metodológico 30
2.5.1 Concepto de sistema de gestión 30
2.5.2 Ciclo de mejora continua PHVA 30
2.5.3 Comparación entre la LOPDP, la ISO/IEC 27001, la ISO/IEC 27701 y la gestión de riesgos 31
2.6. Gestión de riesgos aplicada a la protección de datos.....32
2.6.1 Activo, amenaza, vulnerabilidad y riesgo.....32
2.6.2 Norma ISO/IEC 27005 32
2.6.3 Norma ISO 31000.....33
2.6.4 Matriz de riesgos.....33
2.6.5 Tratamiento del riesgo 33
2.6.6 Evaluación de impacto en la protección de datos 34
2.7. Técnicas y herramientas para el diagnóstico del tratamiento de datos personales 34
2.7.1 Análisis de brechas (GAP analysis).....34
2.7.2 Levantamiento y mapeo de procesos 34
2.7.3 Fichas e instrumentos de diagnóstico 35
2.8. Componentes del sistema de gestión de protección de datos personales.....35
2.8.1 Políticas de protección de datos.....35
2.8.2 Procedimientos.....35
2.8.3 Roles y responsabilidades: el delegado de Protección de Datos.....36
2.8.4 Registro de actividades de tratamiento 36
2.8.5 Matriz de riesgos y controles 36
2.8.6 Gestión de incidentes y brechas de seguridad.....37
2.9. Contextualización de la Cooperativa de Ahorro y Crédito Achik Inti Ltda. 37
2.9.1 El sector financiero popular y solidario en el Ecuador.....37
2.9.2 Tratamiento de datos personales en las cooperativas de ahorro y crédito 37
2.9.3 La Cooperativa de Ahorro y Crédito Achik Inti Ltda.....38
CAPÍTULO III.....39

3. MARCO METODOLÓGICO....39
3.1. Enfoque de la investigación....39
3.2. Nivel de la investigación....40
3.3. Población y muestra....41
3.4. Técnicas e instrumentos de recolección de información....41
3.4.1 Revisión documental....42
3.4.2 Encuesta de diagnóstico basada en la norma ISO/IEC 27002....42
3.4.3 Ficha de inventario y valoración de activos según MAGERIT....43
3.5. Metodología de análisis y gestión de riesgos: MAGERIT versión 3....44
3.6. Fases metodológicas de la investigación....46
CAPÍTULO IV....47
4. PROPUESTA....47
4.1. Presentación de la propuesta....47
4.2. Resultados del diagnóstico institucional....48
4.2.1 Nivel de cumplimiento por dominio de control....48
4.2.2 Identificación de los activos críticos....49
4.3. Análisis de riesgos....50
4.3.1 Escalas de probabilidad, impacto y nivel de riesgo....51
4.3.2 Matriz de riesgos....51
4.4. Tratamiento del riesgo y selección de salvaguardas....53
4.5. Diseño del sistema de gestión de protección de datos personales....54
4.5.1 Estructura documental del sistema....54
4.5.2 Política de protección de datos personales....55
4.5.3 Roles y responsabilidades....55
4.5.4 Registro de actividades de tratamiento....56
4.5.5 Procedimiento de atención de los derechos de los titulares....56
4.5.6 Gestión de incidentes y brechas de seguridad....57
4.5.7 Mejora continua del sistema....57
4.6. Cumplimiento de los objetivos de la investigación....58
Conclusiones....59
Recomendaciones....60
Referencias....62
Anexos....65
Anexo 1: Protocolo de Investigación....65
DIRECTOR: ING. CRISTINA MARIUXI FLORES URGILES....75
Anexo 2. Manual de Políticas de Protección de Datos Personales....78

INDICE DE TABLAS

Tabla 1. Comparación de la LOPDP, la ISO/IEC 27001, la ISO/IEC 27701 y la gestión de riesgos 31
Tabla 2. Dominios de diagnóstico adaptados a partir de la norma ISO/IEC 27002 42
Tabla 3. Escala de valoración de la criticidad de los activos 44
Tabla 4. Activos identificados en la cooperativa por categoría MAGERIT 44
Tabla 5. Inventario y valoración de activos de la Cooperativa de Ahorro y Crédito Achik Inti Ltda 45
Tabla 6. Fases metodológicas del proyecto y su correspondencia con los objetivos específicos 46
Tabla 7. Nivel de cumplimiento por dominio de control de la norma ISO/IEC 27002 48
Tabla 8. Activos críticos de la Cooperativa de Ahorro y Crédito Achik Inti Ltda 50
Tabla 9. Escalas de probabilidad, impacto y niveles de riesgo 51
Tabla 10. Matriz de riesgos de los activos críticos 51
Tabla 11. Plan de tratamiento del riesgo y salvaguardas propuestas 53
Tabla 12. Matriz de roles y responsabilidades del sistema de gestión 56
Tabla 13. Registro inicial de actividades de tratamiento 56
Tabla 14. Cumplimiento de los objetivos específicos de la investigación 58

INDICE DE ILUSTRACIONES

Figura 1. Nivel de cumplimiento por dominio de control 49
Figura 2. Mapa de calor probabilidad–impacto de los riesgos identificados 52
Figura 3. Distribución de los riesgos por nivel 52
Figura 4. Comparación entre el riesgo inherente y el riesgo residual esperado 54
Figura 5. Estructura documental del sistema de gestión de protección de datos personales 55
Figura 6. Flujograma del procedimiento de atención de los derechos de los titulares 57
Figura 7. Ciclo de mejora continua PHVA aplicado al sistema de gestión 58

INTRODUCCIÓN A

CAPÍTULO I

1.1. Planteamiento del problema

La Cooperativa de Ahorro y Crédito Achik Inti Ltda. es una entidad financiera ubicada en el sector cooperativo ecuatoriano. De acuerdo con información pública, la institución se identifica como una cooperativa de ahorro y crédito, dispone de banca virtual y se encuentra registrada como COAC activa en el segmento 5, dentro de la Zonal 6 Cuenca. Esto evidencia que la entidad desarrolla actividades financieras que implican el tratamiento de información de socios, clientes, trabajadores y usuarios de servicios financieros.

En el contexto actual, las cooperativas de ahorro y crédito gestionan información sensible y estratégica, como datos de identificación, información de contacto, datos financieros, historial crediticio, solicitudes de crédito, documentación contractual y registros transaccionales. Este tipo de información requiere controles adecuados para evitar accesos no autorizados, pérdida de datos, uso indebido, divulgación no autorizada o incumplimiento normativo. La Ley Orgánica de Protección de Datos Personales del Ecuador y su reglamento establecen obligaciones para responsables y encargados del tratamiento, así como procedimientos para garantizar derechos como acceso, rectificación, actualización, eliminación, oposición y portabilidad (Información, s. f.).

El problema principal radica en la necesidad de contar con un sistema formal de gestión de protección de datos personales que permita organizar políticas, procedimientos, responsables, controles, registros de tratamiento, gestión de riesgos, atención de derechos del titular y mecanismos de mejora continua. La ausencia de un sistema estructurado puede generar debilidades en el cumplimiento legal, exposición a incidentes de seguridad, afectación a la confianza de los socios y dificultades para demostrar responsabilidad proactiva ante la

autoridad competente. Además, estudios recientes sobre datos crediticios en Ecuador señalan que las instituciones financieras deben obtener autorización del titular y aplicar medidas estrictas en el tratamiento de información financiera y crediticia.

Por lo tanto, se plantea el diseño de un sistema de gestión de protección de datos personales para la Cooperativa de Ahorro y Crédito Achik Inti Ltda., con el propósito de establecer una propuesta técnica y normativa que permita identificar los tratamientos de datos, evaluar riesgos, definir controles, asignar responsabilidades y fortalecer el cumplimiento de la normativa ecuatoriana vigente, tomando como referencia buenas prácticas internacionales como ISO/IEC 27001:2022 e ISO/IEC 27701:2025.

1.1.1 Formulación del problema

Actualmente, la Cooperativa de Ahorro y Crédito Achik Inti Ltda. no cuenta con un sistema estructurado de gestión de protección de datos personales, lo que podría representar un problema para la entidad debido al manejo de información sensible de socios, clientes, trabajadores y usuarios de servicios financieros. Esta situación resulta especialmente crítica considerando que las cooperativas de ahorro y crédito administran datos de identificación, información económica, historial crediticio, documentación contractual y registros transaccionales, los cuales requieren controles adecuados para evitar accesos no autorizados, pérdida de información, uso indebido o incumplimiento de la normativa vigente.

¿Cómo puede la Cooperativa de Ahorro y Crédito Achik Inti Ltda. gestionar adecuadamente la protección de datos personales de sus socios, clientes y colaboradores, considerando la ausencia de un sistema estructurado para su tratamiento, control y cumplimiento normativo?

1.2. Antecedentes de la Investigación

En el ámbito internacional, Haggag et al. (2025), en el estudio titulado “An analysis of privacy regulations and user concerns of finance mobile applications”, analizaron las preocupaciones de privacidad de los usuarios y el impacto de las regulaciones de protección de datos en aplicaciones financieras móviles de Alemania, Australia y Estados Unidos. La investigación destaca que las aplicaciones financieras gestionan información altamente sensible, como datos personales, información bancaria e historiales transaccionales, lo que las convierte en objetivos relevantes para ataques informáticos y riesgos de privacidad. Este trabajo resulta pertinente para el presente anteproyecto porque evidencia que las entidades financieras deben fortalecer sus políticas de privacidad, transparentar el uso de los datos y establecer controles adecuados para proteger la información de sus usuarios.

Asimismo, Carneiro et al. (2025), en el artículo “A flexible ISO 27701-based framework for assessing cybersecurity maturity: a proposition and a case application”, propusieron un marco flexible basado en ISO/IEC 27701 para evaluar el nivel de madurez de la gestión de ciberseguridad y privacidad en organizaciones. El estudio utilizó ISO/IEC 27701 como base para estructurar un cuestionario de evaluación y aplicó técnicas como análisis jerárquico de clústeres, análisis de frecuencia y Fuzzy TOPSIS. Los resultados evidencian la utilidad de los estándares de privacidad para identificar brechas, evaluar controles y orientar la mejora institucional. Este antecedente es importante para el presente trabajo porque respalda la necesidad de diseñar un sistema de gestión de protección de datos personales basado en políticas, controles, responsabilidades, evaluación de riesgos y mejora continua.

En el contexto nacional, Mancero-Gavilanes et al. (2025),en el estudio “Protección de datos personales crediticios y administración del perfil de riesgo en Ecuador”, realizaron un análisis crítico-jurídico sobre el tratamiento de datos personales crediticios en el sistema

financiero ecuatoriano. La investigación examina la relación entre la protección de los datos crediticios y la necesidad de las instituciones financieras de administrar perfiles de riesgo. Los autores destacan que las entidades deben cumplir medidas estrictas, entre ellas obtener autorización del titular antes del tratamiento de datos personales crediticios. Este trabajo se relaciona directamente con el anteproyecto porque las cooperativas de ahorro y crédito tratan información financiera y crediticia de socios y clientes, por lo que requieren mecanismos internos para garantizar consentimiento, finalidad legítima, confidencialidad y seguridad en el tratamiento de datos.

En el ámbito local, Romero (2024), desarrolló una investigación sobre el cumplimiento de la normativa de seguridad de la información para la COAC Achik Inti del cantón Cañar, en el marco de su progresión de segmento bajo la regulación de la Superintendencia de Economía Popular y Solidaria. El estudio identificó brechas en seguridad de la información y propuso acciones de mejora relacionadas con políticas, infraestructura tecnológica, capacitación y gestión de riesgos. Este antecedente resulta especialmente pertinente porque muestra que la cooperativa ya ha sido objeto de investigaciones relacionadas con seguridad, cumplimiento normativo y gestión de riesgos, aspectos que sirven como base para proponer un sistema de gestión de protección de datos personales.

1.3. Justificación de la investigación

La protección de datos personales se ha convertido en una necesidad prioritaria para las organizaciones que gestionan información de personas naturales, especialmente en el sector financiero, donde se administran datos de identificación, información económica, historial crediticio, documentación contractual y registros asociados a la relación entre la institución y sus socios. En Ecuador, la Ley Orgánica de Protección de Datos Personales y su

reglamento establecen obligaciones para los responsables y encargados del tratamiento, así como mecanismos para garantizar los derechos de los titulares de datos.

El desarrollo de este proyecto se justifica porque una cooperativa de ahorro y crédito requiere mecanismos formales que le permitan demostrar cumplimiento normativo, reducir riesgos asociados al tratamiento inadecuado de información y fortalecer la confianza de sus socios. En este sentido, los datos financieros y crediticios deben ser gestionados bajo principios de licitud, transparencia, finalidad, minimización, confidencialidad, seguridad y responsabilidad proactiva. Por ello, resulta necesario contar con un sistema que permita organizar, controlar y documentar los procesos relacionados con la protección de datos personales.

Desde el punto de vista técnico, el diseño de un sistema de gestión permitirá identificar los tratamientos de datos personales realizados por la Cooperativa de Ahorro y Crédito Achik Inti Ltda., establecer responsabilidades internas, definir políticas y procedimientos, gestionar riesgos de privacidad y generar evidencia documental para auditorías, revisiones internas o procesos de mejora institucional. Además, el análisis de marcos como la LOPDP, ISO/IEC 27001 e ISO/IEC 27701 permitirá seleccionar un enfoque metodológico adecuado para estructurar la propuesta de manera ordenada, verificable y alineada con buenas prácticas internacionales.

Finalmente, el anteproyecto aportará una propuesta aplicable al contexto de la Cooperativa de Ahorro y Crédito Achik Inti Ltda., contribuyendo al fortalecimiento de la gobernanza de datos, la seguridad de la información, el cumplimiento normativo y la cultura institucional de privacidad. De esta manera, el proyecto no solo responde a una exigencia legal, sino también a una necesidad organizacional orientada a proteger la información personal de socios, clientes, colaboradores y demás partes relacionadas.

1.4. Objetivos

1.4.1 Objetivo General

Diseñar un sistema de gestión de protección de datos personales para la Cooperativa de Ahorro y Crédito Achik Inti Ltda., mediante el análisis normativo, diagnóstico institucional y definición de políticas, procedimientos y controles de privacidad, con el fin de fortalecer el cumplimiento legal, la seguridad de la información y la protección de los datos de socios, clientes y colaboradores.

1.4.2 Objetivos Específicos

- Realizar un estudio teórico y normativo sobre protección de datos personales y datos crediticios, mediante la revisión de literatura científica, normativa ecuatoriana y estándares internacionales, con el fin de sustentar legal y conceptualmente el sistema de gestión.
- Analizar metodologías y marcos de referencia aplicables a la gestión de protección de datos personales, mediante la comparación de la Ley Orgánica de Protección de Datos Personales, ISO/IEC 27001, ISO/IEC 27701 y gestión de riesgos, con el fin de seleccionar el enfoque metodológico del proyecto.
- Diagnosticar la situación actual de la Cooperativa de Ahorro y Crédito Achik Inti Ltda. sobre el tratamiento de datos personales, mediante revisión documental, levantamiento de procesos y fichas de diagnóstico, con el fin de identificar riesgos, brechas y necesidades de control.
- Diseñar el sistema de gestión de protección de datos personales para la Cooperativa de Ahorro y Crédito Achik Inti Ltda., mediante políticas, procedimientos, roles, matriz de riesgos y registros de tratamiento, con el fin de fortalecer el cumplimiento normativo y la seguridad de la información.

1.5. Limitaciones

- Disponibilidad de tiempo, dado que la investigación se desarrollará en un periodo aproximado de tres meses, lo que podría limitar la profundidad del diagnóstico y validación del sistema de gestión de protección de datos personales.

- Acceso a la información interna, ya que el levantamiento de procesos, tipos de datos personales, responsables y controles dependerá de la disponibilidad y autorización de la Cooperativa de Ahorro y Crédito Achik Inti Ltda.

- Recursos económicos, humanos y tecnológicos, podrían ser un factor limitante, debido a que el proyecto se enfocará en el diseño del sistema de gestión, sin contemplar su implementación completa, adquisición de herramientas tecnológicas ni certificación bajo normas ISO.

1.6. Delimitaciones

- Este estudio se centrará en los procesos relacionados con la recolección, almacenamiento, uso, consulta, transferencia, conservación y eliminación de datos personales dentro de la Cooperativa de Ahorro y Crédito Achik Inti Ltda.

- El presente trabajo se limita solo a la elaboración de una propuesta técnica y metodológica, cuya implementación quedará sujeta a la evaluación y decisión de la Cooperativa de Ahorro y Crédito Achik Inti Ltda.

- La investigación se centrará en los responsables relacionados con el tratamiento de datos personales y el área de sistemas de la cooperativa, mas no en otras áreas externas o instituciones ajenas a la organización.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Protección de datos personales

La protección de datos personales constituye un derecho fundamental orientado a garantizar que toda persona natural pueda conocer, controlar y decidir sobre el uso de la

información que la identifica o la hace identificable. Este derecho se ejerce frente a cualquier persona, pública o privada, que recolecte, almacene, procese o difunda datos personales, e impone a estos actores obligaciones de licitud, transparencia y seguridad. En un entorno digital e hiperconectado, la protección de datos habilita la confianza de los ciudadanos frente a los proveedores de servicios, y se convierte en un factor crítico para las instituciones financieras que gestionan grandes volúmenes de información sensible de sus socios (Asamblea Nacional del Ecuador, 2021).

2.1.1 Concepto de datos personales

Los datos personales son aquellos que identifican o hacen identificable a una persona natural. Esta categoría incluye nombres, números de identificación, direcciones, teléfonos, correos electrónicos, datos financieros, información laboral, registros contractuales y cualquier elemento asociado directa o indirectamente con una persona (Asamblea Nacional del Ecuador, 2021).

La Ley Orgánica de Protección de Datos Personales reconoce que el tratamiento de datos personales debe ajustarse a principios como juridicidad, lealtad, transparencia, finalidad, pertinencia, minimización, confidencialidad, calidad, conservación limitada y responsabilidad proactiva. Estos principios obligan a que la organización no solo proteja técnicamente los datos, sino que también documente finalidades, bases de legitimación, responsables, medidas de seguridad, tiempos de conservación y procedimientos para atender derechos de los titulares (Asamblea Nacional del Ecuador, 2021).

2.1.2 Clasificación de los datos personales

Los datos personales sensibles son aquellos cuyo tratamiento indebido puede generar discriminación o afectar de manera grave los derechos y libertades fundamentales del titular. Dentro de esta categoría se incluyen los datos relativos a la etnia, la religión, la afiliación política o sindical, la orientación sexual, la salud y los datos biométricos. Debido a su naturaleza, la normativa establece un régimen reforzado de protección: su tratamiento se encuentra prohibido de forma general y solo se admite en supuestos específicos, principalmente cuando media el consentimiento explícito del titular o una habilitación legal. Este régimen exige a las organizaciones aplicar medidas de seguridad más estrictas sobre este tipo de información (Merino, 2025).

a) Datos crediticios y financieros

Los datos crediticios y financieros comprenden la información asociada a la situación económica, el comportamiento de pago, la capacidad de endeudamiento y el historial crediticio de una persona. En el contexto de una cooperativa de ahorro y crédito, estos datos incluyen los ingresos, las obligaciones vigentes, las garantías, la calificación de riesgo y el historial de operaciones del socio. Su tratamiento resulta indispensable para la actividad de intermediación financiera, pero también representa un riesgo elevado, ya que su exposición o uso no autorizado puede ocasionar perjuicios económicos y reputacionales al titular. Por ello, estos datos deben tratarse bajo bases de legitimación claras y con controles de seguridad proporcionales al riesgo que representan (Asamblea Nacional del Ecuador, 2021).

2.1.3 Tratamiento de datos personales

El tratamiento de datos personales es cualquier operación o conjunto de operaciones realizadas sobre los datos, tanto en soportes automatizados como manuales. Comprende la recolección, el registro, la organización, el almacenamiento, la consulta, la utilización, la comunicación, la transferencia y la supresión de la información. El ciclo de vida del tratamiento inicia con la captación del dato y concluye con su eliminación o anonimización, y en cada una de sus fases deben aplicarse controles que garanticen la protección de la información. Entender el tratamiento como un proceso integral permite a la organización identificar en qué momentos y actividades se manipulan datos personales, lo que constituye la base para el levantamiento de procesos y el registro de actividades de tratamiento (Innodev Solutions S.A., 2026).

a) Principios del tratamiento de datos personales

Los principios rectores constituyen los criterios que deben orientar todo tratamiento de datos personales y actúan como marco de interpretación de las obligaciones de responsables y encargados. La Ley Orgánica de Protección de Datos Personales del Ecuador reconoce, entre otros, los principios de juridicidad, lealtad y transparencia, legitimidad, consentimiento, finalidad, pertinencia y minimización, proporcionalidad, confidencialidad, calidad, conservación, seguridad y aplicación favorable al titular. El eje central de la norma es el principio de responsabilidad proactiva y demostrada, que exige a las organizaciones no solo cumplir con la ley, sino estar en capacidad de acreditar en todo momento las medidas adoptadas para ello, lo que justifica precisamente la existencia de un sistema de gestión documentado (Asamblea Nacional del Ecuador, 2021).

2.1.4 Derechos de los titulares

La normativa ecuatoriana dota al titular de un catálogo de derechos que le permiten controlar el tratamiento de su información y que deben ejercerse de forma gratuita. Entre ellos se encuentran el derecho de acceso, el derecho de rectificación y actualización, el derecho de eliminación, el derecho de oposición, el derecho de portabilidad, el derecho a la limitación del tratamiento, el derecho a no ser objeto de decisiones automatizadas, el derecho de consulta y el derecho a la educación digital. Para garantizar su ejercicio, las organizaciones deben establecer canales accesibles de atención y responder las solicitudes en un plazo de quince días, dejando registro documental de cada gestión como evidencia de cumplimiento (Orizontel, 2025).

2.2. Marco normativo de la protección de datos personales

El marco normativo aplicable a la protección de datos personales en el Ecuador se estructura de manera jerárquica, partiendo de la Constitución como norma suprema, seguida por la ley orgánica especializada, su reglamento y las resoluciones emitidas por la autoridad de control. A este cuerpo normativo interno se suman los referentes internacionales que inspiraron la legislación nacional. Conocer este marco es indispensable para sustentar legalmente el sistema de gestión y para asegurar que las políticas y procedimientos diseñados respondan a obligaciones exigibles (Orizontel, 2025).

2.2.1 Constitución de la República del Ecuador

La Constitución de la República del Ecuador reconoce, en el numeral 19 de su artículo 66, el derecho a la protección de datos de carácter personal como un derecho fundamental autónomo. Este derecho incluye el acceso y la decisión sobre la información y datos de este carácter, así como su correspondiente protección, y establece que la recolección, archivo, procesamiento, distribución o difusión de estos datos requerirá la autorización del titular o el mandato de la ley. Esta disposición constituye el fundamento jurídico superior sobre el cual se desarrolla toda la normativa especializada en la materia (Asamblea Constituyente, 2008).

2.2.2 Ley Orgánica de Protección de Datos Personales (LOPDP)

La Ley Orgánica de Protección de Datos Personales es el marco jurídico fundamental que regula el tratamiento de datos personales en el Ecuador. Fue aprobada por la Asamblea Nacional y publicada en el Registro Oficial Suplemento 459 el 26 de mayo de 2021, con el objetivo de garantizar el ejercicio del derecho a la protección de datos personales mediante el

desarrollo de principios, derechos, obligaciones y mecanismos de tutela. La ley recoge una clara influencia de la normativa europea, incorpora el criterio de extraterritorialidad, otorgó plazos de adecuación a las organizaciones y estableció un régimen sancionador cuyas multas pueden oscilar entre el 0,7 % y el 1 % del volumen de negocios del infractor, lo que evidencia la relevancia de su cumplimiento (Asamblea Nacional del Ecuador, 2021).

2.2.3 Reglamento a la Ley Orgánica de Protección de Datos Personales

El Reglamento General a la Ley Orgánica de Protección de Datos Personales, publicado en noviembre de 2023, desarrolla y operativiza las disposiciones de la ley, estableciendo procedimientos específicos, plazos y requisitos detallados para su cumplimiento. Entre sus aportes se encuentran la regulación de la evaluación de impacto del tratamiento, entendida como un análisis preventivo de naturaleza técnica para identificar y mitigar riesgos, la obligación de mantener un registro de actividades de tratamiento para responsables con cien o más trabajadores, y las obligaciones del responsable de aplicar medidas apropiadas atendiendo al estado de la técnica, la naturaleza del tratamiento y la gravedad de los riesgos. Este instrumento resulta esencial para traducir las obligaciones legales en controles concretos (Presidencia de la República del Ecuador, 2023).

2.2.4 Superintendencia de Protección de Datos Personales

La Superintendencia de Protección de Datos Personales es la autoridad de control encargada de supervisar y vigilar el cumplimiento de la ley, su reglamento y las resoluciones que emita, con el fin de proteger los derechos y libertades fundamentales de las personas naturales respecto al tratamiento de sus datos. Entre sus funciones se encuentra la emisión de normativa técnica, guías interpretativas y resoluciones complementarias, así como la instrucción de los procedimientos sancionadores. La existencia de esta autoridad refuerza la exigibilidad del cumplimiento y obliga a las organizaciones a mantenerse actualizadas respecto de las disposiciones que se publiquen (Orizontel, 2025).

2.2.5 El RGPD (Reglamento General de Protección de Datos) como referente internacional

El Reglamento General de Protección de Datos de la Unión Europea constituye el referente internacional más influyente en la materia y sirvió de base para la construcción de la legislación ecuatoriana. Este cuerpo normativo consolidó principios como la responsabilidad proactiva, la protección de datos desde el diseño y por defecto, la evaluación de impacto y la

figura del delegado de protección de datos. El propio reglamento europeo advierte que la protección de datos no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y aplicarse de forma proporcional, equilibrando los derechos de los titulares con los intereses legítimos en juego. Su estudio permite comprender el sentido y alcance de las obligaciones adoptadas por el Ecuador (Merino, 2025).

2.2.6 Obligaciones del responsable y del encargado del tratamiento.

La Ley Orgánica de Protección de Datos Personales (LOPDP) y su Reglamento General, expedido mediante Decreto Ejecutivo No. 904, distinguen dos figuras centrales en toda operación de tratamiento. El artículo 4 de la LOPDP define al responsable del tratamiento como la persona natural o jurídica que, sola o conjuntamente con otras, decide sobre la finalidad y el tratamiento de los datos personales, y al encargado del tratamiento como aquella que trata datos personales a nombre y por cuenta del responsable (Asamblea Nacional del Ecuador, 2021).

El artículo 47 de la LOPDP concentra el catálogo de deberes exigibles al responsable, entre los cuales destacan tratar los datos en apego a los principios y derechos reconocidos en la ley, implementar y verificar periódicamente medidas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, aplicar metodologías de análisis y gestión de riesgos, incorporar la protección de datos desde el diseño y por defecto, notificar las vulneraciones de seguridad, suscribir acuerdos de confidencialidad, mantener el Registro Nacional de Protección de Datos Personales, designar delegado cuando corresponda y permitir la realización de auditorías. La misma disposición extiende al encargado las obligaciones del responsable en todo lo que resulte aplicable (Asamblea Nacional del Ecuador, 2021). En el plano reglamentario, el artículo 33 del Reglamento General precisa que estas medidas deben adoptarse tanto al determinar los medios del tratamiento como durante su ejecución, atendiendo al estado de la técnica, los costos de aplicación, la naturaleza, el alcance, las circunstancias y los fines del tratamiento, así como a la probabilidad y gravedad de los riesgos para los titulares (Presidencia de la República del Ecuador, 2023).

Respecto del encargado, el artículo 34 de la LOPDP establece que el acceso a datos personales por parte de un tercero para prestar un servicio al responsable no constituye transferencia ni comunicación de datos, sino que convierte a ese tercero en encargado, y exige que dicho tratamiento se regule mediante contrato en el que conste que actuará únicamente conforme a las instrucciones del responsable (Asamblea Nacional del Ecuador, 2021). El

Reglamento General desarrolla esta relación al disponer que el encargado debe ofrecer garantías suficientes de idoneidad (art. 40), que el vínculo se rige por un contrato escrito que detalle objeto, duración, naturaleza, finalidad, categorías de datos, identificación de titulares y obligaciones del encargado (art. 41), que la subcontratación requiere previsión contractual expresa o autorización escrita (art. 45), que al término de la relación los datos deben devolverse o eliminarse (art. 46) y que el encargado debe permitir al responsable la revisión de sus registros y procesos para verificar el cumplimiento (art. 47). Asimismo, el encargado que por cualquier causa determine los fines y medios del tratamiento será considerado responsable respecto de ese tratamiento (art. 43) (Presidencia de la República del Ecuador, 2023).

2.3. Estándares internacionales para la gestión de la privacidad

Los estándares internacionales proporcionan marcos de referencia estructurados que permiten a las organizaciones gestionar la seguridad de la información y la privacidad de manera sistemática, basada en riesgos y orientada a la mejora continua. Su adopción facilita el cumplimiento normativo, ordena las funciones y controles, y aporta evidencia verificable ante las partes interesadas. En el ámbito de la protección de datos, la familia de normas ISO/IEC 27000 ofrece un conjunto de estándares complementarios que sirven de base para el diseño del sistema de gestión (International Organization for Standardization / International Electrotechnical Commission, 2022).

2.3.1 Familia de normas ISO/IEC 27000

La familia de normas ISO/IEC 27000 agrupa un conjunto de estándares internacionales dedicados a la gestión de la seguridad de la información. Dentro de esta familia, la norma ISO/IEC 27001 define los requisitos del sistema de gestión de seguridad de la información, la ISO/IEC 27002 ofrece un catálogo de controles, la ISO/IEC 27005 orienta la gestión de riesgos y la ISO/IEC 27701 extiende el modelo hacia la gestión de la privacidad. La coherencia entre estas normas permite integrar en un mismo sistema los aspectos de seguridad y de protección de datos, aprovechando una estructura común y evitando la duplicación de esfuerzos (International Organization for Standardization / International Electrotechnical Commission, 2022).

2.3.2 Norma ISO/IEC 27001:2022

La norma ISO/IEC 27001:2022 es el estándar internacional que describe los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de

seguridad de la información. Su estructura de alto nivel comprende el contexto de la organización, el liderazgo, la planificación, el soporte, la operación, la evaluación del desempeño y la mejora, lo que facilita su integración con otros sistemas de gestión. Su enfoque basado en riesgos protege la confidencialidad, integridad y disponibilidad de la información, y proporciona el marco sobre el cual se sustentan las políticas y controles de seguridad de una organización, incluidos aquellos necesarios para proteger los datos personales (International Organization for Standardization & International Electrotechnical Commission, 2022).

2.3.3 Norma ISO/IEC 27002:2022 Controles de seguridad de la información

La norma ISO/IEC 27002:2022 es el estándar complementario de la ISO/IEC 27001 que desarrolla en detalle los controles de seguridad de la información. Mientras la ISO/IEC 27001 establece los requisitos del sistema de gestión, la ISO/IEC 27002 ofrece un catálogo de referencia con orientaciones para la selección, implementación y gestión de dichos controles. En su versión 2022, la norma organiza noventa y tres controles en cuatro categorías: controles organizacionales, controles de personas, controles físicos y controles tecnológicos, que abarcan desde las políticas de seguridad y la gestión de activos hasta el control de accesos, la seguridad física, la seguridad en las operaciones y el cumplimiento normativo (International Organization for Standardization; International Electrotechnical Commission, 2022).

2.3.4 Norma ISO/IEC 27701:2025 (PIMS)

La ISO/IEC 27701:2025 es una norma internacional que establece los requisitos y directrices para implementar, mantener y mejorar un Sistema de Gestión de la Información de Privacidad (Privacy Information Management System, PIMS) como una extensión de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la ISO/IEC 27001. Su objetivo es proporcionar un marco para gestionar los riesgos asociados al tratamiento de datos personales, definir responsabilidades para responsables y encargados del tratamiento, e incorporar controles de privacidad que permitan cumplir los requisitos legales y regulatorios aplicables. De esta manera, la norma integra la gestión de la privacidad con la seguridad de la información, promoviendo la protección de los datos personales, la transparencia y la mejora continua en las organizaciones (International Organization for Standardization & International Electrotechnical Commission, 2025).

2.3.5 Norma ISO/IEC 29100 Marco de privacidad

La norma ISO/IEC 29100, con su enmienda de 2018, establece el marco conceptual y terminológico de la privacidad en el ámbito de las tecnologías de la información. Define nociones fundamentales como información de identificación personal, responsable de información de identificación personal y encargado de dicha información, y formula un conjunto de principios de privacidad entre los que se encuentran el consentimiento y la elección, la legitimidad y especificación del propósito, la limitación de la recolección, la minimización de datos, la limitación de uso, retención y divulgación, la exactitud y calidad, la apertura y transparencia, la participación y el acceso individual, la responsabilidad, la seguridad de la información y el cumplimiento en materia de privacidad. Su valor para este proyecto es doble: proporciona el vocabulario común que emplean las demás normas de la familia y ofrece un conjunto de principios comparable con los establecidos en el artículo 10 de la LOPDP, lo que permite construir una matriz de correspondencia entre el marco técnico y el marco legal ecuatoriano (International Organization for Standardization & International Electrotechnical Commission, 2011).

2.3.6 Norma ISO/IEC 29134:2023 Evaluación de Impacto en la Privacidad (PIA)

La ISO/IEC 29134:2023 proporciona directrices para realizar una Evaluación de Impacto en la Privacidad (Privacy Impact Assessment, PIA), entendida como un proceso sistemático para identificar, analizar y tratar los riesgos que el tratamiento de datos personales puede generar sobre la privacidad de las personas. La norma establece un marco para planificar la evaluación, documentar los riesgos asociados al tratamiento de información personal, definir medidas de mitigación y elaborar un informe estructurado que facilite la toma de decisiones y el cumplimiento de requisitos legales y organizacionales. Su aplicación es adecuada para organizaciones de cualquier tamaño y sector que diseñen, desarrollen u operen sistemas, servicios o proyectos que impliquen el tratamiento de información personal (International Organization for Standardization & International Electrotechnical Commission, 2023).

2.3.7 Encargados del tratamiento y servicios en la nube (ISO/IEC 27018:2025 e ISO/IEC 27036)

La ISO/IEC 27018:2025 establece un conjunto de controles y buenas prácticas para proteger la información personal identificable (Personally Identifiable Information, PII) procesada por proveedores de servicios en la nube que actúan como encargados del tratamiento.

La norma complementa los controles de seguridad de la ISO/IEC 27002 e incorpora medidas relacionadas con el consentimiento, la transparencia, la limitación del tratamiento, la eliminación segura de datos, la notificación de incidentes y la protección de la privacidad durante todo el ciclo de vida de la información. Su finalidad es fortalecer la confianza en los servicios en la nube y facilitar el cumplimiento de los requisitos legales sobre protección de datos personales (International Organization for Standardization & International Electrotechnical Commission, 2025).

Por su parte, la serie ISO/IEC 27036 proporciona directrices para gestionar la seguridad de la información en las relaciones con proveedores y terceros. Este conjunto de normas establece recomendaciones para identificar riesgos asociados a la cadena de suministro, definir responsabilidades contractuales, supervisar el cumplimiento de controles de seguridad y gestionar los riesgos derivados de la contratación de servicios tecnológicos, incluidos los servicios en la nube. Su aplicación permite reducir vulnerabilidades derivadas de proveedores externos y fortalecer la gestión integral de la seguridad de la información (International Organization for Standardization & International Electrotechnical Commission, 2023).

2.4. Seguridad de la información en el tratamiento de datos personales

2.4.1 Conceptos básicos de la seguridad de la información

La seguridad de la información es el conjunto de principios, políticas, procesos y controles destinados a proteger la información frente a amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad. Su finalidad es preservar el valor de la información durante todo su ciclo de vida mediante la identificación y tratamiento de riesgos, garantizando que únicamente las personas autorizadas accedan a los datos, que estos permanezcan completos y exactos, y que estén disponibles cuando sean requeridos. En el contexto de la transformación digital, la seguridad de la información constituye un elemento estratégico para asegurar la continuidad de las operaciones, fortalecer la confianza de las partes interesadas y cumplir con los requisitos legales y regulatorios aplicables (International Organization for Standardization & International Electrotechnical Commission, 2025).

2.4.2 Confidencialidad, integridad y disponibilidad de la información

La confidencialidad es la propiedad por la cual la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. En el ámbito de la protección de datos personales esta propiedad tiene un correlato normativo expreso: el artículo 10, literal

g, de la Ley Orgánica de Protección de Datos Personales consagra el principio de confidencialidad, según el cual el tratamiento debe concebirse sobre la base del debido sigilo y secreto, de modo que los datos no se traten ni se comuniquen para un fin distinto de aquel para el cual fueron recogidos, salvo que concurra una causal de tratamiento legítimo; para tal efecto, el responsable debe adecuar las medidas técnicas y organizativas correspondientes. En una cooperativa de ahorro y crédito, la confidencialidad se traduce en el control de accesos al sistema financiero, la segregación de funciones entre áreas y los acuerdos de confidencialidad suscritos con el personal y con los proveedores (Asamblea Nacional del Ecuador, 2021).

La disponibilidad es la propiedad de que la información sea accesible y utilizable cuando lo requiera una entidad autorizada. Aunque la ley no la enuncia como principio autónomo, constituye una condición necesaria para el cumplimiento de las obligaciones legales, dado que sin ella el responsable no puede atender las solicitudes de acceso, rectificación, eliminación o portabilidad dentro de los plazos previstos, ni sostener la continuidad del servicio financiero que los socios requieren. Por esta razón, las medidas de respaldo, recuperación y continuidad operativa forman parte del deber de seguridad y no de una preocupación meramente técnica (International Organization for Standardization & International Electrotechnical Commission, 2025).

2.4.3 Relación entre seguridad de la información y privacidad

La seguridad de la información y la privacidad son conceptos estrechamente relacionados, pero no idénticos. La seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de todo tipo de información, mientras que la privacidad se centra específicamente en el tratamiento lícito y legítimo de los datos personales y en el respeto de los derechos de sus titulares. La seguridad es una condición necesaria para la privacidad, dado que sin medidas de seguridad adecuadas no es posible garantizar la protección de los datos personales; sin embargo, no constituye una condición suficiente, puesto que un tratamiento puede ser técnicamente seguro y a la vez ilícito por carecer de base legitimadora o por exceder la finalidad informada al titular. Por esta razón, los modelos modernos integran ambos enfoques, tomando la seguridad de la información como fundamento y añadiendo los controles de privacidad requeridos por la normativa (Bureau Veritas, s. f.).

2.4.4 Controles de seguridad y privacidad

Los controles constituyen las medidas técnicas y organizativas que las organizaciones implementan para tratar los riesgos identificados y proteger la información. La ISO/IEC 27002:2022 clasifica los controles en cuatro grupos: organizacionales, relativos a las personas, físicos y tecnológicos. La ISO/IEC 27701, por su parte, añade controles específicos orientados a la privacidad, como la gestión del consentimiento, la atención a los derechos de los titulares y la minimización de datos, diferenciados según la organización actúe como responsable o como encargado del tratamiento. A ellos se suma la ISO/IEC 29151:2017, código de buenas prácticas para la protección de la información de identificación personal, que desarrolla objetivos de control derivados de los principios establecidos en la ISO/IEC 29100 (ISO/IEC, 2025).

2.5. Sistemas de gestión y selección del enfoque metodológico

El diseño de un sistema de gestión de protección de datos personales requiere seleccionar un enfoque metodológico que articule las obligaciones legales con marcos de gestión reconocidos. Para ello se analizan el concepto de sistema de gestión, el ciclo de mejora continua que lo sustenta y la comparación entre la Ley Orgánica de Protección de Datos Personales, la ISO/IEC 27001, la ISO/IEC 27701 y la gestión de riesgos, con el fin de determinar el enfoque más adecuado para la Cooperativa (Jennings, 2026).

2.5.1 Concepto de sistema de gestión

Un sistema de gestión es un conjunto de políticas, procesos, procedimientos y responsabilidades que una organización establece para alcanzar sus objetivos de manera ordenada y sostenible. Aplicado a la protección de datos, integra los aspectos técnicos, humanos y organizativos necesarios para tratar la información de forma coherente con el marco legal, los objetivos institucionales y las expectativas de las partes interesadas. A diferencia de las medidas aisladas, un sistema de gestión formaliza las responsabilidades, documenta las decisiones y establece mecanismos de seguimiento, lo que permite demostrar el cumplimiento y mejorar de forma continua (Domínguez Domínguez, Flores Laguna, & del Valle López, 2023).

2.5.2 Ciclo de mejora continua PHVA

El ciclo de mejora continua Planificar, Hacer, Verificar y Actuar constituye la base metodológica de los sistemas de gestión normalizados. En la fase de planificación se identifican

los riesgos, los objetivos y los controles necesarios; en la fase de ejecución se implementan las políticas y procedimientos; en la fase de verificación se evalúa el desempeño mediante auditorías, indicadores y revisiones; y en la fase de actuación se adoptan las acciones correctivas requeridas. La aplicación de este ciclo fomenta la evolución del nivel de madurez del sistema y permite abordar de forma progresiva las brechas identificadas, evitando que la protección de datos sea un ejercicio estático (International Organization for Standardization & International Electrotechnical Commission, 2022).

2.5.3 Comparación entre la LOPDP, la ISO/IEC 27001, la ISO/IEC 27701 y la gestión de riesgos

Las referencias que orientan el diseño de un sistema de gestión de protección de datos personales pertenecen a planos distintos, por lo que resulta necesario contrastarlas de forma sistemática. Para ello se comparan la Ley Orgánica de Protección de Datos Personales, la ISO/IEC 27001, la ISO/IEC 27701 y la gestión de riesgos según cinco criterios tomados de la literatura especializada. Cevallos-Salas et al. (2026) señalan que los marcos legales de privacidad establecen principios generales sin detalle técnico sobre cómo alcanzar el cumplimiento, con sanciones asociadas a su incumplimiento, mientras que la ISO/IEC 27701:2025 es voluntaria, flexible y autónoma respecto de la ISO/IEC 27001; de esa distinción provienen los criterios de naturaleza, enfoque y requisito previo. El criterio de aporte al sistema retoma la lógica de Carneiro et al. (2025), quienes valoran la madurez organizacional a partir de la contribución de cada marco de referencia al ciclo de gestión. Finalmente, la gestión de riesgos se incorpora como criterio de contraste porque la autoridad de control la establece como requisito para determinar las medidas de seguridad aplicables (Superintendencia de Protección de Datos Personales, 2025).

Tabla 1

Comparación de la LOPDP, la ISO/IEC 27001, la ISO/IEC 27701 y la gestión de riesgos

Criterio	LOPDP	ISO/IEC 27001	ISO/IEC 27701	Gestión de riesgos
Naturaleza	Norma jurídica de cumplimiento obligatorio en el Ecuador.	Estándar internacional voluntario y certificable.	Estándar internacional autónomo, voluntario y certificable (ed. 2025).	Proceso metodológico transversal, no certificable.
Objeto de protección	Derechos del titular sobre sus datos personales.	Confidencialidad, integridad y disponibilidad de la información.	Privacidad de la información de identificación personal.	Nivel de exposición de los activos y de los derechos de los titulares.

Criterio	LOPDP	ISO/IEC 27001	ISO/IEC 27701	Gestión de riesgos
Enfoque	Principios, derechos y obligaciones exigibles.	Gestión de la seguridad basada en riesgos (PHVA).	Controles de privacidad para responsable y encargado.	Identificación, análisis, evaluación y tratamiento del riesgo.
Aporte al sistema	Define qué debe cumplirse legalmente.	Aporta la estructura y los controles de seguridad.	Traduce la seguridad en controles de protección de datos.	Determina la prioridad y la proporcionalidad de los controles.
Requisito previo	Aplicación directa a toda organización que trate datos.	No requiere otro estándar.	No requiere un SGSI previo; integrable con la ISO/IEC 27001.	Requiere el inventario de activos y de tratamientos.

Nota. Elaboración propia con base en Asamblea Nacional del Ecuador (2021), Presidencia de la República del Ecuador (2023), ISO/IEC (2022), Superintendencia de Protección de Datos Personales (2025) y Cevallos-Salas et al. (2026).

La comparación evidencia que la diferencia decisiva entre las referencias no se encuentra en el objeto de protección, sino en el nivel de prescripción: la LOPDP y su Reglamento son exigibles y determinan resultados obligatorios, pero no especifican los procesos mediante los cuales una organización debe alcanzarlos, mientras que las normas técnicas, de adopción voluntaria, prescriben esos procesos sin definir el contenido jurídico del deber. La gestión de riesgos, por su parte, no constituye un marco equiparable a los anteriores, sino el proceso transversal que ambos planos requieren para establecer qué medidas resultan proporcionales.

2.6. Gestión de riesgos aplicada a la protección de datos

La gestión de riesgos constituye el eje que permite dirigir los recursos de la organización hacia la protección de los activos más críticos. En el ámbito de la protección de datos, consiste en identificar, analizar, evaluar y tratar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de los datos personales, así como los derechos de sus titulares. Un enfoque basado en riesgos evita la aplicación indiscriminada de controles y asegura que las medidas adoptadas sean proporcionales a las amenazas reales (International Organization for Standardization & International Electrotechnical Commission, 2022).

2.6.1 Activo, amenaza, vulnerabilidad y riesgo

Los activos de información son los recursos que poseen valor para la organización, como las bases de datos de socios, los sistemas de crédito y los expedientes físicos. Una amenaza es un evento potencial capaz de causar daño a un activo, mientras que una vulnerabilidad es una debilidad que puede ser aprovechada por una amenaza. El riesgo es la

combinación de la probabilidad de que una amenaza explote una vulnerabilidad y del impacto que ello ocasionaría. La comprensión de estos conceptos permite valorar la exposición de la organización y fundamentar la selección de controles adecuados (Instituto Nacional de Ciberseguridad, 2025).

2.6.2 Norma ISO/IEC 27005

La norma ISO/IEC 27005 es una guía para gestionar los riesgos de seguridad de la información en apoyo a la implementación de un sistema de gestión basado en la ISO/IEC 27001. Ofrece un proceso sistemático para identificar, analizar, evaluar, tratar y comunicar los riesgos, y se caracteriza por ser adaptable al tamaño, contexto y madurez de la organización, sin prescribir una metodología única. Además, admite el uso de técnicas cualitativas, cuantitativas o mixtas para la evaluación de riesgos, y guarda relación con la ISO 31000, de la que retoma sus principios generales de gestión de riesgos (ISO/IEC, 2022).

2.6.3 Norma ISO 31000

La norma ISO 31000 proporciona principios y directrices generales para la gestión de riesgos aplicables a cualquier tipo de organización y a cualquier categoría de riesgo. Establece un marco compuesto por principios, estructura y proceso, y promueve que la gestión de riesgos sea integrada, estructurada, personalizada e inclusiva. Su carácter transversal permite alinear la gestión de riesgos de seguridad de la información y de privacidad con la gestión de riesgos institucional de la Cooperativa, dotando de coherencia a las decisiones sobre controles y recursos (International Organization for Standardization & International Electrotechnical Commission, 2022).

2.6.4 Matriz de riesgos

La matriz de riesgos es una herramienta que permite representar y priorizar los riesgos en función de su probabilidad de ocurrencia y de su impacto potencial. Mediante la combinación de ambos factores se obtiene un nivel de riesgo que facilita clasificar cada situación como baja, media, alta o crítica, y determinar el orden en que deben tratarse. En un sistema de gestión de protección de datos, la matriz de riesgos vincula los activos, las amenazas y las vulnerabilidades con los controles seleccionados, y constituye un insumo esencial para la toma de decisiones y para evidenciar el cumplimiento del principio de responsabilidad proactiva (Rodríguez, 2022).

2.6.5 Tratamiento del riesgo

El tratamiento del riesgo consiste en seleccionar y aplicar las opciones más adecuadas para modificar el nivel de riesgo identificado. Las alternativas habituales son mitigar el riesgo mediante la implementación de controles, transferirlo a un tercero, evitarlo eliminando la actividad que lo origina o aceptarlo cuando se encuentra dentro de los niveles tolerables por la organización. Tras aplicar los controles, subsiste un riesgo residual que debe ser evaluado y aprobado por la dirección. Este proceso iterativo asegura que los recursos se destinen a los riesgos más relevantes y que las decisiones queden debidamente documentadas (International Organization for Standardization / International Electrotechnical Commission, 2022).

2.6.6 Evaluación de impacto en la protección de datos

La evaluación de impacto en la protección de datos es un análisis preventivo de naturaleza técnica mediante el cual el responsable valora los impactos reales de un tratamiento, con el fin de identificar y mitigar los riesgos relacionados con el cumplimiento de los principios y el respeto de los derechos de los titulares. El reglamento ecuatoriano la incorpora como una obligación en los tratamientos que puedan implicar un riesgo elevado, y su resultado orienta la adopción de medidas de seguridad específicas. Esta evaluación conecta directamente la gestión de riesgos con las exigencias normativas, por lo que resulta un componente clave del sistema de gestión (Presidencia de la República del Ecuador, 2023).

2.7. Técnicas y herramientas para el diagnóstico del tratamiento de datos personales

El diagnóstico de la situación actual permite conocer cómo la organización trata los datos personales e identificar los riesgos, brechas y necesidades de control que deberá atender el sistema de gestión. Para llevarlo a cabo se aplican diversas técnicas y herramientas, como el análisis de brechas, el levantamiento y mapeo de procesos y los instrumentos de recolección de información, que ofrecen una visión objetiva del estado de cumplimiento y sustentan las decisiones posteriores del sistema de gestión (Innodev Solutions S.A., 2026).

2.7.1 Análisis de brechas (GAP analysis)

El análisis de brechas es una técnica que compara la situación actual de la organización con un estado deseado definido por la normativa o el estándar de referencia. Al contrastar los requisitos exigidos con las prácticas existentes, permite identificar las brechas de cumplimiento y priorizar las acciones necesarias para cerrarlas. En el contexto de la protección de datos, el

análisis de brechas se realiza frente a las obligaciones de la LOPDP y los controles de las normas ISO, y proporciona una base sólida para planificar el diseño e implementación del sistema de gestión (NQA, s.f.).

2.7.2 Levantamiento y mapeo de procesos

El levantamiento y mapeo de procesos consiste en documentar las actividades de la organización en las que se tratan datos personales, identificando las entradas, las salidas, los responsables y los flujos de información. Esta técnica permite reconocer en qué puntos se recolectan, almacenan, utilizan o comunican datos, así como los sistemas y actores involucrados. El mapeo de procesos es indispensable para elaborar el registro de actividades de tratamiento y para localizar los riesgos asociados a cada operación, constituyendo un insumo directo para el diseño de controles (Innodev Solutions S.A., 2026).

2.7.3 Fichas e instrumentos de diagnóstico

Las fichas e instrumentos de diagnóstico son herramientas estructuradas para recolectar de manera ordenada la información necesaria sobre el tratamiento de datos en la organización. Incluyen cuestionarios, listas de verificación, entrevistas y fichas de levantamiento que permiten registrar los hallazgos de forma sistemática y comparable. Su aplicación facilita la obtención de evidencia sobre las prácticas actuales, la identificación de vulnerabilidades y la determinación de las necesidades de control, y aporta trazabilidad al proceso de diagnóstico que sustenta las decisiones posteriores del sistema de gestión (NQA, s.f.).

2.8. Componentes del sistema de gestión de protección de datos personales

El sistema de gestión de protección de datos personales se materializa a través de un conjunto de componentes que articulan las obligaciones normativas con la operación de la organización. Estos componentes incluyen las políticas, los procedimientos, la definición de roles, el registro de actividades de tratamiento, la matriz de riesgos y controles, y la gestión de incidentes, orientados a fortalecer el cumplimiento normativo y la seguridad de la información (Jennings, 2026).

2.8.1 Políticas de protección de datos

Las políticas de protección de datos son declaraciones formales que expresan el compromiso de la organización con el tratamiento lícito y seguro de los datos personales y que establecen las reglas de comportamiento esperadas de sus integrantes. Una política efectiva

debe ser clara, aprobada por la alta dirección, comunicada a todo el personal y revisada periódicamente. Estas políticas constituyen el marco de referencia a partir del cual se desarrollan los procedimientos operativos y se orientan las decisiones sobre el tratamiento de datos dentro de la organización (Whitman & Mattord, 2022).

2.8.2 Procedimientos

Los procedimientos traducen las políticas en instrucciones operativas concretas que describen cómo deben ejecutarse las actividades relacionadas con el tratamiento de datos personales. Entre ellos se encuentran los procedimientos para la atención de los derechos de los titulares, la obtención y gestión del consentimiento, la contratación de encargados, la gestión de incidentes y la conservación y eliminación de datos. Su documentación permite estandarizar las prácticas, reducir la discrecionalidad y asegurar que las obligaciones normativas se cumplan de forma coherente en toda la organización (Jennings, 2026).

2.8.3 Roles y responsabilidades: el delegado de Protección de Datos

La definición de roles y responsabilidades es esencial para asignar de forma clara quién ejecuta, supervisa y aprueba las actividades del sistema de gestión. Una figura central es el delegado de protección de datos, responsable de asesorar a la organización, supervisar el cumplimiento normativo y actuar como punto de contacto con la autoridad de control y con los titulares. La normativa ecuatoriana prevé la designación de este delegado en determinados supuestos, y su rol resulta clave para garantizar la independencia y la continuidad de la gestión de la privacidad dentro de la entidad (Gesdata Consulting, 2024).

2.8.4 Registro de actividades de tratamiento

El registro de actividades de tratamiento es un inventario documentado de las operaciones que la organización realiza sobre los datos personales, en el que se describen las finalidades, las categorías de datos y de titulares, los destinatarios, los plazos de conservación y las medidas de seguridad aplicadas. El reglamento ecuatoriano exige mantener este registro a los responsables que cuenten con cien o más trabajadores, aunque su elaboración constituye una buena práctica para cualquier organización. Este registro permite demostrar el cumplimiento del principio de responsabilidad proactiva y sirve de base para el análisis de riesgos y la definición de controles (Presidencia de la República del Ecuador, 2023).

2.8.5 Matriz de riesgos y controles

La matriz de riesgos y controles vincula los riesgos identificados sobre los datos personales con las medidas seleccionadas para tratarlos, estableciendo una relación trazable entre las amenazas, las vulnerabilidades, el nivel de riesgo y los controles implementados. Este instrumento permite verificar que cada riesgo relevante cuenta con al menos un control asociado, evaluar el riesgo residual y priorizar las acciones de mejora. Como componente del sistema de gestión, la matriz aporta evidencia del tratamiento del riesgo y facilita el seguimiento por parte de la dirección y de la autoridad de control (Rodríguez, 2022).

2.8.6 Gestión de incidentes y brechas de seguridad

La gestión de incidentes y brechas de seguridad comprende el conjunto de procedimientos destinados a detectar, contener, evaluar y notificar las vulneraciones de seguridad que afecten a los datos personales. La normativa ecuatoriana establece la obligación de notificar las brechas a la autoridad de control en un plazo determinado desde su detección y, cuando el riesgo para los derechos de los titulares sea alto, de comunicar el incidente a los afectados. Contar con un procedimiento formal de gestión de incidentes permite reaccionar oportunamente, reducir el impacto de las brechas y cumplir con las obligaciones de notificación previstas en la ley (Innodev Solutions S.A., 2026).

2.9. Contextualización de la Cooperativa de Ahorro y Crédito Achik Inti Ltda.

Para orientar el diseño del sistema de gestión al caso de estudio, es necesario comprender el contexto del sector financiero popular y solidario en el que opera la Cooperativa, las particularidades del tratamiento de datos personales en las cooperativas de ahorro y crédito, y las características de la entidad objeto del proyecto.

2.9.1 El sector financiero popular y solidario en el Ecuador

Las cooperativas de ahorro y crédito forman parte del sector financiero popular y solidario del Ecuador y se encuentran bajo la supervisión y control de la Superintendencia de Economía Popular y Solidaria, organismo técnico que promueve la sostenibilidad y el correcto funcionamiento de estas entidades para proteger a sus socios. La Superintendencia segmenta a las cooperativas según el nivel de sus activos, lo que determina distintas obligaciones y niveles de cobertura del seguro de depósitos. Este sector concentra a millones de socios en el país y desempeña un papel relevante en la inclusión financiera, lo que hace especialmente sensible la

protección de la información que manejan (Superintendencia de Economía Popular y Solidaria, s. f.).

2.9.2 Tratamiento de datos personales en las cooperativas de ahorro y crédito

Las cooperativas de ahorro y crédito tratan de manera intensiva datos personales y financieros de sus socios, entre ellos datos de identificación, información de contacto, ingresos, historial crediticio y datos de sus operaciones. Por esta razón, deben adecuar sus procesos para cumplir tanto con la normativa de protección de datos personales como con las normas de control de la seguridad de la información aplicables a las entidades del sector financiero popular y solidario, que son complementarias entre sí. El cumplimiento de estas obligaciones exige elaborar inventarios de activos, realizar análisis de riesgos e implementar controles, lo que evidencia la pertinencia de un sistema de gestión estructurado (Díaz, 2025).

2.9.3 La Cooperativa de Ahorro y Crédito Achik Inti Ltda.

La Cooperativa de Ahorro y Crédito Achik Inti Ltda. es una entidad del sector financiero popular y solidario que ofrece servicios de intermediación financiera a sus socios, principalmente la captación de ahorros y la colocación de créditos. Como responsable del tratamiento, la Cooperativa recolecta y gestiona datos personales y financieros de sus socios en el desarrollo de su actividad, lo que la sujeta a las obligaciones de la Ley Orgánica de Protección de Datos Personales y de la normativa de control del sector. En este contexto, el diseño de un sistema de gestión de protección de datos personales le permitirá identificar sus riesgos y brechas, fortalecer sus controles y avanzar hacia el cumplimiento normativo y la seguridad de la información de sus socios (Superintendencia de Economía Popular y Solidaria, s. f.).

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. Enfoque de la investigación

La presente investigación es de tipo aplicada y de carácter proyectivo, por cuanto su propósito final no se limita a describir una realidad, sino que culmina en el diseño de una propuesta concreta: un sistema de gestión de protección de datos personales para la Cooperativa de Ahorro y Crédito Achik Inti Ltda. Responde a un diseño no experimental, dado que las variables no se manipulan sino que se observan en su contexto institucional, y de corte transversal, puesto que la recolección de la información se efectuó en un único momento temporal (julio de 2026). Sobre esta base, el estudio adopta un enfoque mixto con predominio cuantitativo, cuyos componentes se describen a continuación.

El componente cuantitativo se sustenta en la aplicación de un cuestionario tipo lista de verificación (checklist), administrado mediante encuesta estructurada, integrado por cincuenta y cinco preguntas cerradas organizadas en diez dominios temáticos que agrupan, con fines de diagnóstico, controles de las cuatro categorías (organizacionales, de personas, físicos y tecnológicos) de la norma ISO/IEC 27002 en su edición 2022, descrita en el marco teórico. Las respuestas se registran en una escala ordinal de tres valores (Sí / No / En Proceso) que, para efectos del análisis, se cuantifica asignando los valores Sí = 1, En Proceso = 0,5 y No = 0, lo que permite calcular el nivel porcentual de cumplimiento por dominio e identificar brechas de manera objetiva. El instrumento se aplicó bajo la modalidad de censo al personal responsable de las cuatro áreas técnicas de la cooperativa la Dirección de Tecnologías de la Información y los departamentos de Seguridad de la Información, Desarrollo de Software y Soporte Técnico, conforme se detalla en la sección de población y muestra. La validez de contenido del cuestionario se sustenta en la derivación directa de sus ítems a partir de los controles de la norma, y su pertinencia y claridad fueron verificadas mediante juicio de expertos previo a su aplicación.

Dentro del mismo componente cuantitativo, la valoración de los activos de información se realiza mediante una escala numérica de 0 a 10 aplicada a las cinco dimensiones de seguridad definidas por la metodología MAGERIT versión 3: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Esta valoración posibilita jerarquizar los activos según su criticidad y constituye la base del análisis de riesgos desarrollado en este capítulo.

El componente cualitativo emplea la revisión documental como técnica de recolección, y el análisis de contenido, complementado con la comparación normativa, como procedimientos de tratamiento de la información. Se examinaron tres grupos de fuentes: (a) la normativa ecuatoriana de protección de datos personales, integrada por la Ley Orgánica de Protección de Datos Personales, su Reglamento General y las resoluciones de la Superintendencia de Protección de Datos Personales; (b) los estándares internacionales analizados en el marco teórico; y (c) la documentación institucional de la cooperativa, que comprende la descripción de su estructura organizacional y de sus áreas técnicas, el detalle de su infraestructura tecnológica (servidores, equipos de cómputo, redes y sistemas de videovigilancia) y la documentación de sus aplicaciones y servicios digitales. El acceso a la información sobre la infraestructura y los procesos no se limitó a fuentes documentales: se complementó con la ficha de inventario y valoración de activos descrita en la sección de técnicas e instrumentos, elaborada con la participación del personal técnico responsable de cada área.

La combinación de ambos componentes permite triangular tres fuentes de evidencia: los niveles porcentuales de cumplimiento por dominio de control (cuantitativa), la valoración de la criticidad de los activos de información (cuantitativa) y los hallazgos del análisis normativo e institucional (cualitativa). De esta triangulación resulta un diagnóstico integral que constituye el insumo directo para el diseño del sistema de gestión de protección de datos personales, en coherencia con el principio de responsabilidad proactiva y demostrada que exige la LOPDP.

3.2. Nivel de la investigación

La investigación es de nivel descriptivo con alcance proyectivo. Es descriptiva porque caracteriza la situación actual de la cooperativa respecto de la seguridad de la información y del tratamiento de datos personales, a partir de la aplicación de un instrumento de diagnóstico estructurado sobre sus dominios de control, de la valoración de sus activos de información y del análisis de sus prácticas institucionales. Es proyectiva porque, sobre la base del diagnóstico obtenido, se diseña una propuesta técnica y normativa orientada a transformar la situación descrita: el sistema de gestión de protección de datos personales, integrado por políticas, procedimientos, roles, matriz de riesgos y registros de actividades de tratamiento. Ambos niveles se desarrollan bajo el corte transversal señalado en el enfoque de la investigación, al recolectarse la información en un único momento temporal.

3.3. Población y muestra

La población de estudio está conformada por el personal de la Cooperativa de Ahorro y Crédito Achik Inti Ltda. vinculado a la gestión tecnológica y al tratamiento de datos personales. A partir de esta población se seleccionó una muestra intencional y no probabilística de cuatro personas (n = 4), correspondiente al responsable de cada una de las áreas técnicas de la institución: la Dirección de Tecnologías de la Información, el Departamento de Seguridad de la Información, el Departamento de Desarrollo de Software y el Departamento de Soporte Técnico. Los criterios de inclusión aplicados fueron tres: (a) ejercer responsabilidad directa sobre la administración de los sistemas, servicios o datos institucionales; (b) desempeñarse como responsable del área respectiva; y (c) poseer conocimiento de primera mano de la infraestructura tecnológica y de los procesos de tratamiento de datos personales. Dado que el instrumento se aplicó a la totalidad de los responsables que cumplen estos criterios, la muestra coincide con el censo de las áreas técnicas de la cooperativa.

De manera complementaria, se definió como unidad de análisis técnica el conjunto de activos de información de la cooperativa. La identificación de los activos se realizó mediante la ficha de inventario basada en el Catálogo de Elementos de la metodología MAGERIT versión 3 (Libro II), aplicada en sesiones de trabajo con los responsables que integran la muestra y contrastada con la documentación técnica institucional; de este modo, la muestra humana constituye la fuente de información a partir de la cual se construye la unidad de análisis técnica. Como resultado se identificaron veinticuatro activos distribuidos en ocho de las categorías del catálogo estándar de la metodología, aquellas aplicables al contexto institucional; las categorías restantes, como las claves criptográficas [K] o el equipamiento auxiliar [AUX], no registraron activos relevantes en el levantamiento. Estos veinticuatro activos constituyen el objeto de la valoración de criticidad y del posterior análisis de riesgos.

Al tratarse de un muestreo no probabilístico, los hallazgos deben interpretarse como un análisis específico del caso de estudio y no son generalizables a otras entidades del sector; no obstante, esta aproximación resulta pertinente para un estudio de caso orientado al diseño de una propuesta institucional.

3.4. Técnicas e instrumentos de recolección de información

Para el levantamiento de la información se emplearon tres técnicas complementarias: la revisión documental, la encuesta de diagnóstico basada en dominios de la norma ISO/IEC 27002 y la ficha de inventario y valoración de activos conforme a la metodología MAGERIT

versión 3. Estas técnicas materializan el análisis de brechas (GAP analysis) y el levantamiento de procesos descritos en el marco teórico, y proporcionan la evidencia necesaria para el diagnóstico institucional.

3.4.1 Revisión documental

La revisión documental abarcó la normativa ecuatoriana aplicable, los estándares internacionales de referencia (ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27701) y la documentación institucional de la cooperativa relacionada con su infraestructura tecnológica, sus servicios digitales y la organización de sus áreas técnicas. Esta técnica permitió delimitar los requisitos legales y de control que el sistema de gestión debe satisfacer.

3.4.2 Encuesta de diagnóstico basada en la norma ISO/IEC 27002

Como instrumento principal de diagnóstico se aplicó una encuesta estructurada (instrumento código A001, versión 01, aplicada el 23 de julio de 2026), integrada por cincuenta y cinco preguntas cerradas organizadas en diez dominios de diagnóstico adaptados a partir de la norma ISO/IEC 27002. Dichos dominios retoman la estructura temática de la edición 2013 de la norma que organiza sus controles en catorce dominios, de los cuales se seleccionaron y agruparon diez en función de su pertinencia para el contexto de la cooperativa y para los fines del diagnóstico; su contenido es trazable a las cuatro categorías de controles (organizacionales, de personas, físicos y tecnológicos) de la edición 2022 descrita en el marco teórico.

Las respuestas se registran en la escala Sí / No / En Proceso y se cuantifican conforme a la ponderación definida en el enfoque de la investigación (Sí = 1; En Proceso = 0,5; No = 0), lo que permite estimar el nivel porcentual de cumplimiento por dominio. El instrumento fue respondido por los cuatro responsables de las áreas técnicas de la cooperativa (n = 4), y su validez de contenido se sustenta en la derivación directa de los ítems a partir de los controles de la norma, verificada mediante juicio de expertos previo a la aplicación. La Tabla 2 presenta los dominios evaluados y el número de ítems por dominio.

Tabla 2

Dominios de diagnóstico adaptados a partir de la norma ISO/IEC 27002

Dominio evaluado	Ítems	Aspectos considerados
Políticas de la seguridad	4	Existencia, difusión, revisión y conocimiento del documento de políticas de seguridad de la información.
Aspectos organizativos de la seguridad	6	Comité de seguridad, personal especializado, roles y responsabilidades, acuerdos de cooperación, auditorías independientes y contratos con terceros.

Seguridad ligada a los recursos humanos	5	Desvinculación y retiro de accesos, acuerdos de confidencialidad, capacitación, reporte de incidentes y procesos disciplinarios.
Gestión de activos	5	Inventario de activos, clasificación de la información, controles por nivel de protección, etiquetado y protección de medios en tránsito.
Control de accesos	10	Políticas de acceso, niveles de privilegio, auditoría de derechos, uso de la red, acceso a servidores, control de tráfico, monitoreo, cómputo móvil y controles criptográficos.
Seguridad física y ambiental	8	Protección contra desastres y accesos físicos no autorizados, retiro autorizado de equipos, mantenimiento, tratamiento previo al reúso y áreas seguras.
Seguridad en la operativa	9	Documentación de procedimientos, manejo de incidentes, protección contra malware, pruebas de sistemas, respaldos, protección de la red y control de instalación de software.
Seguridad en las telecomunicaciones	3	Protección de la información en redes y en tránsito, y seguridad de la mensajería electrónica.
Gestión de incidentes de seguridad	3	Documentación de debilidades, valoración de eventos y preservación de evidencia.
Cumplimiento	2	Políticas de protección de datos personales y gestión de la propiedad intelectual.

Nota. Elaboración propia a partir del instrumento de diagnóstico aplicado en la Cooperativa de Ahorro y Crédito Achik Inti Ltda. (código A001, versión 01). Total: 55 ítems. Dominios adaptados a partir de la estructura temática de la ISO/IEC 27002:2013 (catorce dominios), agrupados para fines del diagnóstico; su contenido es trazable a las cuatro categorías de controles de la edición 2022.

Los resultados de la aplicación de este instrumento se procesan mediante la cuantificación de la escala descrita en el enfoque de la investigación (Sí = 1; En Proceso = 0,5; No = 0) y el cálculo del nivel de cumplimiento por dominio, lo que permite identificar los controles implementados, los controles ausentes y aquellos que se encuentran en proceso de implementación. Dichos resultados se presentan y analizan en el capítulo IV como insumo del diseño del sistema de gestión.

3.4.3 Ficha de inventario y valoración de activos según MAGERIT

Para la identificación de los activos de información se utiliza una ficha de inventario construida a partir del Catálogo de Elementos de la metodología MAGERIT versión 3 (Libro II). La ficha registra, para cada activo, el código de identificación, la categoría y el tipo según el catálogo, el nombre y la descripción del activo, la cantidad o estado, el responsable o propietario, la ubicación y la valoración de criticidad. La valoración se realiza sobre cinco dimensiones de seguridad: disponibilidad (D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T), mediante una escala de 0 a 10; el valor global del activo corresponde al máximo de las cinco dimensiones. La Tabla 3 presenta la escala de valoración empleada.

Tabla 3

Escala de valoración de la criticidad de los activos

Rango	Nivel	Criterio de interpretación
0 – 1	Despreciable	La afectación del activo resulta irrelevante para la operación institucional.
2 – 3	Bajo	La afectación del activo genera un impacto menor y fácilmente recuperable.
4 – 6	Medio	La afectación del activo perjudica la operación de procesos internos relevantes.
7 – 8	Alto	La afectación del activo compromete servicios institucionales o información importante.
9 – 10	Muy alto / Crítico	La afectación del activo compromete gravemente la operación, la información de los socios o el cumplimiento normativo.

Nota. Adaptado de la metodología MAGERIT versión 3, Libro II — Catálogo de Elementos.

La aplicación de la ficha sobre la infraestructura tecnológica de la cooperativa permitió identificar veinticuatro activos, distribuidos en las categorías del catálogo MAGERIT que se resumen en la Tabla 4.

Tabla 4

Activos identificados en la cooperativa por categoría MAGERIT

Categoría MAGERIT	Activos	Activos identificados
[D] Datos / Información	1	Base de datos institucional de socios, cuentas y transacciones.
[S] Servicios	3	ACHIK EMPRENDE y ACHIK MÓVIL; DIMA COF; página web institucional (www.achikinti.fin.ec).
[SW] Software	4	Aplicaciones ACHIK EMPRENDE y ACHIK MÓVIL (desarrollo propio); DIMA COF (desarrollo a medida); sistema de gestión de bases de datos; sistema operativo CentOS.
[HW] Equipamiento informático	7	Servidores HP DL380 y Proliant ML110; computadora de escritorio; computadora portátil; impresora; cámaras de videovigilancia; routers.
[COM] Redes de comunicaciones	2	Red local (LAN) institucional y conectividad a Internet.
[Media] Soportes de información	1	Discos de almacenamiento de la infraestructura tecnológica.
[L] Instalaciones	1	Centro de datos de la sede institucional.
[P] Personal	5	Director de TI; Departamento de Seguridad de la Información; Departamento de Desarrollo de Software; Departamento de Soporte Técnico; socios (usuarios externos).

Nota. Elaboración propia a partir del inventario de activos MAGERIT v3 de la Cooperativa de Ahorro y Crédito Achik Inti Ltda. Total: 24 activos.

3.5. Metodología de análisis y gestión de riesgos: MAGERIT versión 3

Para el componente de gestión de riesgos del sistema propuesto se seleccionó la metodología MAGERIT versión 3, elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España. Su elección se fundamenta en tres criterios: primero, es

plenamente compatible con las normas ISO/IEC 27005 e ISO 31000 analizadas en el marco teórico, por lo que se integra sin fricciones con el enfoque basado en la LOPDP, la ISO/IEC 27001 y la ISO/IEC 27701 seleccionado en el cuadro comparativo del capítulo II; segundo, ofrece un catálogo estructurado de tipos de activos, amenazas y salvaguardas (Libro II) que sistematiza y hace repetible el proceso de identificación; y tercero, es una metodología pública, documentada en español y de amplia adopción en entidades financieras y de la administración pública hispanoamericana, lo que facilita su comprensión y sostenibilidad dentro de la cooperativa.

El proceso de análisis de riesgos se desarrolla en cinco fases: (a) caracterización y valoración de los activos, mediante la ficha de inventario descrita en la sección anterior; (b) identificación de las amenazas que pueden afectar a cada activo, a partir del catálogo de amenazas de MAGERIT; (c) identificación de las salvaguardas existentes, contrastadas con los resultados de la encuesta de diagnóstico ISO/IEC 27002; (d) estimación del impacto y del riesgo, en función del valor del activo, la probabilidad de la amenaza y la eficacia de las salvaguardas; y (e) propuesta de tratamiento del riesgo, que alimenta directamente la matriz de riesgos y controles del sistema de gestión. En el presente trabajo, las fases (a) y (b) forman parte del diagnóstico institucional, mientras que las fases restantes se desarrollan como parte de la propuesta del capítulo IV.

La Tabla 5 presenta el inventario de activos de la cooperativa con su valoración por dimensiones. Los resultados evidencian que los activos esenciales de la institución son la base de datos institucional, los servicios y aplicaciones ACHIK EMPRENDE y ACHIK MÓVIL, el sistema de gestión de bases de datos y el Departamento de Seguridad de la Información, todos con valor global de criticidad de 10, lo que confirma que la información de los socios y los servicios que la tratan constituyen el núcleo a proteger por el sistema de gestión de protección de datos personales.

Tabla 5

Inventario y valoración de activos de la Cooperativa de Ahorro y Crédito Achik Inti Ltda

Código	Activo	Categoría	D	I	C	A	T	Valor global
ACT-D-01	Base de datos institucional	[D] Datos	9	10	10	10	9	10
ACT-S-01	ACHIK EMPRENDE y ACHIK MÓVIL	[S] Servicios	9	10	10	10	9	10
ACT-S-02	DIMA COF	[S] Servicios	8	9	9	9	9	9
ACT-S-03	Página web institucional	[S] Servicios	8	8	6	8	7	8
ACT-SW-01	ACHIK EMPRENDE y ACHIK MÓVIL (desarrollo propio)	[SW] Software	9	10	10	10	9	10

ACT-SW-02	DIMA COF (desarrollo a medida)	[SW] Software	8	9	9	8	8	9
ACT-SW-03	Sistema de gestión de base de datos	[SW] Software	9	10	10	9	9	10
ACT-SW-04	Sistema operativo CentOS	[SW] Software	8	8	7	7	7	8
ACT-HW-01	Servidor HP DL380	[HW] Hardware	9	9	9	9	8	9
ACT-HW-02	Servidor Proliant ML110	[HW] Hardware	8	8	8	8	7	8
ACT-HW-03	Computadora de escritorio (CPU LG)	[HW] Hardware	6	6	7	5	5	7
ACT-HW-04	Computadora portátil Lenovo (Ryzen 5)	[HW] Hardware	6	6	7	5	5	7
ACT-HW-05	Impresora Epson M128 C	[HW] Hardware	4	4	4	3	3	4
ACT-HW-06	Cámaras de videovigilancia (CCTV)	[HW] Hardware	7	6	8	6	7	8
ACT-HW-07	Routers (AMSR 900, AMSR 901, Mikrotik)	[HW] Hardware	8	7	7	7	6	8
ACT-COM-01	Red local (LAN)	[COM] Redes	9	8	7	6	6	9
ACT-COM-02	Conectividad a Internet	[COM] Redes	9	7	6	7	7	9
ACT-MEDIA-01	Almacenamiento (discos)	[Media] Soportes	8	8	9	5	5	9
ACT-L-01	Centro de datos	[L] Instalaciones	9	6	8	5	6	9
ACT-P-01	Director de Tecnologías de la Información	[P] Personal	8	8	9	8	8	9
ACT-P-02	Departamento de Seguridad de la Información	[P] Personal	8	8	10	8	8	10
ACT-P-03	Departamento de Desarrollo de Software	[P] Personal	7	8	8	7	7	8
ACT-P-04	Departamento de Soporte Técnico	[P] Personal	7	7	7	6	6	7
ACT-P-05	Socios de la cooperativa (usuarios externos)	[P] Personal	7	7	8	7	6	8

Nota. Elaboración propia a partir del inventario de activos MAGERIT v3. D = disponibilidad; I = integridad; C = confidencialidad; A = autenticidad; T = trazabilidad. Escala 0–10; el valor global corresponde al máximo de las cinco dimensiones. Las valoraciones son estimaciones preliminares sujetas a validación con el propietario de cada activo.

3.6. Fases metodológicas de la investigación

El desarrollo del proyecto se organiza en cuatro fases secuenciales, cada una vinculada a un objetivo específico de la investigación. La primera fase corresponde al estudio teórico y normativo, desarrollado mediante revisión documental y materializado en el marco teórico del capítulo II. La segunda fase corresponde al análisis comparativo de la LOPDP, la ISO/IEC 27001, la ISO/IEC 27701 y la gestión de riesgos, del cual se derivó el enfoque metodológico del proyecto, complementado en este capítulo con la selección de MAGERIT como metodología de análisis de riesgos. La tercera fase corresponde al diagnóstico institucional, ejecutado mediante la encuesta ISO/IEC 27002 y el inventario y valoración de activos MAGERIT. La cuarta fase corresponde al diseño del sistema de gestión de protección de datos personales, que integra los productos de las fases anteriores. La Tabla 6 sintetiza esta correspondencia.

Tabla 6

Fases metodológicas del proyecto y su correspondencia con los objetivos específicos

Fase	Objetivo específico asociado	Técnicas e instrumentos	Producto

Fase 1	Realizar el estudio teórico y normativo sobre protección de datos personales y datos crediticios.	Revisión documental de literatura científica, normativa ecuatoriana y estándares internacionales.	Marco teórico y normativo (capítulo II).
Fase 2	Analizar metodologías y marcos de referencia aplicables a la gestión de protección de datos personales.	Matriz comparativa LOPDP – ISO/IEC 27001 – ISO/IEC 27701 – gestión de riesgos; selección de MAGERIT v3.	Enfoque metodológico del proyecto.
Fase 3	Diagnosticar la situación actual de la cooperativa sobre el tratamiento de datos personales.	Encuesta de diagnóstico ISO/IEC 27002 (55 ítems, 10 dominios); ficha de inventario y valoración de activos MAGERIT (24 activos).	Diagnóstico de brechas de control y mapa de activos críticos.
Fase 4	Diseñar el sistema de gestión de protección de datos personales.	Síntesis del diagnóstico; catálogos de amenazas y salvaguardas MAGERIT; requisitos LOPDP.	Políticas, procedimientos, roles, matriz de riesgos y registro de actividades de tratamiento (capítulo IV).

Nota. Elaboración propia.

De esta manera, el marco metodológico articula los instrumentos aplicados en la cooperativa con los estándares y la normativa analizados en el marco teórico, y garantiza que el diseño del sistema de gestión propuesto en el capítulo siguiente se sustente en evidencia diagnóstica verificable y en una metodología de análisis de riesgos reconocida.

CAPÍTULO IV

4. PROPUESTA

4.1. Presentación de la propuesta

El presente capítulo desarrolla la propuesta del proyecto: el diseño del Sistema de Gestión de Protección de Datos Personales (SGPD) para la Cooperativa de Ahorro y Crédito Achik Inti Ltda. En primer lugar se presentan y analizan los resultados del diagnóstico institucional ejecutado en el Capítulo III mediante la encuesta ISO/IEC 27002 y el inventario de activos MAGERIT; a continuación se completan las fases de análisis de riesgos —identificación de amenazas, estimación del riesgo y tratamiento— y, finalmente, se diseñan los componentes del sistema de gestión: la estructura documental, la política de protección de datos, los roles y responsabilidades, el registro de actividades de tratamiento, los

procedimientos de atención de derechos y de gestión de incidentes, y el ciclo de mejora continua. De este modo, la propuesta corresponde a la cuarta fase metodológica y da cumplimiento al objetivo general de la investigación.

4.2. Resultados del diagnóstico institucional

4.2.1 Nivel de cumplimiento por dominio de control

La encuesta de diagnóstico (instrumento A001) se aplicó a los cuatro responsables de las áreas técnicas de la cooperativa. Las respuestas se cuantificaron según la ponderación definida en el Capítulo III (Sí = 1; En Proceso = 0,5; No = 0) y se calculó el nivel de cumplimiento por dominio como el cociente entre la puntuación obtenida y el número de ítems del dominio. La Tabla 7 resume estos resultados.

Tabla 7

Nivel de cumplimiento por dominio de control de la norma ISO/IEC 27002

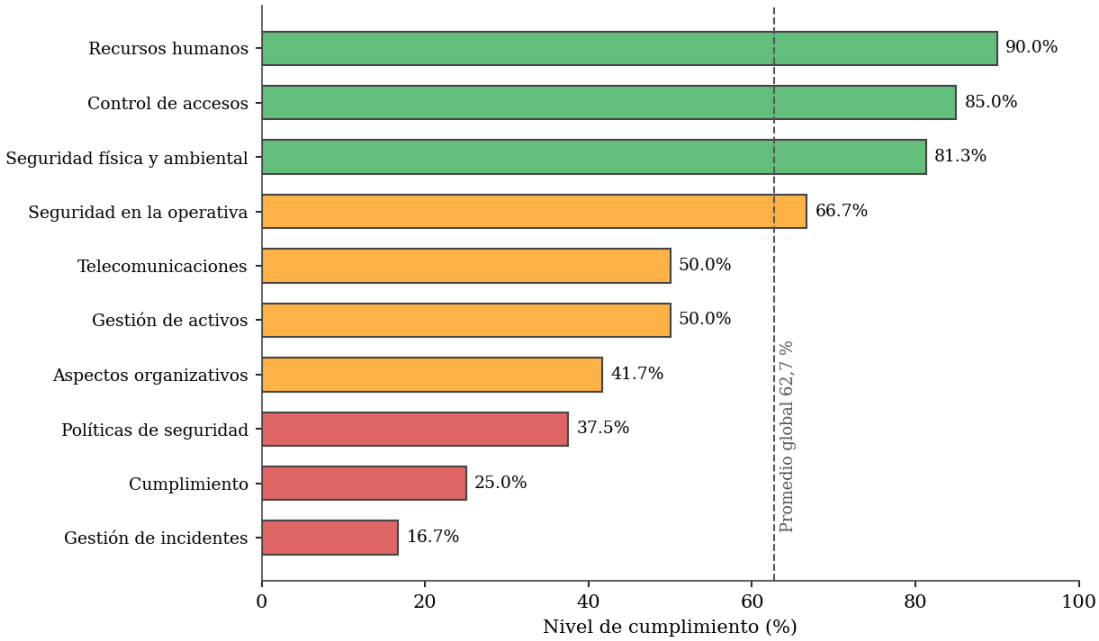
Dominio	Ítems	Sí	En proceso	No	Punt.	% cumpl.
Políticas de la seguridad	4	1	1	2	1,5	37,5
Aspectos organizativos de la seguridad	6	2	1	3	2,5	41,7
Seguridad ligada a los recursos humanos	5	4	1	0	4,5	90,0
Gestión de activos	5	2	1	2	2,5	50,0
Control de accesos	10	8	1	1	8,5	85,0
Seguridad física y ambiental	8	6	1	1	6,5	81,3
Seguridad en la operativa	9	5	2	2	6,0	66,7
Seguridad en las telecomunicaciones	3	1	1	1	1,5	50,0
Gestión de incidentes de seguridad	3	0	1	2	0,5	16,7
Cumplimiento	2	0	1	1	0,5	25,0
Total	55	29	11	15	34,5	62,7

Nota. Elaboración propia a partir del instrumento A001 (versión 01) aplicado el 23 de julio de 2026. Puntuación ponderada: Sí = 1; En Proceso = 0,5; No = 0. El porcentaje corresponde a la puntuación sobre el total de ítems del dominio.

El nivel de cumplimiento global de la cooperativa es del 62,7 %, lo que refleja una entidad con controles operativos consolidados pero con brechas relevantes en su gobierno de la seguridad y en la protección de los datos personales. La Figura 1 ordena los dominios de menor a mayor cumplimiento.

Figura 1

Nivel de cumplimiento por dominio de control



Nota. Elaboración propia a partir de los resultados del instrumento A001. La línea discontinua indica el promedio global (62,7 %).

Las mayores fortalezas se concentran en la seguridad ligada a los recursos humanos (90,0 %), el control de accesos (85,0 %) y la seguridad física y ambiental (81,3 %), lo que evidencia que la cooperativa dispone de mecanismos operativos para proteger sus sistemas, equipos e instalaciones. En contraste, las brechas críticas se localizan en la gestión de incidentes de seguridad (16,7 %), el cumplimiento (25,0 %) y las políticas de la seguridad (37,5 %). Resulta determinante que, en el dominio de cumplimiento, el control relativo a la política de protección de datos personales se encuentre únicamente en proceso: este hallazgo confirma el problema planteado en el Capítulo I y justifica el diseño del SGPD, orientado a formalizar las políticas, los procedimientos, los roles y los controles que permitan a la cooperativa demostrar responsabilidad proactiva conforme a la LOPDP.

4.2.2 Identificación de los activos críticos

A partir de la valoración de los veinticuatro activos inventariados en el Capítulo III (Tabla 5), se identificaron trece activos con valor global de criticidad igual o superior a 9, que constituyen el núcleo a proteger por el sistema de gestión. La Tabla 8 los presenta ordenados por criticidad.

Tabla 8

Activos críticos de la Cooperativa de Ahorro y Crédito Achik Inti Ltda

Código	Activo	Categoría	Valor global
ACT-D-01	Base de datos institucional	[D] Datos	10
ACT-S-01	ACHIK EMPRENDE y ACHIK MÓVIL	[S] Servicios	10
ACT-SW-01	ACHIK EMPRENDE y ACHIK MÓVIL (desarrollo propio)	[SW] Software	10
ACT-SW-03	Sistema de gestión de base de datos	[SW] Software	10
ACT-P-02	Departamento de Seguridad de la Información	[P] Personal	10
ACT-S-02	DIMA COF	[S] Servicios	9
ACT-SW-02	DIMA COF (desarrollo a medida)	[SW] Software	9
ACT-HW-01	Servidor HP DL380	[HW] Hardware	9
ACT-COM-01	Red local (LAN)	[COM] Redes	9
ACT-COM-02	Conectividad a Internet	[COM] Redes	9
ACT-MEDIA-01	Almacenamiento (discos)	[Media] Soportes	9
ACT-L-01	Centro de datos	[L] Instalaciones	9
ACT-P-01	Director de Tecnologías de la Información	[P] Personal	9

Nota. Elaboración propia a partir de la Tabla 5 (Capítulo III). Se incluyen los activos con valor global ≥ 9. D = disponibilidad; I = integridad; C = confidencialidad; A = autenticidad; T = trazabilidad.

Los activos esenciales corresponden a la información y a los servicios que la tratan: la base de datos institucional, las aplicaciones ACHIK EMPRENDE y ACHIK MÓVIL, el sistema de gestión de base de datos y el Departamento de Seguridad de la Información alcanzan la criticidad máxima, con la confidencialidad y la integridad como dimensiones predominantes. En torno a ellos se articulan los activos de soporte críticos: el servidor HP DL380, la red local, la conectividad a Internet, los soportes de almacenamiento, el centro de datos y el personal técnico. Esta jerarquía determina el orden de prioridad del análisis de riesgos.

4.3. Análisis de riesgos

Completando las fases (c), (d) y (e) del proceso MAGERIT descrito en el Capítulo III, se identificaron las amenazas del catálogo de la metodología aplicables a los activos críticos, se estimó su probabilidad e impacto y se determinó el nivel de riesgo. La probabilidad se estimó considerando las brechas del diagnóstico: la ausencia o debilidad de un control eleva la probabilidad de las amenazas asociadas.

4.3.1 Escalas de probabilidad, impacto y nivel de riesgo

Tabla 9

Escalas de probabilidad, impacto y niveles de riesgo

Valor	Probabilidad / Impacto	Nivel de riesgo	Rango (P × I)
1	Muy baja / Muy bajo	Bajo	1 – 4
2	Baja / Bajo	Medio	5 – 9
3	Media / Medio	Alto	10 – 15
4	Alta / Alto	Crítico	16 – 25
5	Muy alta / Muy alto		

Nota. Elaboración propia con base en MAGERIT v3 e ISO/IEC 27005. El nivel de riesgo resulta del producto de la probabilidad por el impacto.

4.3.2 Matriz de riesgos

La Tabla 10 presenta la matriz de riesgos de los activos críticos, con catorce riesgos codificados de R01 a R14. La Figura 2 los ubica en el mapa de calor probabilidad–impacto y la Figura 3 resume su distribución por nivel.

Tabla 10

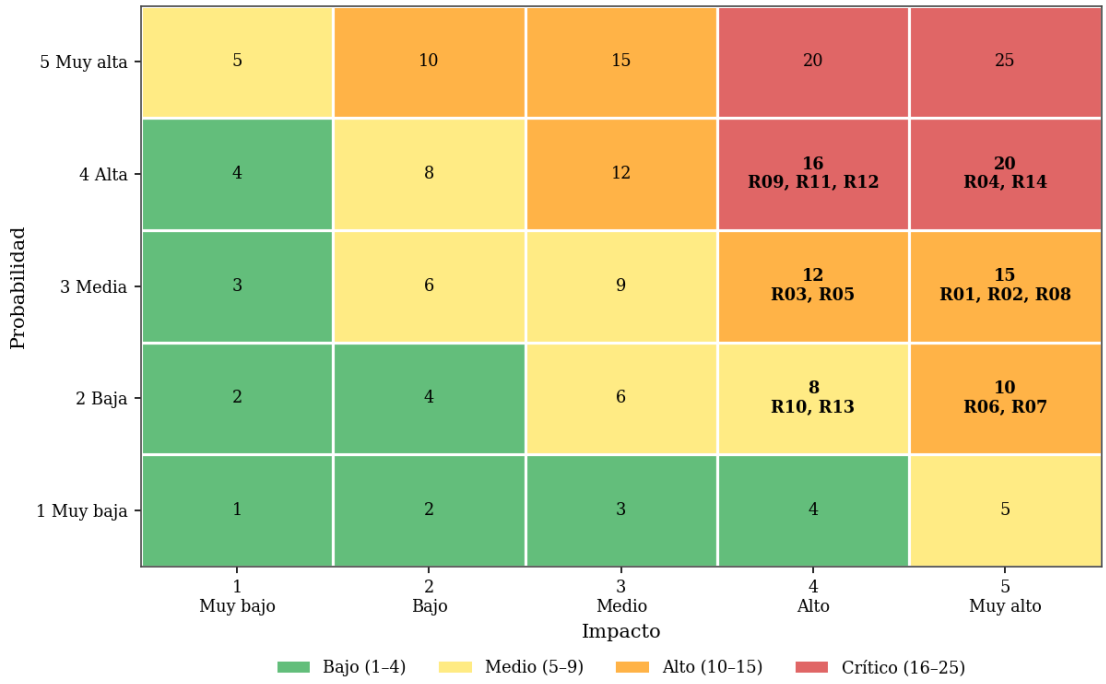
Matriz de riesgos de los activos críticos

Cód.	Activo afectado	Amenaza (MAGERIT)	P	I	P×I	Nivel
R01	ACT-D-01 Base de datos	[A.11] Acceso no autorizado	3	5	15	Alto
R02	ACT-D-01 Base de datos	[A.19] Divulgación de información	3	5	15	Alto
R03	ACT-SW-03 SGBD	[E.2] Errores del administrador	3	4	12	Alto
R04	ACT-S-01 / SW-01 ACHIK	[A.8] Difusión de software dañino	4	5	20	Crítico
R05	ACT-S-01 ACHIK MÓVIL	[A.24] Denegación de servicio	3	4	12	Alto
R06	ACT-SW-03 SGBD	[I.5] Avería de origen físico o lógico	2	5	10	Alto
R07	ACT-HW-01 Servidor	[N.1]/[N.2] Fuego y daños por agua	2	5	10	Alto
R08	ACT-MEDIA-01 Discos	[A.25] Robo de soportes sin cifrado	3	5	15	Alto
R09	Equipos y soportes	[E.18] Borrado no seguro en desincorporación	4	4	16	Crítico
R10	ACT-COM-01 LAN	[A.11] Acceso no autorizado a la red	2	4	8	Medio
R11	Mensajería electrónica	[A.14] Interceptación de información	4	4	16	Crítico
R12	ACT-P Personal	[E.19] Fugas de información por error	4	4	16	Crítico
R13	ACT-L-01 Centro de datos	[A.7] Acceso físico no previsto	2	4	8	Medio
R14	Institucional (cumplimiento)	Incumplimiento de la LOPDP por ausencia de política	4	5	20	Crítico

Nota. Elaboración propia. P = probabilidad; I = impacto. Las probabilidades reflejan las brechas del diagnóstico del Capítulo IV.

Figura 2

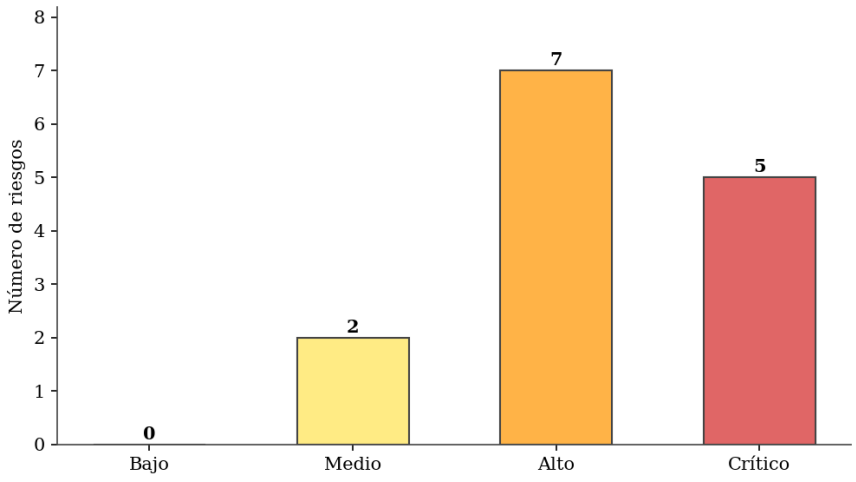
Mapa de calor probabilidad–impacto de los riesgos identificados



Nota. Elaboración propia. Los códigos R01–R14 corresponden a la Tabla 10.

Figura 3

Distribución de los riesgos por nivel



Nota. Elaboración propia a partir de la Tabla 10.

El análisis arroja cinco riesgos críticos (R04, R09, R11, R12 y R14), siete altos y dos medios, sin riesgos de nivel bajo. La concentración de riesgos en los cuadrantes superiores

confirma la exposición de los datos personales de los socios y la necesidad de un tratamiento estructurado que priorice los activos esenciales.

4.4. Tratamiento del riesgo y selección de salvaguardas

Para cada riesgo se definió la opción de tratamiento —mitigar, transferir, evitar o aceptar— y se seleccionaron salvaguardas con base en los controles de la norma ISO/IEC 27002:2022, los controles de privacidad de la ISO/IEC 27701 y las obligaciones de la LOPDP y su Reglamento General, conforme resume la Tabla 11.

Tabla 11

Plan de tratamiento del riesgo y salvaguardas propuestas

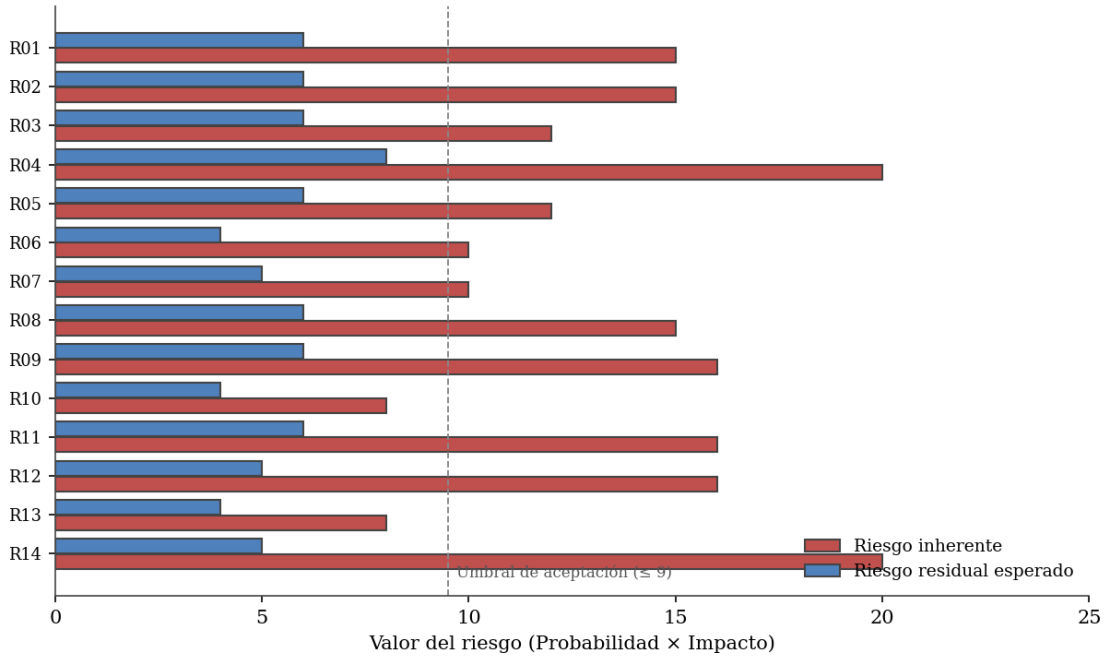
Riesgo	Tratamiento	Salvaguardas principales	Referencia normativa
R01	Mitigar	Gestión de identidades y accesos, autenticación multifactor y revisión de privilegios	ISO/IEC 27002: 5.15–5.18, 8.2
R02	Mitigar	Clasificación de la información, acuerdos de confidencialidad y prevención de fuga de datos	ISO/IEC 27002: 5.12, 5.13, 8.12; 27701
R03	Mitigar	Segregación de funciones, registro y monitoreo de actividades y gestión de cambios	ISO/IEC 27002: 5.3, 8.15, 8.32
R04	Mitigar	Protección contra malware, gestión de vulnerabilidades y actualización de plataformas	ISO/IEC 27002: 8.7, 8.8
R05	Mitigar	Gestión de capacidad, redundancia y protección perimetral de los servicios digitales	ISO/IEC 27002: 8.6, 8.20–8.22
R06	Mitigar	Política de respaldos con verificación periódica y plan de recuperación	ISO/IEC 27002: 8.13, 8.14
R07	Transferir / mitigar	Protección física del centro de datos, detección de incendios y aseguramiento	ISO/IEC 27002: 7.1–7.5, 7.8, 7.11
R08	Mitigar	Política de criptografía y cifrado de soportes de almacenamiento	ISO/IEC 27002: 8.24; Reglamento LOPDP
R09	Mitigar	Procedimiento de borrado seguro y disposición final de equipos y soportes	ISO/IEC 27002: 7.14, 8.10
R10	Mitigar	Segmentación de la red y control de acceso a los servicios de red	ISO/IEC 27002: 8.20–8.22
R11	Mitigar	Cifrado del canal y protección de la mensajería electrónica	ISO/IEC 27002: 5.14, 8.24
R12	Mitigar	Programa permanente de capacitación y concienciación	ISO/IEC 27002: 6.3; LOPDP
R13	Mitigar	Control de acceso físico, bitácoras y videovigilancia del centro de datos	ISO/IEC 27002: 7.1–7.4
R14	Mitigar	Implementación integral del SGPD: política, delegado de protección de datos, RAT y EIPD	LOPDP y Reglamento; ISO/IEC 27701

Nota. Elaboración propia. Las salvaguardas se priorizan según el nivel de riesgo, atendiendo primero los riesgos críticos (R04, R09, R11, R12 y R14).

La Figura 4 compara el riesgo inherente estimado con el riesgo residual esperado tras aplicar las salvaguardas. Con el plan de tratamiento, los catorce riesgos se reducirían a valores iguales o inferiores al umbral de aceptación institucional (valor 9), quedando el riesgo residual sujeto a la aprobación de la dirección y al monitoreo del ciclo de mejora continua.

Figura 4

Comparación entre el riesgo inherente y el riesgo residual esperado



Nota. Elaboración propia. El riesgo residual es una estimación sujeta a verificación durante la implementación.

4.5. Diseño del sistema de gestión de protección de datos personales

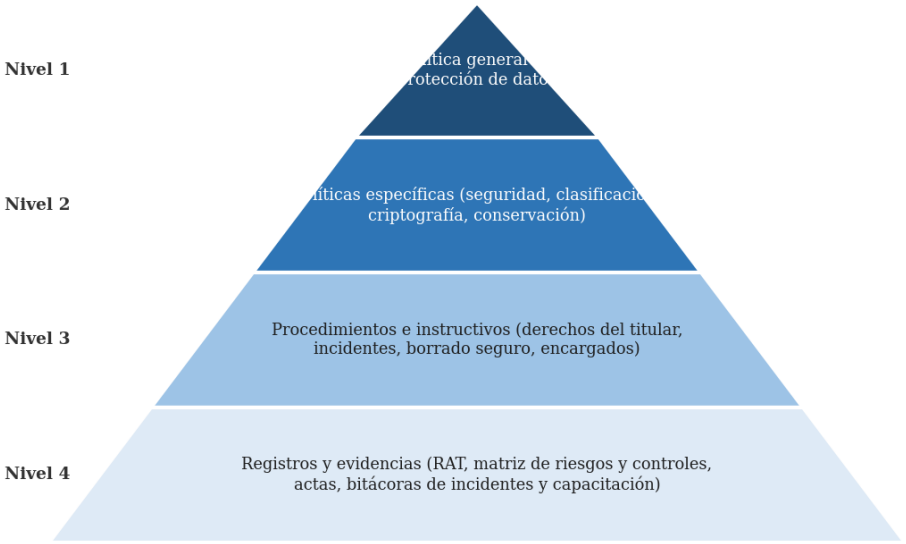
El sistema de gestión traduce las salvaguardas seleccionadas en componentes documentales y organizativos verificables, conforme a los componentes descritos en el marco teórico del Capítulo II.

4.5.1 Estructura documental del sistema

La documentación se organiza en cuatro niveles jerárquicos, como muestra la Figura 5: la política general aprobada por la alta dirección, las políticas específicas que la desarrollan, los procedimientos e instructivos operativos y los registros que evidencian el cumplimiento. Esta estructura garantiza la trazabilidad entre el compromiso institucional y la operación diaria.

Figura 5

Estructura documental del sistema de gestión de protección de datos personales



Nota. Elaboración propia con base en la estructura de alto nivel de la ISO/IEC 27001.

4.5.2 Política de protección de datos personales

La política general declara el compromiso de la cooperativa con el tratamiento lícito, leal y transparente de los datos personales y establece: el alcance del sistema; los principios rectores del tratamiento conforme a la LOPDP; las bases de legitimación admitidas; los lineamientos para la atención de los derechos de los titulares; las condiciones para la contratación de encargados; y el compromiso de revisión periódica. Debe ser aprobada por el Consejo de Administración, comunicada al personal y publicada para conocimiento de los socios. Su desarrollo íntegro se recoge en el Manual de Políticas de Protección de Datos Personales que acompaña a esta propuesta.

4.5.3 Roles y responsabilidades

La Tabla 12 define la matriz de roles del sistema, en la que destaca la designación del delegado de protección de datos como asesor, supervisor y punto de contacto con la autoridad de control y con los titulares.

Tabla 12

Matriz de roles y responsabilidades del sistema de gestión

Rol	Responsabilidades principales
Consejo de Administración y Gerencia	Aprobar la política, asignar recursos y revisar periódicamente el desempeño del sistema.
Delegado de Protección de Datos	Asesorar y supervisar el cumplimiento de la LOPDP, gestionar la relación con la SPDP y atender a los titulares.
Dirección de Tecnologías de la Información	Implementar los controles técnicos y administrar accesos, respaldos e infraestructura.
Departamento de Seguridad de la Información	Gestionar riesgos e incidentes, monitorear controles y mantener la matriz de riesgos.
Departamentos de Desarrollo y Soporte	Aplicar la privacidad desde el diseño y atender los requerimientos técnicos de los tratamientos.
Todo el personal	Cumplir las políticas, guardar confidencialidad y reportar incidentes o debilidades.

Nota. Elaboración propia con base en la LOPDP, su Reglamento General y la norma ISO/IEC 27701.

4.5.4 Registro de actividades de tratamiento

El registro de actividades de tratamiento (RAT) inventaría los tratamientos de datos personales de la cooperativa y constituye la evidencia central del principio de responsabilidad proactiva. La Tabla 13 presenta el registro inicial de los cinco tratamientos principales.

Tabla 13

Registro inicial de actividades de tratamiento

Actividad	Finalidad	Categorías de datos	Base de legitimación	Conservación
Afiliación y gestión de socios	Vinculación y administración de cuentas	Identificación, contacto y socioeconómicos	Ejecución del contrato y consentimiento	Vigencia más plazos legales
Crédito (DIMA COF)	Evaluación crediticia, concesión y cobranza	Financieros y crediticios	Contrato y obligación legal	Plazos regulatorios y contables
Banca digital (ACHIK MÓVIL y EMPRENDE)	Servicios financieros digitales	Identificación, credenciales y transaccionales	Ejecución del contrato	Vigencia de la relación
Videovigilancia (CCTV)	Seguridad de personas e instalaciones	Imagen	Interés legítimo	Período limitado definido en la política
Talento humano	Administración laboral y de nómina	Identificación, laborales y de salud (sensibles)	Obligación legal y contrato	Plazos de la normativa laboral

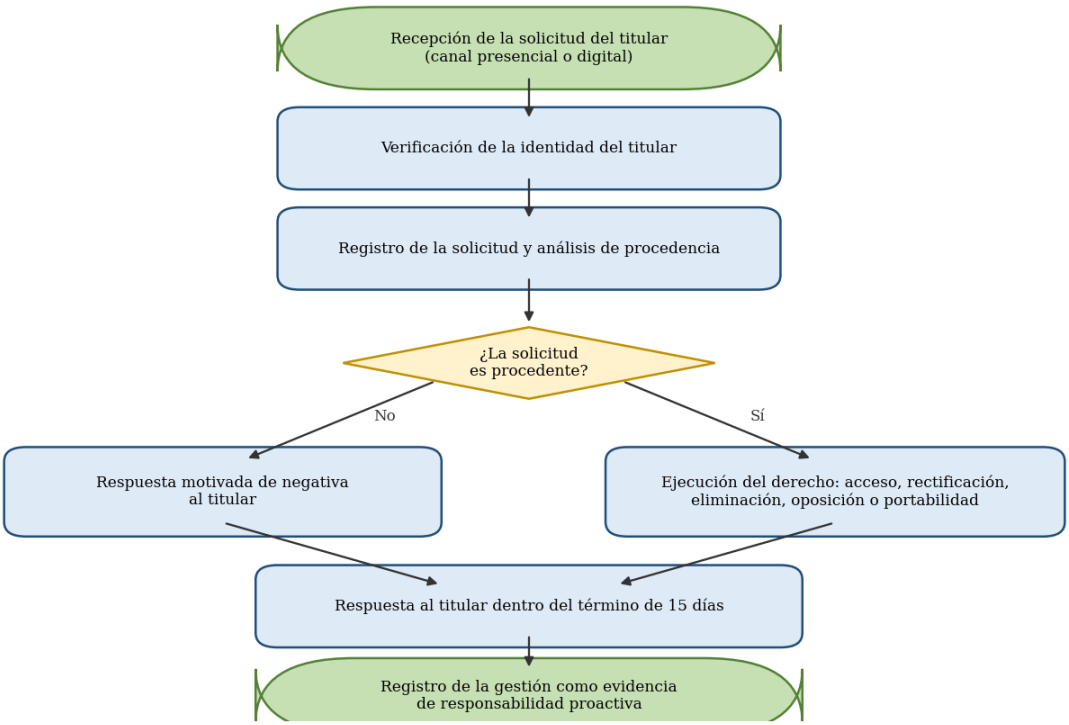
Nota. Elaboración propia. El registro debe completarse con los destinatarios, las transferencias y las medidas de seguridad de cada tratamiento, conforme al Reglamento General de la LOPDP.

4.5.5 Procedimiento de atención de los derechos de los titulares

El procedimiento formaliza la atención de los derechos de acceso, rectificación y actualización, eliminación, oposición, portabilidad y demás derechos reconocidos por la LOPDP, garantizando la respuesta dentro del término de quince días previsto en el Reglamento General y el registro de cada gestión como evidencia. La Figura 6 presenta el flujo propuesto.

Figura 6

Flujograma del procedimiento de atención de los derechos de los titulares



Nota. Elaboración propia con base en los derechos y plazos establecidos en la LOPDP.

4.5.6 Gestión de incidentes y brechas de seguridad

El procedimiento de gestión de incidentes establece las etapas de detección y reporte interno, contención, evaluación del riesgo para los derechos de los titulares, notificación a la Superintendencia de Protección de Datos Personales dentro del término previsto en el Reglamento General a la LOPDP, comunicación a los titulares afectados en los casos de alto riesgo, erradicación, recuperación y registro del incidente con las lecciones aprendidas. Este componente atiende directamente la brecha más severa del diagnóstico (16,7 % en gestión de incidentes) y se articula con las salvaguardas de los riesgos R04, R11 y R12.

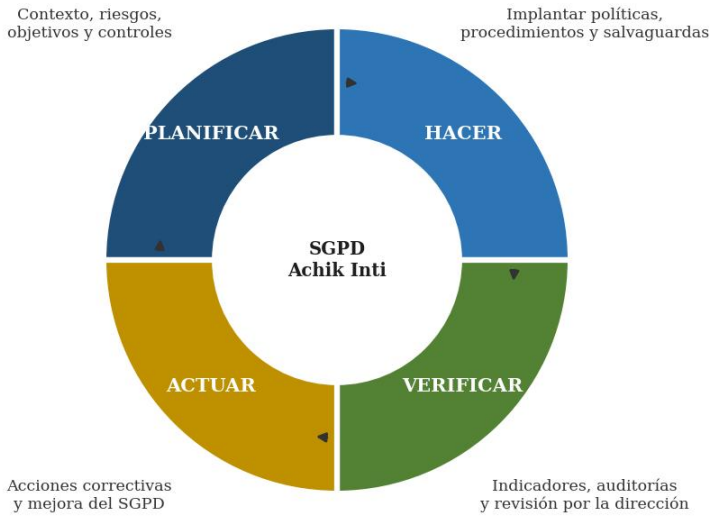
4.5.7 Mejora continua del sistema

El sistema opera bajo el ciclo Planificar–Hacer–Verificar–Actuar, como ilustra la Figura 7: la planificación comprende el diagnóstico, la valoración de activos y la matriz de riesgos; el hacer corresponde a la implantación de las políticas, los procedimientos y las salvaguardas; la verificación se sustenta en indicadores, auditorías internas y la revisión por la dirección; y el actuar recoge las acciones correctivas y las oportunidades de mejora, reiniciando

el ciclo. Así, el sistema evoluciona su madurez y se adapta a los cambios normativos, tecnológicos y organizacionales.

Figura 7

Ciclo de mejora continua PHVA aplicado al sistema de gestión



Nota. Elaboración propia con base en la estructura de la ISO/IEC 27001 y el ciclo PHVA.

4.6. Cumplimiento de los objetivos de la investigación

La Tabla 14 sintetiza la correspondencia entre los objetivos específicos, los productos obtenidos y su ubicación en el documento, evidenciando el cumplimiento del objetivo general.

Tabla 14

Cumplimiento de los objetivos específicos de la investigación

Objetivo específico	Producto obtenido	Ubicación
Realizar el estudio teórico y normativo sobre protección de datos personales y datos crediticios.	Marco teórico que integra la LOPDP, su Reglamento y la familia ISO/IEC 27000.	Capítulo II
Analizar metodologías y marcos de referencia aplicables y seleccionar el enfoque metodológico.	Matriz comparativa LOPDP–27001–27701–gestión de riesgos y selección de MAGERIT v3.	Capítulos II y III
Diagnosticar la situación actual del tratamiento de datos personales en la cooperativa.	Diagnóstico por diez dominios (62,7 % de cumplimiento) e inventario de 24 activos con 13 activos críticos.	Capítulos III y IV
Diseñar el sistema de gestión de protección de datos personales.	Matriz de 14 riesgos, plan de tratamiento, política, roles, RAT, procedimientos y ciclo PHVA.	Capítulo IV

Nota. Elaboración propia.

En conjunto, la propuesta transforma los hallazgos del diagnóstico en un sistema de gestión estructurado: los cinco riesgos críticos cuentan con salvaguardas priorizadas, la brecha del dominio de cumplimiento se atiende mediante la política de protección de datos y el registro de actividades de tratamiento, y la sostenibilidad del sistema queda garantizada por el ciclo de mejora continua y la asignación formal de roles. Con ello se da cumplimiento al objetivo general de diseñar un sistema de gestión de protección de datos personales que fortalezca el cumplimiento legal, la seguridad de la información y la protección de los datos de socios, clientes y colaboradores de la Cooperativa de Ahorro y Crédito Achik Inti Ltda.

Conclusiones

El estudio teórico y normativo permitió establecer el marco conceptual y legal que sustenta la protección de datos personales en la Cooperativa. Se determinó que la Ley Orgánica de Protección de Datos Personales y su Reglamento General definen las obligaciones exigibles y los derechos de los titulares, mientras que las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27701 aportan la estructura y los controles para gestionar la seguridad y la privacidad de la información; ambos planos convergen en la gestión de riesgos como el proceso que dota de proporcionalidad a las medidas. Asimismo, se evidenció que el tratamiento de los datos crediticios y financieros de los socios constituye información especialmente sensible en el sector financiero popular y solidario, lo que confirma la pertinencia de un tratamiento normativo y técnico integrado como base del sistema de gestión.

El análisis comparativo de la LOPDP, la ISO/IEC 27001, la ISO/IEC 27701 y la gestión de riesgos demostró que la diferencia decisiva entre estas referencias no radica en el objeto de protección, sino en su nivel de prescripción: la ley determina resultados obligatorios y las normas técnicas prescriben los procesos para alcanzarlos. De este análisis se derivó un enfoque metodológico integrado que articula ambos planos, y se seleccionó la metodología MAGERIT versión 3 para el componente de gestión de riesgos, por su compatibilidad con las normas ISO/IEC 27005 e ISO 31000, su catálogo estructurado de activos, amenazas y salvaguardas, y su amplia adopción en entidades financieras y públicas. Con ello se dispuso de un marco metodológico coherente y replicable para el diseño del sistema.

El diagnóstico de la situación actual reveló un nivel global de cumplimiento del 62,7 % respecto de los controles evaluados, con fortalezas en la seguridad ligada a los recursos humanos (90,0 %), el control de accesos (85,0 %) y la seguridad física y ambiental (81,3 %), y brechas críticas en la gestión de incidentes de seguridad (16,7 %), el cumplimiento (25,0 %) y las políticas de la seguridad (37,5 %). El inventario de activos identificó veinticuatro activos,

de los cuales trece resultaron críticos, encabezados por la base de datos institucional y las aplicaciones ACHIK EMPRENDE y ACHIK MÓVIL, con la valoración de criticidad máxima. El hecho de que el control relativo a la política de protección de datos personales se encontrara únicamente en proceso confirmó el problema que originó la investigación y permitió priorizar los catorce riesgos identificados, cinco de ellos de nivel crítico.

El sistema de gestión de protección de datos personales diseñado integra los componentes necesarios para que la Cooperativa gestione el tratamiento de datos conforme a la LOPDP: la estructura documental, la política de protección de datos, la matriz de roles con la figura del delegado de protección de datos, el registro de actividades de tratamiento, la matriz de riesgos y controles, los procedimientos de atención de los derechos de los titulares y de gestión de incidentes, y el ciclo de mejora continua. El plan de tratamiento, sustentado en los controles de la ISO/IEC 27002:2022 y la ISO/IEC 27701 y en las obligaciones de la LOPDP, permite reducir los catorce riesgos a niveles residuales aceptables. De este modo se cumplió el objetivo general de diseñar un sistema de gestión de protección de datos personales que fortalece el cumplimiento legal, la seguridad de la información y la protección de los datos de socios, clientes y colaboradores.

Recomendaciones

Se recomienda mantener actualizado el marco teórico y normativo que sustenta el sistema, mediante el seguimiento permanente de las reformas de la LOPDP, de las resoluciones y guías que emita la Superintendencia de Protección de Datos Personales y de las nuevas ediciones de las normas ISO/IEC, de modo que las obligaciones y los controles del sistema evolucionen con el marco jurídico y técnico vigente, con especial atención al tratamiento de los datos crediticios de los socios.

Se recomienda adoptar formalmente la metodología MAGERIT versión 3 como método institucional de análisis y gestión de riesgos, integrarla con la gestión de riesgos general de la Cooperativa alineada a la ISO 31000 y capacitar al personal técnico en su aplicación, para asegurar que el proceso de identificación, estimación y tratamiento de riesgos sea sostenible y repetible en el tiempo.

Se recomienda priorizar el cierre de las brechas críticas detectadas en el diagnóstico, comenzando por la implementación del procedimiento de gestión de incidentes, la formalización y difusión de las políticas de seguridad y de protección de datos, la conformación de un comité de seguridad de la información y el establecimiento de un esquema de

clasificación de la información y de controles criptográficos. Asimismo, se recomienda validar las valoraciones de criticidad con los propietarios de cada activo y volver a aplicar el instrumento de diagnóstico de forma periódica para medir la evolución del nivel de cumplimiento.

Se recomienda implementar el sistema de gestión de manera progresiva bajo el ciclo de mejora continua, iniciando con la aprobación y comunicación de la política de protección de datos, la designación del delegado de protección de datos y la puesta en marcha del registro de actividades de tratamiento. La ejecución del plan de tratamiento debe atender en primer lugar los riesgos críticos (R04, R09, R11, R12 y R14), acompañarse de evaluaciones de impacto en los tratamientos de alto riesgo, y verificarse mediante auditorías internas y revisiones por la dirección que permitan validar el sistema en su operación real más allá de su diseño.

Referencias

Asamblea Constituyente. (2008). *Constitución de la República del Ecuador*. Registro Oficial No. 449, 20 de octubre de 2008.

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento No. 459. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Carneiro, F. D., Rampasso, I. S., Matos Mello, S. L., Sigahi, T. F. A. C., Lespay, H., & Anholon, R. (2025). A flexible ISO 27701-based framework for assessing cybersecurity maturity: A proposition and a case application. *Computers & Security, 158*, 104645. https://doi.org/10.1016/j.cose.2025.104645

Cevallos-Salas, D., Estrada-Jiménez, J., & Guamán, D. S. (2026). A GPT-based assessment of alignment between privacy legal frameworks & ISO/IEC 27701:2025: A Latin American case study. *Technologies, 14*(5), 273. https://doi.org/10.3390/technologies14050273

Haggag, O., Pedace, A., Pan, S., & Grundy, J. (2025). An analysis of privacy regulations and user concerns of finance mobile applications. *Information and Software Technology, 184*, 107756. https://doi.org/10.1016/j.infsof.2025.107756

Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Education.

Hurtado de Barrera, J. (2010). *Metodología de la investigación: Guía para la comprensión holística de la ciencia* (4.ª ed.). Quirón Ediciones.

Innodev Solutions S.A. (2026). *Guía definitiva de la Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador*. https://www.innodevsolutionsec.com/articles/lopdp-ecuador-guia-definitiva

International Organization for Standardization & International Electrotechnical Commission. (2022a). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. ISO. https://www.iso.org/standard/27001

International Organization for Standardization & International Electrotechnical Commission. (2022b). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy*

protection - Information security controls. ISO. https://www.iso.org/standard/75652.html

International Organization for Standardization & International Electrotechnical Commission. (2025). *ISO/IEC 27701:2025 Information security, cybersecurity and privacy protection - Privacy information management systems - Requirements and guidance*. ISO. https://www.iso.org/standard/27701

Mancero-Gavilanes, S. L., Proaño-Reyes, G. M., & Castro-Sánchez, F. de J. (2025). Protección de datos personales crediticios y administración del perfil de riesgo en Ecuador. *Noesis. Revista Electrónica de Investigación, 7*(2), 814-831. https://doi.org/10.35381/noesisin.v7i2.619

Ministerio de Hacienda y Administraciones Públicas de España. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos*. Consejo Superior de Administración Electrónica, Gobierno de España.

Orizontel. (2025). *Guía de la Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador*. https://orizontel.ec/guia-lopdp-ecuador/

Presidencia de la República del Ecuador. (2023). *Reglamento General a la Ley Orgánica de Protección de Datos Personales*. Decreto Ejecutivo No. 904. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Decreto-Ejecutivo-No.-904.pdf

República del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento No. 459. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Superintendencia de Protección de Datos Personales. (2025a). *Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales*. Resolución Nro. SPDP-SPD-2025-0003-R. https://spdp.gob.ec/guias-spdp/

Superintendencia de Protección de Datos Personales. (2025b). *Reglamento del Delegado de Protección de Datos Personales*. Resolución Nro. SPDP-SPD-2025-0028-R. https://spdp.gob.ec/

Superintendencia de Protección de Datos Personales. (2026). *Guías SPDP*. https://spdp.gob.ec/guias-spdp/

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7.ª ed.). Cengage Learning.

Anexos

Anexo 1: Protocolo de Investigación

Anexo: Formato del Anteproyecto.

A. TÍTULO
Diseño de un sistema de gestión de protección de datos personales para la Cooperativa de Ahorro y Crédito Achik Inti Ltda.

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	Inteligencia de Negocios	
		Sistemas de Información	
		Gobierno y administración de tecnologías de información	
		Auditoría Informática	
		Seguridad Informática	x
		Redes y comunicación	
		Arquitectura de Hardware	
		Arquitectura de desarrollo de software	
		Ingeniería de Software	
		Gestión y gobierno de proyectos de tecnología informática	
		Ingeniería de requerimientos	
		Algoritmos y programación	
		Ciencias exactas y naturales (Matemáticas, Física, Química, Biología, etc.)	
		Modelaje y simulación	

C. PLANTEAMIENTO DEL PROBLEMA

La Cooperativa de Ahorro y Crédito Achik Inti Ltda. es una entidad financiera ubicada en el sector cooperativo ecuatoriano. De acuerdo con información pública, la institución se identifica como una cooperativa de ahorro y crédito, dispone de banca virtual y se encuentra registrada como COAC activa en el segmento 5, dentro de la Zonal 6 Cuenca. Esto evidencia que la entidad desarrolla actividades financieras que implican el tratamiento de información de socios, clientes, trabajadores y usuarios de servicios financieros.

En el contexto actual, las cooperativas de ahorro y crédito gestionan información sensible y estratégica, como datos de identificación, información de contacto, datos financieros, historial crediticio, solicitudes de crédito, documentación contractual y registros transaccionales. Este tipo de información requiere controles adecuados para evitar accesos no autorizados, pérdida de datos, uso indebido, divulgación no autorizada o incumplimiento normativo. La Ley Orgánica de Protección de Datos Personales del Ecuador y su reglamento establecen obligaciones para responsables y encargados del tratamiento, así como procedimientos para garantizar derechos como acceso, rectificación, actualización, eliminación, oposición y portabilidad (Información, s. f.).

El problema principal radica en la necesidad de contar con un sistema formal de gestión de protección de datos personales que permita organizar políticas, procedimientos, responsables, controles, registros de tratamiento, gestión de riesgos, atención de derechos del titular y mecanismos de mejora continua. La ausencia de un sistema estructurado puede generar debilidades en el cumplimiento legal, exposición a incidentes de seguridad, afectación a la confianza de los socios y dificultades para demostrar responsabilidad proactiva ante la autoridad competente. Además, estudios recientes sobre datos crediticios en Ecuador señalan que las instituciones financieras deben obtener autorización del titular y aplicar medidas estrictas en el tratamiento de información financiera y crediticia.

Por lo tanto, se plantea el diseño de un sistema de gestión de protección de datos personales para la Cooperativa de Ahorro y Crédito Achik Inti Ltda., con el propósito de establecer una propuesta técnica y normativa que permita identificar los tratamientos de datos, evaluar riesgos, definir controles, asignar responsabilidades y fortalecer el cumplimiento de la normativa ecuatoriana vigente, tomando como referencia buenas prácticas internacionales como ISO/IEC 27001:2022 e ISO/IEC 27701:2025.

D. OBJETIVO GENERAL

Diseñar un sistema de gestión de protección de datos personales para la Cooperativa de Ahorro y Crédito Achik Inti Ltda., mediante el análisis normativo, diagnóstico institucional y definición de políticas, procedimientos y controles de privacidad, con el fin de fortalecer el cumplimiento legal, la seguridad de la información y la protección de los datos de socios, clientes y colaboradores.

E. OBJETIVOS ESPECÍFICOS

1. Realizar un estudio teórico y normativo sobre protección de datos personales y datos crediticios, mediante la revisión de literatura científica, normativa ecuatoriana y estándares internacionales, con el fin de sustentar legal y conceptualmente el sistema de gestión.
2. Analizar metodologías y marcos de referencia aplicables a la gestión de protección de datos personales, mediante la comparación de la Ley Orgánica de Protección de Datos Personales, ISO/IEC 27001, ISO/IEC

27701 y gestión de riesgos, con el fin de seleccionar el enfoque metodológico del proyecto.
3. Diagnosticar la situación actual de la Cooperativa de Ahorro y Crédito Achik Inti Ltda. sobre el tratamiento de datos personales, mediante revisión documental, levantamiento de procesos y fichas de diagnóstico, con el fin de identificar riesgos, brechas y necesidades de control.
4. Diseñar el sistema de gestión de protección de datos personales para la Cooperativa de Ahorro y Crédito Achik Inti Ltda., mediante políticas, procedimientos, roles, matriz de riesgos y registros de tratamiento, con el fin de fortalecer el cumplimiento normativo y la seguridad de la información.

F. JUSTIFICACIÓN

La protección de datos personales se ha convertido en una necesidad prioritaria para las organizaciones que gestionan información de personas naturales, especialmente en el sector financiero, donde se administran datos de identificación, información económica, historial crediticio, documentación contractual y registros asociados a la relación entre la institución y sus socios. En Ecuador, la Ley Orgánica de Protección de Datos Personales y su reglamento establecen obligaciones para los responsables y encargados del tratamiento, así como mecanismos para garantizar los derechos de los titulares de datos.

El desarrollo de este proyecto se justifica porque una cooperativa de ahorro y crédito requiere mecanismos formales que le permitan demostrar cumplimiento normativo, reducir riesgos asociados al tratamiento inadecuado de información y fortalecer la confianza de sus socios. En este sentido, los datos financieros y crediticios deben ser gestionados bajo principios de licitud, transparencia, finalidad, minimización, confidencialidad, seguridad y responsabilidad proactiva. Por ello, resulta necesario contar con un sistema que permita organizar, controlar y documentar los procesos relacionados con la protección de datos personales.

Desde el punto de vista técnico, el diseño de un sistema de gestión permitirá identificar los tratamientos de datos personales realizados por la Cooperativa de Ahorro y Crédito Achik Inti Ltda., establecer responsabilidades internas, definir políticas y procedimientos, gestionar riesgos de privacidad y generar evidencia documental para auditorías, revisiones internas o procesos de mejora institucional. Además, el análisis de marcos como la LOPDP, ISO/IEC 27001 e ISO/IEC 27701 permitirá seleccionar un enfoque metodológico adecuado para estructurar la propuesta de manera ordenada, verificable y alineada con buenas prácticas internacionales.

Finalmente, el anteproyecto aportará una propuesta aplicable al contexto de la Cooperativa de Ahorro y Crédito Achik Inti Ltda., contribuyendo al fortalecimiento de la gobernanza de datos, la seguridad de la información, el cumplimiento normativo y la cultura institucional de privacidad. De esta manera, el proyecto no solo responde a una exigencia legal, sino también a una necesidad organizacional orientada a proteger la información personal de socios, clientes, colaboradores y demás partes relacionadas.

G. ALCANCE

El presente proyecto se centrará en el diseño de un sistema de gestión de protección de datos personales para la Cooperativa de Ahorro y Crédito Achik Inti Ltda. El estudio abordará los procesos institucionales relacionados con la recolección, almacenamiento, uso, consulta, transferencia, conservación y eliminación de datos personales de socios, clientes, empleados, proveedores y terceros vinculados con la cooperativa.

El alcance incluirá el levantamiento de información sobre los procesos que tratan datos personales, la identificación de

los tipos de datos utilizados, el análisis de riesgos de privacidad, la revisión de la normativa ecuatoriana vigente y la comparación de marcos de referencia como la LOPDP, ISO/IEC 27001 e ISO/IEC 27701. Esto permitirá seleccionar un enfoque metodológico adecuado para estructurar la propuesta del sistema de gestión.

Asimismo, el proyecto contemplará la definición de roles y responsabilidades, el diseño de políticas internas, la elaboración de procedimientos para consentimiento informado, atención de derechos del titular, gestión de incidentes, conservación documental, registros de tratamiento, matriz de riesgos y mecanismos de mejora continua. Estos elementos constituirán la base documental y técnica del sistema de gestión de protección de datos personales.

El proyecto no contempla la implementación completa del sistema en ambiente productivo, la adquisición de herramientas tecnológicas, la ejecución de auditorías externas ni la certificación formal bajo normas ISO. Su propósito será elaborar una propuesta técnica y metodológica que pueda ser utilizada por la cooperativa como base para una futura implementación, auditoría interna o proceso de adecuación normativa.

H. CONCEPTOS RELACIONADOS

Protección de datos personales

La protección de datos personales se refiere al conjunto de principios, normas, procedimientos y medidas técnicas orientadas a garantizar que la información relacionada con una persona natural sea tratada de manera lícita, segura, transparente y respetuosa de sus derechos. En el contexto ecuatoriano, este derecho se encuentra regulado por la Ley Orgánica de Protección de Datos Personales, la cual establece obligaciones para las organizaciones que recolectan, almacenan, usan o transfieren información personal de sus clientes, socios, trabajadores o usuarios. En una cooperativa de ahorro y crédito, este concepto resulta fundamental debido al manejo de información financiera, crediticia, económica y contractual de los socios (Pimboza Ninacuri, 2025).

Datos personales

Los datos personales son aquellos que permiten identificar o hacer identificable, directa o indirectamente, a una persona natural. Estos pueden incluir nombres, números de cédula, direcciones, teléfonos, correos electrónicos, información financiera, historial crediticio, datos laborales y cualquier otro elemento asociado a la identidad de una persona. Para una cooperativa de ahorro y crédito, los datos personales constituyen un activo crítico, ya que son utilizados en procesos de apertura de cuentas, otorgamiento de créditos, actualización de información, atención al socio y cumplimiento normativo (Borbor Suárez & Chaca Bravo, 2024).

Datos personales crediticios

Los datos personales crediticios corresponden a la información relacionada con el comportamiento financiero de una persona, su capacidad de pago, obligaciones pendientes, historial de crédito y cumplimiento de compromisos económicos. En el sistema financiero ecuatoriano, este tipo de información es especialmente relevante porque permite evaluar el perfil de riesgo de los socios o clientes antes de otorgar productos financieros. Sin embargo, su tratamiento debe realizarse con autorización del titular, finalidad legítima y medidas adecuadas de protección, debido a que un uso inadecuado puede afectar derechos económicos, reputacionales y patrimoniales de las personas (Mancero-Gavilanes, Proaño-Reyes, & Castro-Sánchez, 2025).

Tratamiento de datos personales

El tratamiento de datos personales comprende toda operación realizada sobre datos personales, como recolección, registro, almacenamiento, conservación, modificación, consulta, uso, comunicación, transferencia, eliminación o bloqueo. En una cooperativa, el tratamiento se presenta en actividades como la actualización de datos de socios, análisis

de solicitudes de crédito, gestión de cartera, atención al cliente, envío de notificaciones y cumplimiento de obligaciones legales. Por ello, el tratamiento debe estar documentado, responder a una finalidad específica y cumplir con los principios establecidos por la normativa vigente (Cabezas Azuero, 2023).

Responsable y encargado del tratamiento

El responsable del tratamiento es la persona natural o jurídica que decide sobre la finalidad, medios y condiciones del tratamiento de los datos personales. Por su parte, el encargado del tratamiento es quien procesa los datos por cuenta del responsable, siguiendo sus instrucciones. En una cooperativa, la institución puede actuar como responsable cuando define cómo y para qué se usarán los datos de sus socios; mientras que proveedores externos de software, almacenamiento, soporte tecnológico o cobranza podrían actuar como encargados. Por esta razón, es necesario establecer políticas, contratos, responsabilidades y controles que regulen la relación entre responsable y encargado del tratamiento (Tacha Torres, 2024).

Consentimiento informado

El consentimiento informado es la manifestación libre, específica, informada e inequívoca mediante la cual el titular autoriza el tratamiento de sus datos personales para una o varias finalidades determinadas. En el ámbito financiero, este consentimiento es esencial para procesos como consulta de historial crediticio, actualización de datos, envío de información institucional, análisis de capacidad de pago o transferencia de información a terceros autorizados. El Reglamento General a la Ley Orgánica de Protección de Datos Personales establece que el responsable debe poder demostrar que obtuvo el consentimiento del titular y que este fue informado previamente sobre las finalidades del tratamiento, tiempo de conservación y medidas de protección aplicables (Díaz Gamboa & Rivera Ramírez, 2024).

Seguridad de la información

La seguridad de la información es el conjunto de controles, políticas y procedimientos destinados a proteger la confidencialidad, integridad y disponibilidad de la información. En el contexto de protección de datos personales, la seguridad de la información permite evitar accesos no autorizados, filtraciones, alteraciones, pérdidas o destrucción indebida de datos. La norma ISO/IEC 27001:2022 establece requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información, basado en la gestión de riesgos y en la aplicación de controles organizacionales, tecnológicos y humanos (ISO/IEC, 2022).

Sistema de gestión de protección de datos personales

Un sistema de gestión de protección de datos personales puede entenderse como un conjunto organizado de políticas, procedimientos, responsables, controles, registros, mecanismos de evaluación y acciones de mejora continua orientadas a garantizar el cumplimiento de la normativa de protección de datos. Este sistema permite a una organización identificar qué datos trata, con qué finalidad, quién accede a ellos, qué riesgos existen y qué medidas deben aplicarse para protegerlos. La norma ISO/IEC 27701:2025 establece requisitos y orientación para implementar un Sistema de Gestión de Información de Privacidad, conocido como PIMS, enfocado en la gestión responsable de la información de identificación personal (ISO/IEC, 2025).

Gestión de riesgos de privacidad

La gestión de riesgos de privacidad consiste en identificar, analizar, evaluar y tratar los riesgos asociados al tratamiento de datos personales. Estos riesgos pueden incluir acceso indebido, uso no autorizado, pérdida de información, suplantación de identidad, filtración de datos financieros o incumplimiento legal. En las aplicaciones y servicios financieros, el tratamiento de datos personales, bancarios y transaccionales representa un objetivo importante para ciberataques, por lo que las organizaciones deben aplicar medidas preventivas y correctivas que reduzcan la probabilidad e impacto de incidentes de privacidad (Maldonado Almeida, 2023).

I. TRABAJOS RELACIONADOS

En el ámbito internacional, Haggag et al. (2025), en el estudio titulado "An analysis of privacy regulations and user concerns of finance mobile applications", analizaron las preocupaciones de privacidad de los usuarios y el impacto de las regulaciones de protección de datos en aplicaciones financieras móviles de Alemania, Australia y Estados Unidos. La investigación destaca que las aplicaciones financieras gestionan información altamente sensible, como datos personales, información bancaria e historiales transaccionales, lo que las convierte en objetivos relevantes para ataques informáticos y riesgos de privacidad. Este trabajo resulta pertinente para el presente anteproyecto porque evidencia que las entidades financieras deben fortalecer sus políticas de privacidad, transparentar el uso de los datos y establecer controles adecuados para proteger la información de sus usuarios.

Asimismo, Carneiro et al. (2025), en el artículo "A flexible ISO 27701-based framework for assessing cybersecurity maturity: a proposition and a case application", propusieron un marco flexible basado en ISO/IEC 27701 para evaluar el nivel de madurez de la gestión de ciberseguridad y privacidad en organizaciones. El estudio utilizó ISO/IEC 27701 como base para estructurar un cuestionario de evaluación y aplicó técnicas como análisis jerárquico de clústeres, análisis de frecuencia y Fuzzy TOPSIS. Los resultados evidencian la utilidad de los estándares de privacidad para identificar brechas, evaluar controles y orientar la mejora institucional. Este antecedente es importante para el presente trabajo porque respalda la necesidad de diseñar un sistema de gestión de protección de datos personales basado en políticas, controles, responsabilidades, evaluación de riesgos y mejora continua.

En el contexto nacional, Mancero-Gavilanes et al. (2025), en el estudio "Protección de datos personales crediticios y administración del perfil de riesgo en Ecuador", realizaron un análisis crítico-jurídico sobre el tratamiento de datos personales crediticios en el sistema financiero ecuatoriano. La investigación examina la relación entre la protección de los datos crediticios y la necesidad de las instituciones financieras de administrar perfiles de riesgo. Los autores destacan que las entidades deben cumplir medidas estrictas, entre ellas obtener autorización del titular antes del tratamiento de datos personales crediticios. Este trabajo se relaciona directamente con el anteproyecto porque las cooperativas de ahorro y crédito tratan información financiera y crediticia de socios y clientes, por lo que requieren mecanismos internos para garantizar consentimiento, finalidad legítima, confidencialidad y seguridad en el tratamiento de datos.

En el ámbito local, Romero (2024), desarrolló una investigación sobre el cumplimiento de la normativa de seguridad de la información para la COAC Achik Inti del cantón Cañar, en el marco de su progresión de segmento bajo la regulación de la Superintendencia de Economía Popular y Solidaria. El estudio identificó brechas en seguridad de la información y propuso acciones de mejora relacionadas con políticas, infraestructura tecnológica, capacitación y gestión de riesgos. Este antecedente resulta especialmente pertinente porque muestra que la cooperativa ya ha sido objeto de investigaciones relacionadas con seguridad, cumplimiento normativo y gestión de riesgos, aspectos que sirven como base para proponer un sistema de gestión de protección de datos personales.

J. METODOLOGÍA

La presente investigación adoptará un enfoque mixto, debido a que combinará el análisis cualitativo de normativa, procesos internos, políticas, procedimientos y responsabilidades institucionales, con una valoración cuantitativa de riesgos, brechas de cumplimiento y controles requeridos. El nivel de investigación será descriptivo y proyectivo, ya

que primero se caracterizará la situación actual de la Cooperativa de Ahorro y Crédito Achik Inti Ltda. respecto al tratamiento de datos personales y, posteriormente, se diseñará una propuesta de sistema de gestión orientada a fortalecer la protección de la información. El tipo de investigación será aplicado, porque busca resolver una necesidad concreta dentro de la cooperativa: contar con un sistema estructurado para gestionar la protección de datos personales.

El diseño metodológico se apoyará en el enfoque de Design Science Research, debido a que permite desarrollar una solución organizacional o artefacto metodológico a partir de la identificación de un problema, el análisis del contexto, el diseño de una propuesta, su estructuración y su validación mediante criterios técnicos. Como parte del proceso metodológico, se realizará un análisis comparativo de marcos normativos y técnicos aplicables a la protección de datos personales, considerando la Ley Orgánica de Protección de Datos Personales, su reglamento, la norma ISO/IEC 27001:2022, la norma ISO/IEC 27701:2025 y enfoques de gestión de riesgos. Esta comparación permitirá seleccionar el enfoque metodológico más adecuado para estructurar el sistema de gestión, tomando en cuenta criterios de cumplimiento normativo, seguridad de la información, privacidad, gestión documental, gestión de riesgos y mejora continua.

El desarrollo de la propuesta se organizará en fases: fundamentación teórica y normativa, análisis comparativo de marcos de referencia, diagnóstico de la situación actual de la cooperativa y diseño del sistema de gestión de protección de datos personales. Para la recolección de información se emplearán técnicas como revisión documental, entrevistas al personal clave, observación de procesos y aplicación de matrices de diagnóstico. Los instrumentos previstos serán ficha de levantamiento de procesos, matriz de inventario de datos personales, matriz de riesgos de privacidad, lista de verificación normativa, matriz comparativa de marcos de referencia y matriz de controles propuestos. Como resultado, se espera obtener una propuesta técnica y documentada que pueda servir como base para una futura implementación, auditoría interna o proceso de adecuación normativa.

K. CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD	MES						
		I	II	III	IV	V	VI	MEDIOS DE VERIFICACIÓN
1	Realizar la fundamentación teórica sobre protección de datos personales, datos crediticios, seguridad de la información y gestión de privacidad.	x						Documento de conceptos relacionados y marco teórico preliminar.
2	Revisar la normativa ecuatoriana vigente relacionada con protección de datos personales,	x	x					Matriz normativa sobre obligaciones, principios y derechos del titular.

	especialmente la LOPDP y su reglamento.							
3	Analizar marcos de referencia aplicables al sistema de gestión, como ISO/IEC 27001, ISO/IEC 27701 y enfoques de gestión de riesgos.		x					Matriz comparativa de normas, metodologías y marcos de referencia.
4	Seleccionar el enfoque metodológico que guiará el diseño del sistema de gestión de protección de datos personales.		x					Informe de selección metodológica del proyecto.
5	Levantar información sobre los procesos institucionales relacionados con el tratamiento de datos personales en la cooperativa.		x	x				Fichas de levantamiento de procesos y registro de información institucional.
6	Identificar los tipos de datos personales tratados, responsables, finalidades, medios de almacenamiento y procesos asociados.			x				Inventario de datos personales y registro de actividades de tratamiento.
7	Diagnosticar riesgos, brechas de cumplimiento y necesidades de control relacionadas con la protección de datos personales.							Matriz de riesgos de privacidad y matriz de brechas de cumplimiento.

				x	x			
8	Diseñar las políticas internas para el sistema de gestión de protección de datos personales.				x			Documento de políticas internas de protección de datos personales.
9	Elaborar procedimientos para consentimiento informado, atención de derechos del titular, gestión de incidentes y conservación documental.				x	x		Manual de procedimientos del sistema de gestión.
10	Definir roles, responsabilidades, controles de seguridad, registros de tratamiento y mecanismos de mejora continua.					x		Matriz de roles, matriz de controles y registros documentales del sistema.
11	Integrar la propuesta final del sistema de gestión de protección de datos personales para la cooperativa.					x		Documento de propuesta técnica del sistema de gestión.
12	Validar la propuesta mediante revisión técnica, juicio de expertos o revisión académica.							Matriz de validación de la propuesta.

						x		
13	Redactar conclusiones, recomendaciones y versión final del documento.						x	Documento final del anteproyecto/proyecto de tesis.

L. DECLARACIÓN FINAL
Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES	
DIRECTOR:	**ING. CRISTINA MARIUXI FLORES URGILES**
ESTUDIANTE 1	Hendry Alfredo Sanchez Paucar

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	Cañar
Fecha:	17 de abril del 2026
Firmas:	

Nombre: Ing. Cristina Mariuxi Flores Urgiles CC: 0302090535 **Director del Proyecto**	Nombre: Hendry Alfredo Sanchez Paucar C.C.: 0350337853 **Estudiante / Egresado**

O. APROBACIÓN	
Firmas:	
Nombre: CC: **Primer Par Revisor**	Nombre: C.C.: **Segundo Par Revisor**

P. REFERENCIAS
Véase la sección Referencias del documento principal.

Anexo 2. Manual de Políticas de Protección de Datos Personales

COOPERATIVA DE AHORRO Y CRÉDITO

“ACHIK INTI” LTDA.

MANUAL DE POLÍTICAS DE

PROTECCIÓN DE DATOS PERSONALES

Sistema de Gestión de Protección de Datos Personales (SGPD)

Elaborado conforme a la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento General, y las normas ISO/IEC 27001 e ISO/IEC 27701

Código del documento	MPD-PDP-001
Versión	01
Fecha de aprobación	____ / ____ / _____
Clasificación	Uso interno

REGISTRO DE FIRMAS

Elaborado por	Revisado por	Aprobado por
_____ Delegado de Protección de Datos	_____ Dirección de TI	_____ Consejo de Administración

CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Responsable
01	____/____/____	Emisión inicial del manual	Delegado de Protección de Datos

Este manual constituye una propuesta técnica elaborada en el marco del proyecto de titulación y debe ser validado y aprobado formalmente por los órganos de gobierno de la cooperativa antes de su entrada en vigor. Las referencias legales deben contrastarse con el texto vigente de la LOPDP y su Reglamento General al momento de la aprobación.

ÍNDICE DEL MANUAL

1. Objeto

2. Alcance

3. Marco legal y normativo de referencia

4. Definiciones

5. Principios rectores del tratamiento

6. Bases de legitimación del tratamiento

7. Roles y responsabilidades

8. Políticas específicas

- 8.1. Política de tratamiento lícito y transparente
- 8.2. Política de consentimiento
- 8.3. Política de calidad y minimización de datos
- 8.4. Política de derechos de los titulares
- 8.5. Política de seguridad de la información
- 8.6. Política de control de acceso
- 8.7. Política de clasificación de la información
- 8.8. Política de cifrado (criptografía)
- 8.9. Política de conservación y eliminación segura
- 8.10. Política de gestión de incidentes y vulneraciones de seguridad
- 8.11. Política de transferencias y encargados del tratamiento
- 8.12. Política de datos sensibles y datos crediticios
- 8.13. Política de capacitación y concienciación

9. Registro de actividades de tratamiento

10. Evaluación de impacto relativa a la protección de datos

11. Incumplimiento y régimen disciplinario

12. Vigencia, revisión y aprobación

1. OBJETO

El presente manual establece las políticas que rigen el tratamiento de datos personales en la Cooperativa de Ahorro y Crédito “Achik Inti” Ltda. (en adelante, “la Cooperativa”), con el fin de garantizar el ejercicio del derecho fundamental a la protección de datos personales de socios, clientes, colaboradores y terceros, y de demostrar el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento General y la normativa emitida por la Superintendencia de Protección de Datos Personales (SPDP).

Las políticas aquí definidas integran los requisitos legales con los controles de seguridad de la información de la norma ISO/IEC 27001, los controles de privacidad de la ISO/IEC 27701 y la gestión de riesgos basada en la metodología MAGERIT v3, conformando el Sistema de Gestión de Protección de Datos Personales (SGPD) de la Cooperativa.

2. ALCANCE

Este manual aplica a todos los tratamientos de datos personales realizados por la Cooperativa, en cualquier soporte físico o digital, automatizado o no, en las fases de recolección, registro, almacenamiento, uso, consulta, transferencia, conservación y eliminación. Es de observancia obligatoria para:

- El Consejo de Administración, la Gerencia y todo el personal, cualquiera sea su relación contractual.
- Los encargados del tratamiento y proveedores que accedan a datos personales por cuenta de la Cooperativa.
- Los activos de información identificados en la infraestructura tecnológica institucional, con énfasis en los activos críticos: la base de datos institucional, las aplicaciones ACHIK EMPRENDE y ACHIK MÓVIL, el sistema DIMA COF y los servidores que los soportan.

3. MARCO LEGAL Y NORMATIVO DE REFERENCIA

- Constitución de la República del Ecuador, artículo 66, numeral 19.
- Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Registro Oficial Suplemento 459 del 26 de mayo de 2021.
- Reglamento General a la LOPDP y las resoluciones y guías técnicas emitidas por la Superintendencia de Protección de Datos Personales.

- Normas ISO/IEC 27001 (sistema de gestión de seguridad de la información), ISO/IEC 27002 (controles), ISO/IEC 27701 (gestión de información de privacidad) e ISO/IEC 27005 (gestión de riesgos).
- Metodología MAGERIT v3 de análisis y gestión de riesgos.
- Normativa de la Superintendencia de Economía Popular y Solidaria (SEPS) aplicable a la Cooperativa.

4. DEFINICIONES

Término	Definición
Dato personal	Toda información que identifica o hace identificable a una persona natural, directa o indirectamente.
Dato sensible	Dato relativo a etnia, salud, biometría, situación financiera, ideología, orientación sexual u otros que requieran protección reforzada.
Titular	Persona natural a quien corresponden los datos personales objeto de tratamiento.
Responsable del tratamiento	La Cooperativa, que decide sobre la finalidad y los medios del tratamiento.
Encargado del tratamiento	Persona natural o jurídica que trata datos personales por cuenta del responsable.
Tratamiento	Cualquier operación realizada sobre datos personales, automatizada o no.
Consentimiento	Manifestación de voluntad libre, específica, informada e inequívoca del titular.
DPD	Delegado de Protección de Datos, responsable de supervisar el cumplimiento de la normativa.
RAT	Registro de Actividades de Tratamiento que inventaría los tratamientos de la Cooperativa.
Vulneración de seguridad	Incidente que ocasiona la destrucción, pérdida, alteración o acceso no autorizado a datos personales.

5. PRINCIPIOS RECTORES DEL TRATAMIENTO

Todo tratamiento de datos personales en la Cooperativa se rige por los siguientes principios establecidos en la LOPDP:

a) Juridicidad: el tratamiento se fundamenta en una base de legitimación válida.

b) Lealtad y transparencia: los datos se tratan de forma leal y el titular es informado de manera clara sobre el tratamiento.

c) Finalidad: los datos se recogen para finalidades determinadas, explícitas y legítimas, y no se tratan de modo incompatible con ellas.

d) Pertinencia y minimización: solo se tratan los datos adecuados, pertinentes y limitados a lo necesario.

e) Proporcionalidad: el tratamiento es proporcional a la finalidad perseguida.

f) Confidencialidad: los datos se protegen frente a accesos no autorizados y quienes intervienen guardan reserva.

g) Calidad y exactitud: los datos se mantienen exactos y actualizados, y se rectifican o eliminan cuando sean inexactos.

h) Conservación: los datos se conservan solo durante el tiempo necesario para la finalidad y los plazos legales aplicables.

i) Seguridad de datos: se aplican medidas técnicas y organizativas apropiadas al nivel de riesgo.

j) Responsabilidad proactiva (accountability): la Cooperativa adopta medidas para cumplir la normativa y puede demostrarlo en todo momento.

6. BASES DE LEGITIMACIÓN DEL TRATAMIENTO

La Cooperativa solo trata datos personales cuando concurre al menos una de las siguientes bases de legitimación previstas en la LOPDP:

- Consentimiento del titular.
- Ejecución de medidas precontractuales o cumplimiento de un contrato del que el titular es parte (por ejemplo, la vinculación como socio o el otorgamiento de un crédito).
- Cumplimiento de una obligación legal aplicable a la Cooperativa.
- Cumplimiento de una misión de interés público o el ejercicio de potestades públicas.

- Interés legítimo del responsable, siempre que no prevalezcan los derechos del titular (por ejemplo, la videovigilancia de las instalaciones).
- Protección de intereses vitales del titular u otra persona natural.

7. ROLES Y RESPONSABILIDADES

La Cooperativa designa un **Delegado de Protección de Datos (DPD)**, dado que su actividad principal implica el tratamiento a gran escala de datos financieros y crediticios de sus socios. La matriz de responsabilidades es la siguiente:

Rol	Responsabilidades principales
Consejo de Administración y Gerencia	Aprobar las políticas, asignar recursos y revisar periódicamente el desempeño del SGPD.
Delegado de Protección de Datos	Asesorar y supervisar el cumplimiento de la LOPDP, gestionar la relación con la SPDP y atender a los titulares.
Dirección de Tecnologías de la Información	Implementar los controles técnicos, administrar accesos, respaldos e infraestructura.
Departamento de Seguridad de la Información	Gestionar riesgos e incidentes, monitorear controles y mantener la matriz de riesgos.
Responsables de proceso	Aplicar los procedimientos en su área y mantener actualizado el RAT.
Todo el personal	Cumplir las políticas, guardar confidencialidad y reportar incidentes o debilidades.

8. POLÍTICAS ESPECÍFICAS

8.1. Política de tratamiento lícito y transparente

La Cooperativa informa a los titulares, mediante avisos de privacidad claros y accesibles, sobre la identidad del responsable, las finalidades y la base de legitimación del tratamiento, los destinatarios, los plazos de conservación y la forma de ejercer sus derechos. Ningún tratamiento se realiza sin una finalidad determinada y una base de legitimación válida.

8.2. Política de consentimiento

Cuando la base de legitimación sea el consentimiento, este se obtiene de forma libre, específica, informada e inequívoca, mediante una acción afirmativa del titular. El consentimiento se documenta y puede ser retirado en cualquier momento con la misma facilidad con que se otorgó. Para el tratamiento de datos sensibles se requiere consentimiento expreso, salvo las excepciones legales.

8.3. Política de calidad y minimización de datos

La Cooperativa recoge únicamente los datos necesarios para cada finalidad y adopta mecanismos para mantenerlos exactos y actualizados. Los formularios y sistemas se diseñan bajo los principios de privacidad desde el diseño y por defecto, evitando la recolección de datos superfluos.

8.4. Política de derechos de los titulares

La Cooperativa garantiza el ejercicio de los derechos de acceso, rectificación y actualización, eliminación, oposición, portabilidad, y el derecho a no ser objeto de decisiones automatizadas, así como los demás derechos reconocidos por la LOPDP. Las solicitudes se atienden a través de un canal habilitado y se responden dentro del término de quince (15) días previsto en el Reglamento General a la LOPDP, previa verificación de la identidad del solicitante. Toda gestión se registra como evidencia de cumplimiento.

8.5. Política de seguridad de la información

La Cooperativa implementa medidas técnicas y organizativas apropiadas al nivel de riesgo para proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos personales, conforme a la norma ISO/IEC 27002 y a los resultados del análisis de riesgos MAGERIT. Estas medidas se revisan y actualizan periódicamente.

8.6. Política de control de acceso

El acceso a los datos personales se otorga bajo los principios de necesidad de conocer y mínimo privilegio. Cada usuario dispone de credenciales individuales, se aplica autenticación reforzada para los sistemas críticos y los privilegios se revisan periódicamente. Las altas, cambios y bajas de acceso se gestionan formalmente, especialmente ante la desvinculación del personal.

8.7. Política de clasificación de la información

La información se clasifica según su sensibilidad (por ejemplo: pública, interna, confidencial y restringida) y se etiqueta y protege conforme a su nivel. Los datos personales y, en particular, los datos financieros y crediticios de los socios se clasifican como confidenciales o restringidos y reciben controles reforzados.

8.8. Política de cifrado (criptografía)

La Cooperativa cifra los datos personales en reposo en los soportes de almacenamiento y en tránsito por los canales de comunicación, así como la mensajería electrónica que contenga datos personales. La gestión de claves criptográficas se realiza de forma segura y documentada.

8.9. Política de conservación y eliminación segura

Los datos personales se conservan solo durante el tiempo necesario para la finalidad y los plazos legales y regulatorios aplicables. Cumplido el plazo, los datos se eliminan o anonimizan mediante procedimientos de borrado seguro, incluyendo el tratamiento de los soportes y equipos previo a su desincorporación o reúso.

8.10. Política de gestión de incidentes y vulneraciones de seguridad

Ante una vulneración de la seguridad de los datos personales, la Cooperativa activa el procedimiento de gestión de incidentes: detección y reporte interno, contención, evaluación del riesgo para los derechos de los titulares, notificación a la Superintendencia de Protección de Datos Personales dentro del término máximo previsto en el Reglamento General a la LOPDP, comunicación a los titulares afectados cuando exista un riesgo alto para sus derechos, erradicación, recuperación y registro del incidente con las lecciones aprendidas.

8.11. Política de transferencias y encargados del tratamiento

Toda comunicación o transferencia de datos a terceros se realiza sobre una base de legitimación válida. La contratación de encargados del tratamiento se formaliza mediante un contrato que incluye las cláusulas de protección de datos exigidas por la normativa, garantiza medidas de seguridad equivalentes y prohíbe usos distintos a los instruidos. Las transferencias internacionales solo se realizan a destinos que ofrezcan un nivel adecuado de protección o mediante garantías apropiadas.

8.12. Política de datos sensibles y datos crediticios

El tratamiento de datos sensibles y de datos financieros y crediticios se limita a los casos legalmente habilitados, requiere consentimiento expreso cuando corresponda y se sujeta a medidas de seguridad reforzadas. El análisis del perfil de riesgo crediticio se realiza con criterios de proporcionalidad y transparencia hacia el titular.

8.13. Política de capacitación y concienciación

La Cooperativa ejecuta un programa permanente de capacitación y concienciación en protección de datos dirigido a todo el personal, con el fin de reducir el riesgo de fugas de información por error humano y de fortalecer la cultura de protección de datos.

9. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

La Cooperativa mantiene y actualiza un Registro de Actividades de Tratamiento (RAT) que inventaría cada tratamiento con su finalidad, categorías de datos y de titulares, base de legitimación, destinatarios, transferencias, plazos de conservación y medidas de seguridad. El RAT constituye evidencia central de la responsabilidad proactiva y se actualiza ante cualquier cambio en los tratamientos.

10. EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

Antes de iniciar tratamientos que puedan entrañar un alto riesgo para los derechos de los titulares —por ejemplo, tratamientos a gran escala de datos financieros o el uso de nuevas tecnologías—, la Cooperativa realiza una Evaluación de Impacto relativa a la Protección de Datos (EIPD), que describe el tratamiento, evalúa su necesidad y proporcionalidad, identifica los riesgos y define las medidas para mitigarlos.

11. INCUMPLIMIENTO Y RÉGIMEN DISCIPLINARIO

El incumplimiento de las políticas de este manual se sujeta al régimen disciplinario interno de la Cooperativa, sin perjuicio de las responsabilidades administrativas, civiles o penales previstas en la LOPDP. El régimen sancionatorio de la ley contempla multas calculadas sobre el volumen de negocio del responsable, por lo que el cumplimiento de estas políticas protege tanto a los titulares como a la propia entidad.

12. VIGENCIA, REVISIÓN Y APROBACIÓN

Este manual entra en vigor a partir de su aprobación por el Consejo de Administración y se revisa al menos una vez al año, o antes si se producen cambios normativos, tecnológicos u organizacionales relevantes, en el marco del ciclo de mejora continua del SGPD.

Elaborado por	Revisado por	Aprobado por
_____ Delegado de Protección de Datos	_____ Dirección de TI	_____ Consejo de Administración

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

HENDRY ALFREDO SANCHEZ PAUCAR portador de la cédula de ciudadanía N.º **0350337853**. En calidad de autor y titular de los derechos patrimoniales del trabajo de titulación "**DISEÑO DE UN SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA.**" de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, 29 de septiembre 2026



HENDRY ALFREDO SANCHEZ PAUCAR

C.I. 0350337853