

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE SOFTWARE

Tema:

AUDITORÍA TÉCNICA DEL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN LOS SISTEMAS DE INFORMACIÓN DEL CORE FINANCIERO DE LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA

.

Trabajo de titulación modalidad Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero de Software.

ÁREA: Gestión de Software
LÍNEA DE INVESTIGACIÓN: Software, Tecnologías de la Información y Ciencia de Datos.

AUTOR: Ezequiel Andrés Sánchez López
TUTOR: Ing. Julio Enrique Balarezo López, Mg.

Ambato - Ecuador
julio – 2026

APROBACIÓN DEL TUTOR

En calidad de tutor del trabajo de titulación con el tema: AUDITORÍA TÉCNICA DEL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN LOS SISTEMAS DE INFORMACIÓN DEL CORE FINANCIERO DE LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA, desarrollado bajo la modalidad Proyecto de Investigación por el señor Ezequiel Andrés Sánchez López, estudiante de la Carrera de Software, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.3 del instructivo del reglamento referido.

Ambato, julio 2026



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JULIO ENRIQUE BALAREZO LOPEZ

Ing. Julio Enrique Balarezo López Mg.
TUTOR

AUTORÍA

El presente trabajo de titulación con el tema: AUDITORÍA TÉCNICA DEL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN LOS SISTEMAS DE INFORMACIÓN DEL CORE FINANCIERO DE LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA es absolutamente original, auténtico y personal y ha observado los preceptos establecidos en la Disposición General Quinta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, julio 2026



Ezequiel Andrés Sánchez López

C.C. 1850179316

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato para que reproduzca total o parcialmente este trabajo de titulación dentro de las regulaciones legales e institucionales correspondientes. Además, cedo todos mis derechos de autor a favor de la institución con el propósito de su difusión pública, por lo tanto, autorizo su publicación en el repositorio virtual institucional como un documento disponible para la lectura y uso con fines académicos e investigativos de acuerdo con la Disposición General Cuarta del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato.

Ambato, julio 2026.



Ezequiel Andrés Sánchez López

C.C. 1850179316

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del informe final del trabajo de titulación presentado por el/la señor/señorita Ezequiel Andrés Sánchez López, estudiante de la Carrera de Software, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado AUDITORÍA TÉCNICA DEL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN LOS SISTEMAS DE INFORMACIÓN DEL CORE FINANCIERO DE LA COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la Titulación de Grado en la Universidad Técnica de Ambato y el numeral 6.4 del instructivo del reglamento referido. Para cuya constancia suscribimos, conjuntamente con el señor Presidente del Tribunal.

Ambato, julio 2026.

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
FRANKLIN OSWALDO MAYORGA MAYORGA

Ing. Franklin Oswaldo Mayorga Mayorga, Mg.
PRESIDENTE DEL TRIBUNAL

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
DANIEL SEBASTIAN JEREZ MAYORGA

Ing. Daniel Sebastián Jerez Mayorga, Msc.
PROFESOR CALIFICADOR

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
EDWIN HERNANDO BUENANO VALENCIA

Ing, Edwin Hernando Buenaño Valencia, Mg
PROFESOR CALIFICADOR

DEDICATORIA

Quiero dedicar este trabajo a mi madre, por haber estado conmigo en cada etapa de mi vida universitaria, acompañándome con amor, paciencia y apoyo constante. Su presencia ha sido fundamental en este camino, porque en los momentos difíciles siempre encontré en ella una palabra de aliento y la fuerza necesaria para continuar.

A mi padre, quien desde que era pequeño impulsó mis sueños y me enseñó a creer en lo que podía lograr. Aunque hoy no esté físicamente conmigo, sé que desde el cielo estaría orgulloso de cada meta alcanzada. Este logro también es para él, por todo lo que significó en mi vida y por el amor que sigue acompañándome en cada paso.

A mis hermanos, por estar siempre presentes, por apoyarme de manera incondicional y por celebrar mis logros como si fueran suyos. Gracias por su cariño, por su compañía y por ser parte importante de este proceso que hoy culmina.

Finalmente, dedico este trabajo a Dios, por darme la fortaleza, la sabiduría y la bendición de llegar hasta el final. Por sostenerme en los momentos más difíciles y permitirme culminar esta etapa con gratitud, esperanza y fe.

AGRADECIMIENTO

Agradezco a los docentes universitarios, quienes con sus enseñanzas contribuyeron a mi formación académica y despertaron en mí un mayor amor por la carrera, motivándome a esforzarme cada día para ser un buen profesional y alcanzar nuevas oportunidades. De manera especial, agradezco al Ing. Julio Balarezo, por su guía y acompañamiento durante el desarrollo de mi trabajo de titulación.

A la Cooperativa de Ahorro y Crédito Credi Ya, por abrirme sus puertas para realizar mi proyecto de titulación y por confiar en mí al brindarme mi primera oportunidad laboral. De igual manera, agradezco a mi jefe, José Acán, por su apoyo, orientación y confianza durante este proceso.

A mis amigos, quienes desde nivelación me han acompañado en esta etapa universitaria, compartiendo momentos de alegría, apoyo y compañerismo que hicieron más especial este camino.

Finalmente, agradezco a mi polola, quien en poco tiempo se ha convertido en una parte muy importante de mi vida. Gracias por su apoyo, cariño y compañía, por motivarme a seguir adelante y por estar presente en esta etapa tan significativa para mí.

ÍNDICE GENERAL DE CONTENIDOS

PORTADA i

APROBACIÓN DEL TUTOR ii

AUTORÍA iii

DERECHOS DE AUTOR iv

APROBACIÓN DEL TRIBUNAL DE GRADO v

DEDICATORIA vi

AGRADECIMIENTO vii

ÍNDICE GENERAL DE CONTENIDOS 8

ÍNDICE DE TABLAS 11

ÍNDICE DE ILUSTRACIONES 13

ÍNDICE DE ANEXOS 14

RESUMEN EJECUTIVO 15

ABSTRACT 16

CAPÍTULO I. MARCO TEÓRICO 17

1.1 Tema de investigación 17

1.1.1 Planteamiento del problema 17

1.2 Antecedentes investigativos 19

1.3 Fundamentación teórica 21

1.3.1 Protección de datos personales 21

1.3.2 Ley Orgánica de Protección de Datos Personales y su Reglamento 22

1.3.3 Principios del tratamiento de datos 22

1.3.4 Derechos del titular 22

1.3.5 Seguridad de la información 22
1.3.6 Gestión de la privacidad y cumplimiento 23
1.3.7 Protección de datos desde el diseño y por defecto 23
1.3.8 Gestión de incidentes de seguridad 23
1.3.9 Core financiero y tratamiento de datos personales 24
1.3.10 Auditoría técnica de cumplimiento 24
1.4 Objetivos 24
1.4.1 Objetivo general 24
1.4.2 Objetivos específicos 25
CAPÍTULO II. METODOLOGÍA 26
2.1 Materiales 26
Modelo de encuesta dirigida a empleados 27
Modelo de encuesta dirigida a socios/clientes 30
Modelo de entrevista semiestructurada 33
Modelo de ficha bibliográfica-documental 34
2.2 Métodos 34
2.2.1 Modalidad de la investigación 35
2.2.2 Población y muestra 35
2.2.3 Recolección de información 37
2.2.4 Procesamiento y análisis de datos 38
CAPÍTULO III. RESULTADOS Y DISCUSIÓN 70
3.1 Enfoque de la auditoría y operacionalización de los objetivos específicos 70
3.1.1 Trazabilidad del capítulo con los objetivos específicos 71
3.2 Planificación y delimitación de la auditoría técnica 72
3.2.1 Ámbito de la auditoría técnica 72

3.2.2 Cronograma de ejecución de pruebas....73
3.3 Evaluación del cumplimiento técnico-normativo del core financiero frente a los artículos seleccionados de la LOPDP....74
3.3.1 Selección de artículos de la LOPDP y su Reglamento para la evaluación....74
3.3.2 Criterios legales, documentales y técnicos aplicados en la auditoría...75
3.3.3 Evidencia documental y técnica utilizada para la evaluación....76
3.3.4 Lista de verificación sustentada en evidencia documental y técnica ...76
3.3.5 Resultados de la evaluación del cumplimiento técnico-normativo....80
3.4 Identificación de brechas de cumplimiento, riesgos y vulnerabilidades técnicas y organizativas asociadas al tratamiento de datos personales 82
3.4.1 Evaluación del proceso de atención de derechos ARCO+....83
3.4.2 Evaluación del proceso de gestión y notificación de brechas 84
3.4.3 Brechas normativas consolidadas de auditoría....84
3.5 Elaboración del informe técnico de auditoría con hallazgos clasificados por criticidad y plan de acción priorizado 86
3.5.1 Clasificación de hallazgos por criticidad bajo el enfoque ISO 31000 .86
3.5.2 Plan de acción priorizado con medidas correctivas y preventivas 91
3.5.3 Informe técnico final de auditoría 93
3.6 Discusión de resultados....93
CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES 95
REFERENCIAS BIBLIOGRÁFICAS 98
ANEXOS 104
Evidencias institucionales y técnicas base....104

ÍNDICE DE TABLAS

Tabla 1 Guía de Entrevista Semiestructurada.....33
Tabla 2 Ficha de revisión bibliográfica - documental 34
Tabla 3 Población y muestra del estudio. 37
Tabla 4 Coeficiente alfa de Cronbach en la encuesta. 37
Tabla 5 Criterios de la escala de consistencia del alfa de Cronbach. 38
Tabla 6 Resultados de la encuesta a empleados - pregunta 1. 39
Tabla 7 Resultados de la encuesta a empleados - pregunta 2. 40
Tabla 8 Resultados de la encuesta a empleados - pregunta 3. 41
Tabla 9 Resultados de la encuesta a empleados - pregunta 4. 42
Tabla 10 Resultados de la encuesta a empleados - pregunta 5. 43
Tabla 11 Resultados de la encuesta a empleados - pregunta 6. 44
Tabla 12 Resultados de la encuesta a empleados - pregunta 7. 45
Tabla 13 Resultados de la encuesta a empleados - pregunta 8. 46
Tabla 14 Resultados de la encuesta a empleados - pregunta 9. 47
Tabla 15 Resultados de la encuesta a empleados - pregunta 10. 48
Tabla 16 Resultados de la encuesta a empleados - pregunta 11. 49
Tabla 17 Resultados de la encuesta a socios/clientes - pregunta 1. 50
Tabla 18 Resultados de la encuesta a socios/clientes - pregunta 2. 51
Tabla 19 Resultados de la encuesta a socios/clientes - pregunta 3. 52
Tabla 20 Resultados de la encuesta a socios/clientes - pregunta 4. 53
Tabla 21 Resultados de la encuesta a socios/clientes - pregunta 5. 54
Tabla 22 Resultados de la encuesta a socios/clientes - pregunta 6. 55
Tabla 23 Resultados de la encuesta a socios/clientes - pregunta 7. 56
Tabla 24 Resultados de la encuesta a socios/clientes - pregunta 8. 57
Tabla 25 Resultados de la encuesta a socios/clientes - pregunta 9. 58
Tabla 26 Resultados de la encuesta a socios/clientes - pregunta 10. 59
Tabla 27 Entrevista 1 aplicada a personal clave. 60
Tabla 28 Entrevista 2 aplicada a personal clave. 62
Tabla 29 Entrevista 3 aplicada a personal clave. 64
Tabla 30 Ficha bibliográfica-documental desarrollada 2. 65

Tabla 31 Ficha bibliográfica-documental desarrollada 3. 66
Tabla 32 Ficha bibliográfica-documental desarrollada 4. 66
Tabla 33 Ficha bibliográfica-documental desarrollada 5. 67
Tabla 34 Relación del capítulo con los objetivos específicos. 70
Tabla 35 Operacionalización de los objetivos 71
Tabla 36 Definición del ámbito de auditoría. 73
Tabla 41 Cronograma de ejecución de pruebas de auditoría. 73
Tabla 38 Artículos y criterios normativos aplicados en la auditoría técnica. 74
Tabla 37 Marco legal, documental y técnico aplicado. 75
Tabla 39 Evidencias institucionales utilizadas como anexos de auditoría. 76
Tabla 40 Definición de pruebas de auditoría. 77
Tabla 42 Ejecución de pruebas y resultados. 81
Tabla 46 Hallazgos consolidados de auditoría. 85
Tabla 43 Escala de probabilidad e impacto para la clasificación de hallazgos 87
Tabla 44 Rangos de criticidad aplicados a los hallazgos. 87
Tabla 45 Valoración de criticidad de los hallazgos 88
Tabla 47 Plan de acción priorizado. 92

ÍNDICE DE ILUSTRACIONES

Ilustración 1 Resultados de la encuesta a empleados - pregunta 1. 39
Ilustración 2 Resultados de la encuesta a empleados - pregunta 2. 40
Ilustración 3 Resultados de la encuesta a empleados - pregunta 3. 41
Ilustración 4 Resultados de la encuesta a empleados - pregunta 8. 46
Ilustración 5 Resultados de la encuesta a empleados - pregunta 9. 47
Ilustración 6 Resultados de la encuesta a empleados - pregunta 10. 48
Ilustración 7 Resultados de la encuesta a empleados - pregunta 11. 49
Ilustración 8 Resultados de la encuesta a socios/clientes - pregunta 1. 50
Ilustración 9 Resultados de la encuesta a socios/clientes - pregunta 2. 51
Ilustración 10 Resultados de la encuesta a socios/clientes - pregunta 3. 52
Ilustración 11 Resultados de la encuesta a socios/clientes - pregunta 4. 53
Ilustración 12 Resultados de la encuesta a socios/clientes - pregunta 5. 54
Ilustración 13 Resultados de la encuesta a socios/clientes - pregunta 6. 55
Ilustración 14 Resultados de la encuesta a socios/clientes - pregunta 7. 56
Ilustración 15 Resultados de la encuesta a socios/clientes - pregunta 8. 57
Ilustración 16 Resultados de la encuesta a socios/clientes - pregunta 9. 58
Ilustración 17 Resultados de la encuesta a socios/clientes - pregunta 10. 59
Ilustración 18 Flujo del subproceso de atención de derechos ARCO+. 83
Ilustración 19 Flujo del subproceso de gestión y notificación de brechas. 84
Ilustración 20 Mapa de calor para la evaluación de criticidad 91

ÍNDICE DE ANEXOS

Anexo 1 Política para la Protección y Tratamiento de Datos Personales 104
Anexo 2 Manual de Seguridad de la Información 105
Anexo 3 Formulario de solicitud para el ejercicio de derechos ARCO+ 106
Anexo 4 Subproceso Atención de Derechos ARCO+ 107
Anexo 5 Subproceso Gestión y Notificación de Brechas de Datos 108
Anexo 6 Metodología para la Gestión de Riesgos y Evaluación de Impacto 109
Anexo 7 Plan de Capacitación en Protección de Datos Personales 110
Anexo 8 Formulario de consentimiento para socios/clientes 111
Anexo 9 Formulario de consentimiento para colaboradores 112
Anexo 10 Formulario de consentimiento para proveedores 113
Anexo 11 Formulario de consentimiento para visitantes 114
Anexo 12 Formulario de consentimiento para pasantes 115
Anexo 13 Formulario de consentimiento para directivos 116
Anexo 14 Extracto de Matriz RAT 117
Anexo 15 Extracto de Matriz de Evaluación de Impacto 117
Anexo 16 Dashboard de pruebas SQL complementarias 118
Anexo 17 Flujo BPMN de atención de derechos ARCO+ 118
Anexo 18 Flujo BPMN de gestión y notificación de brechas 119
Anexo 19 Informe final de auditoría técnica entregado a la Cooperativa 120

RESUMEN EJECUTIVO

La presente investigación tuvo como objetivo realizar una auditoría técnica del cumplimiento de la Ley Orgánica de Protección de Datos Personales en los sistemas de información asociados al core financiero Softbank de la Cooperativa de Ahorro y Crédito Credi Ya Ltda. El estudio se desarrolló bajo la modalidad de proyecto de investigación, con enfoque mixto y alcance aplicado, mediante revisión documental, encuestas a empleados y socios/clientes, entrevistas a personal clave y pruebas técnicas de auditoría informática. La auditoría consideró criterios de la LOPDP, su Reglamento General, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701 y marcos NIST, aplicados a consentimiento, derechos ARCO, gestión de brechas, evaluación de impacto, control de accesos, trazabilidad, retención, proveedores y seguridad técnica. Los resultados evidencian un cumplimiento parcial: la Cooperativa cuenta con una base documental relevante, formularios, subprocesos y metodología de riesgos; sin embargo, requiere fortalecer la evidencia operativa, la recertificación de accesos, la depuración de usuarios, la segregación de funciones, la trazabilidad de eventos críticos, la minimización de datos y la formalización de controles de retención y eliminación segura. Como producto final se elaboró un informe de auditoría con hallazgos priorizados y plan de acción. Se concluye que el cumplimiento de la LOPDP debe gestionarse como un proceso continuo, medible y sustentado en evidencias técnicas verificables.

Palabras clave: Auditoría informática, LOPDP, core financiero, seguridad de la información, Cooperativa Credi Ya.

ABSTRACT

This research aimed to conduct a technical audit of compliance with the Organic Law on Personal Data Protection in the information systems associated with the Softbank financial core of Cooperativa de Ahorro y Crédito Credi Ya Ltda. The study was developed as a research project with a mixed and applied approach, using documentary review, surveys applied to employees and members/clients, semi-structured interviews with key personnel, and technical information systems audit tests. The audit considered criteria from the Ecuadorian personal data protection law and its regulation, together with ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, and NIST frameworks, applied to consent, data subject rights, breach management, impact assessment, access control, traceability, retention, providers, and technical security. The results show partial compliance: the cooperative has a relevant documentary basis, forms, subprocesses, and a risk methodology; however, it still needs to strengthen operational evidence, access recertification, user cleanup, segregation of duties, traceability of critical events, data minimization, and formal retention and secure deletion controls. As a final product, an audit report was prepared with prioritized findings and an action plan. It is concluded that compliance with personal data protection regulations must be managed as a continuous, measurable process supported by verifiable technical evidence.

Keywords: IT audit, personal data protection, LOPDP, financial core, information security.

CAPÍTULO I. MARCO TEÓRICO

1.1 Tema de investigación

Auditoría técnica del cumplimiento de la Ley Orgánica de Protección de Datos Personales en los sistemas de información del core financiero de la Cooperativa de Ahorro y Crédito Credi Ya.

1.1.1 Planteamiento del problema

El avance de la tecnología obligó a las empresas a transformar por completo su forma de trabajar, sobre todo al capturar, guardar y transferir datos de sus usuarios. Hoy en día, resguardar esta información dejó de ser una opción técnica para convertirse en una obligación legal y organizativa crítica, especialmente para las entidades que manejan datos delicados de sus clientes o socios. En el contexto ecuatoriano, la Ley Orgánica de Protección de Datos Personales (LOPDP), vigente desde 2021 establece obligaciones de cumplimiento para responsables y encargados del tratamiento, reconoce principios y derechos para los titulares, y exige que el tratamiento de la información se realice bajo criterios de juridicidad, lealtad, transparencia, finalidad, pertinencia y seguridad [1]. El Reglamento General de la LOPDP contempla este marco y desarrolla aspectos operativos relacionados con el ejercicio de derechos, el tratamiento por parte de responsables y encargados, y los mecanismos de aplicación de la normativa [2].

Para las cooperativas del sector financiero popular y solidario, la presión de esta normativa es todavía mayor por la naturaleza de la información que manejan día a día. Estas instituciones custodian historiales crediticios, saldos, transacciones y patrimonios de sus socios; por esa misma razón cualquier vulnerabilidad en sus controles internos no solo expone a la organización a sanciones, sino que afecta directamente la privacidad y los derechos fundamentales de las personas. Adicionalmente, la segmentación de las entidades del Sector Financiero Popular y Solidario, actualizada por la Superintendencia de Economía Popular y Solidaria (SEPS), evidencia que el entorno regulatorio del sector exige mecanismos cada vez más robustos de control, trazabilidad y gestión del riesgo [3].

El National Institute of Standards and Technology (NIST), que es una agencia federal de Estados Unidos, plantea que la gestión del riesgo de privacidad debe integrarse en la

administración empresarial del riesgo y servir como guía para identificar y tratar impactos sobre las personas [4]. De manera complementaria, la norma ISO/IEC 27701 define un sistema de gestión de información de privacidad orientado a responsables y encargados del tratamiento de información personal identificable [5].

Desde la perspectiva de seguridad de la información, la protección de los datos personales requiere preservar la confidencialidad, la integridad y la disponibilidad de la información. El glosario del NIST define estas propiedades como componentes esenciales de la seguridad, vinculadas a impedir divulgaciones no autorizadas, proteger la exactitud y completitud de los activos, y garantizar que la información se encuentre disponible para las entidades autorizadas cuando sea requerida [7]. A su vez, la norma ISO/IEC 27001 proporciona un marco reconocido para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información basado en riesgos [6].

En este contexto institucional, la Cooperativa de Ahorro y Crédito Credi Ya se encuentra en un proceso de fortalecimiento de sus controles internos y de madurez tecnológica, especialmente por la sensibilidad del core financiero que soporta sus operaciones principales. Dicho sistema concentra la mayor parte del tratamiento de datos personales de los socios, por lo que constituye un punto crítico para verificar el cumplimiento de la LOPDP desde una perspectiva técnica. A pesar de la existencia de medidas de seguridad implementadas en la organización, la ausencia de una auditoría técnica formal dificulta determinar, con evidencia verificable, el nivel real de cumplimiento frente a la normativa vigente.

El problema que enfrenta la institución no solo se enfoca a la falta de documentación, también conlleva la posibilidad de que existan brechas de seguridad en puntos importantes como la base legal del tratamiento, la gestión del consentimiento, la atención de derechos del titular, el control de accesos, la clasificación de la información, la trazabilidad de operaciones, la conservación y retención de datos, la relación con terceros y encargados, la gestión de incidentes y la protección de datos desde el diseño. Estas dimensiones exigen una evaluación estructurada y apoyada en marcos de gestión de privacidad y seguridad.

1.2 Antecedentes investigativos

Los antecedentes investigativos permiten ubicar la presente investigación dentro de una línea de trabajo que incluye la protección de datos, seguridad de la información y cumplimiento normativo. En el caso ecuatoriano, la discusión académica y profesional ha cobrado fuerza desde la aprobación de la LOPDP, debido a la necesidad de trasladar sus principios y obligaciones al funcionamiento real de los sistemas de información. Ordóñez Pineda y Correa Quezada [2] realizan un estudio de las políticas públicas de protección de datos en Ecuador y destacan que la aplicación correcta de este derecho no solo requiere reconocimiento normativo, sino que también procesos concretos de implementación y supervisión.

En el ámbito de buenas prácticas, Velasco-Urgilés, Proaño-Reyes y Castro-Sánchez [3] proponen lineamientos para fortalecer el cumplimiento normativo y la manera en la que se manejan los datos para asegurar una protección correcta de los mismos. Su estudio identifica problemas comunes en el sector privado, tales como falta de capacitación, ausencia de procesos específicos y debilidades en la manera en la que las instituciones manejan esta privacidad, lo cual es importante destacar en todas las organizaciones que manejan información sensible de manera masiva.

Con un estudio un poco más profundo relacionado al tema, Mancero-Gavilanes, Proaño-Reyes y Castro-Sánchez [5] examinan la relación entre la protección de datos personales crediticios y la administración del perfil de riesgo en Ecuador. Las autoras hacen un señalamiento en la necesidad de equilibrar el tratamiento legítimo de la información financiera con las exigencias de consentimiento, finalidad y minimización, evidenciando que el sector financiero enfrenta desafíos importantes cuando busca adaptar sus procesos a la nueva normativa.

Por otra parte, Rosas y Pila [6] proponen un recorrido histórico y normativo sobre cómo ha evolucionado la protección de datos en el Ecuador. Lo valioso de su análisis es que demuestra que las fallas actuales no nacieron de golpe con la LOPDP en 2021. Al contrario, el país arrastra un historial de vacíos legales e instituciones débiles que hacían urgente la creación de verdaderos mecanismos de control; una perspectiva clave que le da un piso jurídico sólido a la auditoría técnica que aquí se plantea.

De igual manera, Carrillo Rosero [7] analiza los puntos más importantes de la protección de datos en Ecuador, con un enfoque especial en los principios de consentimiento y finalidad. El trabajo realizado asegura que estos principios aportan estándares mínimos e indispensables para garantizar el correcto ejercicio del derecho, y aporta que una norma no es suficiente si no se enfoca en límites concretos al tratamiento de datos y en herramientas que ayudan a las sanciones y al control. Este enfoque resulta especialmente valioso para la presente investigación, ya que el análisis del core financiero exige verificar precisamente cómo esos principios se reflejan en prácticas y controles institucionales.

Otro antecedente importante es el de Astudillo Alvear, Once González, Alvarado Ajila y García Segarra, quienes estudian la aplicación de la LOPDP en el sistema empresarial privado ecuatoriano. Los autores identifican retos como la ambigüedad interpretativa, la falta de comprensión legal homogénea y el riesgo de aplicación inconsistente dentro de las organizaciones [8]. Este aporte se relaciona directamente con la presente tesis, porque evidencia que el problema del cumplimiento no se limita al sector público o a grandes corporaciones, sino que también afecta a entidades privadas que deben traducir la ley en procedimientos, roles, evidencias y controles concretos.

Asimismo, Cardet Sarduy y Cárdenas Cobo desarrollan un análisis histórico de la evolución normativa de la protección de datos personales en Ecuador. Su estudio organiza hitos normativos, compara el desarrollo ecuatoriano con referentes internacionales e identifica brechas de conocimiento todavía presentes en la materia [9]. Este antecedente es útil porque refuerza la idea de que la protección de datos en el país aún atraviesa una etapa de consolidación doctrinal y operativa, lo cual justifica investigaciones aplicadas que evalúen el cumplimiento real dentro de organizaciones concretas.

Desde un enfoque más técnico, Castro-Paredes, Mendoza-Masache, Loja-Mora y Loján-Alvarado analizan cómo los principios de protección de datos desde el diseño pueden aplicarse en el desarrollo de software, relacionándose con la LOPDP. En su estudio se demuestra que considerar los requisitos legales desde las primeras etapas del ciclo de vida del software contribuye a mejorar la seguridad, la transparencia y el cumplimiento normativo de los sistemas desarrollados [10]. Esta investigación resulta importante para el proyecto que se está desarrollando, ya que permite comprender que la protección de

datos personales no depende únicamente de políticas o documentos institucionales, sino también de la forma en que los sistemas de información son diseñados, configurados y operados en la práctica.

La literatura internacional ha aportado con enfoques metodológicos útiles para investigaciones aplicadas. El NIST Privacy Framework ofrece una estructura para integrar el riesgo de privacidad a la gestión institucional, mientras que la ISO/IEC 27701 extiende los sistemas de gestión hacia controles específicos de privacidad. Por su parte, la propuesta de Privacy by Design de Cavoukian enfatiza que la privacidad debe incorporarse desde la fase de diseño de los sistemas y no como una corrección posterior, incorporando principios como la prevención, la configuración por defecto y la privacidad embebida en la arquitectura tecnológica [16].

Los antecedentes revisados muestran que el cumplimiento efectivo de la normativa de protección de datos no puede reducirse a la existencia de documentos formales. Requiere controles técnicos verificables, evidencia de trazabilidad, procedimientos definidos para atender derechos, gestión de riesgos, respuesta ante incidentes y una cultura organizacional orientada a la responsabilidad proactiva. En consecuencia, la presente investigación se justifica como un estudio aplicado que busca trasladar esos enfoques a un caso concreto: el core financiero de la Cooperativa Credi Ya.

1.3 Fundamentación teórica

1.3.1 Protección de datos personales

La protección de datos personales comprende el conjunto de principios, medidas técnicas, procedimientos y responsabilidades orientadas a garantizar que la información vinculada a personas naturales sea tratada de forma lícita, segura y transparente. En el caso ecuatoriano, la LOPDP reconoce este derecho y establece obligaciones para quienes actúan como responsables o encargados del tratamiento [1]. En términos organizacionales, proteger datos personales implica gestionar adecuadamente todo su ciclo de vida: recolección, almacenamiento, consulta, uso, transferencia, conservación y eliminación.

1.3.2 Ley Orgánica de Protección de Datos Personales y su Reglamento

La LOPDP constituye el marco jurídico central para la presente investigación. Esta ley fija principios aplicables al tratamiento, regula derechos de los titulares, define categorías de actores y establece obligaciones relacionadas con seguridad, riesgos, transferencias, incidentes y responsabilidad demostrada [1]. El Reglamento General desarrolla operativamente varias de estas disposiciones, precisando procedimientos para el ejercicio de derechos, el alcance territorial de la normativa y criterios para la actuación de responsables y encargados [2]. Para una auditoría técnica, ambos instrumentos permiten traducir la norma en criterios de verificación concretos.

1.3.3 Principios del tratamiento de datos

Los principios del tratamiento constituyen la base sobre la cual debe evaluarse cualquier sistema que procese datos personales. La juridicidad exige un motivo claro para usar datos de personas, la finalidad conlleva que la información se use para propósitos explícitos y legítimos; la minimización obliga a tratar únicamente los datos necesarios; y la transparencia requiere informar claramente al titular sobre el uso de su información [1]. Estos principios son vitales en el sector cooperativista, donde el uso excesivo de información y la manera en la que se muestran en los procesos que realizan puede generar riesgos significativos para la privacidad.

1.3.4 Derechos del titular

La normativa ecuatoriana reconoce derechos como información, acceso, rectificación y actualización, eliminación, oposición y portabilidad [1], [2]. Desde el punto de vista técnico, esto implica que los sistemas de información deben permitir localizar, consultar, corregir, bloquear o eliminar datos cuando corresponda, además de registrar las solicitudes realizadas por los titulares. Por ello, la auditoría no solo verifica la existencia formal de políticas, sino la capacidad operativa del sistema para atender dichos requerimientos.

1.3.5 Seguridad de la información

La seguridad de la información es un componente indispensable del cumplimiento normativo. El NIST define la seguridad a partir de la preservación de la integridad, confidencialidad y disponibilidad de la información [7]. En consecuencia, la protección

de los datos personales requiere mecanismos de autenticación, control de acceso, segregación de funciones, registros de actividad, copias de respaldo, cifrado, monitoreo y gestión de vulnerabilidades. La ISO/IEC 27001 establece requisitos para implementar un sistema de gestión de seguridad de la información y propone un enfoque integral basado en riesgo, lo cual resulta especialmente útil en entornos financieros [6].

1.3.6 Gestión de la privacidad y cumplimiento

El NIST Privacy Framework señala que la privacidad debe gestionarse como parte del riesgo empresarial, de modo que la organización pueda identificar impactos sobre las personas y adoptar respuestas proporcionales [4]. La ISO/IEC 27701 establece requisitos y pasos a seguir para un sistema de gestión de información de privacidad, aplicable a controladores y procesadores de información personal identificable [5]. Los dos enfoques son útiles para una auditoría técnica, porque permiten evaluar no solo controles aislados, sino la forma en que la institución tiene la estructura para la gestión integral de privacidad.

1.3.7 Protección de datos desde el diseño y por defecto

La propuesta de Privacy by Design, desarrollada por Cavoukian, sostiene que la privacidad debe integrarse de manera proactiva en los sistemas, procesos y prácticas de negocio [8]. Entre sus principios se encuentran la prevención antes que la corrección, la privacidad como configuración predeterminada y su integración directa en el diseño arquitectónico. Este enfoque es especialmente relevante para los sistemas financieros, ya que promueve que la protección de datos sea considerada desde el diseño de formularios, perfiles de usuario, módulos de auditoría, reportes y transferencias de información.

1.3.8 Gestión de incidentes de seguridad

La gestión de incidentes es fundamental para reducir el impacto de eventos que comprometan la seguridad de la información. NIST SP 800-61r3 plantea recomendaciones para incorporar la respuesta a incidentes dentro de la gestión del riesgo de ciberseguridad, con el fin de mejorar la preparación, reducir la cantidad e impacto de los incidentes y aumentar la efectividad de la detección, respuesta y recuperación [9]. En el marco de la protección de datos personales, esta gestión se relaciona además con la obligación de

documentar y, cuando corresponda, notificar vulneraciones de seguridad a la autoridad y a los titulares afectados.

1.3.9 Core financiero y tratamiento de datos personales

El core financiero es el sistema que soporta las operaciones críticas de una cooperativa, tales como administración de socios, colocación de crédito, pagos, transacciones, consultas y reportes. Debido a que concentra información financiera y personal de alta sensibilidad, constituye un activo tecnológico crítico. Desde la perspectiva de auditoría, evaluar el core financiero implica revisar no solo la funcionalidad del sistema, sino la manera en que sus componentes procesan datos personales, restringe accesos, generan trazabilidad y mantienen evidencia sobre operaciones sensibles.

1.3.10 Auditoría técnica de cumplimiento

La auditoría técnica de cumplimiento puede definirse como un proceso sistemático de revisión que busca determinar si los controles implementados en una organización permiten satisfacer los requerimientos de un marco normativo específico. En este caso, la auditoría busca verificar el nivel de cumplimiento entre los artículos seleccionados de la LOPDP y la realidad operativa del core financiero de Credi Ya. Para esto se debe examinar evidencia documental y técnica, identificar brechas, valorar riesgos y formular recomendaciones según el nivel de importancia para la mejora continua. Los estudios ecuatorianos recientes muestran precisamente que las mayores debilidades se encuentran en la capacidad de aplicar la norma y demostrar cumplimiento de manera verificable [10]–[12].

1.4 Objetivos

1.4.1 Objetivo general

Realizar una auditoría técnica del cumplimiento de la Ley Orgánica de Protección de Datos Personales en los sistemas de información del core financiero de la Cooperativa de Ahorro y Crédito Credi Ya, con el fin de identificar brechas normativas y proponer acciones correctivas que garanticen la protección adecuada de los datos personales.

1.4.2 Objetivos específicos

- Evaluar el cumplimiento técnico-normativo del core financiero de Credi Ya frente a los artículos seleccionados de la LOPDP, mediante una lista de verificación sustentada en evidencia documental y técnica.
- Identificar brechas de cumplimiento, riesgos y vulnerabilidades técnicas y organizativas asociadas al tratamiento de datos personales, con énfasis en control de acceso, trazabilidad, cifrado, minimización, retención, gestión de incidentes y continuidad operativa.
- Elaborar un informe técnico de auditoría con hallazgos clasificados por criticidad, nivel de cumplimiento por artículo y un plan de acción priorizado con medidas correctivas y preventivas para fortalecer la protección de datos personales.

CAPÍTULO II. METODOLOGÍA

2.1 Materiales

Para la recolección de información se emplearon tres instrumentos principales: encuesta dirigida a empleados y a los socios/clientes, entrevista semiestructurada a personal clave y ficha de revisión bibliográfica-documental. La incorporación de una encuesta para socios/clientes permite fortalecer el estudio, debido a que la LOPDP se orienta precisamente a proteger los derechos de los titulares de los datos personales. Con ello, la metodología permitió recoger tanto el punto de vista de quienes tratan la información dentro de la cooperativa como la percepción de quienes entregan sus datos para acceder a servicios financieros.

La encuesta aplicada a los empleados tuvo como objetivo conocer qué tanto manejan internamente temas relacionados con la gobernanza de datos, el delegado de protección de datos, el registro de actividades, el consentimiento informado, las bases legales para el tratamiento de datos, la exactitud de datos crediticios, el tratamiento de datos sensibles o biométricos, la atención de derechos ARCO+, la seguridad de la información, la gestión de incidentes, los proveedores y la evaluación de impacto.

Por otro lado, la encuesta dirigida a socios y clientes permitió identificar su percepción sobre la información que reciben, la claridad del consentimiento, el conocimiento de sus derechos, los canales de atención disponibles, la confianza en la confidencialidad, el uso de datos crediticios, la comunicación de información a terceros, la revocatoria del consentimiento y la necesidad de fortalecer las medidas de protección.

Finalmente, las entrevistas semiestructuradas se enfocaron en profundizar cómo se aplican, en la práctica, las líneas de acción de la LOPDP dentro de la cooperativa. Se consideraron tres perfiles clave: Delegada de Protección de Datos Personales, Coordinador de TI y Responsable de Atención al Socio u Operaciones. Finalmente, la ficha bibliográfica-documental permitió organizar la información normativa y técnica necesaria para construir los criterios de auditoría.

Modelo de encuesta dirigida a empleados

Objetivo: recopilar información sobre el nivel de conocimiento, aplicación y percepción del personal de la cooperativa respecto a las líneas de acción de la LOPDP en el tratamiento de datos personales dentro del core financiero.

Pregunta 1. ¿Conoce si la cooperativa mantiene un registro de actividades de tratamiento de datos personales?

a) Nada

b) Poco

c) Parcialmente

d) Completamente

Pregunta 2. ¿Conoce usted quién cumple la función de Delegado de Protección de Datos Personales y cuál es su rol?

a) Nada

b) Poco

c) Moderadamente

d) Mucho

Pregunta 3. ¿Los formularios de consentimiento informan con claridad para qué se usan los datos personales de socios y clientes?

a) Nunca

b) Rara vez

c) Frecuentemente

d) Siempre

Pregunta 4. ¿Conoce usted las bases legales que permiten tratar datos personales además del consentimiento?

a) Nada

b) Poco

c) Moderadamente

d) Mucho

Pregunta 5. ¿Considera que los datos crediticios de socios y clientes se mantienen exactos y actualizados?

a) En desacuerdo

b) Neutral

c) De acuerdo

d) Muy de acuerdo

Pregunta 6. ¿El tratamiento de datos sensibles o biométricos cuenta con medidas reforzadas de seguridad?

a) Nada

b) Poco

c) Moderadamente

d) Mucho

Pregunta 7. ¿Existen protocolos claros para atender derechos ARCO+ de los socios?

a) No existen

b) Poco claros

c) Parcialmente claros

d) Claros

Pregunta 8. ¿Los canales para ejercer derechos de protección de datos son sencillos, gratuitos y conocidos por el personal?

a) Nada

b) Poco

c) Parcialmente

d) Totalmente

Pregunta 9. ¿Se aplican controles técnicos como contraseñas, perfiles, cifrado o restricciones para proteger información financiera?

a) Nunca

b) Rara vez

c) Frecuentemente

d) Siempre

Pregunta 10. ¿Conoce usted un procedimiento para reportar incidentes o vulneraciones que afecten datos personales?

a) Nada

b) Poco

c) Moderadamente

d) Mucho

Pregunta 11. ¿La cooperativa controla que proveedores o encargados cumplan estándares de confidencialidad y seguridad?

a) Nada

b) Poco

c) Parcialmente

d) Totalmente

Modelo de encuesta dirigida a socios/clientes

Objetivo: recopilar información sobre la percepción de los socios y clientes como titulares de datos personales, especialmente respecto a transparencia, consentimiento, derechos, confidencialidad, transferencias, revocatoria y notificación de incidentes.

Pregunta 1. ¿La cooperativa le informó para qué utilizaría sus datos personales al momento de vincularse como socio/cliente?

a) Nunca

b) Poco

c) Suficientemente

d) Totalmente

Pregunta 2. ¿El consentimiento que firmó o aceptó le pareció claro y fácil de entender?

a) Nada claro

b) Poco claro

c) Claro

d) Muy claro

Pregunta 3. ¿Conoce sus derechos de acceso, rectificación, eliminación, oposición y portabilidad de datos?

a) Nada

b) Poco

c) Moderadamente

d) Mucho

Pregunta 4. ¿Conoce los canales para solicitar corrección, eliminación u oposición al uso de sus datos?

a) Nada

b) Poco

c) Moderadamente

d) Mucho

Pregunta 5. ¿Confía en que la cooperativa protege la confidencialidad de su información financiera y crediticia?

a) Nada

b) Poco

c) Confío

d) Confío mucho

Pregunta 6. ¿Sabe que sus datos crediticios se usan para analizar capacidad de pago y perfil de riesgo?

a) No sabía

b) Lo sabía poco

c) Sí sabía

d) Lo sabía claramente

Pregunta 7. ¿La cooperativa le ha informado si sus datos pueden ser compartidos con terceros autorizados?

a) Nunca

b) Poco

c) Suficientemente

d) Totalmente

Pregunta 8. ¿Conoce que puede revocar su consentimiento cuando corresponda?

a) Nada

b) Poco

c) Moderadamente

d) Mucho

Pregunta 9. ¿Considera importante que la cooperativa le notifique si ocurre una vulneración de seguridad que afecte sus datos?

a) Nada importante

b) Poco importante

c) Importante

d) Muy importante

Pregunta 10. ¿Considera que la cooperativa debe fortalecer sus medidas de protección de datos personales?

a) En desacuerdo

b) Neutral

c) De acuerdo

d) Muy de acuerdo

Modelo de entrevista semiestructurada

Objetivo: obtener información estratégica, técnica y operativa sobre la aplicación de las líneas de acción de la LOPDP en la cooperativa, considerando gobernanza, registro de actividades, consentimiento, derechos, datos crediticios, seguridad, incidentes, proveedores y evaluación de impacto.

Tabla 1 Guía de Entrevista Semiestructurada

N.°	Pregunta	Respuesta	Observación
1	¿Cómo se ha organizado la gobernanza de protección de datos personales dentro de la cooperativa?		
2	¿La cooperativa mantiene un registro de actividades de tratamiento donde se identifique finalidad, responsables, usuarios con acceso y tiempo de conservación?		
3	¿Cómo se asegura que el consentimiento de socios/clientes sea libre, específico, informado e inequívoco?		
4	¿Qué mecanismos existen para diferenciar tratamientos basados en consentimiento, cumplimiento legal y ejecución contractual?		
5	¿Cómo se gestiona la exactitud, actualización y seguridad de los datos crediticios de socios/clientes?		
6	¿Existen medidas reforzadas para datos sensibles o biométricos, en caso de ser tratados por la cooperativa?		
7	¿Qué protocolos existen para atender derechos de acceso, rectificación, eliminación, oposición y portabilidad?		
8	¿Cómo se gestionan incidentes o vulneraciones de seguridad que puedan afectar datos personales?		
9	¿Cómo se controla que proveedores o encargados del tratamiento cumplan estándares de confidencialidad y seguridad?		
10	¿Se realizan evaluaciones de impacto o análisis de riesgo antes de nuevos tratamientos, tecnologías o integraciones?		

Modelo de ficha bibliográfica-documental

Objetivo: registrar, organizar y analizar información proveniente de leyes, reglamentos, normas técnicas, documentos institucionales y marcos de seguridad y privacidad relacionados con la auditoría técnica del cumplimiento de la LOPDP.

Tabla 2 Ficha de revisión bibliográfica - documental

Campo	Contenido
Tipo de fuente	( ) Ley ( ) Reglamento ( ) Norma técnica ( ) Informe técnico ( ) Documento institucional ( ) Artículo científico ( ) Otro
Título del documento	
Autor(es) / institución	
Año de publicación	
Referencia bibliográfica	
Tema principal	
Resumen del contenido	
Aporte para la investigación	
Relación con la auditoría LOPDP	
Categorías identificadas	Gobernanza; Consentimiento; Derechos ARCO+; Datos crediticios; Seguridad; Incidentes; Proveedores; Evaluación de impacto
Observaciones	

2.2 Métodos

La presente investigación emplea un enfoque mixto, con predominio cualitativo. El componente cuantitativo se utiliza para organizar y analizar las respuestas de empleados y socios/clientes mediante frecuencias, porcentajes y gráficos descriptivos. El componente cualitativo se aplica en las entrevistas y en la revisión bibliográfica-documental, permitiendo interpretar el nivel de cumplimiento, las brechas institucionales y los elementos técnicos que deben ser considerados en la auditoría.

El enfoque se mantiene alineado con una auditoría técnica, debido a que no se limita a medir percepciones, sino que permite relacionar los resultados con criterios normativos y controles de seguridad de la información. En consecuencia, los datos obtenidos sirven como base para identificar procesos críticos, evaluar el cumplimiento de la LOPDP y construir hallazgos en el desarrollo de la auditoría.

2.2.1 Modalidad de la investigación

Investigación de campo

La investigación se desarrollará bajo una modalidad de campo, ya que la información se obtendrá directamente de la agencia matriz de la cooperativa Credi Ya y de los titulares de datos personales que interactúan con la institución. Esta modalidad permitirá conocer cómo se gestionan los datos personales desde la perspectiva interna del personal y desde la percepción externa de socios/clientes.

La investigación de campo se apoyará en encuestas aplicadas a empleados y socios/clientes, así como en entrevistas semiestructuradas a personal clave. Esta aproximación permitirá contrastar la existencia de procesos, controles y canales institucionales con la forma en que son conocidos, percibidos y utilizados por los sujetos involucrados en el tratamiento de datos personales.

Investigación bibliográfica-documental

La investigación adoptará una modalidad bibliográfica-documental porque se fundamentará en la revisión de la LOPDP, su Reglamento General, normas técnicas de seguridad y privacidad, documentos institucionales y literatura académica relacionada. La revisión documental permitirá identificar criterios de auditoría y categorías de análisis vinculadas con gobernanza, consentimiento, derechos, seguridad, incidentes, proveedores y evaluación de impacto.

Investigación aplicada

La investigación se considerará aplicada, porque se orientará a un caso institucional específico: el cumplimiento de la LOPDP en el core financiero de la cooperativa Credi Ya. Los resultados no se limitarán a una descripción teórica, sino que permitirán sustentar la auditoría técnica, identificar brechas y proponer acciones de mejora orientadas al fortalecimiento de la gestión de datos personales.

2.2.2 Población y muestra

La población de la investigación se organizó en tres grupos: empleados relacionados con el tratamiento de datos personales, socios/clientes de la agencia matriz e informantes clave

vinculados con la gestión, operación y seguridad de la información. El primer grupo está conformado por empleados de la cooperativa que mantienen relación directa con el tratamiento de datos personales dentro del core financiero. El segundo grupo está conformado por socios/clientes de la agencia matriz, en calidad de titulares de datos personales tratados por la cooperativa para procesos de ahorro, crédito, atención, actualización de información y cumplimiento regulatorio.

Población de empleados

La población de empleados se encuentra integrada por 25 personas: 3 miembros del equipo técnico, 20 colaboradores administrativos y operativos, y 2 directivos vinculados con supervisión, control o cumplimiento institucional. Debido a que se trata de una población pequeña y accesible, se trabajará con la totalidad de empleados relacionados con el objeto de estudio.

Población de socios/clientes

Para el grupo de socios/clientes, se considerará como población de referencia a las personas que mantienen relación activa con la cooperativa y que acuden o interactúan con la agencia matriz durante el periodo de levantamiento de información. Al tratarse de un modelo académico y debido a la imposibilidad de encuestar a la totalidad de socios de la institución, se aplicará un muestreo no probabilístico por conveniencia a 60 socios/clientes, seleccionados por su disponibilidad y relación directa con los servicios financieros de la cooperativa, enfocado a las personas que tengan un crédito en la institución.

Muestra

La muestra para la aplicación de encuestas estuvo conformada por 85 participantes: 25 empleados y 60 socios/clientes. Además, se aplicaron tres entrevistas semiestructuradas a informantes clave: Delegada de Protección de Datos Personales, Coordinador de TI y Coordinador de Operaciones. En total, se consideraron 88 fuentes primarias de información.

Tabla 3 Población y muestra del estudio.

Grupo	Descripción	Población	Muestra	Tipo de muestreo
Empleados	Personal técnico, administrativo, operativo y directivo relacionado con tratamiento de datos personales.	25	25	Censo institucional
Socios/clientes	Titulares de datos personales que interactúan con la agencia matriz.	Población accesible de agencia matriz	60	No probabilístico por conveniencia
Informantes clave	Delegada de Protección de Datos, Coordinador de TI y Responsable de Atención al Socio/Operaciones.	3	3	Selección intencional
Total	Participantes considerados para levantamiento de información.	-	88	Mixto

2.2.3 Recolección de información

a) Validación de encuesta por coeficiente de alfa de Cronbach

Con el fin de valorar la consistencia interna de la encuesta, se estimó el coeficiente alfa de Cronbach, cuyos valores se presentan en la Tabla 4 sobre cinco ítems de tipo Likert asociados a conocimiento, lineamientos, control de acceso, confidencialidad y necesidad de fortalecimiento de controles. El cálculo permitió obtener un nivel aceptable 0.78 de confiabilidad para un instrumento de carácter descriptivo aplicado en un contexto institucional.

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum \sigma_i^2}{\sigma_{total}^2}\right)$$

Tabla 4 Coeficiente alfa de Cronbach en la encuesta.

Simbología	Valor
A	0,78
K	5
Σ varianza de los ítems	7,31
Varianza total del instrumento	19,43

Tabla 5 Criterios de la escala de consistencia del alfa de Cronbach.

Rango	Interpretación
0,90 - 1,00	Excelente
0,80 - 0,89	Buena
0,70 - 0,79	Aceptable
0,60 - 0,69	Cuestionable
0,50 - 0,59	Pobre
< 0,50	Inaceptable

2.2.4 Procesamiento y análisis de datos

El procesamiento de datos se realizó mediante la organización de las respuestas en tablas de frecuencia y porcentaje, acompañadas de gráficos de barras para facilitar la interpretación visual. Los resultados de empleados y socios/clientes se analizaron de forma separada y posteriormente se integraron con las entrevistas y fichas bibliográficas-documentales. Esta integración permitió relacionar la percepción institucional con la percepción de los titulares de datos personales y con los criterios normativos derivados de la LOPDP.

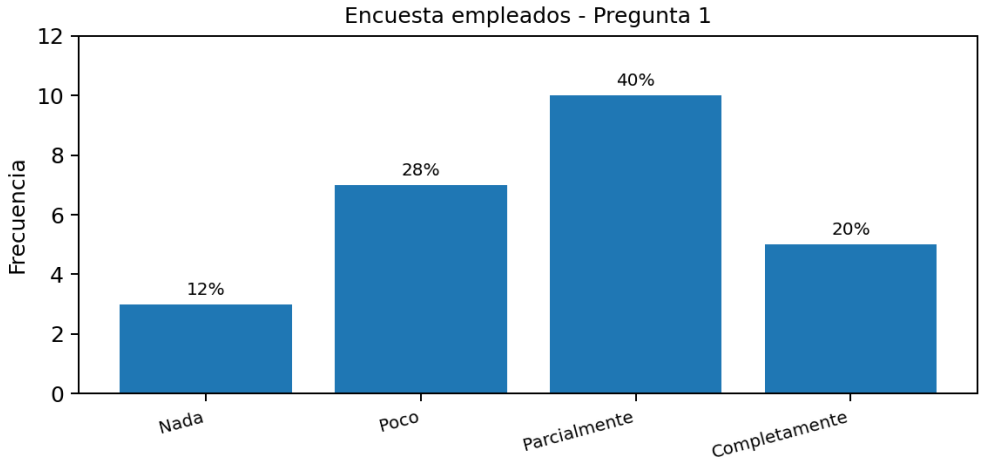
a) Resultados de la encuesta dirigida a empleados

Pregunta 1. ¿Conoce si la cooperativa mantiene un registro de actividades de tratamiento de datos personales?

Tabla 6 Resultados de la encuesta a empleados - pregunta 1.

Indicador	Frecuencia	Porcentaje
Nada	3	12%
Poco	7	28%
Parcialmente	10	40%
Completamente	5	20%
Total	25	100%

Ilustración 1 Resultados de la encuesta a empleados - pregunta 1.



Análisis e interpretación

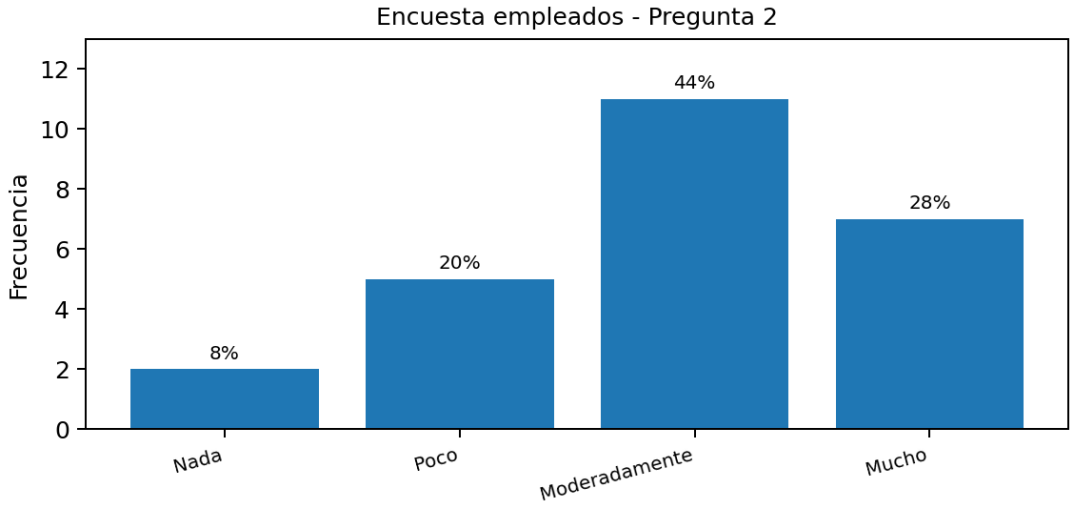
Los resultados muestran que el 60% del personal identifica de forma parcial o completa la existencia de registros de actividades de tratamiento, mientras que el 40% indica conocer poco o nada sobre este aspecto. Esto evidencia que la documentación de procesos que involucran datos personales todavía no se encuentra plenamente socializada entre los colaboradores.

Pregunta 2. ¿Conoce usted quién cumple la función de Delegado de Protección de Datos Personales y cuál es su rol?

Tabla 7 Resultados de la encuesta a empleados - pregunta 2.

Indicador	Frecuencia	Porcentaje
Nada	2	8%
Poco	5	20%
Moderadamente	11	44%
Mucho	7	28%
Total	25	100%

Ilustración 2 Resultados de la encuesta a empleados - pregunta 2.



Análisis e interpretación

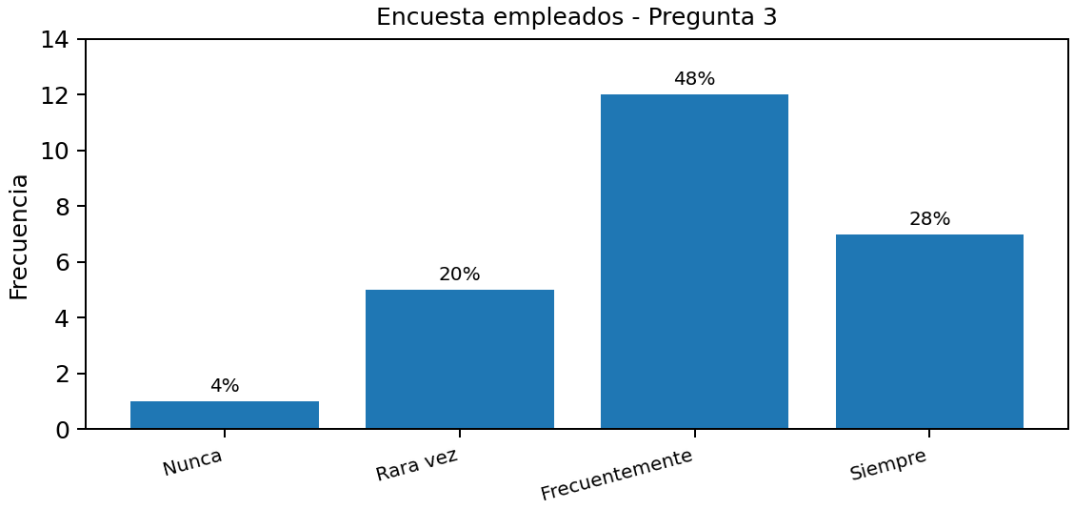
El 72% de los encuestados manifiesta un conocimiento moderado o alto sobre la figura del Delegado de Protección de Datos Personales. Este resultado es favorable para la gobernanza de privacidad; sin embargo, el 28% restante demuestra que aún se requiere reforzar la comunicación interna sobre funciones, canales y responsabilidades del delegado.

Pregunta 3. ¿Los formularios de consentimiento informan con claridad para qué se usan los datos personales de socios y clientes?

Tabla 8 Resultados de la encuesta a empleados - pregunta 3.

Indicador	Frecuencia	Porcentaje
Nunca	1	4%
Rara vez	5	20%
Frecuentemente	12	48%
Siempre	7	28%
Total	25	100%

Ilustración 3 Resultados de la encuesta a empleados - pregunta 3.



Análisis e interpretación

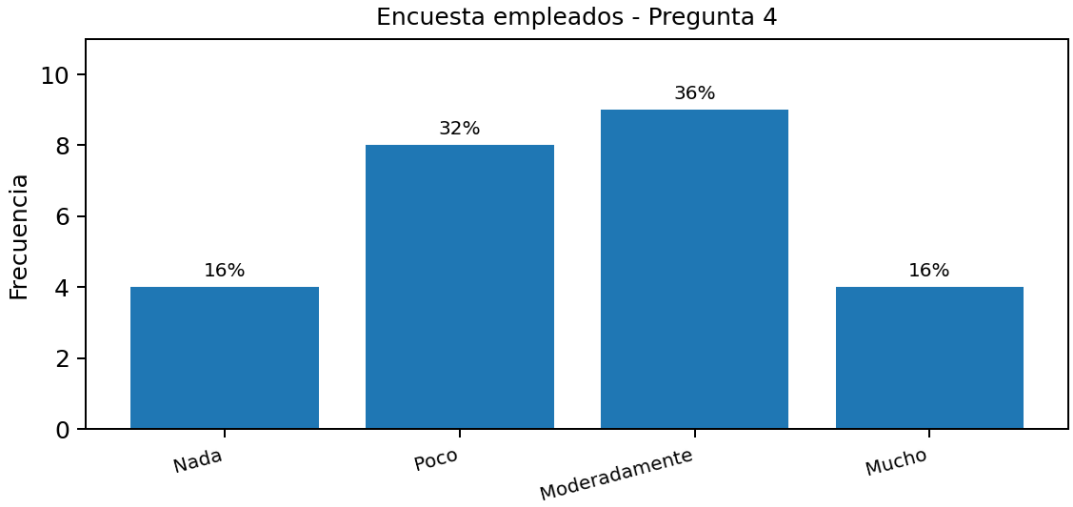
El 76% del personal considera que los formularios informan frecuentemente o siempre la finalidad del tratamiento. No obstante, la existencia de respuestas en categorías bajas evidencia la necesidad de revisar el lenguaje de los formularios para garantizar que el consentimiento sea informado, específico e inequívoco.

Pregunta 4. ¿Conoce usted las bases legales que permiten tratar datos personales además del consentimiento?

Tabla 9 Resultados de la encuesta a empleados - pregunta 4.

Indicador	Frecuencia	Porcentaje
Nada	4	16%
Poco	8	32%
Moderadamente	9	36%
Mucho	4	16%
Total	25	100%

Ilustración 4 Resultados de la encuesta a empleados - pregunta 4.



Análisis e interpretación

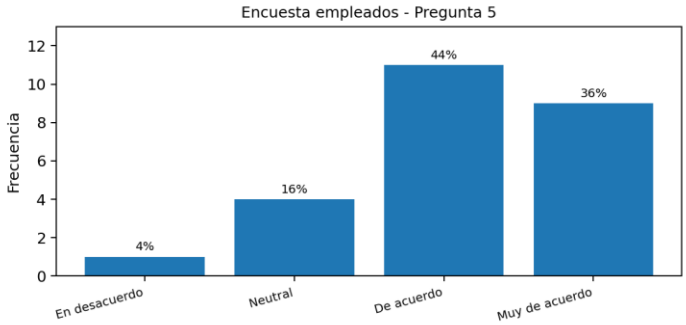
El conocimiento sobre bases de licitud alternativas al consentimiento es limitado, ya que el 48% señaló conocer poco o nada sobre este tema. Este resultado es relevante porque en una cooperativa también se tratan datos por obligaciones legales, ejecución de contratos financieros y gestión de riesgos, por lo que el personal debe diferenciar estos supuestos.

Pregunta 5. ¿Considera que los datos crediticios de socios y clientes se mantienen exactos y actualizados?

Tabla 10 Resultados de la encuesta a empleados - pregunta 5.

Indicador	Frecuencia	Porcentaje
En desacuerdo	1	4%
Neutral	4	16%
De acuerdo	11	44%
Muy de acuerdo	9	36%
Total	25	100%

Ilustración 5 Resultados de la encuesta a empleados - pregunta 5.



Análisis e interpretación

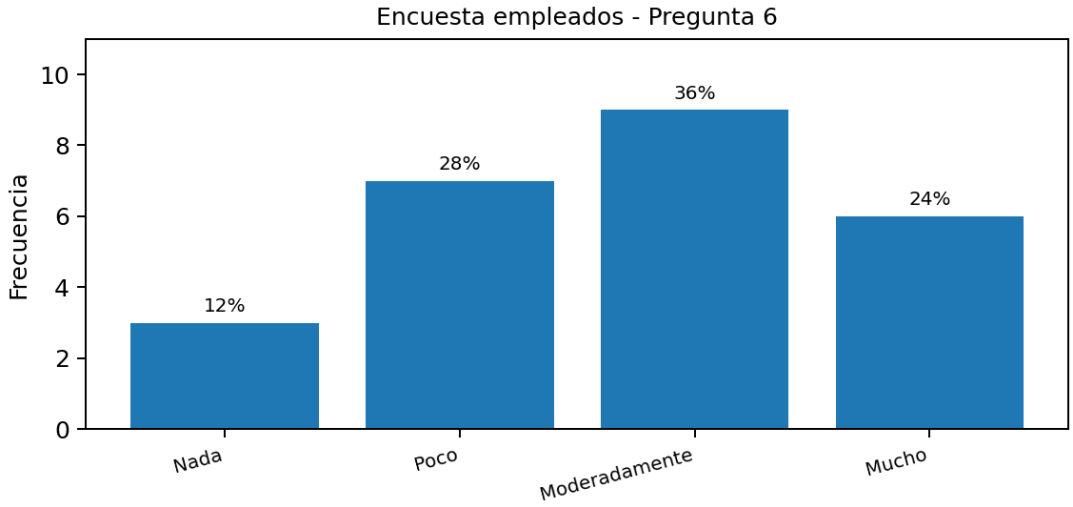
El 80% de los participantes se ubicó entre de acuerdo y muy de acuerdo respecto a la exactitud y actualización de datos crediticios. Este resultado refleja una percepción positiva sobre la calidad de la información financiera; sin embargo, debe complementarse con controles de actualización, validación y trazabilidad.

Pregunta 6. ¿El tratamiento de datos sensibles o biométricos cuenta con medidas reforzadas de seguridad?

Tabla 11 Resultados de la encuesta a empleados - pregunta 6.

Indicador	Frecuencia	Porcentaje
Nada	3	12%
Poco	7	28%
Moderadamente	9	36%
Mucho	6	24%
Total	25	100%

Ilustración 6 Resultados de la encuesta a empleados - pregunta 6.



Análisis e interpretación

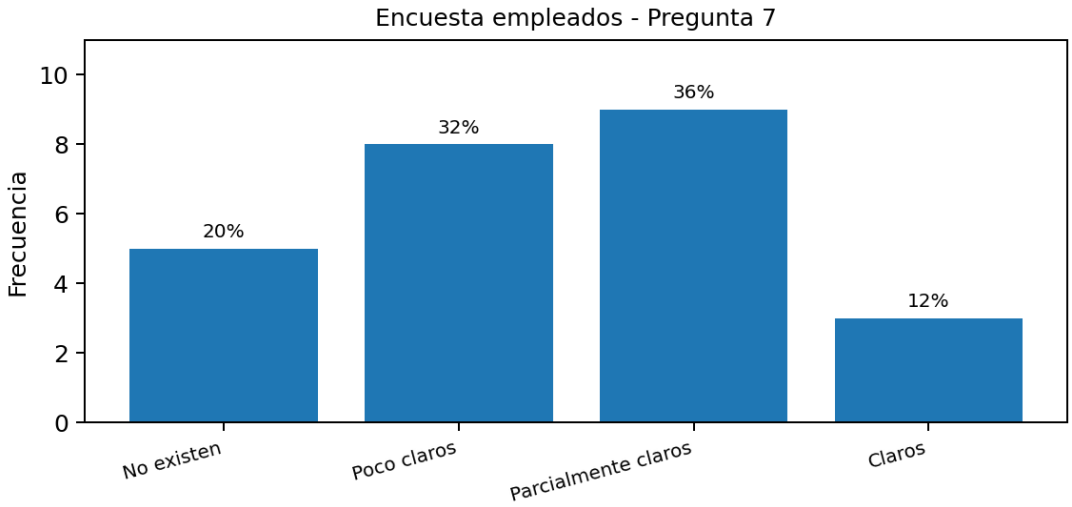
El 60% considera que existen medidas moderadas o altas para datos sensibles o biométricos, pero el 40% percibe que estas medidas son bajas o inexistentes. Este resultado indica que la cooperativa debe fortalecer la difusión y evidencia de controles especiales para información de mayor sensibilidad.

Pregunta 7. ¿Existen protocolos claros para atender derechos ARCO+ de los socios?

Tabla 12 Resultados de la encuesta a empleados - pregunta 7.

Indicador	Frecuencia	Porcentaje
No existen	5	20%
Poco claros	8	32%
Parcialmente claros	9	36%
Claros	3	12%
Total	25	100%

Ilustración 7 Resultados de la encuesta a empleados - pregunta 7.



Análisis e interpretación

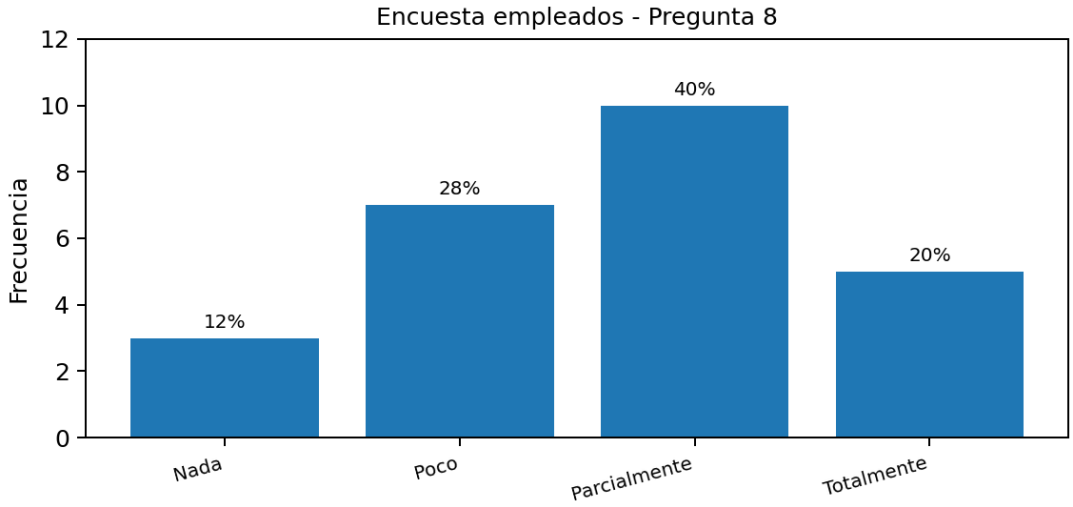
Solo el 48% identifica protocolos parcial o claramente definidos para atender derechos ARCO+, mientras que el 52% los percibe inexistentes o poco claros. Este hallazgo refleja una brecha en la formalización y socialización de procesos para acceso, rectificación, eliminación, oposición y portabilidad.

Pregunta 8. ¿Los canales para ejercer derechos de protección de datos son sencillos, gratuitos y conocidos por el personal?

Tabla 13 Resultados de la encuesta a empleados - pregunta 8.

Indicador	Frecuencia	Porcentaje
Nada	3	12%
Poco	7	28%
Parcialmente	10	40%
Totalmente	5	20%
Total	25	100%

Ilustración 4 Resultados de la encuesta a empleados - pregunta 8.



Análisis e interpretación

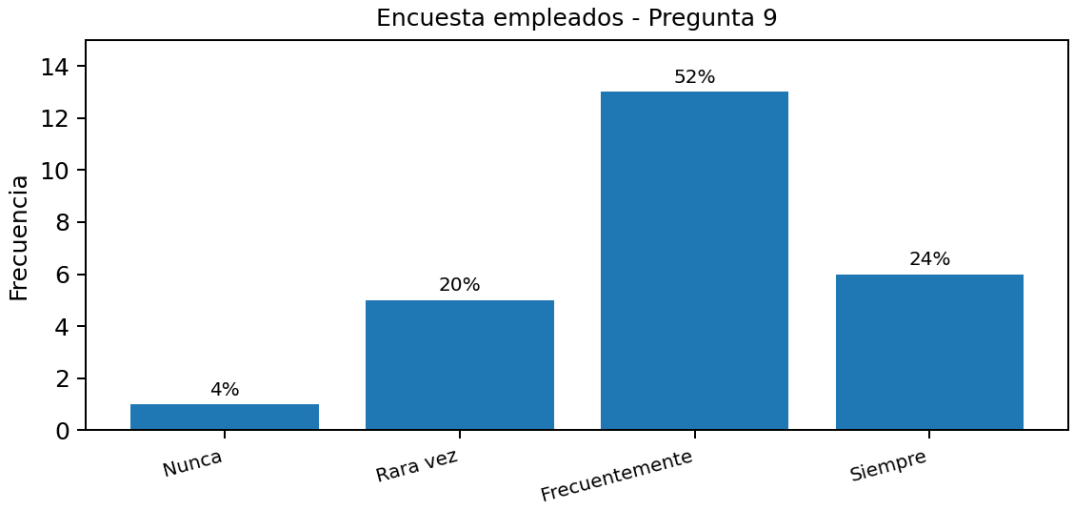
El 60% reconoce parcial o totalmente la existencia de canales sencillos y gratuitos para derechos del titular. Sin embargo, el 40% muestra desconocimiento o baja claridad, por lo que es necesario fortalecer la comunicación interna y la señalización de canales físicos y digitales.

Pregunta 9. ¿Se aplican controles técnicos como contraseñas, perfiles, cifrado o restricciones para proteger información financiera?

Tabla 14 Resultados de la encuesta a empleados - pregunta 9.

Indicador	Frecuencia	Porcentaje
Nunca	1	4%
Rara vez	5	20%
Frecuentemente	13	52%
Siempre	6	24%
Total	25	100%

Ilustración 5 Resultados de la encuesta a empleados - pregunta 9.



Análisis e interpretación

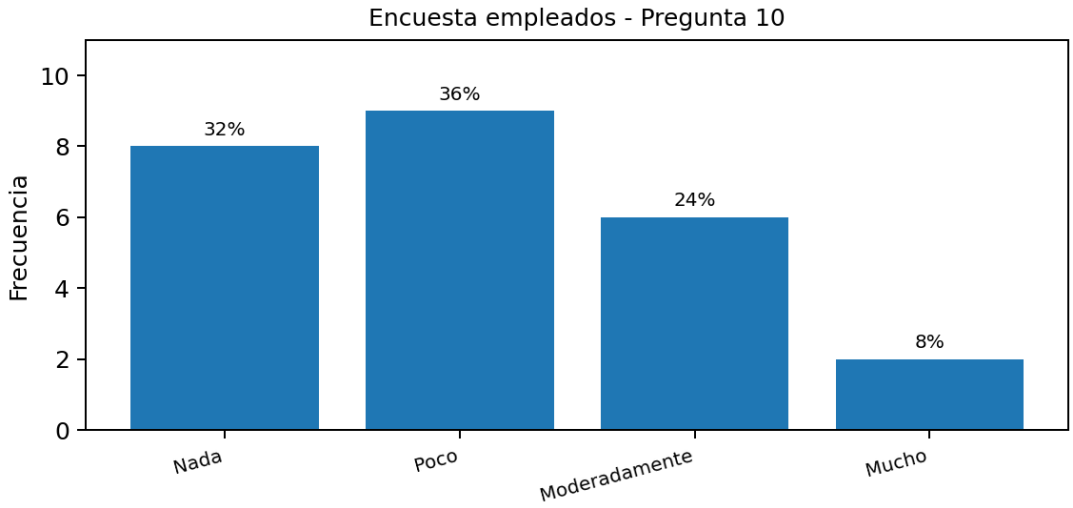
El 76% del personal considera que los controles técnicos se aplican frecuentemente o siempre. Este resultado es positivo desde la perspectiva de seguridad de la información, aunque debe ser respaldado con evidencia técnica como matrices de perfiles, políticas de contraseñas, bitácoras y reportes de revisión.

Pregunta 10. ¿Conoce usted un procedimiento para reportar incidentes o vulneraciones que afecten datos personales?

Tabla 15 Resultados de la encuesta a empleados - pregunta 10.

Indicador	Frecuencia	Porcentaje
Nada	8	32%
Poco	9	36%
Moderadamente	6	24%
Mucho	2	8%
Total	25	100%

Ilustración 6 Resultados de la encuesta a empleados - pregunta 10.



Análisis e interpretación

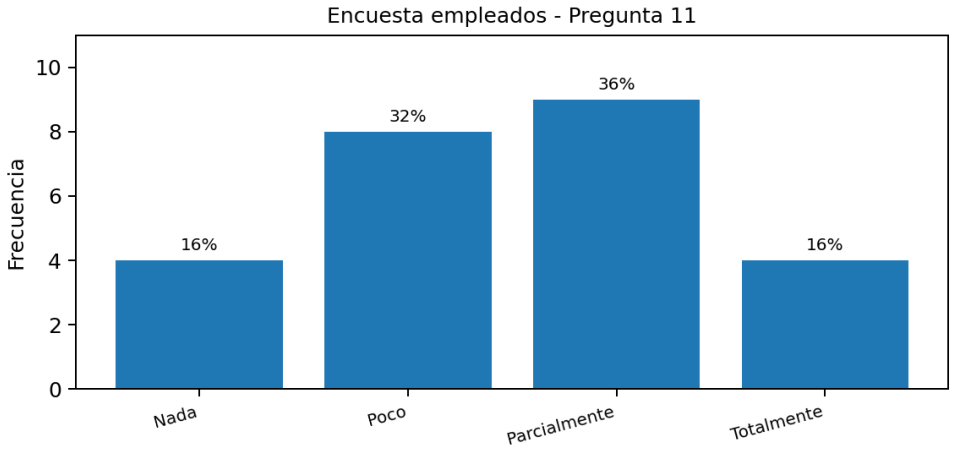
El 68% de los encuestados conoce poco o nada sobre el procedimiento de reporte de incidentes o vulneraciones. Este resultado constituye una alerta metodológica, pues la seguridad y gestión de incidentes es una de las líneas de acción centrales para el cumplimiento de la LOPDP en cooperativas.

Pregunta 11. ¿La cooperativa controla que proveedores o encargados cumplan estándares de confidencialidad y seguridad?

Tabla 16 Resultados de la encuesta a empleados - pregunta 11.

Indicador	Frecuencia	Porcentaje
Nada	4	16%
Poco	8	32%
Parcialmente	9	36%
Totalmente	4	16%
Total	25	100%

Ilustración 7 Resultados de la encuesta a empleados - pregunta 11.



Análisis e interpretación

El 52% identifica controles parciales o totales sobre proveedores, pero el 48% percibe poco o ningún control. Esto evidencia la necesidad de fortalecer el inventario de encargados, contratos de confidencialidad, evaluación periódica de proveedores y evidencia de garantías técnicas.

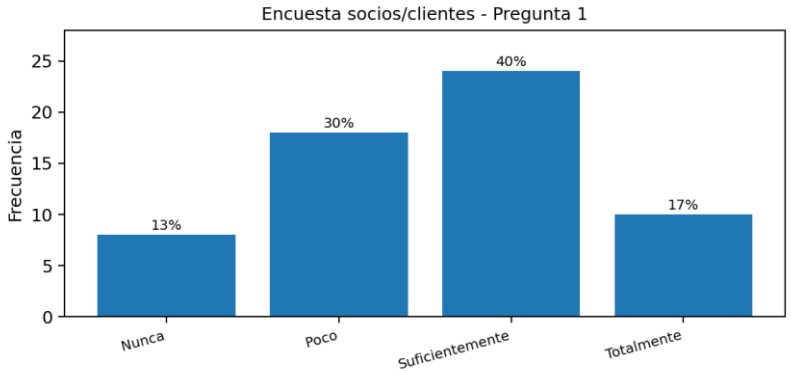
b) Resultados de la encuesta dirigida a socios/clientes

Pregunta 1. ¿La cooperativa le informó para qué utilizaría sus datos personales al momento de vincularse como socio/cliente?

Tabla 17 Resultados de la encuesta a socios/clientes - pregunta 1.

Indicador	Frecuencia	Porcentaje
Nunca	8	13.3%
Poco	18	30.0%
Suficientemente	24	40.0%
Totalmente	10	16.7%
Total	60	100%

Ilustración 8 Resultados de la encuesta a socios/clientes - pregunta 1.



Análisis e interpretación

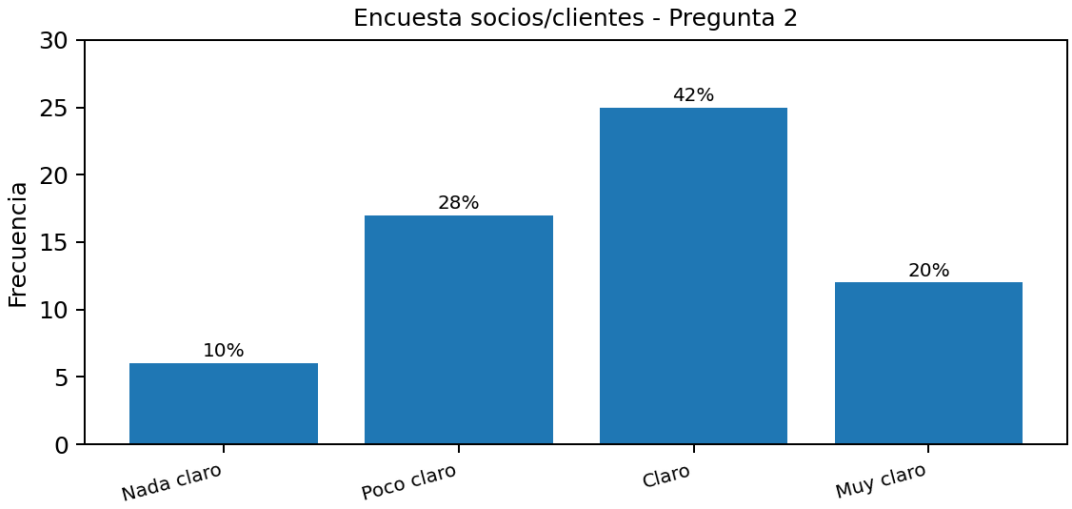
El 56,7% de los socios considera que recibió información suficiente o total sobre el uso de sus datos al momento de vincularse. No obstante, el 43,3% percibe información insuficiente, lo que demuestra la necesidad de mejorar la claridad del aviso de privacidad y del consentimiento informado.

Pregunta 2. ¿El consentimiento que firmó o aceptó le pareció claro y fácil de entender?

Tabla 18 Resultados de la encuesta a socios/clientes - pregunta 2.

Indicador	Frecuencia	Porcentaje
Nada claro	6	10.0%
Poco claro	17	28.3%
Claro	25	41.7%
Muy claro	12	20.0%
Total	60	100%

Ilustración 9 Resultados de la encuesta a socios/clientes - pregunta 2.



Análisis e interpretación

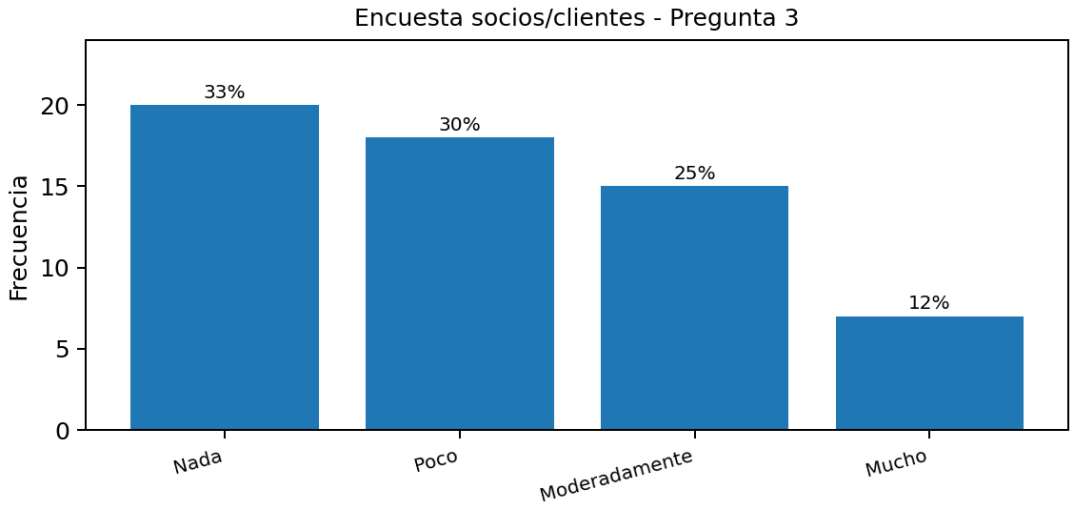
El 61,7% de los encuestados indica que el consentimiento fue claro o muy claro. Sin embargo, el 38,3% considera que fue poco claro o nada claro. Este resultado muestra que los formularios cumplen su propósito solo de manera parcial, por lo que sería necesario utilizar un lenguaje más sencillo y explicar de forma más directa las finalidades del tratamiento, los derechos de los titulares y los canales de atención disponibles.

Pregunta 3. ¿Conoce sus derechos de acceso, rectificación, eliminación, oposición y portabilidad de datos?

Tabla 19 Resultados de la encuesta a socios/clientes - pregunta 3.

Indicador	Frecuencia	Porcentaje
Nada	20	33.3%
Poco	18	30.0%
Moderadamente	15	25.0%
Mucho	7	11.7%
Total	60	100%

Ilustración 10 Resultados de la encuesta a socios/clientes - pregunta 3.



Análisis e interpretación

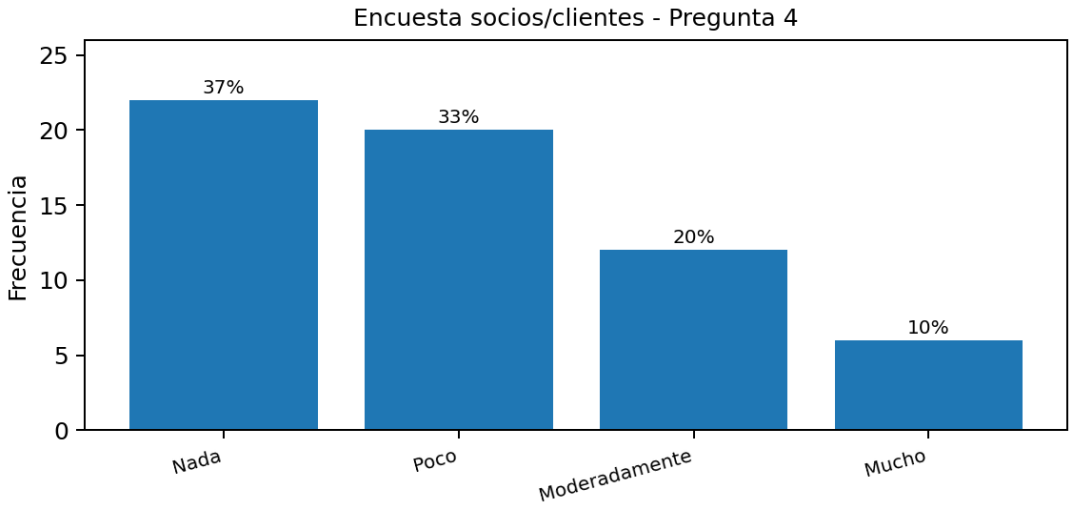
El 63,3% de los socios conoce poco o nada sobre sus derechos ARCO+. Este resultado evidencia una brecha de transparencia hacia los titulares y justifica la necesidad de campañas informativas, carteleras, material web y comunicación en lenguaje sencillo.

Pregunta 4. ¿Conoce los canales para solicitar corrección, eliminación u oposición al uso de sus datos?

Tabla 20 Resultados de la encuesta a socios/clientes - pregunta 4.

Indicador	Frecuencia	Porcentaje
Nada	22	36.7%
Poco	20	33.3%
Moderadamente	12	20.0%
Mucho	6	10.0%
Total	60	100%

Ilustración 11 Resultados de la encuesta a socios/clientes - pregunta 4.



Análisis e interpretación

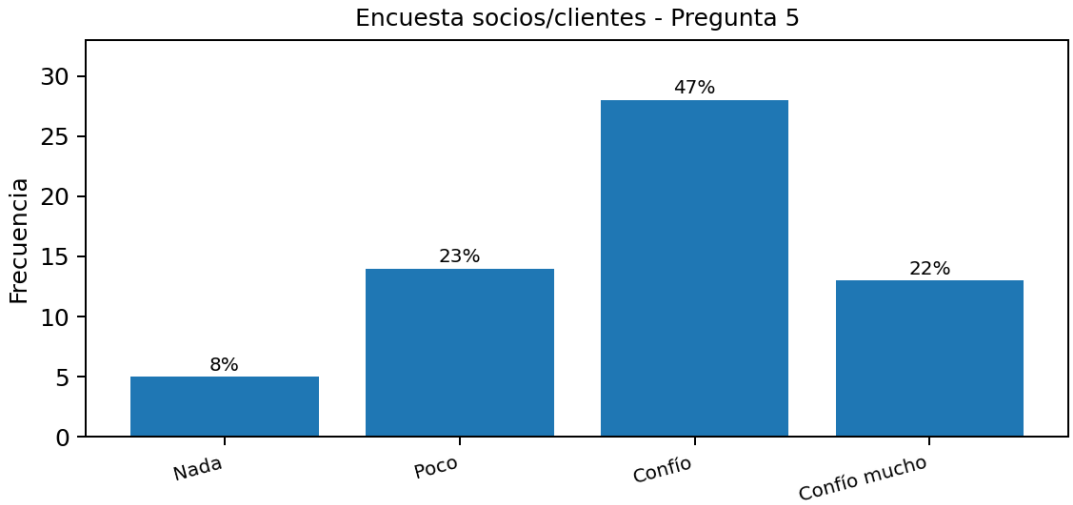
El 70% de los socios conoce poco o nada sobre los canales para ejercer derechos. Este hallazgo refuerza que no basta con disponer de canales internos; estos deben ser visibles, gratuitos, sencillos y comunicados de manera permanente.

Pregunta 5. ¿Confía en que la cooperativa protege la confidencialidad de su información financiera y crediticia?

Tabla 21 Resultados de la encuesta a socios/clientes - pregunta 5.

Indicador	Frecuencia	Porcentaje
Nada	5	8.3%
Poco	14	23.3%
Confío	28	46.7%
Confío mucho	13	21.7%
Total	60	100%

Ilustración 12 Resultados de la encuesta a socios/clientes - pregunta 5.



Análisis e interpretación

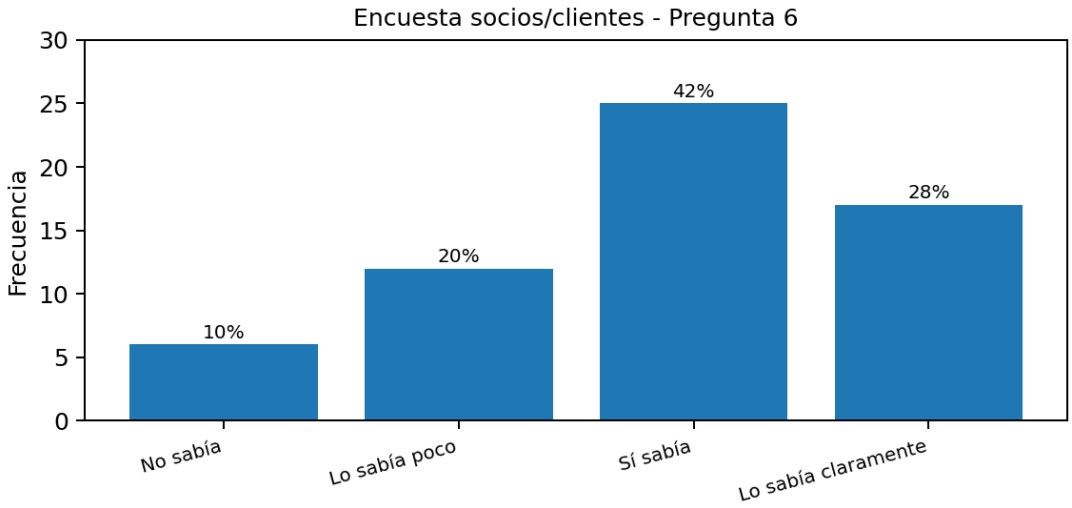
El 68,3% de los socios manifiesta confianza o mucha confianza en la protección de su información financiera. Sin embargo, el 31,7% mantiene una confianza baja o nula, por lo que el fortalecimiento de controles y su comunicación al titular es importante para sostener la confianza institucional.

Pregunta 6. ¿Sabe que sus datos crediticios se usan para analizar capacidad de pago y perfil de riesgo?

Tabla 22 Resultados de la encuesta a socios/clientes - pregunta 6.

Indicador	Frecuencia	Porcentaje
No sabía	6	10.0%
Lo sabía poco	12	20.0%
Sí sabía	25	41.7%
Lo sabía claramente	17	28.3%
Total	60	100%

Ilustración 13 Resultados de la encuesta a socios/clientes - pregunta 6.



Análisis e interpretación

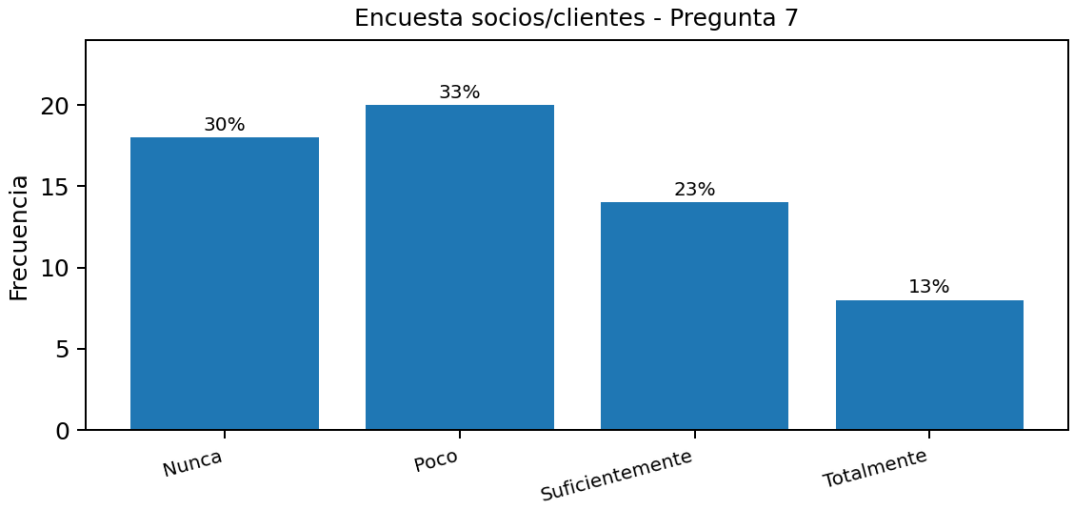
El 70% de los socios manifiesta conocer que sus datos crediticios se utilizan para evaluar capacidad de pago y perfil de riesgo. Este resultado es positivo, aunque debe mantenerse información clara sobre finalidad, exactitud y actualización de los datos crediticios.

Pregunta 7. ¿La cooperativa le ha informado si sus datos pueden ser compartidos con terceros autorizados?

Tabla 23 Resultados de la encuesta a socios/clientes - pregunta 7.

Indicador	Frecuencia	Porcentaje
Nunca	18	30.0%
Poco	20	33.3%
Suficientemente	14	23.3%
Totalmente	8	13.3%
Total	60	100%

Ilustración 14 Resultados de la encuesta a socios/clientes - pregunta 7.



Análisis e interpretación

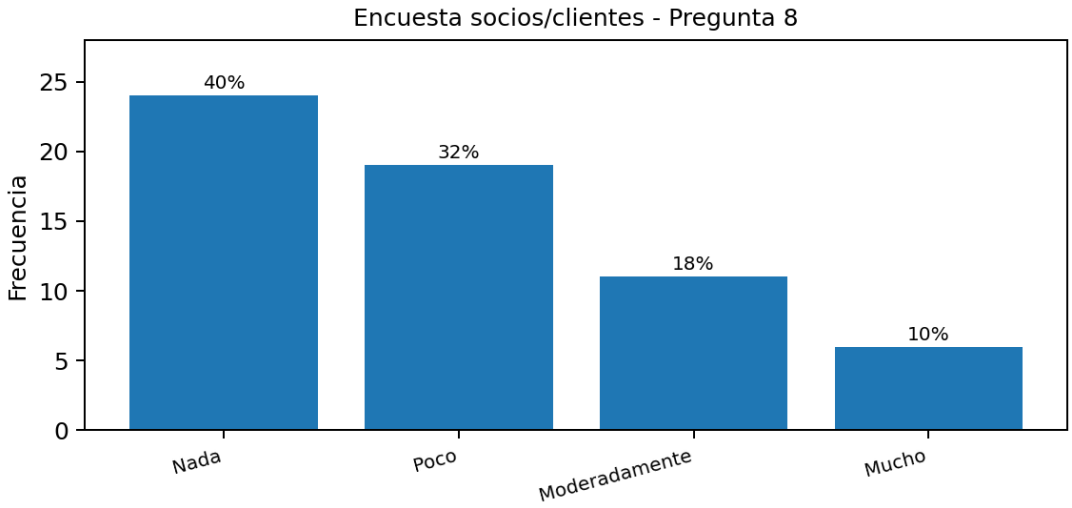
El 63,3% de los socios percibe que nunca o poco se le ha informado sobre posibles transferencias a terceros. Este resultado evidencia la necesidad de reforzar la transparencia sobre proveedores, organismos de control, burós, aseguradoras u otros destinatarios autorizados.

Pregunta 8. ¿Conoce que puede revocar su consentimiento cuando corresponda?

Tabla 24 Resultados de la encuesta a socios/clientes - pregunta 8.

Indicador	Frecuencia	Porcentaje
Nada	24	40.0%
Poco	19	31.7%
Moderadamente	11	18.3%
Mucho	6	10.0%
Total	60	100%

Ilustración 15 Resultados de la encuesta a socios/clientes - pregunta 8.



Análisis e interpretación

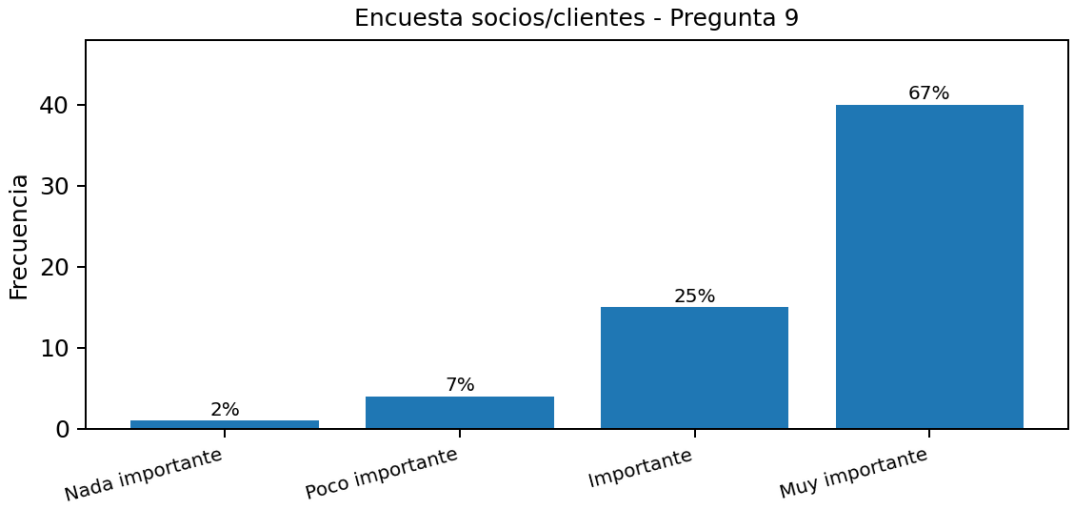
El 71,7% de los socios conoce poco o nada sobre la posibilidad de revocar el consentimiento. Este resultado justifica la implementación de formularios y canales específicos para revocatoria, diferenciados de reclamos generales.

Pregunta 9. ¿Considera importante que la cooperativa le notifique si ocurre una vulneración de seguridad que afecte sus datos?

Tabla 25 Resultados de la encuesta a socios/clientes - pregunta 9.

Indicador	Frecuencia	Porcentaje
Nada importante	1	1.7%
Poco importante	4	6.7%
Importante	15	25.0%
Muy importante	40	66.7%
Total	60	100%

Ilustración 16 Resultados de la encuesta a socios/clientes - pregunta 9.



Análisis e interpretación

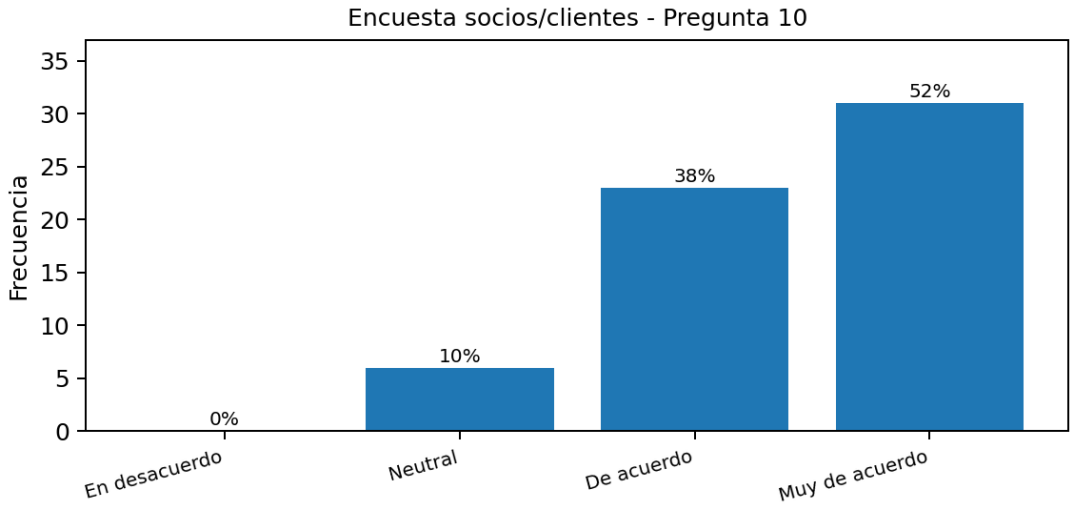
El 91,7% considera importante o muy importante recibir notificación ante una vulneración de seguridad. Esta percepción confirma que la gestión de incidentes no solo es una obligación normativa, sino también una expectativa directa de los titulares.

Pregunta 10. ¿Considera que la cooperativa debe fortalecer sus medidas de protección de datos personales?

Tabla 26 Resultados de la encuesta a socios/clientes - pregunta 10.

Indicador	Frecuencia	Porcentaje
En desacuerdo	0	0.0%
Neutral	6	10.0%
De acuerdo	23	38.3%
Muy de acuerdo	31	51.7%
Total	60	100%

Ilustración 17 Resultados de la encuesta a socios/clientes - pregunta 10.



Análisis e interpretación

El 90% de los socios está de acuerdo o muy de acuerdo con fortalecer medidas de protección de datos. Este resultado respalda la pertinencia de la auditoría técnica y de las acciones de mejora orientadas a seguridad, derechos, transparencia y gestión de incidentes.

c) Resultados de las entrevistas

Entrevista 1

Lugar y fecha: Ambato, Tungurahua, 15 de abril de 2026

Cargo: Delegada de Protección de Datos Personales

Tabla 27 Entrevista 1 aplicada a personal clave.

N.°	Pregunta	Respuesta	Observación
1	¿Cómo se ha organizado la gobernanza de protección de datos personales dentro de la cooperativa?	La cooperativa ha designado una Delegada de Protección de Datos y se encuentra consolidando responsabilidades internas para que las áreas de tecnología, operaciones, atención al socio y dirección participen en el cumplimiento.	Se evidencia un enfoque de gobernanza transversal.
2	¿La cooperativa mantiene un registro de actividades de tratamiento?	Hay información sobre los procesos que se manejan en relación con datos personales, sin embargo, es necesario organizar dicha información en registros que establezcan su finalidad, sus destinatarios, base legal y plazos de almacenamiento.	Necesidad de registro formal de actividades.
3	¿Cómo se asegura que el consentimiento sea libre, específico, informado e inequívoco?	Se utilizan formularios de consentimiento en el momento que el socio o cliente contrata un producto con nosotros	Consentimiento existente con oportunidad de mejora.
4	¿Qué mecanismos existen para diferenciar bases legales del tratamiento?	Se reconoce que no todo tratamiento depende del consentimiento, porque también existen obligaciones legales y contratos financieros; no obstante, esta diferenciación debe documentarse mejor.	Se requiere matriz de bases de licitud.
5	¿Cómo se gestiona la exactitud de datos crediticios?	La actualización se realiza en procesos operativos y de crédito, pero debe reforzarse la evidencia de validación y actualización periódica.	La calidad del dato requiere seguimiento.
6	¿Existen medidas reforzadas para datos sensibles o biométricos?	Cuando existen datos de mayor sensibilidad se aplican controles de acceso	Necesidad de clasificación de datos.

7	¿Qué protocolos existen para atender derechos ARCO+?	Existe un modelo de formulario ARCO que actualmente se encuentra en revisión, pero que aún no ha sido aprobado.	Derechos ARCO+ requieren formalización.
8	¿Cómo se gestionan incidentes o vulneraciones?	La gestión de incidentes de seguridad existe a nivel general, pero debe articularse con la obligación de notificar vulneraciones de datos personales.	Necesidad de procedimiento específico.
9	¿Cómo se controla a proveedores o encargados?	Se revisan contratos y acuerdos de confidencialidad, especialmente con proveedores tecnológicos, pero se debe crear un inventario y evaluación periódica de encargados.	Control de terceros parcialmente establecido.
10	¿Se realizan evaluaciones de impacto?	Actualmente existe una matriz en la cual evaluamos los posibles riesgos en los datos y de qué manera impactarán en la institución.	EIPD en proceso de consolidación.

Conclusión de la entrevista: La entrevista con la Delegada de Protección de Datos Personales confirma que la cooperativa cuenta con una base inicial de gobernanza, consentimiento y atención institucional; sin embargo, requiere consolidar el registro de actividades, diferenciar formularios de derechos, articular incidentes con notificación de vulneraciones y formalizar la evaluación de impacto del tratamiento de datos personales.

Entrevista 2

Lugar y fecha: Ambato, Tungurahua, 16 de abril de 2026

Cargo: Coordinador de TI

Tabla 28 Entrevista 2 aplicada a personal clave.

N.°	Pregunta	Respuesta	Observación
1	¿Cómo se ha organizado la gobernanza de protección de datos personales dentro de la cooperativa?	Desde TI se apoya con controles de acceso, respaldos, usuarios, perfiles y reportes; sin embargo, la gobernanza debe integrar mejor la parte legal, operativa y tecnológica.	TI cumple rol de soporte técnico.
2	¿La cooperativa mantiene un registro de actividades de tratamiento?	No se trata como inventario único desde TI; existen procesos e identificación de sistemas, pero no obtenemos logs directos desde el sistema	Registro técnico no consolidado.
3	¿Cómo se asegura que el consentimiento sea libre, específico, informado e inequívoco?	Desde TI no gestiona el consentimiento del socio, pero en el sistema se guarda su información y donde están incluidos los documentos de aceptación	Necesidad de trazabilidad documental.
4	¿Qué mecanismos existen para diferenciar bases legales del tratamiento?	El sistema soporta procesos contractuales y regulatorios, pero no identifica cada tratamiento según su fundamento jurídico.	Falta clasificación por base de licitud.
5	¿Cómo se gestiona la exactitud de datos crediticios?	La información se actualiza a partir de procesos de crédito y operativos	Relevancia de control de cambios.
6	¿Existen medidas reforzadas para datos sensibles o biométricos?	Existen perfiles de acceso y restricciones, pero la aplicación de controles reforzados debe documentarse según la categoría de datos.	Necesidad de clasificación y controles diferenciados.
7	¿Qué protocolos existen para atender derechos ARCO+?	TI puede apoyar con búsquedas, modificaciones o reportes, pero requiere solicitudes formalizadas para evitar cambios sin respaldo.	El flujo ARCO+ debe integrarse con TI.
8	¿Cómo se gestionan incidentes o vulneraciones?	Se manejan las incidentes tecnológicos que puedan surgir, aunque no hay un playbook para el caso de una vulneración de datos personales.	Se requiere procedimiento especializado.

9	¿Cómo se controla a proveedores o encargados?	Hay relación contractual con el proveedor del core, pero se recomienda revisar periódicamente acceso, soporte y confidencialidad en el caso.	Seguimiento a proveedores debe fortalecerse.
10	¿Se realizan evaluaciones de impacto?	Actualmente hay una evaluación de impacto, pero que está en estado de revisión, aún no ha sido aprobada por gerencia	EIPD existente, pero pendiente de aprobación y socialización.

Conclusión de la entrevista: La entrevista con el Coordinador de TI demuestra que los controles técnicos existen en aspectos como usuarios, perfiles, respaldos y seguridad operativa, pero necesitan conectarse con evidencias de privacidad, clasificación de datos, trazabilidad, revisión de proveedores y análisis de impacto antes de nuevas tecnologías o integraciones.

Entrevista 3

Lugar y fecha: Ambato, Tungurahua, 17 de abril de 2026

Cargo: Coordinador de Operaciones

Tabla 29 Entrevista 3 aplicada a personal clave.

N.°	Pregunta	Respuesta	Observación
1	¿Cómo se ha organizado la gobernanza de protección de datos personales dentro de la cooperativa?	Desde atención al socio se aplican formularios y procesos de recepción de información, pero se requiere mayor capacitación sobre protección de datos.	Gobernanza debe llegar al nivel operativo.
2	¿La cooperativa mantiene un registro de actividades de tratamiento?	El personal conoce procesos donde se recopilan datos, pero no siempre se maneja un registro formal visible para el área.	Registro poco conocido por operaciones.
3	¿Cómo se asegura que el consentimiento sea libre, específico, informado e inequívoco?	Se entrega documentación al socio durante la vinculación, aunque algunos formularios podrían explicarse con lenguaje más sencillo.	Se requiere mejorar comunicación al titular.
4	¿Qué mecanismos existen para diferenciar bases legales del tratamiento?	El personal operativo no siempre distingue entre consentimiento, obligación legal o contrato; normalmente sigue el procedimiento establecido.	Necesidad de capacitación práctica.
5	¿Cómo se gestiona la exactitud de datos crediticios?	Se solicita actualización de datos cuando el socio realiza trámites o cuando el área de crédito lo requiere.	Actualización asociada a trámites.
6	¿Existen medidas reforzadas para datos sensibles o biométricos?	El personal maneja información con reserva, pero necesita lineamientos más claros sobre datos sensibles y su tratamiento.	Sensibilización necesaria.
7	¿Qué protocolos existen para atender derechos ARCO+?	Las solicitudes se canalizan como requerimientos o reclamos, pero sería útil tener formularios específicos para protección de datos.	Se confirma necesidad de formularios independientes.
8	¿Cómo se gestionan incidentes o vulneraciones?	El personal reporta novedades a jefaturas o TI, pero no todos conocen un procedimiento específico para vulneraciones de datos personales.	Canal general, no especializado.

9	¿Cómo se controla a proveedores o encargados?	Esa gestión se maneja desde áreas administrativas o legales; el personal operativo no participa directamente.	Control de proveedores no visible para operaciones.
10	¿Se realizan evaluaciones de impacto?	No es un proceso conocido por el área operativa.	EIPD no socializada.

Conclusión de la entrevista: La entrevista con el área de Operaciones evidencia que la protección de datos debe fortalecerse en el punto de contacto con el titular. Se requiere lenguaje claro, capacitación práctica, formularios específicos y canales visibles para que los socios comprendan el uso de su información y puedan ejercer sus derechos.

d) Fichas bibliográficas-documentales desarrolladas

Tabla 30 Ficha bibliográfica-documental desarrollada 2.

Campo	Contenido
Tipo de fuente	Norma / Ley
Título del documento	Ley Orgánica de Protección de Datos Personales
Autor(es) / institución	Asamblea Nacional del Ecuador
Año de publicación	2021
Institución / fuente	Registro Oficial Suplemento 459
Tema principal	Principios, derechos y obligaciones en protección de datos personales.
Resumen del contenido	Establece el marco jurídico de protección de datos personales en Ecuador, incluyendo principios del tratamiento, derechos de titulares, obligaciones de responsables y encargados, seguridad y responsabilidad demostrada.
Aporte para la investigación	Constituye el criterio normativo principal para evaluar el cumplimiento en el core financiero.
Categorías identificadas	Protección de datos y derechos del titular

Tabla 31 Ficha bibliográfica-documental desarrollada 3.

Campo	Contenido
Tipo de fuente	Reglamento
Título del documento	Reglamento General de la Ley Orgánica de Protección de Datos Personales
Autor(es) / institución	Presidencia de la República del Ecuador
Año de publicación	2023
Institución / fuente	Gobierno del Ecuador
Tema principal	Desarrollo operativo de la LOPDP.
Resumen del contenido	Desarrolla procedimientos y condiciones aplicables a consentimiento, revocatoria, ejercicio de derechos, registro de solicitudes, vulneraciones, evaluación de impacto y relación con encargados.
Aporte para la investigación	Permite convertir las obligaciones legales en criterios observables mediante formularios, registros, procedimientos y evidencias.
Categorías identificadas	Consentimiento; revocatoria; ARCO+; incidentes; evaluación de impacto

Tabla 32 Ficha bibliográfica-documental desarrollada 4.

Campo	Contenido
Tipo de fuente	Norma técnica
Título del documento	NIST Privacy Framework
Autor(es) / institución	National Institute of Standards and Technology
Año de publicación	2020
Institución / fuente	NIST
Tema principal	Gestión del riesgo de privacidad.
Resumen del contenido	Propone una estructura para identificar, gobernar, controlar, comunicar y proteger la privacidad como parte de la gestión de riesgos institucional.
Aporte para la investigación	Aporta criterios para interpretar riesgos de privacidad y relacionarlos con controles técnicos y organizativos.
Categorías identificadas	Gestión de riesgos; privacidad; controles; gobierno

Tabla 33 Ficha bibliográfica-documental desarrollada 5.

Campo	Contenido
Tipo de fuente	Norma técnica
Título del documento	ISO/IEC 27701
Autor(es) / institución	International Organization for Standardization
Año de publicación	2025
Institución / fuente	ISO
Tema principal	Sistema de gestión de información de privacidad.
Resumen del contenido	Extiende la gestión de seguridad de la información hacia controles específicos de privacidad para responsables y encargados del tratamiento de información personal identificable.
Aporte para la investigación	Permite vincular la auditoría con gestión de privacidad, responsables, encargados, mejora continua y evidencia documentada.
Categorías identificadas	Privacidad; responsable; encargado; mejora continua

e) Análisis integrado de resultados

- Los resultados de las preguntas 1 y 2 de la encuesta a empleados evidencian que la gobernanza de protección de datos se encuentra en proceso de consolidación. Aunque la mayoría reconoce parcialmente el registro de actividades y el rol del Delegado de Protección de Datos Personales, todavía existe un grupo que no identifica con claridad estos elementos. Esto coincide con la entrevista a la Delegada de Protección de Datos, quien destacó la necesidad de formular un registro formal de actividades de tratamiento.
- Las preguntas 3 y 4 de la encuesta a empleados, y las preguntas 1 y 2 de la encuesta a socios/clientes demuestran la existencia de consentimiento informado, pero con necesidad de mejora. Por un lado, el empleado reconoce la frecuencia con la que los formularios reportan las finalidades; por el otro, en un sentido de titular, un importante número de socios percibe que la información recibida en los formularios no está claramente definida. Es así como se llega a la conclusión de que el mejoramiento debe ir más allá de contar con formularios, y se traduce en hacer que estos sean comprensibles para el socio.
- Las preguntas 3, 4 y 8 de la encuesta a socios/clientes indican la existencia de un importante vacío en el conocimiento de ARCO+ y la posibilidad de revocar el consentimiento. Una gran mayoría de socios tiene conocimiento limitado o ningún

conocimiento acerca de sus derechos, canales de ejercicio y posibilidad de revocación de consentimiento. Esto queda confirmado con la entrevista realizada a la Unidad de Atención al Socio, quien manifestó que las solicitudes suelen manejarse de manera general, como requerimientos o reclamos, y que es necesario contar con formularios específicos para estas solicitudes.

- Las preguntas 5 y 6 de la encuesta a empleados, y las preguntas 5 y 6 de la encuesta a socios/clientes permiten establecer que el tratamiento de datos crediticios es una tarea bastante bien ejecutada, particularmente en términos de exactitud, actualización y análisis de riesgo. Pero la importancia de esto se pone de manifiesto con la ayuda de las entrevistas, las cuales advierten que esta buena práctica debe ir acompañada de controles técnicos de actualización, bitácoras de modificaciones y clasificación de datos de sensibilidad o criticidad elevada.
- Las preguntas 9 y 10 de la encuesta a empleados, y la pregunta 9 de la encuesta a socios/clientes demuestran la importancia de la seguridad de datos y de la gestión de incidentes. Mientras el empleado reconoce la existencia de controles técnicos, como son los perfiles, contraseñas u otros elementos de acceso restrictivo, la mayoría del personal conoce muy poco o nada de los protocolos de notificación de incidentes. En cambio, los socios se sienten bastante seguros de que serán notificados en caso de violaciones de seguridad. La correlación entre estos resultados da cuenta de que la gestión de incidentes debe ser una gestión técnica y comunicacional.
- Las preguntas 11 de la encuesta a empleados, y la pregunta 7 de la encuesta a socios/clientes muestran una falta de formalización en la gestión de proveedores y transferencias de datos. Mientras el personal cree estar manejando ciertos controles acerca de los encargados de tratamiento, hay un número significativo de socios que carecen de claridad sobre si sus datos pueden ser transferidos a terceros. Por lo tanto, la auditoría deberá revisar las cláusulas de confidencialidad en los contratos, los inventarios de proveedores y, sobre todo, la transparencia hacia el titular.
- Las entrevistas a la Delegada de Protección de Datos y al Coordinador de TI coinciden en que la evaluación de impacto aún no ha sido completamente formalizada. Esto deja claro que la EIPD constituirá una prioridad de auditoría particular, ya que es

imprescindible realizarla antes de cualquier proceso tecnológico nuevo, o de alta criticidad.

- Las fichas bibliográficas-documentales han demostrado que el estudio tiene un fundamento adecuado y sustentable. En primer lugar, el resumen institucional de la LOPDP permitió que los instrumentos fueran construidos acorde a las líneas de acción aplicables a cooperativas; luego la LOPDP y su Reglamento proporcionaron las exigencias concretas; finalmente, los NIST Privacy Framework e ISO/IEC 27701 relacionaron cumplimiento con gestión de riesgos.
- Con base en las encuestas a empleados y socios/clientes, las entrevistas y las fichas bibliográficas-documentales se puede concluir que la cooperativa ha logrado importantes avances en el consentimiento informado, tratamiento de datos crediticios, controles técnicos y en su institucionalidad. Sin embargo, aún quedan brechas en comunicación hacia el titular, conocimiento de ARCO+, revocatoria de consentimiento, gestión de incidentes, proveedores, registro de actividades y evaluación de impacto. Estos resultados justifican el desarrollo de una auditoría técnica enfocada en evidencias, controles, trazabilidad y cumplimiento demostrable.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1 Enfoque de la auditoría y operacionalización de los objetivos específicos

El presente capítulo desarrolla la auditoría técnica del cumplimiento de la Ley Orgánica de Protección de Datos Personales en los sistemas de información asociados al core financiero Softbank de la Cooperativa de Ahorro y Crédito Credi Ya. El enfoque utilizado no se limita a una revisión documental de la normativa, sino que integra evidencia documental y técnica, procesos definidos, matrices de tratamiento, procedimientos internos, pruebas de auditoría informática y marcos técnicos de seguridad y privacidad.

La auditoría se desarrolló en la técnica de auditoría de caja gris ya que se evalúa información institucional autorizada, documentos internos, matrices, formularios, procedimientos, controles técnicos y evidencias de soporte. Se realiza esta auditoría con el propósito de validar si existen procesos, si existe vinculación de obligaciones legales y controles técnicos, documentos internos, trazabilidad y capacidad de la institución de demostrar que cumple estas responsabilidades.

3.1.1 Trazabilidad del capítulo con los objetivos específicos

El capítulo responde directamente a los tres objetivos específicos de la investigación. En primer lugar, evalúa el cumplimiento técnico-normativo frente a la LOPDP y su Reglamento. En segundo lugar, identifica brechas, riesgos y vulnerabilidades técnicas u organizativas asociadas al tratamiento de datos personales. En tercer lugar, consolida hallazgos, recomendaciones, responsables, plazos y evidencias esperadas para la mejora continua.

Tabla 34 Relación del capítulo con los objetivos específicos.

Objetivo específico	Evidencia utilizada en el capítulo	Resultado generado
Evaluar el cumplimiento técnico-normativo del core financiero frente a la LOPDP.	Matriz RAT, matriz EIPD, política de protección de datos, formularios de consentimiento, subprocesos ARCO y brechas, diagnóstico preliminar, ISO 27701 y formatos de auditoría.	Matriz de cumplimiento por artículo, proceso, evidencia, prueba y nivel de criticidad.
Identificar brechas, riesgos y vulnerabilidades técnicas y organizativas.	Pruebas RBAC, SoD, Audit Trail, revisión de logs, EIPD, revisión de procesos, análisis de minimización, retención, incidentes, proveedores y continuidad.	Matriz de vulnerabilidades por dominio con riesgo, criterio, prueba, evidencia y acción correctiva.
Elaborar un informe técnico con hallazgos y lineamientos de mejora.	Cédulas de hallazgo, plan de acción, cronograma, lineamientos ISO/NIST y evidencias documentales.	Informe técnico de auditoría con opinión de cumplimiento parcial y plan priorizado.

3.1.2 Operacionalización de los objetivos específicos

Para atender la operacionalización de los objetivos, cada objetivo específico fue convertido en actividades de auditoría, técnicas de verificación, instrumentos, evidencias y secciones concretas del capítulo donde se demuestra su cumplimiento. De esta manera, el desarrollo del capítulo permite observar en qué momento se evalúa el cumplimiento técnico-normativo, dónde se identifican las brechas y cómo se consolida el informe técnico final.

Con esta relación, las secciones posteriores se desarrollan como evidencia de cumplimiento de los objetivos. Por ello, cada bloque metodológico indica qué objetivo atiende y qué resultado genera para la auditoría técnica

Tabla 35 Operacionalización de los objetivos

Objetivo específico	Actividades de operacionalización en el capítulo	Instrumentos / criterios utilizados	Evidencia y sección donde se cumple
Evaluar el cumplimiento técnico-normativo del core financiero frente a la LOPDP.	Delimitar el sistema auditado, vincular artículos de la LOPDP con procesos reales, revisar evidencia institucional y ejecutar pruebas documentales y técnicas.	LOPDP, Reglamento General, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, NIST, matriz RAT, matriz EIPD y pruebas PT.	Secciones 3.2, 3.3.1, 3.3.2, 3.3.3, 3.3.4 y 3.3.5. Resultado: matriz de cumplimiento, calificación por prueba y evidencia asociada.
Identificar brechas, riesgos y vulnerabilidades técnicas u organizativas.	Analizar procesos del ciclo de vida del dato, revisar ARCO, brechas, accesos, segregación de funciones, trazabilidad, retención, privilegios y exposición de datos.	Pruebas RBAC, SoD, Audit Trail, consultas SQL de solo lectura, cédulas de auditoría, matriz de riesgos y clasificación de hallazgos por criticidad con ISO 31000.	Secciones 3.4, 3.4.1, 3.4.2 y 3.4.3. Resultado: hallazgos consolidados, criticidad y recomendaciones técnicas.
Elaborar un informe técnico de auditoría con hallazgos y lineamientos de mejora.	Consolidar los hallazgos, priorizar acciones correctivas, definir responsables, plazos, evidencias esperadas y documentar el informe final de auditoría.	Cédulas de hallazgo, matriz de plan de acción, mapa de calor, criterios de prioridad, evidencia documental y técnica.	Secciones 3.5, 3.5.1, 3.5.2 y 3.5.3. Resultado: plan de acción priorizado e informe técnico INF-AUD-LOPDP-CCY-001-2026.

3.2 Planificación y delimitación de la auditoría técnica

3.2.1 Ámbito de la auditoría técnica

Para cumplir con el primer objetivo específico, el ámbito de auditoría delimitó el sistema, los procesos, las áreas involucradas y las restricciones de revisión. Esta delimitación permitió que la evaluación técnico-normativa se aplique únicamente sobre componentes relacionados con el tratamiento de datos personales dentro del core financiero y sus procesos de soporte.

El ámbito de la auditoría comprende la revisión técnica, documental y normativa del tratamiento de datos personales realizado en los módulos operativos del core financiero Softbank. Este sistema fue considerado como el núcleo de procesamiento de información de socios y clientes, debido a que concentra datos de identificación, contacto, información financiera, datos crediticios, referencias personales, garantías, transacciones, consultas, reportes y evidencias operativas.

Las alcance comprende los procesos de recolección de datos, consentimiento, derechos ARCO+, revocatoria, registro de la actividad de tratamiento, procesos de evaluación de riesgo y evaluación de impacto, proceso de transferencia de datos o comunicación a terceros y sus características principales, proceso de comunicación con los encargados, procesos de incidente, control de accesos y trazabilidad, cifrado y minimización de datos, retención de datos, capacitación.

La auditoría no contempla explotación ofensiva de vulnerabilidades, alteración de datos productivos ni pruebas que puedan afectar la disponibilidad del core financiero. Las actividades se orientan a revisión documental, exportaciones autorizadas, consultas de solo lectura, validación de matrices, revisión de bitácoras, contraste de roles y evaluación de evidencia generada por los procesos institucionales.

Tabla 36 Definición del ámbito de auditoría.

Elemento	Descripción
Entidad auditada	Cooperativa de Ahorro y Crédito Credi Ya Ltda.
Sistema auditado	Core financiero Softbank y procesos institucionales vinculados al tratamiento de datos personales.
Sede de análisis	En la agencia Matriz de la institución (Ambato), donde se concentran la mayoría de procesos realizados en la cooperativa
Tipo de auditoría	Auditoría técnica de cumplimiento normativo, seguridad de la información y privacidad.
Unidades involucradas	Gerencia General, Delegada de Protección de Datos Personales, Tecnología, Seguridad de la Información, Operaciones, Atención al Socio, Talento Humano, Riesgos, Auditoría y áreas usuarias.
Limitaciones	No se ejecutan pruebas intrusivas en producción; se aplican pruebas no destructivas, documentales y de caja gris.

3.2.2 Cronograma de ejecución de pruebas

Tabla 37 Cronograma de ejecución de pruebas de auditoría.

Actividad	Entregable	Semana 1	Semana 2	Semana 3	Semana 4
Planificación, alcance y criterios	Plan de auditoría y matriz normativa	X			
Solicitud y clasificación de evidencias	Lista de evidencias y repositorio de soporte	X	X		
Revisión de consentimiento, política y RAT	Cédula legal-documental	X	X		
Aplicación de pruebas ARCO y revocatoria	Cédula ARCO y registro de recorrido		X		
Revisión de brechas e incidentes	Acta de tabletop y matriz de notificación		X	X	
Revisión EIPD y riesgos	Matriz de riesgos y evaluación de impacto		X	X	
Pruebas RBAC, SoD y accesos	Matriz de usuarios, roles y privilegios			X	
Prueba Audit Trail y logs	Cédula de trazabilidad y catálogo de eventos			X	
Evaluación ISO/NIST y diagnóstico	Diagnóstico light, SoA y dashboard			X	
Hallazgos, plan de acción e informe	Informe técnico y matriz de seguimiento				X

3.3 Evaluación del cumplimiento técnico-normativo del core financiero frente a los artículos seleccionados de la LOPDP

3.3.1 Selección de artículos de la LOPDP y su Reglamento para la evaluación

Los artículos seleccionados fueron vinculados con procesos y evidencias concretas. La auditoría no se limita a indicar que la cooperativa posee documentos; revisa si cada obligación cuenta con proceso definido, responsable, evidencia generada, registro de ejecución y control técnico asociado.

Tabla 38 Artículos y criterios normativos aplicados en la auditoría técnica.

Criterio legal	Elemento auditado	Evidencia / prueba asociada
LOPDP art. 10 - Principios	Juridicidad, transparencia, finalidad, minimización, confidencialidad, seguridad y responsabilidad proactiva.	Política de protección de datos, formatos de consentimiento, matriz RAT, diagnóstico inicial y evidencias de minimización de datos.
LOPDP arts. 12 al 17 - Derechos del titular	Información, acceso, rectificación, eliminación, oposición, portabilidad y suspensión/revocatoria.	Formulario ARCO, subproceso correspondiente, bitácora de solicitudes, soporte documental de plazos y trazabilidad.
LOPDP arts. 25, 26 y 28 - Categorías especiales y titulares vulnerables	Datos sensibles, biométricos, salud, niñas, niños, adolescentes y grupos de especial protección.	Formatos aplicables a colaboradores, directivos, pasantes, socios/clientes y metodología para la evaluación de impacto.
LOPDP arts. 40 y 42 - Riesgos y evaluación de impacto	Identificación, análisis, evaluación y tratamiento de riesgos del tratamiento.	Metodología de riesgos, matriz EIPD, matriz RAT y evidencia PT-EIPD.
LOPDP art. 47 - Obligaciones del responsable y encargado	Políticas, medidas técnicas y organizativas, protección desde el diseño, registros y seguridad.	Política institucional, manuales, formatos de auditoría, controles basados en ISO/NIST y soportes técnicos.
Reglamento art. 5 - Recogida del consentimiento	Consentimiento libre, específico, informado e inequívoco.	Formularios dirigidos a socios/clientes, proveedores, visitantes, colaboradores, pasantes y directivos.
Reglamento art. 6 - Revocatoria del consentimiento	Mecanismos para suspender o revocar consentimiento.	Formulario ARCO, subproceso ARCO, campos relacionados con suspensión o revocatoria y bitácora de seguimiento.
Reglamento arts. 12, 13 y 15 - Medios, contenido y registro de solicitudes	Canales, requisitos mínimos, plazos y registro institucional.	Solicitud ARCO, procedimiento interno, bitácora y prueba de recorrido documental.
Reglamento arts. 24, 27 y 28 - Vulneraciones	Notificación por responsable, encargado y titular afectado.	Subproceso de brechas, matriz de evaluación de impacto, simulacro de escritorio y registro de incidentes.
Reglamento art. 29 - Evaluación de impacto	Análisis preventivo de tratamientos de riesgo.	Metodología de gestión de riesgos, matriz EIPD y cédula PT-EIPD.
Reglamento art. 34 - Estado de la técnica	Medidas técnicas y organizativas actualizadas.	Manual de seguridad de la información, revisión de cifrado, accesos, logs, respaldos y continuidad operativa.
Reglamento art. 41 - Responsable y encargado	Relación contractual, instrucciones y garantías del encargado.	Formularios de proveedores, política, revisión de contratos/acuerdos y matriz de encargados.
Reglamento arts. 55 y 57 - Delegada y confidencialidad	Cumplimiento de requisitos, funciones y acuerdo de confidencialidad.	Expediente de la Delegada, designación institucional, política y registros.

3.3.2 Criterios legales, documentales y técnicos aplicados en la auditoría

El marco de auditoría combina tres dimensiones: la dimensión legal, representada por la LOPDP y su Reglamento General; la dimensión institucional, conformada por políticas, manuales, formularios, subprocesos y matrices entregadas como evidencia; y la dimensión técnica, sustentada en ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, NIST Privacy Framework, NIST Cybersecurity Framework 2.0 y NIST SP 800-61r3.

La combinación hace posible transformar los compromisos legales en criterios de auditoría controlables. El consentimiento se verifica con la ayuda de formularios, finalidades informadas, derechos y pruebas de archivos; el derecho se evalúa a través del formulario ARCO, subprocesos, bitácoras y tiempos de plazo; incidentes se evalúan con el procedimiento de brecha, matriz de impacto, registros y notificaciones; y la seguridad de información se verifica con controles de acceso, registros, cifrado, respaldos, roles, funcionalidades y capacitación.

Tabla 39 Marco legal, documental y técnico aplicado.

Norma / documento / marco	Aplicación dentro de la auditoría
LOPDP	Base normativa para evaluar los principios, derechos, obligaciones, seguridad, riesgos, responsabilidad demostrada y protección de la privacidad desde el diseño.
Reglamento General de la LOPDP	Criterio operativo para verificar consentimiento, revocatoria de consentimiento, derechos ARCO+, registro de solicitudes, notificaciones de vulneraciones de la privacidad, EIPD, estado de la técnica y encargados de tratamiento.
Política y manuales institucionales	Evidencia de gobernanza, responsable, principios, lineamientos, roles, procesos, conservación de datos, seguridad y capacitación.
Matriz RAT y matriz de EIPD	Evidencia para verificar registro de actividades de tratamiento, identificación de riesgos, evaluación de impacto y controles asociados.
ISO/IEC 27001:2022	Referencia para gestión de la seguridad de la información basada en riesgos, mejoramiento continuo, evaluación de desempeño y controles operativos.
ISO/IEC 27002:2022	Referencia para controles de acceso, identidad, proveedores, registros de actividad, monitoreo, criptografía, incidentes de privacidad
ISO/IEC 27701	Referencia para gestión de información de privacidad, derechos del titular, responsable, encargado de tratamiento, retención de datos y evidencias de tratamiento.
NIST Privacy Framework	Referencia para gestión de riesgos de privacidad e impacto sobre los titulares.
NIST CSF 2.0 / NIST SP 800-61r3	Referencia para gobierno de privacidad, identificación de datos personales, protección, detección de incidentes, respuesta a incidentes y recuperación de datos personales.

3.3.3 Evidencia documental y técnica utilizada para la evaluación

Tabla 40 Evidencias institucionales utilizadas como anexos de auditoría.

Anexo	Evidencia	Uso dentro de la auditoría
Anexo 1	Política para la Protección y Tratamiento de Datos Personales	Gobernanza, principios, responsables, derechos, conservación, medidas de seguridad e incidentes.
Anexo 2	Manual de Políticas y Procedimientos de Protección de Datos	Roles, responsabilidades, cadena de valor, indicadores y actualización del RAT.
Anexo 3	Formulario de solicitud para el ejercicio de derechos ARCO	Derechos ejercidos, identificación del titular, documentos de respaldo, medio de notificación y uso institucional.
Anexo 4	Subproceso Atención de Derechos ARCO	Recepción, revisión, análisis, registro, gestión, respuesta y archivo de las solicitudes recibidas.
Anexo 5	Subproceso Gestión y Notificación de Brechas y Vulneración de Seguridad de Datos	Detección, contención, evaluación, comunicación a la autoridad competente y notificación al titular cuando exista un riesgo alto.
Anexo 6	Metodología para la Gestión de Riesgos y Evaluación de Impacto	Contexto, identificación, análisis, valoración, tratamiento de riesgos y determinación del riesgo residual.
Anexo 7	Plan de Capacitación y Concienciación en Protección de Datos Personales	Temas a desarrollar, público objetivo, cronograma trimestral y productos de capacitación.
Anexo 8	Formularios de consentimiento por tipo de titular	Socios/clientes, colaboradores, directivos, proveedores, visitantes y pasantes.
Anexo 9	Matriz RAT	Registro de actividades de tratamiento, finalidades, responsables, categorías de datos y controles aplicables.
Anexo 10	Matriz de Evaluación de Impacto en Protección de Datos	Identificación de riesgos, impacto, probabilidad, controles implementados y seguimiento correspondiente.
Anexo 11	Manual de Seguridad de la Información	Controles técnicos, seguridad lógica, respaldo, accesos, continuidad y protección de información.
Anexo 12	Anexo 12 Libro de pruebas técnicas de auditoría	Consultas SQL, pruebas documentales, validaciones de control, resultados observados, dashboard, cédulas y plan de acción técnico.

3.3.4 Lista de verificación sustentada en evidencia documental y técnica

Para cumplir con el primer y segundo objetivo específico, las pruebas de auditoría se diseñaron como mecanismos de verificación. Cada prueba relaciona un criterio normativo o técnico con una evidencia esperada, de modo que el cumplimiento y las brechas puedan evaluarse de manera trazable y no únicamente descriptiva.

Las pruebas se definieron para que cada revisión tenga un propósito claro, documentos requeridos y evidencias esperadas. Se separaron dos grupos: pruebas documentales-operativas y pruebas SQL complementarias. Las primeras revisan procesos, formularios y controles institucionales. Las segundas validan condiciones observables en la base de datos y en el core financiero mediante consultas de solo lectura.

La ilustración anterior resume la lógica utilizada para pasar de los objetivos específicos a pruebas concretas, evidencias verificables, hallazgos y acciones de mejora. Esta trazabilidad facilita indicar en qué sección del capítulo se cumple cada objetivo.

Tabla 41 Definición de pruebas de auditoría.

Código de prueba	Nombre de la prueba	Descripción de la prueba	Requisitos / documentación solicitada	Evidencias esperadas
PT-01	Consentimiento y base de licitud	Revisar si los formularios explican de manera clara las finalidades del tratamiento, los derechos del titular, los datos que se recopilan, los canales de contacto y las condiciones aplicables según cada tipo de titular.	Política de protección de datos, formularios de consentimiento, RAT y expedientes de aceptación.	Cédula de consentimiento, matriz campo-finalidad-base legal y observaciones sobre lenguaje poco claro o finalidades demasiado amplias.
PT-02	Integrantes y roles de protección de datos	Identificar a los titulares, responsable del tratamiento, encargados, Delegada de Protección de Datos, áreas de TI, Operaciones, Talento Humano, proveedores y auditoría, verificando su participación dentro del proceso.	Política, manual institucional, designaciones, organigrama y responsabilidades asignadas por área.	Matriz de roles y responsabilidades relacionada con los procesos de protección de datos.
PT-03	Atención de derechos ARCO+	Verificar el recorrido completo de una solicitud, desde su recepción hasta el cierre, incluyendo validación de identidad, registro, gestión interna y respuesta al titular.	Formulario ARCO, subproceso ARCO, bitácora, evidencias de respuesta y documentación de soporte.	Cédula ARCO con trazabilidad de la solicitud, plazo de atención, responsable asignado, respuesta emitida y archivo correspondiente.

PT-04	Revocatoria y suspensión del tratamiento	Validar si el titular cuenta con un mecanismo documentado para solicitar la suspensión o revocatoria del tratamiento de sus datos personales.	Formulario ARCO, subproceso ARCO, política institucional y registros de solicitudes.	Matriz de revocatoria o suspensión, con evidencia de aplicación o identificación de la necesidad de realizar una prueba operativa.
PT-05	Registro de actividades de tratamiento	Evaluar si la matriz RAT refleja los procesos reales del core financiero y si mantiene una relación clara entre finalidad, base legal, datos tratados, responsable y controles aplicados.	Matriz RAT, política, manual institucional y procesos del core financiero.	Cédula RAT con brechas de actualización y mapa de tratamientos críticos.
PT-06	Gestión de riesgos y EIPD	Revisar si la metodología de riesgos y la matriz EIPD se aplican de forma efectiva al tratamiento de datos dentro del core financiero.	Metodología de riesgos, matriz EIPD, RAT, inventario de activos y controles existentes.	Informe de EIPD aplicada al core, riesgos priorizados y plan de tratamiento.
PT-07	Control de accesos RBAC	Comparar usuarios, cargos, estados laborales, perfiles y privilegios para identificar cuentas activas, cuentas huérfanas o permisos que no estén debidamente justificados.	Exportación de usuarios, perfiles, cargos, nómina, estados laborales, manual de seguridad y matriz de accesos.	Matriz RBAC, reporte de cuentas que requieren recertificación y acta de depuración.
PT-08	Segregación de funciones SoD	Analizar posibles combinaciones incompatibles en procesos críticos, como crédito, aprobación, modificación de datos y administración de usuarios.	Perfiles, roles, flujo de crédito, usuarios asignados a cada etapa y políticas de control interno.	Matriz SoD, incompatibilidades identificadas y excepciones debidamente justificadas.
PT-09	Trazabilidad y Audit Trail	Verificar si las acciones sensibles pueden reconstruirse con datos como usuario, fecha, hora, módulo, acción realizada, origen y resultado.	Logs del core, bitácoras, catálogo de eventos, política de retención y evidencias de monitoreo.	Cédula Audit Trail, catálogo de eventos auditables y observaciones sobre la centralización de registros.
PT-10	Gestión y notificación de brechas	Aplicar una prueba de escritorio para validar la detección, contención, evaluación, notificación y cierre de	Subproceso de brechas, matriz EIPD, registro de incidentes, responsables y canales de notificación.	Acta de tabletop, matriz de brecha, tiempos de respuesta y plan de mejora.

		una brecha de seguridad.		
PT-11	Estado de la técnica	Revisar las medidas técnicas y organizativas aplicables al core, como cifrado, autenticación, respaldos, recuperación, hardening y monitoreo.	Manual de seguridad, evidencias de configuración, políticas de contraseña, backups, continuidad y reportes técnicos.	Cédula de estado de la técnica con controles existentes y mejoras requeridas.
PT-12	Responsable, encargados y proveedores	Revisar si los terceros que tratan datos personales cuentan con contratos, cláusulas de confidencialidad, instrucciones claras y controles de acceso.	Formulario de proveedores, contratos, acuerdos de confidencialidad, inventario de encargados y registros de soporte.	Matriz de encargados, revisión de garantías y plan de evaluación periódica.
PT-13	Capacitación y cultura de privacidad	Verificar si existe una planificación de capacitación en protección de datos y si hay evidencias de su ejecución según rol o grupo objetivo.	Plan de capacitación, material utilizado, listas de asistencia, evaluaciones y cronograma.	Matriz de capacitación, nivel de cobertura, actividades pendientes y recomendaciones de medición.
PT-SQL-01	Exposición de datos personales y financieros	Identificar consultas o reportes que muestren datos personales y financieros sin enmascaramiento o sin aplicar el criterio de mínimo dato.	Consulta SQL, permisos de lectura, muestra enmascarada y criterio de finalidad.	Reporte de exposición, campos visibles y recomendación de enmascaramiento.
PT-SQL-02	Segregación de funciones en usuarios y roles	Detectar usuarios que participen de manera simultánea en etapas que podrían ser incompatibles dentro del flujo de crédito.	Tablas de usuarios, roles, etapas de crédito, cargos y perfiles.	Matriz SoD técnica con usuarios observados e incompatibilidades potenciales.
PT-SQL-03	Datos conservados sin productos vigentes	Identificar personas o clientes que ya no tengan productos vigentes ni saldos activos, pero cuyos datos aún se conservan en el sistema.	Tablas de persona, cliente, productos, saldos y estados de relación.	Matriz de retención con registros observados y criterio de depuración, bloqueo o anonimización.
PT-SQL-04	Usuarios de base de datos con privilegios elevados	Identificar usuarios de base de datos que tengan roles administrativos elevados, como db_owner, y revisar si dichos privilegios están justificados.	Catálogo de usuarios de base de datos, roles y permisos asignados.	Cédula de privilegios DB y justificación de cuentas técnicas.

PT-SQL-05	Logins SQL sin política completa de contraseña	Detectar logins activos que no cuenten con complejidad, expiración u otros controles suficientes de contraseña.	Catálogo de logins SQL, estado de políticas y configuración de autenticación.	Reporte de endurecimiento de autenticación SQL.
PT-SQL-06	Empleados desvinculados con usuarios activos	Cruzar la información de nómina con los usuarios del core para identificar colaboradores desvinculados que aún mantengan acceso activo o parcialmente habilitado.	Tablas de usuarios, empleado_usuario, empleado, persona y estados laborales.	Reporte de cuentas huérfanas y acta de bloqueo.
PT-SQL-07	Usuarios activos sin empleado asociado	Detectar cuentas activas que no tengan una asociación válida con un empleado institucional.	Usuarios del core, asociación empleado_usuario y estados de acceso.	Acta de depuración de usuarios y recertificación con jefaturas.
PT-SQL-08	Usuarios inactivos con etapas de crédito asignadas	Identificar usuarios laboralmente inactivos que todavía figuren como responsables en etapas de crédito o flujos operativos.	Usuarios, empleados, etapas de crédito, responsables de flujo y estados.	Cédula de etapas de crédito y reasignación de responsabilidades.
PT-SQL-09	Exportación masiva de información desde Softbank	Validar si una exportación masiva de información requiere autorización, genera bitácora y responde a una finalidad legítima.	Permisos del módulo, logs de exportación, autorización, finalidad y muestra controlada.	Cédula de exportación masiva con evidencia de permiso, finalidad y registro.

3.3.5 Resultados de la evaluación del cumplimiento técnico-normativo

La calificación utilizada en la ejecución diferencia entre cumplimiento documental, cumplimiento parcial, necesidad de validación operativa, acción correctiva y pruebas pendientes. Esta clasificación evita afirmar incumplimientos absolutos cuando existe evidencia documental, pero también evita calificar como cumplido un control que todavía necesita registros, bitácoras, simulacros o depuración técnica.

Tabla 42 Ejecución de pruebas y resultados.

Código de la prueba	Evidencia / anexo	Calificación	Resultados
PT-01	Anexos 1 y 8	Cumple parcialmente	Existen formularios por tipo de titular y una política institucional de protección de datos. Sin embargo, se observó que algunas finalidades son demasiado amplias, por lo que deben relacionarse mejor con una matriz campo-finalidad-base legal.
PT-02	Anexos 1 y 2	Cumple	Se identifican los responsables, la DPD, las áreas de apoyo y las obligaciones generales. La evidencia permite reconocer una estructura institucional de gobierno en protección de datos.
PT-03	Anexos 3 y 4; Ilustración 18	Cumple parcialmente	Existe un formulario y un subproceso ARCO. No obstante, falta fortalecer la evidencia de casos atendidos, mantener la bitácora actualizada, documentar los plazos y dejar constancia del cierre de cada solicitud.
PT-04	Anexos 3 y 4	Cumple parcialmente	El formulario contempla la suspensión o revocatoria del tratamiento. Aun así, se requiere validar casos reales o realizar una prueba controlada que demuestre su efecto en tratamientos no obligatorios.
PT-05	Anexos 1, 2 y 9	Cumple parcialmente	Existe una matriz RAT, pero debe mantenerse alineada con los procesos reales del core, los reportes, los proveedores y los tiempos de conservación.
PT-06	Anexos 6, 9 y 10	Cumple parcialmente	Se cuenta con metodología y matriz EIPD. Sin embargo, se requiere evidenciar su aplicación completa al core financiero y actualizar el riesgo residual.
PT-07	Anexos 11 y 12	Requiere acción correctiva	Las pruebas SQL evidenciaron cuentas activas de usuarios desvinculados o sin empleado asociado. Se necesita una recertificación formal de accesos y un proceso de depuración.
PT-08	Anexo 12	Requiere acción correctiva	Se observaron posibles conflictos de segregación de funciones, además de usuarios inactivos que aún permanecen asignados a etapas de crédito.
PT-09	Anexos 11 y 12	Requiere validación operativa	Se debe demostrar que las acciones sensibles del core generan logs suficientes y que estos registros son revisados de manera periódica.
PT-10	Anexo 5; Ilustración 19	Cumple parcialmente	Existe un subproceso de brechas con plazos y responsables definidos. Falta probarlo mediante un simulacro y conservar el acta con los resultados obtenidos.
PT-11	Anexo 11	Cumple parcialmente	Existen medidas de seguridad documentadas. Se requiere complementar con evidencia técnica periódica sobre cifrado, respaldos, autenticación, hardening y recuperación.
PT-12	Anexos 1 y 8	Cumple parcialmente	Existen formularios y lineamientos para proveedores. Sin embargo, falta contar con un inventario actualizado de encargados, evaluaciones periódicas y evidencia sobre los accesos de soporte.
PT-13	Anexo 7	Cumple parcialmente	Existe un plan anual de capacitación. Se requiere conservar listas de asistencia, evaluaciones, material utilizado y medición de cobertura por rol.
PT-SQL-01	Anexo 12	Requiere acción correctiva	Se observaron 18 registros de nivel alto por exposición de datos de identificación, contacto y valores financieros o crediticios sin enmascaramiento.

PT-SQL-02	Anexo 12	Requiere acción correctiva	Se observaron 14 registros de nivel alto asociados a posibles incompatibilidades entre usuarios y roles.
PT-SQL-03	Anexo 12	Requiere acción correctiva	Se observaron 71 registros de nivel alto correspondientes a personas o clientes sin productos vigentes o sin una relación activa identificable en la consulta.
PT-SQL-04	Anexo 12	Requiere acción correctiva	Se observaron 9 usuarios de base de datos con rol administrativo elevado.
PT-SQL-05	Anexo 12	Requiere acción correctiva	Se observaron 4 logins activos con política de contraseña incompleta; de ellos, 2 fueron calificados como críticos.
PT-SQL-06	Anexo 12	Requiere acción correctiva	Se observaron 75 registros de empleados desvinculados con usuarios activos o parcialmente habilitados: 23 críticos, 45 altos y 7 bajos.
PT-SQL-07	Anexo 12	Requiere acción correctiva	Se observaron 87 usuarios activos sin empleado asociado: 55 críticos, 22 altos y 10 bajos.
PT-SQL-08	Anexo 12	Requiere acción correctiva	Se observaron 21 usuarios laboralmente inactivos que aún tenían etapas de crédito asignadas: 10 críticos, 10 altos y 1 medio.
PT-SQL-09	Anexo 12	Requiere acción correctiva	Se observó que usuarios con perfiles operativos, como cajas, atención al cliente, entre otros; tienen acceso a descargar información histórica de socios y clientes que han contratado algún producto en la institución

3.4 Identificación de brechas de cumplimiento, riesgos y vulnerabilidades técnicas y organizativas asociadas al tratamiento de datos personales

Para cumplir con el segundo objetivo específico, los procesos se revisaron desde el ciclo de vida del dato personal. Esta lectura permitió ubicar en qué momentos pueden generarse brechas, riesgos o vulnerabilidades, especialmente en la recolección, uso, consulta, transferencia, conservación, atención de derechos y gestión de incidentes.

Los procesos revisados se organizaron según el ciclo de vida del dato personal: recolección, registro, uso operativo, actualización, consulta, transferencia o comunicación, conservación, atención de derechos, respuesta ante incidentes y cierre del tratamiento. En la

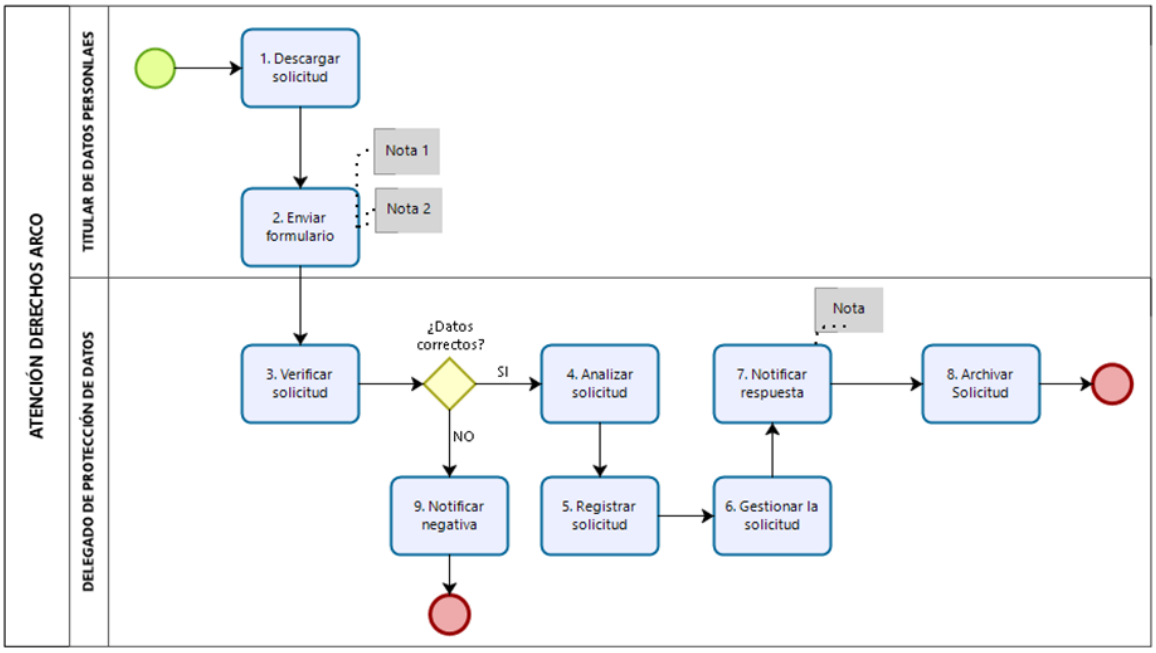
práctica, la mayor concentración de datos se encuentra en los procesos de vinculación, crédito, ahorro, atención al socio, gestión de usuarios, reportes y soporte tecnológico del core financiero.

Los procesos de mayor relevancia para este capítulo son la atención de derechos ARCO y la gestión de brechas de seguridad, porque permiten verificar si la Cooperativa cuenta con mecanismos para responder a los titulares y actuar frente a incidentes que puedan afectar datos personales.

3.4.1 Evaluación del proceso de atención de derechos ARCO+

El subproceso de atención de derechos ARCO+ establece el recorrido que sigue una solicitud desde que el titular descarga y envía el formulario, hasta que la Delegada de Protección de Datos verifica, analiza, registra, gestiona, notifica y archiva la respuesta. Este flujo se relaciona directamente con la prueba PT-03 y con la validación de revocatoria o suspensión del tratamiento en la prueba PT-04.

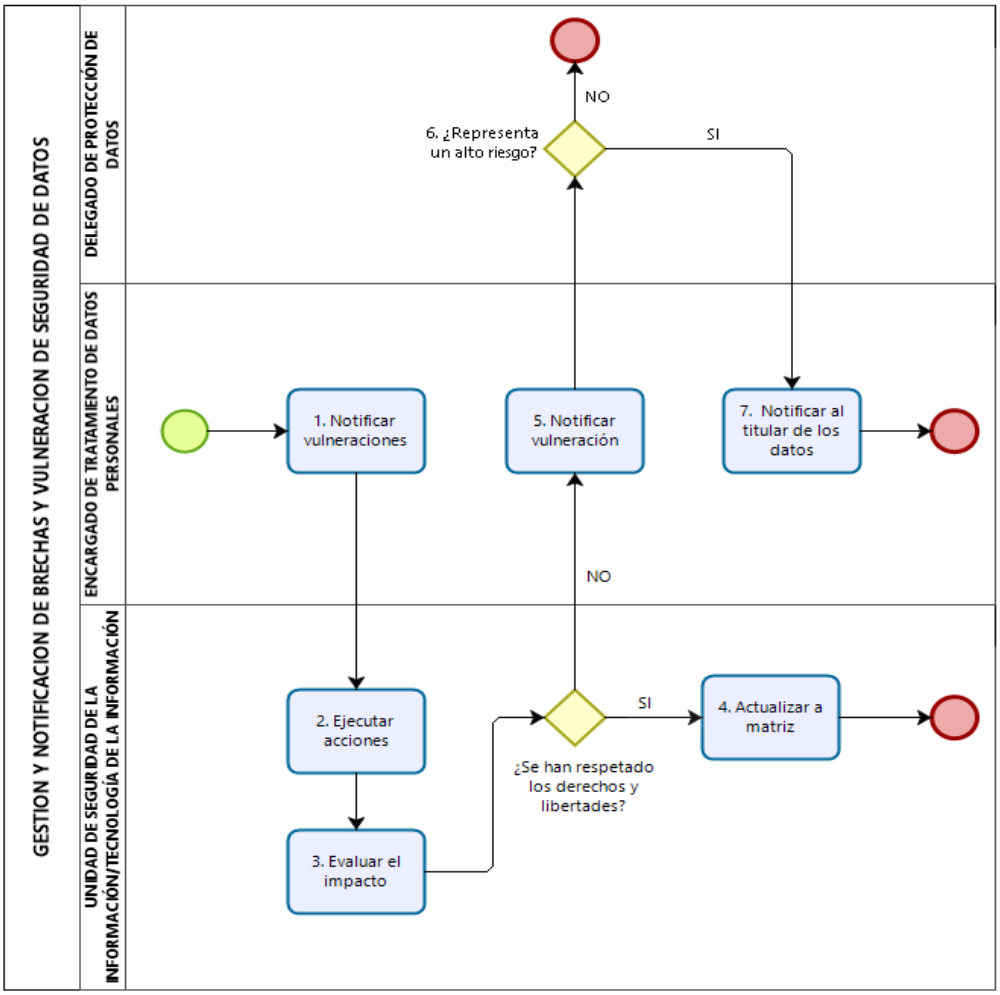
Ilustración 18 Flujo del subproceso de atención de derechos ARCO+.



3.4.2 Evaluación del proceso de gestión y notificación de brechas

El subproceso de gestión y notificación de brechas determinará la responsabilidad de la persona encargada del tratamiento, la unidad de Seguridad de la Información/Tecnología, el responsable del tratamiento y la Delegada de Protección de Datos. El proceso incluye una revisión de acciones de contención, análisis de impacto, revisión de matriz y notificación a la autoridad o al titular en caso de alto riesgo.

Ilustración 19 Flujo del subproceso de gestión y notificación de brechas.



3.4.3 Brechas de cumplimiento, riesgos y vulnerabilidades identificadas

Los hallazgos se consolidaron a partir de la evidencia documental y de los resultados técnicos. En varios casos no se trata de ausencia total de controles, sino de falta de evidencia operativa, ejecución periódica o cierre formal de acciones. Por esa razón se priorizan las

brechas que pueden afectar confidencialidad, trazabilidad, mínimo privilegio, retención y respuesta ante incidentes.

Tabla 43 Hallazgos consolidados de auditoría.

Código	Hallazgo	Condición observada	Prueba asociada	Criticidad	Recomendación
H-01	Trazabilidad técnica parcialmente demostrable	Existen criterios generales de trazabilidad, pero aún es necesario validar los logs reales del core, los eventos críticos, la retención y la integridad de las bitácoras.	PT-09 / PT-SQL-09	Alta	Definir un catálogo de eventos, centralizar los logs, revisar eventos sensibles y documentar reportes periódicos.
H-02	Control de accesos requiere recertificación formal	Se observaron cuentas activas, usuarios sin empleado asociado y empleados desvinculados que todavía mantienen accesos habilitados.	PT-07 / PT-SQL-06 / PT-SQL-07	Alta	Cruzar la información de usuarios con Talento Humano, bloquear cuentas no justificadas y ejecutar una recertificación semestral de accesos.
H-03	Segregación de funciones con conflictos potenciales	Existen usuarios con participación simultánea en procesos o etapas que podrían ser incompatibles entre sí.	PT-08 / PT-SQL-02 / PT-SQL-08	Alta	Definir una matriz SoD, bloquear combinaciones incompatibles y aprobar únicamente excepciones debidamente documentadas.
H-04	Gestión de brechas documentada, pero no probada	Existe un subproceso para la gestión de brechas; sin embargo, falta evidencia de simulacros, tiempos de respuesta, responsables, matriz de severidad y lecciones aprendidas.	PT-10	Alta	Ejecutar un tabletop anual, conservar el acta de resultados y actualizar la matriz de riesgos y controles.
H-05	EIPD del core financiero requiere consolidación	La metodología existe, pero se debe demostrar su aplicación completa sobre los tratamientos críticos del core financiero.	PT-06	Alta	Completar la EIPD del core, incluyendo riesgos, controles, riesgo residual, responsables y seguimiento.
H-06	Minimización y exposición de datos en reportes	Se observaron registros con datos personales y financieros visibles. Además, algunos formularios contienen finalidades	PT-01 / PT-SQL-01	Alta	Crear una matriz campo-finalidad-base legal y aplicar enmascaramiento o

		amplias que requieren mayor precisión.			reducción de campos en los reportes.
H-07	Retención y conservación requieren mayor control técnico	Se observaron registros de personas o clientes sin productos vigentes, pero con datos aún conservados en el sistema.	PT-05 / PT-SQL-03	Alta	Aprobar una tabla de retención y definir criterios de bloqueo, depuración, anonimización o conservación justificada.
H-08	Privilegios administrativos y autenticación SQL deben reforzarse	Se observaron usuarios con rol administrativo elevado y logins con políticas de contraseña incompletas.	PT-11 / PT-SQL-04 / PT-SQL-05	Alta	Revisar los usuarios con rol db_owner, justificar las cuentas técnicas, aplicar el principio de mínimo privilegio y fortalecer las políticas de contraseña.
H-09	Proveedores y encargados requieren evaluación periódica	Existe documentación base, pero falta mantener un inventario actualizado de encargados, accesos de soporte y evaluación de garantías técnicas.	PT-12	Media	Actualizar el inventario de encargados, revisar contratos, cláusulas de confidencialidad, SLA de incidentes y accesos de soporte.
H-10	Capacitación requiere evidencia de ejecución	Existe un plan de capacitación, pero se requiere demostrar su cobertura mediante listas de asistencia, evaluaciones y material aplicado.	PT-13	Media	Ejecutar el plan anual, registrar asistencia, evaluar la comprensión de los contenidos y medir la cobertura por rol.

3.5 Elaboración del informe técnico de auditoría con hallazgos clasificados por criticidad y plan de acción priorizado

3.5.1 Clasificación de hallazgos por criticidad bajo el enfoque ISO 31000

La valoración de criticidad se realizó bajo el enfoque de gestión de riesgos de ISO 31000, considerando la relación entre probabilidad e impacto. La probabilidad representa la posibilidad de ocurrencia o recurrencia de la brecha observada, mientras que el impacto representa la consecuencia sobre confidencialidad, integridad, disponibilidad, derechos del titular, continuidad operativa y exposición frente a la LOPDP. Adicionalmente, se identifica si la afectación normativa es directa, indirecta o de soporte, con el fin de diferenciar

los hallazgos que inciden de manera más clara en obligaciones de protección de datos personales.

El enfoque utilizado sigue la lógica de ISO 31000:2018, que permite adaptar la gestión del riesgo al contexto de la organización. Por ello, parte de criterios definidos para estimar la probabilidad de ocurrencia y la consecuencia del evento sobre los datos personales, el core financiero y la responsabilidad demostrada.

La probabilidad se determinó considerando si la condición fue observada en evidencias documentales, consultas SQL o entrevistas; si puede repetirse por ausencia de control periódico; y si depende de procesos manuales, configuraciones técnicas o terceros. El impacto se valoró según la afectación potencial a confidencialidad, integridad, disponibilidad, derechos ARCO+, minimización, trazabilidad, retención, notificación de brechas y obligaciones del responsable del tratamiento.

Cuando un hallazgo puede afectar directamente principios u obligaciones de la LOPDP, su impacto se eleva porque compromete la capacidad institucional de demostrar cumplimiento. Por esta razón, condiciones como usuarios activos sin relación laboral, privilegios administrativos elevados, exportación masiva de información o conservación de datos sin relación activa fueron tratadas como riesgos de mayor prioridad.

Tabla 44 Escala de probabilidad e impacto para la clasificación de hallazgos

Valor	Probabilidad	Impacto
1	Muy baja: evento aislado o poco probable.	Insignificante: efecto mínimo y controlable.
2	Baja: puede ocurrir en condiciones específicas.	Menor: afecta un proceso limitado.
3	Media: puede repetirse si no se corrige.	Moderado: afecta procesos relevantes o evidencia de cumplimiento.
4	Alta: existe exposición observable o condición recurrente.	Mayor: afecta datos personales, trazabilidad, seguridad o continuidad.
5	Muy alta: condición activa, acumulada o con alta exposición.	Crítico: afecta derechos del titular, control del core, obligaciones legales o respuesta institucional.

Tabla 45 Rangos de criticidad aplicados a los hallazgos.

Puntaje P x I	Nivel de criticidad	Criterio de tratamiento
1 a 4	Baja	Seguimiento ordinario y mejora documental.
5 a 9	Media	Plan de mejora con responsable y seguimiento programado.
10 a 16	Alta	Acción correctiva prioritaria y evidencia de cierre.
17 a 25	Crítica	Atención inmediata, responsable asignado, control compensatorio y seguimiento gerencial.

Con base en la multiplicación de probabilidad e impacto, los resultados se interpretaron de la siguiente forma: de 1 a 4 corresponde a criticidad baja; de 5 a 9, criticidad media; de 10 a 16, criticidad alta; y de 17 a 25, criticidad crítica. Cuando un hallazgo involucró datos sensibles, privilegios administrativos, usuarios desvinculados o ausencia de trazabilidad, se priorizó su tratamiento, aunque existieran controles documentales parciales.

Con el fin de vincular la escala de probabilidad e impacto con los hallazgos obtenidos durante la auditoría, se asignó a cada hallazgo un valor de probabilidad y un valor de impacto. La probabilidad se determinó según la recurrencia, exposición o posibilidad de repetición de la condición observada; mientras que el impacto se valoró considerando la afectación potencial sobre los datos personales, la trazabilidad, el control de accesos, la continuidad operativa, los derechos del titular y la capacidad de la Cooperativa para demostrar cumplimiento frente a la LOPDP.

La criticidad final se obtuvo mediante la multiplicación de ambos valores, de acuerdo con la siguiente fórmula:

Criticidad = Probabilidad x Impacto

Tabla 46 Valoración de criticidad de los hallazgos

Código	Hallazgo	Probabilidad	Impacto	Puntaje P x I	Nivel de criticidad	Justificación
H-01	Trazabilidad técnica parcialmente demostrable	4	4	16	Alta	La falta de evidencia completa sobre logs, eventos críticos, retención e integridad de bitácoras puede afectar la reconstrucción de operaciones sensibles y la demostración de cumplimiento.
H-02	Control de accesos requiere recertificación formal	4	4	16	Alta	La existencia de cuentas activas, usuarios sin empleado asociado y empleados desvinculados con accesos habilitados representa un riesgo relevante para la confidencialidad y el principio de mínimo privilegio.

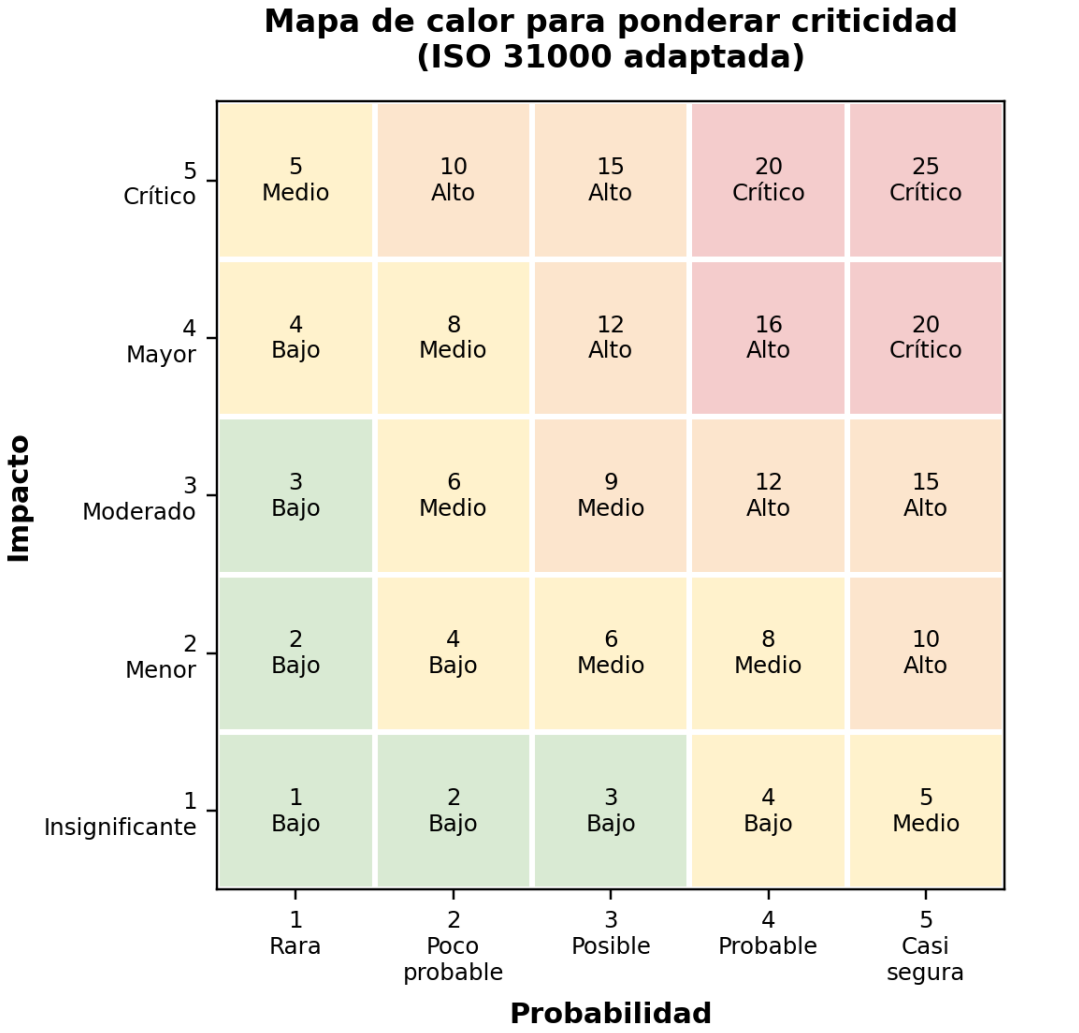
H-03	Segregación de funciones con conflictos potenciales	4	4	16	Alta	Las combinaciones incompatibles de funciones pueden permitir concentración de privilegios en procesos críticos, especialmente en crédito, aprobación, modificación de datos y administración de usuarios.
H-04	Gestión de brechas documentada, pero no probada	3	4	12	Alta	Aunque existe un subproceso documentado, la ausencia de simulacros, actas, tiempos de respuesta y lecciones aprendidas limita la capacidad de respuesta ante vulneraciones de datos personales.
H-05	EIPD del core financiero requiere consolidación	3	4	12	Alta	La Evaluación de Impacto existe como metodología, pero requiere aplicarse de manera completa a los tratamientos críticos del core financiero para evidenciar riesgos, controles y riesgo residual.
H-06	Minimización y exposición de datos en reportes	4	4	16	Alta	La exposición de datos personales, financieros o crediticios sin enmascaramiento puede afectar los principios de minimización, confidencialidad, finalidad y seguridad del tratamiento.
H-07	Retención y conservación requieren mayor control técnico	4	4	16	Alta	La conservación de datos de personas o clientes sin productos vigentes puede generar riesgos de tratamiento innecesario, incumplimiento de plazos de conservación y falta de depuración o anonimización.
H-08	Privilegios administrativos y autenticación SQL deben reforzarse	4	4	16	Alta	Los privilegios elevados y las políticas incompletas de contraseña incrementan el riesgo de acceso no autorizado, modificación indebida o exposición de información crítica del core financiero.

H-09	Proveedores y encargados requieren evaluación periódica	3	3	9	Media	La documentación base existe, pero la falta de inventario actualizado, evaluación periódica y control de accesos de soporte puede afectar la gestión de encargados del tratamiento.
H-10	Capacitación requiere evidencia de ejecución	3	3	9	Media	Aunque existe un plan de capacitación, la ausencia de listas de asistencia, evaluaciones y medición de cobertura limita la demostración de cultura organizacional en protección de datos.

La valoración anterior permite justificar la prioridad asignada a cada hallazgo. Los hallazgos H-01 al H-08 se ubicaron en criticidad alta porque afectan controles técnicos relevantes, evidencias de cumplimiento, accesos, trazabilidad, minimización, retención, incidentes y seguridad del core financiero. Por otro lado, los hallazgos H-09 y H-10 se clasificaron con criticidad media, debido a que existen controles documentales iniciales, pero todavía requieren fortalecimiento, seguimiento y evidencia periódica.

Con esta ponderación, la auditoría no solo identifica brechas, sino que también establece un criterio objetivo para priorizar acciones correctivas. En consecuencia, los hallazgos con mayor puntaje deben atenderse primero, especialmente aquellos relacionados con control de accesos, segregación de funciones, trazabilidad, exposición de datos, retención y privilegios administrativos.

Ilustración 20 Mapa de calor para la evaluación de criticidad



Riesgo = Probabilidad x Impacto | Bajo: 1-4 | Medio: 5-9 | Alto: 10-16 | Crítico: 17-25

3.5.2 Plan de acción priorizado con medidas correctivas y preventivas

El plan de acción se ordena según criticidad y facilidad de verificación. Cada actividad debe cerrarse únicamente cuando exista evidencia suficiente: actas, matrices actualizadas, logs, reportes, aprobaciones, registros, bitácoras o resultados de pruebas.

Tabla 47 Plan de acción priorizado.

N.º	Acción	Responsable sugerido	Plazo	Evidencia esperada	Prioridad
1	Depurar usuarios de empleados desvinculados, cuentas sin empleado asociado y accesos no justificados.	TI / Talento Humano / Jefaturas	30 días	Acta de bloqueo, matriz de usuarios depurada y aprobación de jefaturas.	Alta
2	Revisar usuarios db_owner y logins SQL con política incompleta.	TI / Seguridad de la Información	45 días	Cédula de privilegios DB, reporte de endurecimiento y justificación de cuentas técnicas.	Alta
3	Ejecutar recertificación RBAC/SoD del core y del flujo de crédito.	TI / Operaciones / Crédito / Talento Humano	Semestral	Matriz de roles, incompatibilidades, excepciones y usuarios recertificados.	Alta
4	Centralizar eventos críticos del core y definir catálogo de logs auditables.	TI / Seguridad / Auditoría Informática	120 días	Catálogo de eventos, reportes mensuales, política de retención y evidencia de revisión.	Alta
5	Realizar simulacro de brecha de datos personales.	DPD / Seguridad / TI / Operaciones	60 días	Acta de tabletop, matriz de severidad, tiempos, responsables y lecciones aprendidas.	Alta
6	Completar la EIPD aplicada al core financiero.	DPD / Riesgos / TI / Seguridad	90 días	Informe EIPD, matriz de riesgos, controles, riesgo residual y plan de tratamiento.	Alta
7	Construir matriz campo-finalidad-base legal para formularios, reportes y exportaciones.	DPD / Legal / TI / Áreas propietarias	90 días	Matriz de minimización, reportes ajustados y criterios de enmascaramiento.	Alta
8	Formalizar tabla de retención, bloqueo, anonimización y eliminación segura.	DPD / Legal / TI / Archivo	120 días	Tabla de retención, procedimiento de borrado y actas de eliminación o bloqueo.	Alta
9	Validar exportación masiva con permisos, finalidad y evento de log.	TI / Auditoría Informática	60 días	Cédula de exportación, autorización y registro en bitácora.	Alta
10	Actualizar inventario de encargados y proveedores críticos.	Legal / Compras / TI / DPD	Semestral	Inventario, contratos, acuerdos de confidencialidad, evaluación y SLA de incidentes.	Media
11	Ejecutar plan anual de capacitación y concienciación.	Talento Humano / DPD / Seguridad	Anual	Material, listas de asistencia, evaluaciones y métricas de cobertura.	Media
12	Actualizar matriz de seguimiento LOPDP/ISO/NIST con resultados SQL.	DPD / Auditoría / Seguridad	Trimestral	Matriz con artículo/control, evidencia, responsable, estado y acción correctiva.	Media

3.5.3 Informe técnico final de auditoría

Como resultado del examen practicado, se elaboró un informe final de auditoría técnica dirigido a la Gerencia General y a la Delegada de Protección de Datos Personales de la Cooperativa. Este documento consolida el alcance, criterios aplicados, metodología, pruebas consideradas, resultados generales, hallazgos, plan de acción priorizado, indicadores de seguimiento, dictamen técnico y firmas de entrega y recepción.

Para evitar duplicidad dentro del cuerpo del capítulo, el informe completo no se reproduce en esta sección. El documento íntegro se incorpora como evidencia formal en el Anexo 19 de la presente tesis.

Campo	Detalle
Código del informe	INF-AUD-LOPDP-CCY-001-2026
Entidad auditada	Cooperativa de Ahorro y Crédito Credi Ya Ltda.
Sistema auditado	Core financiero Softbank y procesos institucionales vinculados al tratamiento de datos personales
Opinión emitida	Cumplimiento parcial con necesidad de acciones correctivas prioritarias
Ubicación del informe completo	Anexo 19. Informe final de auditoría técnica entregado a la Cooperativa

3.6 Discusión de resultados

Los resultados confirman que la Cooperativa no parte de cero en materia de protección de datos personales. La política institucional, el manual, los formularios de consentimiento, el formulario ARCO+, los subprocesos y la metodología de riesgos constituyen una base relevante para el cumplimiento. Aun así, desde una auditoría técnica, no basta con que el documento exista; también es necesario demostrar su aplicación mediante registros, bitácoras, responsables definidos, plazos y evidencias de cierre.

La revisión documental permitió precisar la interpretación de algunos hallazgos. Por ejemplo, el proceso ARCO+ y el proceso de gestión de brechas no deben considerarse inexistentes, ya que sí se encuentran documentados. La brecha real está en demostrar su ejecución mediante casos registrados, tiempos de atención, simulacros, bitácoras, comunicaciones y actualización de matrices. Esta precisión mejora el análisis, porque evita exagerar el incumplimiento, pero mantiene la exigencia de contar con evidencia suficiente.

Las pruebas SQL fortalecieron el enfoque técnico del capítulo. Las consultas no reemplazan la evaluación legal, pero sí permiten llevarla a condiciones verificables dentro del sistema. Al revisar usuarios, roles, estados laborales, privilegios de base de datos, etapas de crédito y datos conservados, la auditoría conecta las exigencias de la LOPDP con controles propios de seguridad de la información y auditoría informática.

En conclusión, el cumplimiento de la LOPDP en el core financiero debe gestionarse como un proceso continuo. La Cooperativa cuenta con una base documental importante, pero necesita reforzar la evidencia técnica, el seguimiento periódico y el cierre formal de hallazgos. El plan de acción propuesto permite pasar de un cumplimiento principalmente documental a un esquema más demostrable, controlado y sostenible.

CAPÍTULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

La auditoría técnica permitió determinar que el core financiero Softbank y los procesos institucionales vinculados al tratamiento de datos personales presentan un cumplimiento parcial frente a la Ley Orgánica de Protección de Datos Personales. La Cooperativa cuenta con una base documental importante, conformada por política, manuales, formularios, subprocesos, matriz RAT, metodología de riesgos y plan de capacitación; sin embargo, el cumplimiento requiere reforzarse mediante registros operativos, bitácoras, evidencias periódicas y cierre formal de hallazgos.

Las pruebas documentales-operativas evidenciaron avances en gobernanza, consentimiento, identificación de responsables y existencia de procesos para derechos ARCO+ y gestión de brechas. No obstante, los resultados de encuestas y entrevistas muestran que aún existen brechas de socialización hacia empleados y socios/clientes, especialmente en conocimiento de derechos ARCO+, revocatoria del consentimiento, canales de atención, transferencia de datos a terceros y procedimiento de notificación de vulneraciones.

Las pruebas SQL de auditoría informática aportaron evidencia técnica directa sobre condiciones observables en la base de datos y en el core financiero. Los resultados más críticos se relacionan con usuarios activos sin empleado asociado, empleados desvinculados con accesos habilitados, usuarios inactivos asignados a etapas de crédito, privilegios administrativos elevados, logins con políticas incompletas, registros conservados sin relación activa y exposición de datos personales o financieros en reportes.

La evaluación de riesgos permitió identificar que las prioridades de mejora se concentran en control de accesos, segregación de funciones, trazabilidad, evaluación de impacto aplicada al core, minimización, retención, gestión de brechas, proveedores y capacitación. Estos dominios son determinantes para pasar de un cumplimiento principalmente documental a un cumplimiento demostrable, medible y sostenible.

El informe final de auditoría consolidado como anexo constituye el producto técnico de cierre de la investigación, ya que resume el alcance, criterios, metodología, resultados, hallazgos, criticidad, indicadores y plan de acción priorizado para la Cooperativa. Con

ello se cumple el objetivo de entregar una herramienta útil para fortalecer la responsabilidad proactiva, reducir riesgos legales y operativos, y orientar la mejora continua de la protección de datos personales.

4.2 Recomendaciones

Ejecutar de manera prioritaria la depuración de usuarios del core financiero, cruzando información de Talento Humano con cuentas activas, empleados desvinculados, usuarios sin empleado asociado y responsables asignados a etapas de crédito. El cierre de esta acción debe evidenciarse mediante actas de bloqueo, matriz de usuarios depurada y aprobación de las jefaturas correspondientes.

Implementar una recertificación semestral de accesos basada en RBAC y segregación de funciones, revisando perfiles, cargos, permisos críticos, accesos administrativos, excepciones y combinaciones incompatibles en procesos de crédito, aprobación, modificación de datos y administración de usuarios.

Centralizar y monitorear los eventos críticos del core financiero mediante un catálogo de logs auditables que incluya consultas masivas, exportaciones, modificaciones de datos personales, cambios de perfil, accesos privilegiados y operaciones sensibles. Esta revisión debe generar reportes mensuales y conservar evidencia para auditorías o incidentes.

Completar y aprobar la Evaluación de Impacto de Protección de Datos aplicada específicamente al core financiero, incluyendo tratamientos críticos, categorías de datos, titulares afectados, amenazas, vulnerabilidades, impacto, probabilidad, controles existentes, riesgo residual, responsables y plan de tratamiento.

Fortalecer la minimización y transparencia mediante una matriz campo-finalidad-base legal para formularios, reportes y exportaciones. Esta matriz debe justificar cada dato tratado, diferenciar obligaciones legales, contractuales y consentimientos, y establecer criterios de enmascaramiento o reducción de campos cuando corresponda.

Formalizar una tabla de retención, bloqueo, anonimización y eliminación segura de datos personales, alineada con las obligaciones legales y regulatorias aplicables. Esta tabla debe incluir expedientes físicos, registros del core, respaldos, logs, formularios, solicitudes ARCO+, evidencias de auditoría e incidentes.

Validar periódicamente el subproceso de gestión y notificación de brechas mediante ejercicios documentados, actas, matriz de severidad, responsables, tiempos de respuesta, preservación de evidencia y lecciones aprendidas, de modo que la Cooperativa pueda responder oportunamente ante una vulneración de datos personales.

Actualizar el inventario de encargados y proveedores críticos, incorporando contratos, cláusulas de confidencialidad, finalidad del acceso, datos tratados, controles técnicos, acuerdos de nivel de servicio, obligaciones de notificación de incidentes y evaluación periódica de garantías.

REFERENCIAS BIBLIOGRÁFICAS

[1] Asamblea Nacional del Ecuador, “Ley Orgánica de Protección de Datos Personales,” Registro Oficial Suplemento No. 459, Quito, Ecuador, 26-may-2021. [En línea]. Disponible: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

[2] Presidencia de la República del Ecuador, “Reglamento General a la Ley Orgánica de Protección de Datos Personales,” Decreto Ejecutivo No. 904, Quito, Ecuador, 2023. [En línea]. Disponible: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Decreto-Ejecutivo-No.-904.pdf

[3] Superintendencia de Economía Popular y Solidaria, “Segmentación de entidades del Sector Financiero Popular y Solidario,” SEPS, 2025. [En línea]. Disponible: https://www.seps.gob.ec/institucion/segmentacion-de-esfps/

[4] National Institute of Standards and Technology, “NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0,” NIST, 2020. [En línea]. Disponible: https://www.nist.gov/privacy-framework/privacy-framework

[5] International Organization for Standardization, “ISO/IEC 27701:2019 Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management,” ISO, 2019. [En línea]. Disponible: https://www.iso.org/standard/71670.html

[6] National Institute of Standards and Technology, “Security,” NIST Computer Security Resource Center Glossary. [En línea]. Disponible: https://csrc.nist.gov/glossary/term/security

[7] International Organization for Standardization, “ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements,” ISO, 2022. [En línea]. Disponible: https://www.iso.org/standard/27001

[8] L. Ordóñez Pineda, L. Correa Quezada and A. Correa Conde, “Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria,” Estado & comunes, vol. 2, no. 15, pp. 77-97, 2022, doi: 10.37228/estado_comunes.v2.n15.2022.270.

[9] S. G. Velasco-Urgilés, G. M. Proaño-Reyes and F. de J. Castro-Sánchez, “Buenas prácticas para la protección de datos personales,” Noesis. Revista Electrónica de Investigación, vol. 7, no. 2, ed. esp. II, 2025.

[10] S. L. Mancero-Gavilanes, G. M. Proaño-Reyes and F. de J. Castro-Sánchez, “Protección de datos personales crediticios y administración del perfil de riesgo en Ecuador,” Noesis. Revista Electrónica de Investigación, vol. 7, no. 2, 2025, doi: 10.35381/noesisin.v7i2.619.

[11] G. Rosas-Lanas and G. Pila-Cárdenas, “La protección de datos personales en Ecuador: Una revisión histórica-normativa de este derecho fundamental en el país suramericano,” VISUAL REVIEW. International Visual Culture Review / Revista Internacional de Cultura Visual, vol. 13, no. 2, pp. 1-16, 2023, doi: 10.37467/revvisual.v10.4568.

[12] F. N. Roldán Carrillo, “Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador,” USFQ Law Review, vol. 8, no. 1, pp. 175-202, 2021, doi: 10.18272/ulr.v8i1.2184.

[13] P. A. Astudillo Alvear, V. N. Once González, L. A. Alvarado Ajila and H. G. García Segarra, “Aplicación de la Ley Orgánica de Protección de Datos Personales en el sistema empresarial privado ecuatoriano,” Revista Lex, vol. 7, no. 25, pp. 567-582, 2024, doi: 10.33996/revistalex.v7i25.201.

[14] A. de la C. Cardet Sarduy and J. del P. Cárdenas Cobo, “Evolución normativa de la protección de datos personales en Ecuador: un análisis histórico,” Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, vol. 8, no. 2, pp. 86-101, 2024, doi: 10.33936/isrtic.v8.i2.6978.

[15] J. G. Castro-Paredes, G. R. Mendoza-Masache, N. M. Loja-Mora and H. P. Loján-Alvarado, “Protección de datos por diseño y por defecto. Implicaciones legales en el desarrollo de software,” Ingenium et Potentia, vol. 7, no. 12, pp. 77-96, 2025, doi: 10.35381/i.p.v7i12.4471.

[16] A. Cavoukian, “Privacy by Design: The 7 Foundational Principles,” Information and Privacy Commissioner of Ontario, 2011. [En línea]. Disponible: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

[17] A. Nelson, V. Pillitteri, R. Grimes, K. Boeckl, M. Souppaya and K. Scarfone, “Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile,” NIST SP 800-61 Rev. 3, 2025. [En línea]. Disponible: https://csrc.nist.gov/pubs/sp/800/61/r3/final

[18] International Organization for Standardization, “ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls,” ISO, 2022. [En línea]. Disponible: https://www.iso.org/standard/75652.html

[19] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” NIST CSWP 29, 2024. [En línea]. Disponible: https://www.nist.gov/cyberframework

[20] International Organization for Standardization, “ISO 31000:2018 Risk management - Guidelines,” ISO, 2018. [En línea]. Disponible: https://www.iso.org/iso-31000-risk-management.html

[21] International Organization for Standardization, “ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks,” ISO, 2022. [En línea]. Disponible: https://www.iso.org/standard/80585.html

[22] OWASP Foundation, “OWASP API Security Top 10 - 2023,” OWASP, 2023. [En línea]. Disponible: https://owasp.org/API-Security/editions/2023/en/0x11-t10/

[23] Center for Internet Security, “CIS Critical Security Controls Version 8.1,” CIS, 2024. [En línea]. Disponible: https://www.cisecurity.org/controls/v8-1

[24] European Union Agency for Cybersecurity, “Data Protection Engineering,” ENISA, 2022. [En línea]. Disponible: https://www.enisa.europa.eu/publications/data-protection-engineering

[25] European Union Agency for Cybersecurity, “Privacy and Data Protection by Design - From Policy to Engineering,” ENISA, 2015. [En línea]. Disponible: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[26] European Parliament and Council of the European Union, “Regulation (EU) 2016/679 General Data Protection Regulation,” Official Journal of the European Union, 2016. [En línea]. Disponible: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[27] Organisation for Economic Co-operation and Development, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” OECD, 2013. [En línea]. Disponible: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[28] Agencia Española de Protección de Datos, “Guía de protección de datos por defecto,” AEPD, 2020. [En línea]. Disponible: https://www.aepd.es/documento/guia-proteccion-datos-por-defecto.pdf

[29] Commission Nationale de l’Informatique et des Libertés, “Privacy Impact Assessment (PIA) Methodology,” CNIL, 2018. [En línea]. Disponible: https://www.cnil.fr/en/privacy-impact-assessment-pia

[30] Article 29 Data Protection Working Party, “Guidelines on Data Protection Impact Assessment and determining whether processing is likely to result in a high risk,” WP248 rev.01, 2017. [En línea]. Disponible: https://ec.europa.eu/newsroom/article29/items/611236

[31] Article 29 Data Protection Working Party, “Guidelines on Data Protection Officers (DPOs),” WP243 rev.01, 2017. [En línea]. Disponible: https://ec.europa.eu/newsroom/article29/items/612048

[32] D. J. Solove, Understanding Privacy. Cambridge, MA, USA: Harvard University Press, 2008.

[33] D. J. Solove and P. M. Schwartz, Information Privacy Law, 7th ed. New York, NY, USA: Wolters Kluwer, 2021.

[34] W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th ed. Boston, MA, USA: Pearson, 2018.

[35] M. E. Whitman and H. J. Mattord, Principles of Information Security, 7th ed. Boston, MA, USA: Cengage Learning, 2021.

[36] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Indianapolis, IN, USA: Wiley, 2020.

[37] C. P. Pfleeger, S. L. Pfleeger and J. Margulies, Security in Computing, 5th ed. Boston, MA, USA: Pearson, 2015.

[38] ISACA, COBIT 2019 Framework: Governance and Management Objectives. Schaumburg, IL, USA: ISACA, 2018.

[39] ISACA, COBIT 2019 Framework: Introduction and Methodology. Schaumburg, IL, USA: ISACA, 2018.

[40] S. Garfinkel, "De-identification of Personal Information," NIST IR 8053, 2015. [En línea]. Disponible: https://csrc.nist.gov/publications/detail/nistir/8053/final[41] E. Barker, "Recommendation for Key Management: Part 1 - General," NIST SP 800-57 Part 1 Rev. 5, 2020. [En línea]. Disponible: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

[42] P. A. Grassi, M. E. Garcia and J. L. Fenton, "Digital Identity Guidelines," NIST SP 800-63-3, 2017. [En línea]. Disponible: https://pages.nist.gov/800-63-3/

[43] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," NIST SP 800-53 Rev. 5, 2020. [En línea]. Disponible: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[44] National Institute of Standards and Technology, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," NIST SP 800-161 Rev. 1, 2022. [En línea]. Disponible: https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

[45] Superintendencia de Economía Popular y Solidaria, "Norma de control para el ejercicio de la auditoría externa, auditoría interna y auditoría informática en las cooperativas de ahorro y crédito," Resolución Nro. SEPS-IGT-IGS-INR-INGINT-INSESF-2023-008, 2023. [En línea]. Disponible: https://www.seps.gob.ec/wp-

content/uploads/Resolucio%CC%81n-Nro.-SEPS-IGT-IGS-INR-INGINT-INSESF-2023-008.pdf

[46] A. Narayanan and V. Shmatikov, “Robust De-anonymization of Large Sparse Datasets,” in Proc. IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2008, pp. 111-125, doi: 10.1109/SP.2008.33.

[47] P. Samarati and L. Sweeney, “Protecting Privacy when Disclosing Information: k-Anonymity and its Enforcement through Generalization and Suppression,” SRI International, Tech. Rep., 1998.

[48] C. Dwork, “Differential Privacy,” in Automata, Languages and Programming, Berlin, Germany: Springer, 2006, pp. 1-12, doi: 10.1007/11787006_1.

[49] K. Renaud and V. Zimmermann, “Data Privacy and Security in Organizations: An Empirical Study,” Information & Computer Security, vol. 26, no. 1, pp. 2-17, 2018, doi: 10.1108/ICS-12-2017-0088.

ANEXOS

Evidencias institucionales y técnicas base

Anexo 1 Política para la Protección y Tratamiento de Datos Personales

Activo de la Información: ☐Uso Público ☑ Uso Interno ☐ Restringida ☐ Confidencial	
Código: POL-GPD-PDP-001-2026	**Tipo de Proceso:** ☑ Gobernante ☐ Operativos ☐ Apoyo
Macroproceso: Gestión de Protección de Datos Personales	**Tipo de Manual:** ☐Organizacional ☐ Procesos ☑Políticas
Fecha de Elaboración: 04 de marzo del 2026	**Fecha de Aprobación:** 04 de abril del 2026
Páginas: 29	

POLÍTICA PARA LA PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

VERSIÓN: 2.0

Propietario del documento: *Delegado de Protección de Datos*

RUBRO	NOMBRE	CARGO	FIRMA
Aprobado por:	Tnlga. Luz Chuqui Bueno	Consejo de Administración	
Revisado por:	Ing. Cristina Santamaría, Msc.	Gerente General	
	Ing. Gabriel Reyes	Responsable de Riesgos	
	Ing. Johnny Ganan	Oficial de Seguridad de la Información	
Elaborado por:	Abg. Renata Ocaña	Delegada de Protección de Datos Personales	
	Ing. Nancy Ilbay, Mgtr.	Coordinadora de Procesos	

Anexo 2 Manual de Seguridad de la Información

crediYa cooperativa de ahorro y crédito HONRAMOS TU CONFIANZA

Activo de la Información: ☐ Uso Público ☑ Uso Interno ☐ Restringida ☐ Confidencial	
Código: MDP-GPD-001-2026	**Tipo de Proceso:** ☐ Gobernante ☑ Apoyo ☐ Operativos
Macroproceso: Gestión de Protección de Datos	**Tipo de Manual:** ☐ Organizacional ☑ Procesos ☐ Técnico
Fecha de Elaboración: 02 de marzo del 2026	**Fecha de Aprobación:** 07 de mayo del 2026
Páginas: 9	

MANUAL DE POLITICAS Y PROCEDIMIENTOS DE PROTECCIÓN DE DATOS

VERSIÓN: 1.0

Propietario del documento: *Delegado de Protección de Datos*

RUBRO	NOMBRE	CARGO	FIRMA
Aprobado por:	Tnlga. Luz Chuqui Bueno	Consejo de Administración	
Revisado por:	Ing. Cristina Santamaría, Msc.	Gerente General	
	Ing. Gabriel Reyes	Responsable de Riesgos	
	Ing. Johnny Ganan	Oficial de Seguridad de la Información	
	Ing. José Acán	Coordinador de Tecnologías de la Información	
Elaborado por:	Abg. Renata Ocaña	Delegada de Protección de Datos Personales	
	Ing. Nancy Ilbay	Coordinadora de Procesos	

Derechos reservados de la Cooperativa de Ahorro y Crédito Credi Ya Ltda. Prohibida su reproducción total o parcial sin autorización explícita.

Anexo 3 Formulario de solicitud para el ejercicio de derechos ARCO+

FORMULARIO DE SOLICITUD PARA EL EJERCICIO DE DERECHOS ARCO

1. DATOS DEL TITULAR DE LOS DATOS PERSONALES

Nombres y apellidos: _____

Documento de identificación: _____

N° de Cédula: _____

RUC: _____

Pasaporte: _____

Dirección domiciliaria: _____

Correo electrónico: _____

N° Celular: _____ **Nº Telefónico:** _____

Nombre del Representante Legal (Si aplica): _____

N° de Cédula: _____

N° de Notaria: _____

Pasaporte:

NOTA: En caso que en la presente solicitud se hayan llenado los datos del representante legal se deberá adjuntar una copia simple de la cedula de identidad o pasaporte del representante legal, así como copia del poder otorgado por vía notarial cuando corresponda, adicional deberá anexar los documentos que acredite su facultad, para así ejercer cualquiera de los derechos ARCO.

2. DERECHO QUE SOLICITA EJERCER

DERECHO	DESCRIPCIÓN	MARQUE CON UNA (X)
Acceso a la información	El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información de sus datos personales.	☐
Rectificación y actualización	El titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos.	☐
Eliminación o cancelación	El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales.	☐
Oposición	El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales.	☐
Portabilidad	El titular tiene el derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, inter-operable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables.	☐
Suspensión del tratamiento	El titular tendrá derecho a obtener del responsable del tratamiento la suspensión del tratamiento de los datos o revocar el consentimiento para el tratamiento de sus datos personales en cualquier momento.	☐

Anexo 4 Subproceso Atención de Derechos ARCO+

Activo de la Información: ☐ Uso Público ☑ Uso Interno ☐ Restringida ☐ Confidencial	
Código: SUB-GPD-ADA-001	**Tipo de Proceso:** ☑ Gobernante ☐Operativos ☐ Apoyo
Macroproceso: Gestión de Protección de datos Personales	**Tipo de Manual:** ☐ Organizacional ☐ Técnico ☑ Procesos
Fecha de Elaboración: 02 de marzo del 2026	**Fecha de Aprobación:** 20 de marzo del 2026
Páginas: 12	

SUBPROCESO ATENCION DE DERECHOS ARCO

VERSIÓN: 1.0

Propietario del documento: *Delegado de Protección de Datos*

RUBRO	NOMBRE	CARGO	FIRMA
Aprobado por:	Tnlga. Luz Chuqui Bueno	Consejo de Administración	
Revisado por:	Ing. Cristina Santamaría, Msc.	Gerente General	
	Ing. Gabriel Reyes	Responsable de Riesgos	
	Ing. Johnny Ganan	Oficial de Seguridad de la Información	
	Ing. José Acán	Coordinador de Tecnologías de la Información	
Elaborado por:	Abg. Renata Ocaña	Delegada de Protección de Datos Personales	
	Ing. Nancy Ilbay, Mgtr.	Coordinadora de Procesos	

Anexo 5 Subproceso Gestión y Notificación de Brechas de Datos

crediYa cooperativa de ahorro y crédito HONRAMOS TU CONFIANZA

Activo de la Información: ☐ Uso Público ☑ Uso Interno ☐ Restringida ☐ Confidencial	
Código: SUB-GPD-NOT-001	**Tipo de Proceso:** ☑ Gobernante ☐Operativos ☐ Apoyo
Macroproceso: Gestión de Protección de datos Personales	**Tipo de Manual:** ☐ Organizacional ☐ Técnico ☑ Procesos
Fecha de Elaboración: 02 de marzo del 2026	**Fecha de Aprobación:** 20 de marzo del 2026
Páginas: 09	

SUBPROCESO GESTIÓN Y NOTIFICACION DE BRECHAS Y VULNERACION DE SEGURIDAD DE DATOS

VERSIÓN: 1.0

Propietario del documento: *Delegado de Protección de Datos*

RUBRO	NOMBRE	CARGO	FIRMA
Aprobado por:	Tnlga. Luz Chuqui Bueno	Consejo de Administración	
Revisado por:	Ing. Cristina Santamaría, Msc.	Gerente General	
	Ing. Gabriel Reyes	Responsable de Riesgos	
	Ing. Johnny Ganan	Oficial de Seguridad de la Información	
	Ing. José Acán	Coordinador de Tecnologías de la Información	
Elaborado por:	Abg. Renata Ocaña	Delegada de Protección de Datos Personales	
	Ing. Nancy Ilbay, Mgtr.	Coordinadora de Procesos	

Derechos reservados de la Cooperativa de Ahorro y Crédito Credi Ya Ltda. Prohibida su reproducción total o parcial sin autorización explícita.

Anexo 6 Metodología para la Gestión de Riesgos y Evaluación de Impacto

Activo de la Información: ☐ Uso Público ☑ Uso Interno ☐ Restringida ☐ Confidencial	
Código: MET-GPD-GRE-001-2026	**Tipo de Proceso:** ☐ Gobernante ☐ Operativos ☑ Apoyo
Macroproceso: Gestión de Protección de Datos Personales	**Tipo de Manual:** ☐ Políticas ☐Procesos ☑ Metodología
Fecha de Elaboración: 04 de marzo del 2026	**Fecha de Aprobación:** 04 de abril del 2026
Páginas: 17	

METODOLOGÍA PARA LA GESTION DE RIESGOS Y EVALUACION DE IMPACTO DEL TRATAMIENTO DE DATOS PERSONALES

VERSIÓN: 1.0

Propietario del documento: *Delegado de Protección de Datos*

RUBRO	NOMBRE	CARGO	FIRMA
Aprobado por:	Tnlga. Luz Chuqui Bueno	Consejo de Administración	
Revisado por:	Ing. Cristina Santamaría, Msc.	Gerente General	
	Ing. Gabriel Reyes	Responsable de Riesgos	
	Ing. Johnny Ganan	Oficial de Seguridad de la Información	
Elaborado por:	Abg. Renata Ocaña	Delegada de Protección de Datos Personales	
	Ing. Nancy Ilbay, Mgtr.	Coordinadora de Procesos	

Anexo 7 Plan de Capacitación en Protección de Datos Personales

Activo de la Información: ☐Uso Público ☑ Uso Interno ☐ Restringida ☐ Confidencial	
Código: PLA-GPD-CAP-001-2026	**Tipo de Proceso:** ☑ Gobernante ☐ Operativos ☐ Apoyo
Macroproceso: Gestión de Protección de Datos Personales	**Tipo de Manual:** ☐Organizacional ☐ Procesos ☑Políticas
Fecha de Elaboración: 04 de marzo del 2026	**Fecha de Aprobación:** 04 de abril del 2026
Páginas: 19	

PLAN DE CAPACITACION Y CONCIENCIACION EN PROTECCIÓN DE DATOS PERSONALES

VERSIÓN: 1.0

Propietario del documento: *Delegado de Protección de Datos*

RUBRO	NOMBRE	CARGO	FIRMA
Aprobado por:	Tnlga. Luz Chuqui Bueno	Consejo de Administración	
Revisado por:	Ing. Cristina Santamaría, Msc.	Gerente General	
	Ing. Gabriel Reyes	Responsable de Riesgos	
	Ing. Johnny Ganan	Oficial de Seguridad de la Información	
Elaborado por:	Abg. Renata Ocaña	Delegada de Protección de Datos Personales	
	Ing. Nancy Ilbay, Mgtr.	Coordinadora de Procesos	

Anexo 8 Formulario de consentimiento para socios/clientes

FOR

MULARIO DE CONSENTIMIENTO PARA LA RECOLECCIÓN Y TRATAMIENTO DE DATOS DE LOS SOCIOS/CLIENTES

Autorizo libre, voluntaria, previa, explícita, informada e inequívocamente a la Cooperativa de Ahorro y Crédito Credi Ya Ltda., (en adelante la COOPERATIVA) para que realice el tratamiento de mis datos personales, crediticios y/o datos no públicos, o los de mi representada según fuera el caso (en adelante DATOS o INFORMACIÓN), incluyendo aquellos que entrego, haya entregado o pueda entregar posteriormente bien sea de manera personal o por intermedio de terceros que cuenten con mi suficiente autorización, de igual modo, los que la COOPERATIVA llegue a tener o haya tenido acceso ya sea a través de canales físicos, virtuales, electrónicos, electromecánicos, telefónicos, correos electrónicos, de formularios virtuales y/o cookies, sean estos propios o de redes asociadas. Por lo mencionado, acepto y autorizo el tratamiento inclusive de mis datos sensibles, tales como biométricos, de salud, crediticios, transaccionales, datos sujetos a sigilo o reserva entre otros.

El tratamiento de DATOS tendrá las siguientes finalidades: elaborar y/o segmentar perfiles, realizar análisis crediticios incluso mediante técnicas automáticas, preparar y/o emprender campañas informativas con enfoque de responsabilidad social, desarrollar acciones comerciales de productos y servicios financieros y/o comerciales, realizar nuevos prototipos, versiones o actualizaciones de canales electrónicos y/o comercializar y promocionar (incluyendo el envío de publicidad por cualquier medio) diferentes productos y servicios financieros y/o comerciales.

Para efectos de esta autorización se entiende por tratamiento a cualquier operación o conjunto de operaciones realizadas sobre mis DATOS ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, evaluación, análisis, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, procesamiento, consolidación, anonimización, seudonimización, posesión, aprovechamiento, rentabilización, distribución, cesión, comunicación, disposición, divulgación o transferencia o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción, verificación de identidad para los accesos a canales electrónicos de la COOPERATIVA y en general cualquier uso de DATOS.

De la misma manera autorizo expresamente a la COOPERATIVA tratar, mantener, conservar y almacenar mis DATOS o los de mi representada, lo que fuera del caso, establecidos por la ley, con el objeto de que la COOPERATIVA sus subsidiarias y/o terceros autorizados de manera individual o conjunta puedan prestar servicios, elaborar y segmentar perfiles, realizar análisis crediticios incluso mediante técnicas automáticas que utilicen mis datos actuales, históricos y estadísticos, para la valoración de riesgos, mercadeo, confección y análisis de nuevas propuestas comerciales de servicios de cualquier tipo, inclusive como elemento de análisis en etapas pre-contractuales, contractuales y pos-tcontractuales, con el fin de remitirme comunicaciones comerciales y/o contactarme por cualquier medio para la oferta, promoción y contratación de productos y/o servicios que brinde la institución.

Autorizo la recolección y tratamiento de datos de mis hijos menores de edad, cuando se oferte productos y servicios mismos que no deberán afectar al interés superior de los mismos.

Anexo 9 Formulario de consentimiento para colaboradores

FORMULARIO DE CONSENTIMIENTO PARA LA RECOLECCIÓN Y TRATAMIENTO DE DATOS DE LOS COLABORADORES

De conformidad a lo dispuesto en el Artículo 8 de la Ley Orgánica de Protección de Datos Personales, publicado en el Registro Oficial Suplemento 459 de fecha 26 de mayo del año 2021; y, numerales 8.2 de la Política para la Protección y Tratamiento de datos personales de la Cooperativa de Ahorro y Crédito Credi Ya, autorizo libre, expresa e inequívocamente a la Cooperativa, para que realice la recolección y tratamiento de mis datos personales que suministro de manera veraz y completa los cuales serán utilizados para los siguientes fines:

a) Conocer de manera suficiente al colaborador con quien se propone entablar una relación laboral.
b) Mantener una comunicación eficiente de la información que se requiera en los vínculos contractuales.
c) Cumplir con las obligaciones sociales y tributarias contraídas por la Cooperativa en función de los vínculos laborales (pago de la remuneración, prestaciones sociales, pago de beneficios laborales y otras establecidas en el contrato de trabajo.
d) Informar al empleado sobre cualquier modificación de la relación contractual.
e) Evaluar la calidad y desempeño del colaborador en cumplimiento de sus funciones derivadas del contrato de trabajo.
f) Realizar estudios internos sobre los hábitos del colaborador con el fin de mejorar las políticas de clima organizacional.
g) Realizar los descuentos de nómina autorizados por el colaborador.
h) Documentar y controlar la asignación de activos de información,
i) Suministrar cuando se requiera información a los entes de control para auditorías internas y externas.
j) Asignación de herramientas de trabajo para el desarrollo de sus funciones (creación de cuentas de correo institucional, creación de usuario en el core financiero y asignación de contraseñas), firmas de acuerdos de confidencialidad y no divulgación.
k) Verificar referencias personales y laborales durante el proceso de contratación,
l) Contactar con los familiares en casos de emergencia.
m) Ofertar productos y servicios financieros hasta el monto que la ley y la normativa interna le faculte.
n) Conocer el estado de salud de los colaboradores, con el fin de identificar Patologías Clínicas, enfermedades profesionales, garantizando una adecuada prevención, diagnóstico, tratamiento y rehabilitación.
o) Conocer la salud financiera del colaborador mediante el score crediticio para evitar posibles fraudes.
p) Comprobar el cumplimiento del horario laboral a través de capturas de imágenes faciales y/o dactilares del colaborador.
q) Suministrar los datos recolectados a las autoridades de control y vigilancia, de la policía, judiciales y/o administrativas, en virtud de un requerimiento legal y/o usar o revelar esa información y datos personales en defensa de los derechos de la Cooperativa y/o su patrimonio, en cuanto la referida defensa tenga relación con las actividades que desempeña en la institución.
r) Autorizo la recolección y tratamiento de datos de mis hijos menores de edad, cuando se oferte productos y servicios mismos que no deberán afectar al interés superior de los mismos.
s) Autorizo la recolección y tratamiento de datos recolectada a través de los biométricos, las cámaras de video vigilancia ubicadas en las instalaciones de la Cooperativa, para identificar o precautelar el cometimiento de infracciones administrativas, civiles y penales; y, proporcionar la información a las autoridades de control, policía y judiciales en virtud de requerimiento legal.

Esta autorización se le concede una vez que he sido informado de manera clara y precisa, de los fines de la recolección y tratamiento de mis datos y la posibilidad que tenía de no efectuar la autorización en aquella información considerada sensible.

Como titular de la información, fui informado de los derechos que tengo, especialmente de conocer, actualizar, rectificar, suprimir, eliminar y/o inactivar mi información personal, las cuales podré ejercer a través de las ventanillas de atención al usuario o el correo electrónico: protecciondedatos@crediya.fin.ec, o línea de atención al cliente 032427433 extensión 100.

Ciudad de _____ a los _____días del mes de _____ del 20_____

Apellidos y Nombres del Colaborador: _____

Firma_____

Cedula: _____

Anexo 10 Formulario de consentimiento para proveedores

FORMULARIO DE CONSENTIMIENTO PARA LA RECOLECCIÓN Y TRATAMIENTO DE DATOS DE LOS PROVEEDORES

De conformidad a lo dispuesto en el Artículo 8 de la Ley Orgánica de Protección de Datos Personales, publicado en el Registro Oficial Suplemento 459 de fecha 26 de mayo del año 2021 ; y, numerales 8.4 de la Política para la Protección y Tratamiento de datos personales de la Cooperativa de Ahorro y Crédito Credi Ya, autorizo libre, expresa e inequívocamente a la Cooperativa, para que realice la recolección y tratamiento de mis datos personales que suministro de manera veraz y completa, los cuales serán utilizados para los siguientes fines:

a) Ejercer el derecho de conocer de manera suficiente al proveedor con quien se propone entablar relaciones comerciales.
b) Atender de una manera eficiente cualquier reclamo, aclaración o solicitud.
c) Evaluar la calidad y desempeño del proveedor en cumplimiento de sus funciones derivadas de la relación contractual.
d) Evaluar políticas establecidas en el manual de proveedores.
e) Instar el cumplimiento de los acuerdos de confidencialidad y no divulgación de la información.
f) Suministrar los datos recolectados a las autoridades de control y vigilancia, de policía, judiciales y/o administrativas, en virtud de un requerimiento legal y/o usar o revelar esta información y datos personales en defensa de los derechos de la Cooperativa y/o su patrimonio, en cuanto dicha defensa tenga relación con los productos y/o servicios contratados.
g) Verificar que la información proporcionada por la Cooperativa en la contratación de productos y servicios no sea divulgada, transferida y cedida a ninguna persona natural o jurídica.
h) Entablar relación de compras de productos y servicios.
i) Autorizo la recolección y tratamiento de datos recolectada a través de las cámaras de video vigilancia ubicadas en las instalaciones de la Cooperativa, para identificar o precautelar el cometimiento de infracciones administrativas civiles y penales; y, proporcionar la información a las autoridades de control, policía y judiciales en virtud de requerimiento legal.

Esta autorización se le concede una vez que he sido informado de manera clara y precisa, de los fines de la recolección y tratamiento de mis datos y la posibilidad que tenía de no efectuar la autorización en aquella información considerada sensible.

Como titular de la información, fui informado de los derechos que tengo, especialmente de conocer, actualizar, rectificar, suprimir, eliminar y/o inactivar mi información personal, las cuales podré ejercer a través de las ventanillas de atención al usuario o el correo electrónico: protecciondedatos@crediya.fin.ec, o línea de atención al cliente 032427433 extensión 100.

Ciudad de _____ a los _____días del mes de _____ del 20_____

Apellidos y Nombres del Proveedor:
_____

Firma_____

Cedula: _____

Anexo 11 Formulario de consentimiento para visitantes

FORMULARIO DE CONSENTIMIENTO PARA LA RECOLECCIÓN Y TRATAMIENTO DE DATOS DE LOS VISITANTES

De conformidad a lo dispuesto en el Artículo 8 de la Ley Orgánica de Protección de Datos Personales, publicado en el Registro Oficial Suplemento 459 de fecha 26 de mayo del año 2021; y, numerales 7.9 y 7.10 de la Política para la Protección y Tratamiento de datos personales de la Cooperativa de Ahorro y Crédito Credi Ya, autorizo libre, expresa e inequívocamente a la Cooperativa, para que rea ice la recolección y tratamiento de mis datos personales que suministro de manera veraz y completa, los cuales serán utilizados para los siguientes fines:

a) Identificar en las instalaciones de La Cooperativa con el objeto de garantizar la seguridad del mismo y la de los colaboradores de la Institución,
b) Suministrar los datos recolectados a las autoridades de control y vigilancia, de la policía, judiciales y/o administrativas, en virtud de un requerimiento legal y/o usar o revelar esa información y datos personales en defensa de los derechos de la Cooperativa y/o su patrimonio, en cuanto la referida defensa tenga relación con los productos y servicios contratados.
c) Autorizo la recolección y tratamiento de datos recolectada a través de las cámaras de video vigilancia ubicadas en las instalaciones de la Cooperativa, para identificar o precautelar el cometimiento de infracciones administrativas, civiles y penales; y, proporcionar la información a las autoridades de control, policía y judiciales en virtud de requerimiento legal.

Esta autorización se le concede una vez que he sido informado de manera clara y precisa, de los fines de la recolección y tratamiento de mis datos y la posibilidad que tenía de no efectuar la autorización en aquella información considerada sensible.

Como titular de la información, fui informado de los derechos que tengo, especialmente de conocer, actualizar, rectificar, suprimir, eliminar y/o inactivar mi información personal, las cuales podré ejercer a través de las ventanillas de atención al usuario o el correo electrónico: protecciondedatos@crediya.fin.ec, o línea de atención al cliente 032427433 extensión 107.

Ambato a, _____ días del mes de _____ del _____20_____

Firma_____

Apellidos y Nombres del visitante:
_____

Cedula: _____

Anexo 12 Formulario de consentimiento para pasantes

ANEXO 6

FORMULARIO DE CONSENTIMIENTO PARA LA RECOLECCIÓN Y TRATAMIENTO DE DATOS DE LOS PASANTES

De conformidad a lo dispuesto en el Artículo 8 de la Ley Orgánica de Protección de Datos Personales, publicado en el Registro Oficial Suplemento 459 de fecha 26 de mayo del año 2021; y, numerales 8.2 de la Política para la Protección y Tratamiento de datos personales de la Cooperativa de Ahorro y Crédito Credi Ya, autorizo libre, expresa e inequívocamente a la Cooperativa, para que realice la recolección y tratamiento de mis datos personales que suministro de manera veraz y completa los cuales serán utilizados para los siguientes fines:

a) Conocer de manera suficiente al pasante con quien se propone entablar una relación de pasantías.
b) Mantener una comunicación eficiente de la información que se requiera en la relación formativa.
c) Evaluar la calidad y desempeño del pasante en cumplimiento de sus funciones.
d) Documentar y controlar la asignación de activos de información.
e) Suministrar cuando se requiera información a los entes de control para auditorías internas y externas.
f) Asignación de herramientas de trabajo para el desarrollo de sus funciones (creación de cuentas de correo institucional, creación de usuario en el core financiero y asignación de contraseñas), firmas de acuerdos de confidencialidad y no divulgación.
g) Contactar con los familiares en casos de emergencia.
h) Ofertar productos y servicios financieros hasta el monto que la ley y la normativa interna le faculte.
i) Conocer el estado de salud de los pasantes, con el fin de identificar Patologías Clínicas, enfermedades profesionales, garantizando una adecuada prevención, diagnóstico, tratamiento y rehabilitación.
j) Conocer la salud financiera del pasante mediante el score crediticio para evitar posibles fraudes.
k) Comprobar el cumplimiento del horario laboral a través de bitácoras, capturas de imágenes faciales y/o dactilares del colaborador.
l) Suministrar los datos recolectados a las autoridades de control y vigilancia, de la policía, judiciales y/o administrativas, en virtud de un requerimiento legal y/o usar o revelar esa información y datos personales en defensa de los derechos de la Cooperativa y/o su patrimonio, en cuanto la referida defensa tenga relación con las actividades que desempeña en la institución.
m) Autorizo la recolección y tratamiento de datos recolectada a través de los biométricos, las cámaras de video vigilancia ubicadas en las instalaciones de la Cooperativa, para identificar o precautelar el cometimiento de infracciones administrativas, civiles y penales; y, proporcionar la información a las autoridades de control, policía y judiciales en virtud de requerimiento legal.

Esta autorización se le concede una vez que he sido informado de manera clara y precisa, de los fines de la recolección y tratamiento de mis datos y la posibilidad que tenía de no efectuar la autorización en aquella información considerada sensible.

Como titular de la información, fui informado de los derechos que tengo, especialmente de conocer, actualizar, rectificar, suprimir, eliminar y/o inactivar mi información personal, las cuales podré ejercer a través de las ventanillas de atención al usuario o el correo electrónico: protecciondedatos@crediya.fin.ec, o línea de atención al cliente 032427433 extensión 100.

Ciudad de _____ a los _____días del mes de _____ del 20_____

Apellidos y Nombres del Pasante: _____

Firma_____

Cedula: _____

Anexo 13 Formulario de consentimiento para directivos

FORMULARIO DE CONSENTIMIENTO PARA LA RECOLECCIÓN Y TRATAMIENTO DE DATOS PERSONALES - DIRECTIVOS

De conformidad a lo dispuesto en el Artículo 8 de la Ley Orgánica de Protección de Datos Personales, publicado en el Registro Oficial Suplemento 459 de fecha 26 de mayo del año 2021; y, numerales 7.9 y 7.10 de la Política para la Protección y Tratamiento de datos personales de la Cooperativa de Ahorro y Crédito Credi Ya, autorizo libre, expresa e inequívocamente a la Cooperativa, para que realice la recolección y tratamiento de mis datos personales que suministro de manera veraz y completa, los cuales serán utilizados para los siguientes fines:

a) Suministrar oportunamente la información al órgano regulador.
b) Verificar referencias personales y laborales durante el proceso de posesión de los administradores.
c) Contactar con los familiares en casos de emergencia.
d) Ofertar productos y servicios financieros hasta el monto que la ley y la normativa interna le faculte.
e) Conocer y garantizar el estado de salud de los administradores a fin de evitar y garantizar enfermedades profesionales.
f) Conocer la salud financiera mediante el score crediticio para evitar posibles fraudes,
g) Suministrar los datos recolectados a las autoridades de control y vigilancia, de la policía, judiciales y/o administrativas, en virtud de un requerimiento legal y/o usar o revelar esa información y datos personales en defensa de los derechos de la Cooperativa y/o su patrimonio, en cuanto la referida defensa tenga relación con las actividades que desempeña en la institución,
h) Autorizo la recolección y tratamiento de datos de mis hijos menores de edad, cuando se oferte productos y servicios mismos que no deberán afectar al interés superior de los mismos,
i) Autorizo la recolección y tratamiento de datos recolectada a través de los biométricos, las cámaras de video vigilancia ubicadas en las instalaciones de la Cooperativa, para identificar o precautelar el cometimiento de infracciones administrativas, civiles y penales; y, proporcionar la información a las autoridades de control, policía y judiciales en virtud de requerimiento legal.

Esta autorización se le concede una vez que he sido informado de manera clara y precisa, de los fines de la recolección y tratamiento de mis datos y la posibilidad que tenía de no efectuar la autorización en aquella información considerada sensible.

Como titular de la información, fui informado de los derechos que tengo, especialmente de conocer, actualizar, rectificar, suprimir, eliminar y/o inactivar mi información personal, las cuales podré ejercer a través de las ventanillas de atención al usuario o el correo electrónico: protecciondedatos@crediya.fin.ec, o línea de atención al cliente 032427433 extensión 100.

Ciudad de _____ a los _____días del mes de _____ del 20_____

Apellidos y Nombres del Directivo:
_____

Firma: _____

Cedula: _____

Anexo 14 Extracto de Matriz RAT

E-14. Extracto de Matriz RAT

Extracto del libro: MATRIZ RAT.xlsx | Hoja: RAT

Columna A	Columna B	Columna C	Columna D
UNIDAD DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS			
MATRIZ DE REGISTRO DE TRATAMIENTO DE DATOS PERSONALES			
N°	Codigo	Macroproceso	Proceso
N°	Codigo	Macroproceso	Proceso
1	GTI-TI-AT-1	Gestión de Talento Humano	Talento Humano
2		Gestión de Operaciones	Atención socio / cliente
2	GTI-CC-RIRDC-01	Gestión de Negocios	Consesión de Crédito

Captura generada desde el archivo Excel entregado para el anexo de auditoría.

Anexo 15 Extracto de Matriz de Evaluación de Impacto

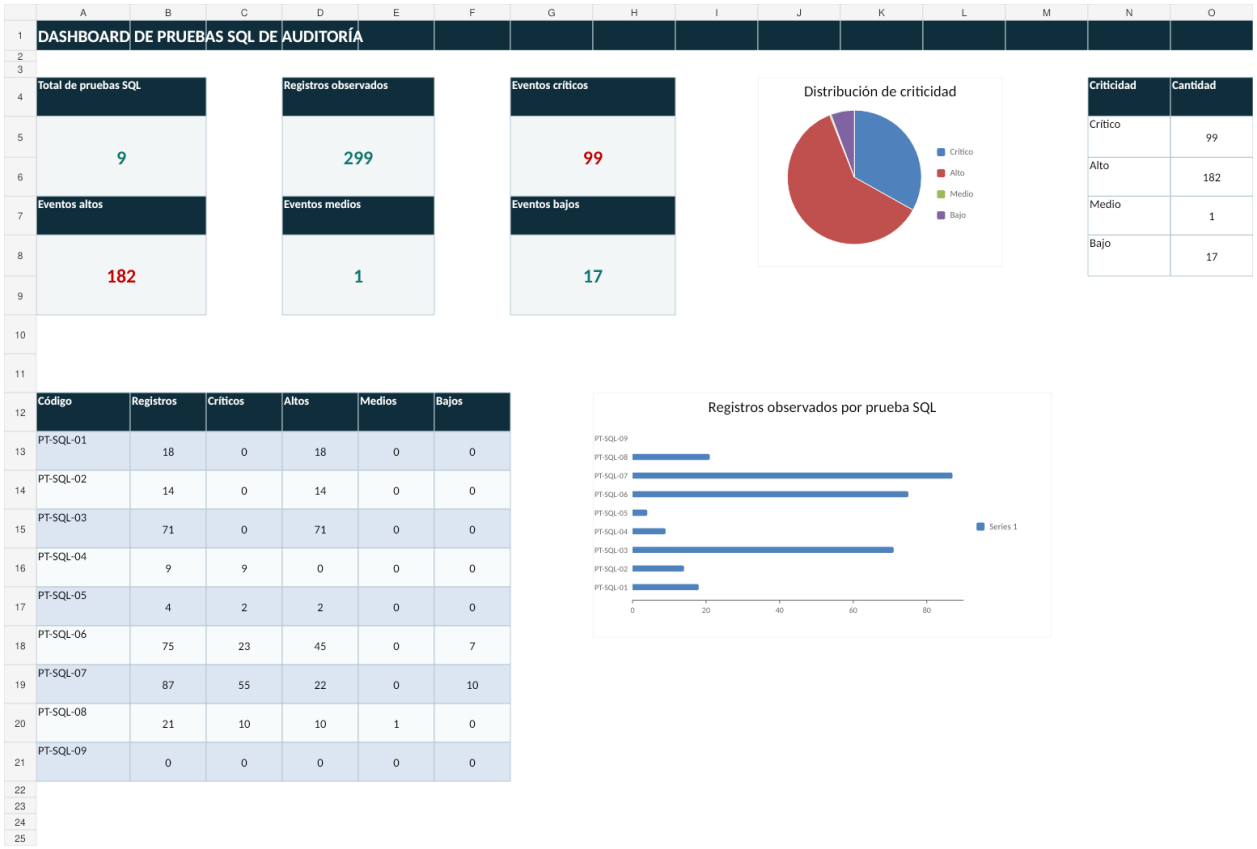
E-15. Extracto de Matriz de Evaluación de Impacto

Extracto del libro: MATRIZ DE EVALUACION DE IMPACTO EN LA PROTECCION DE DATOS.xlsx | Hoja: RAT

Columna A	Columna B	Columna C	Columna D
UNIDAD DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS			
MATRIZ DE REGISTRO DE TRATAMIENTO DE DATOS PERSONALES			
N°	Codigo	Macroproceso	Proceso
N°	Codigo	Macroproceso	Proceso
1	GTI-TI-AT-1	Gestión de Talento Humano	Talento Humano
2		Gestión de Operaciones	Atención socio / cliente
2	GTI-CC-RIRDC-01	Gestión de Negocios	Consesión de Crédito

Captura generada desde el archivo Excel entregado para el anexo de auditoría.

Anexo 16 Dashboard de pruebas SQL complementarias



DASHBOARD DE PRUEBAS SQL DE AUDITORÍA

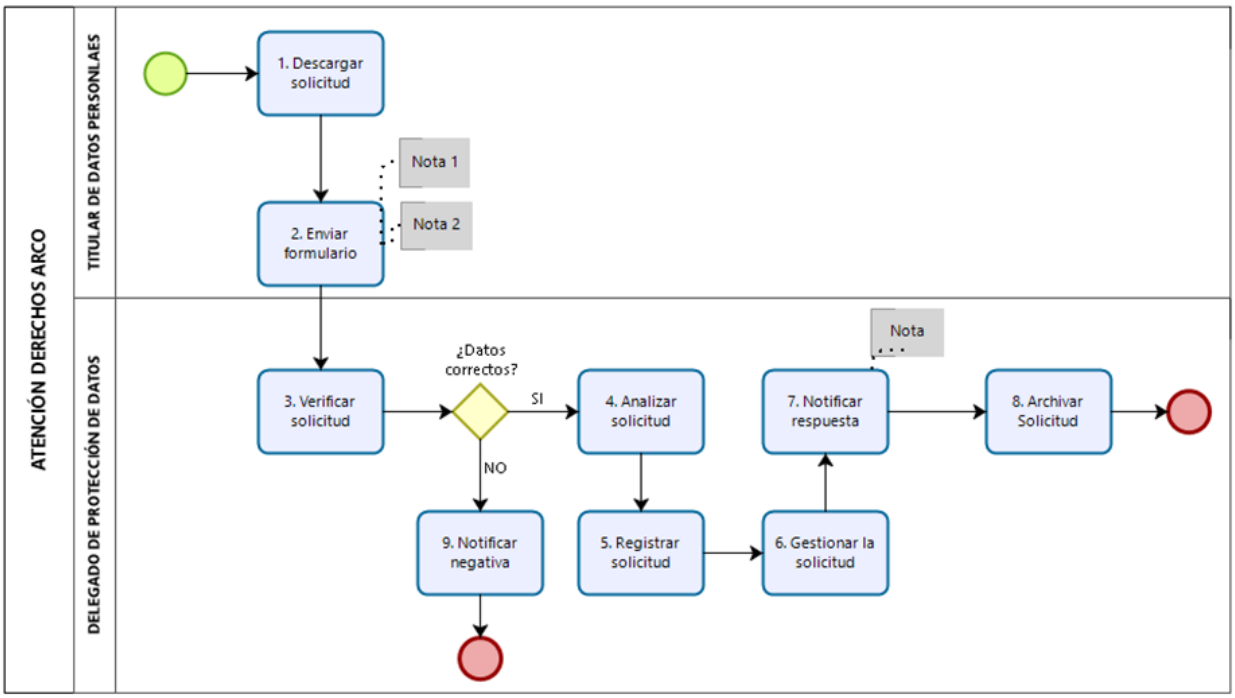
Total de pruebas SQL	Registros observados	Eventos críticos
9	299	99

Eventos altos	Eventos medios	Eventos bajos
182	1	17

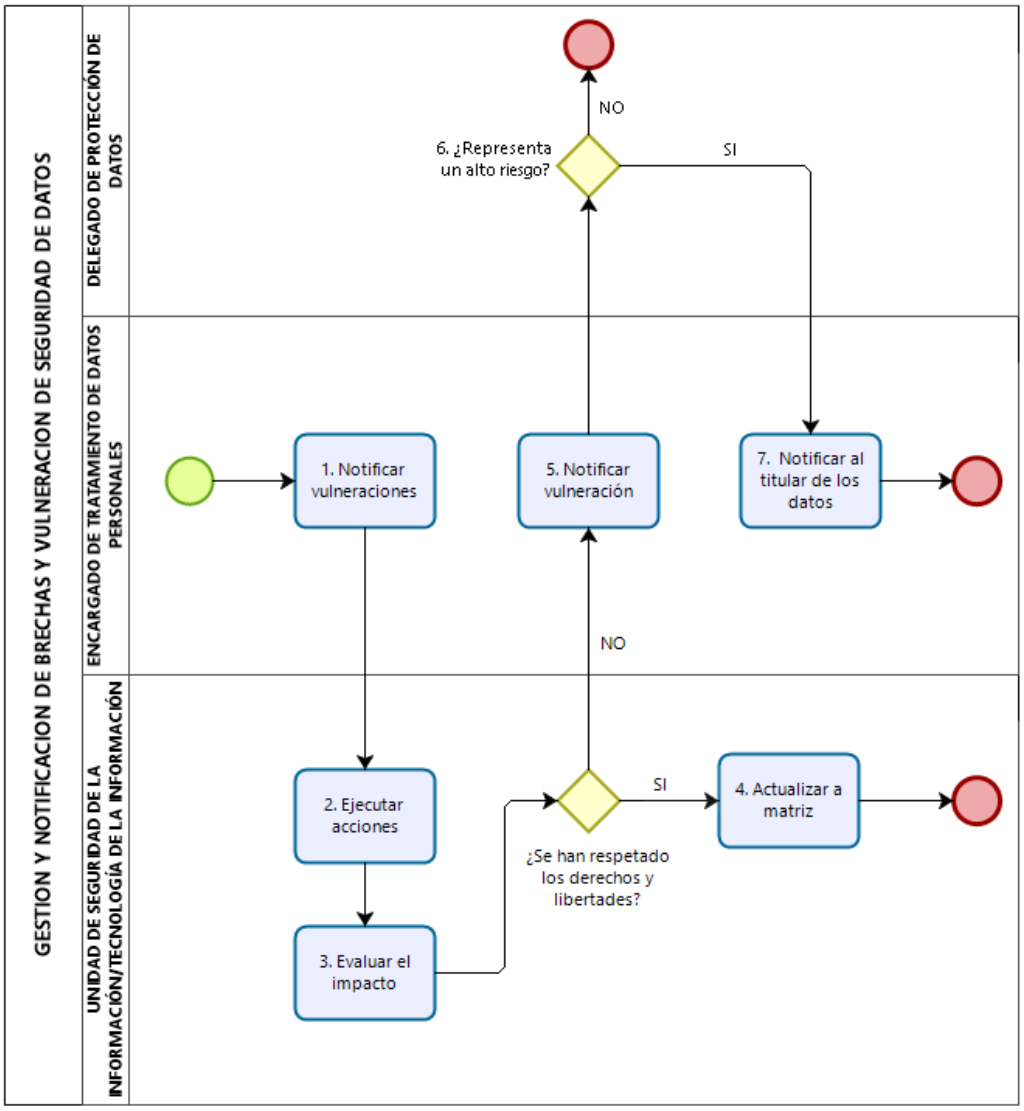
Criticidad	Cantidad
Crítico	99
Alto	182
Medio	1
Bajo	17

Código	Registros	Críticos	Altos	Medios	Bajos
PT-SQL-01	18	0	18	0	0
PT-SQL-02	14	0	14	0	0
PT-SQL-03	71	0	71	0	0
PT-SQL-04	9	9	0	0	0
PT-SQL-05	4	2	2	0	0
PT-SQL-06	75	23	45	0	7
PT-SQL-07	87	55	22	0	10
PT-SQL-08	21	10	10	1	0
PT-SQL-09	0	0	0	0	0

Anexo 17 Flujo BPMN de atención de derechos ARCO+



Anexo 18 Flujo BPMN de gestión y notificación de brechas



Anexo 19 Informe final de auditoría técnica entregado a la Cooperativa

COOPERATIVA DE AHORRO Y CRÉDITO CREDI YA LTDA.

INFORME FINAL DE AUDITORÍA TÉCNICA

Cumplimiento de la Ley Orgánica de Protección de Datos Personales en los sistemas de información asociados al core financiero Softbank

Campo	Detalle
Código del informe	INF-AUD-LOPDP-CCY-001-2026
Entidad auditada	Cooperativa de Ahorro y Crédito Credi Ya Ltda.
Sistema auditado	Core financiero Softbank y procesos institucionales vinculados al tratamiento de datos personales
Tipo de auditoría	Auditoría técnica de cumplimiento normativo, seguridad de la información y privacidad
Lugar y fecha	Ambato, mayo de 2026
Clasificación del documento	Uso interno / Confidencial

Elaborado para entrega a Gerencia General y Delegada de Protección de Datos Personales

Carta de entrega

Ambato, mayo de 2026

Señores
Cooperativa de Ahorro y Crédito Credi Ya Ltda.
Gerencia General y Delegada de Protección de Datos Personales
Presente.

Por medio del presente se entrega el informe final de auditoría técnica orientada a evaluar el cumplimiento de la Ley Orgánica de Protección de Datos Personales en los sistemas de información asociados al core financiero Softbank y en los procesos institucionales vinculados al tratamiento de datos personales.

El informe resume el alcance, criterios, metodología, pruebas ejecutadas, hallazgos, nivel de criticidad, plan de acción y dictamen técnico. La finalidad de este documento es proporcionar a la Cooperativa una visión ejecutiva y técnica sobre el estado de cumplimiento, así como una ruta de mejora priorizada para fortalecer la responsabilidad demostrada, la seguridad de la información y la protección efectiva de los derechos de los titulares.

La auditoría se desarrolló con enfoque de caja gris y se sustentó en documentación institucional autorizada, matrices, formularios, subprocesos, controles técnicos y pruebas de auditoría informática de solo lectura. No se ejecutaron pruebas intrusivas ni acciones que pudieran alterar datos productivos o afectar la disponibilidad del core financiero.

Atentamente,

_____

Elaborado por: Ezequiel Andrés Sánchez López
Fecha: 05/06/2026

Contenido

1. Resumen ejecutivo
2. Objetivo del informe
3. Alcance y limitaciones
4. Criterios de auditoría
5. Metodología aplicada
6. Resultados generales
7. Hallazgos de auditoría
8. Plan de acción priorizado
9. Indicadores de seguimiento
10. Dictamen técnico y conclusión
11. Firmas de entrega y recepción

1. Resumen ejecutivo

La auditoría técnica revisó el tratamiento de datos personales realizado en el core financiero Softbank y en los procesos institucionales relacionados con la protección de datos personales de la Cooperativa de Ahorro y Crédito Credi Ya Ltda. El análisis incluyó documentación institucional, formularios, procesos ARCO, gestión de brechas, matriz RAT, matriz EIPD, controles de seguridad de la información y pruebas SQL de auditoría informática.

El resultado general permite emitir una opinión de cumplimiento parcial. La Cooperativa cuenta con una base documental relevante para la gestión de protección de datos personales; sin embargo, los resultados técnicos evidencian que el cumplimiento debe reforzarse mediante controles operativos, recertificación de accesos, depuración de usuarios, trazabilidad, ejecución periódica de controles, actualización de matrices y cierre formal de hallazgos.

Los aspectos de mayor prioridad se concentran en control de accesos, segregación de funciones, trazabilidad de acciones sensibles, evaluación de impacto aplicada al core financiero, minimización de datos, retención y conservación, gestión de brechas, privilegios administrativos de base de datos y capacitación con evidencia de ejecución.

Tabla 1. Resumen ejecutivo de resultados

Indicador ejecutivo	Resultado
Opinión general	Cumplimiento parcial con necesidad de acciones correctivas prioritarias
Pruebas consideradas	22 pruebas: 13 documentales-operativas y 9 SQL complementarias
Hallazgos consolidados	10 hallazgos: 8 de criticidad alta y 2 de criticidad media
Fortaleza principal	Base documental institucional existente: política, manual, formularios, subprocesos y metodología de riesgos
Riesgo principal	Necesidad de fortalecer evidencia operativa, trazabilidad y control periódico de accesos
Prioridad inmediata	Depuración de usuarios, revisión de privilegios administrativos y recertificación RBAC/SoD

2. Objetivo del informe

2.1 Objetivo general

Presentar los resultados finales de la auditoría técnica de cumplimiento de la Ley Orgánica de Protección de Datos Personales en los sistemas de información asociados al core financiero Softbank de la Cooperativa de Ahorro y Crédito Credi Ya Ltda., identificando brechas, riesgos, hallazgos y acciones de mejora priorizadas.

2.2 Objetivos específicos

- Comunicar a la alta gerencia y a la Delegada de Protección de Datos Personales el estado general de cumplimiento técnico-normativo.
- Consolidar los resultados obtenidos a partir de la revisión documental, procesos institucionales y pruebas SQL complementarias.
- Priorizar los hallazgos que pueden afectar la confidencialidad, integridad, disponibilidad, trazabilidad y responsabilidad demostrada.
- Proponer un plan de acción verificable con responsables sugeridos, plazos, evidencias esperadas y prioridad de atención.

3. Alcance y limitaciones

El alcance de la auditoría comprende la revisión técnica, documental y normativa del tratamiento de datos personales en los módulos operativos del core financiero Softbank y en los procesos institucionales relacionados con protección de datos personales. Se consideraron procesos de recolección, consentimiento, derechos ARCO, revocatoria, registro de actividades de tratamiento, evaluación de riesgos e impacto, gestión de brechas, control de accesos, trazabilidad, minimización, retención, proveedores y capacitación.

Tabla 2. Alcance de la auditoría

Elemento	Descripción
Entidad auditada	Cooperativa de Ahorro y Crédito Credi Ya Ltda.
Sistema auditado	Core financiero Softbank y procesos institucionales vinculados al tratamiento de datos personales
Sede de análisis	Agencia matriz, Ambato
Tipo de auditoría	Auditoría técnica de cumplimiento normativo, seguridad de la información y privacidad

Unidades relacionadas	Gerencia General, Delegada de Protección de Datos, Tecnología, Seguridad de la Información, Operaciones, Talento Humano, Riesgos, Auditoría y áreas usuarias
Limitaciones	No se ejecutaron pruebas intrusivas, destructivas ni alteraciones sobre datos productivos. Las validaciones técnicas se orientaron a consultas de solo lectura y revisión de evidencia autorizada.

4. Criterios de auditoría

Los criterios de auditoría se agruparon en tres dimensiones: normativa legal, evidencia institucional y referencias técnicas. Esta combinación permitió transformar obligaciones legales en pruebas verificables y relacionarlas con controles de seguridad de la información y privacidad.

Tabla 3. Criterios aplicados

Criterio	Aplicación en la auditoría
LOPDP y Reglamento General	Principios, derechos ARCO, consentimiento, revocatoria, vulneraciones, evaluación de impacto, obligaciones del responsable y medidas técnicas u organizativas.
Documentación institucional	Política de protección de datos, manual institucional, formularios, subprocesos ARCO y brechas, matriz RAT, matriz EIPD y plan de capacitación.
ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701 y NIST	Gestión de seguridad, control de accesos, segregación de funciones, trazabilidad, incidentes, proveedores, continuidad y privacidad.
Pruebas SQL de auditoría informática	Validación de condiciones observables en base de datos: usuarios, roles, privilegios, logins, cuentas huérfanas, datos conservados y exposición de información.

5. Metodología aplicada

La metodología se estructuró bajo un enfoque de auditoría de caja gris. Se utilizó información institucional autorizada y se realizaron pruebas técnicas de solo lectura para contrastar los documentos con condiciones observables en el core financiero y su base de datos.

- Planificación del alcance, criterios normativos y criterios técnicos.
- Revisión de políticas, manuales, formularios, subprocesos, matriz RAT, matriz EIPD y plan de capacitación.

- Definición de pruebas documentales-operativas y pruebas SQL complementarias.
- Ejecución de pruebas sobre consentimiento, ARCO, brechas, EIPD, accesos, segregación de funciones, trazabilidad, estado de la técnica y proveedores.
- Consolidación de resultados, calificación, hallazgos, criticidad y recomendaciones.
- Formulación de plan de acción priorizado con evidencias esperadas y responsables sugeridos.

6. Resultados generales

La auditoría consideró 22 pruebas: 13 pruebas documentales-operativas y 9 pruebas SQL complementarias. La calificación diferencia entre cumplimiento, cumplimiento parcial, necesidad de acción correctiva, validación operativa pendiente y prueba pendiente de validación.

Tabla 4. Distribución de resultados por calificación

Estado	Cantidad	Interpretación
Cumple	1	Existe evidencia suficiente para reconocer cumplimiento del criterio revisado.
Cumple parcialmente	9	Existe evidencia documental o control inicial, pero se requiere fortalecer ejecución, trazabilidad o registro.
Requiere acción correctiva	10	La prueba evidenció una condición que requiere depuración, ajuste técnico, control adicional o cierre formal.
Requiere validación operativa	1	Existe criterio o documentación, pero falta validar logs reales, ejecución periódica o funcionamiento práctico.
Pendiente de validación	1	La prueba requiere verificación funcional adicional para confirmar autorización, finalidad y registro.

6.1 Resultados relevantes

- La Cooperativa dispone de política, manual, formularios, subprocesos, metodología de riesgos, plan de capacitación y matrices de protección de datos.
- El proceso ARCO y el proceso de gestión de brechas se encuentran documentados; el principal pendiente es probar su aplicación mediante casos, bitácoras, actas y métricas.

- Las pruebas SQL identificaron condiciones de riesgo en accesos, usuarios desvinculados, usuarios sin empleado asociado, privilegios administrativos, logins con políticas incompletas y registros conservados.
- El cumplimiento documental debe evolucionar hacia un cumplimiento demostrable, sustentado en evidencias técnicas periódicas, reportes de seguimiento y cierre formal de hallazgos.

7. Hallazgos de auditoría

Los hallazgos se presentan de forma consolidada para facilitar la toma de decisiones. La criticidad fue determinada según la afectación potencial a confidencialidad, integridad, disponibilidad, derechos del titular, trazabilidad y capacidad institucional de demostrar cumplimiento.

Tabla 5. Hallazgos consolidados

Código	Hallazgo	Criticidad	Condición observada	Recomendación
H-01	Trazabilidad técnica parcialmente demostrable	Alta	Se requiere validar logs reales del core, eventos críticos, retención e integridad de bitácoras.	Definir catálogo de eventos, centralizar logs y documentar revisiones periódicas.
H-02	Control de accesos requiere recertificación formal	Alta	Se observaron cuentas activas, usuarios sin empleado asociado y empleados desvinculados con accesos habilitados.	Cruzar usuarios con Talento Humano, bloquear cuentas no justificadas y ejecutar recertificación semestral.
H-03	Segregación de funciones con conflictos potenciales	Alta	Existen usuarios con participación simultánea en etapas o procesos potencialmente incompatibles.	Definir matriz SoD, bloquear combinaciones incompatibles y documentar excepciones.
H-04	Gestión de brechas documentada, pero no probada	Alta	Existe subproceso de brechas, pero falta evidencia de simulacros, tiempos, responsables y lecciones aprendidas.	Ejecutar tabletop anual, conservar actas y actualizar matriz de riesgos.

H-05	EIPD del core financiero requiere consolidación	Alta	La metodología existe, pero debe demostrarse su aplicación completa sobre tratamientos críticos del core.	Completar EIPD con riesgos, controles, riesgo residual, responsables y seguimiento.
H-06	Minimización y exposición de datos en reportes	Alta	Se observaron datos personales y financieros visibles; algunos formularios presentan finalidades amplias.	Crear matriz campo-finalidad-base legal y aplicar enmascaramiento o reducción de campos.
H-07	Retención y conservación requieren mayor control técnico	Alta	Se observaron registros de personas o clientes sin productos vigentes, pero con datos conservados.	Aprobar tabla de retención y definir bloqueo, depuración, anonimización o conservación justificada.
H-08	Privilegios administrativos y autenticación SQL deben reforzarse	Alta	Se observaron usuarios con rol administrativo elevado y logins con políticas incompletas.	Revisar db_owner, justificar cuentas técnicas, aplicar mínimo privilegio y fortalecer políticas de contraseña.
H-09	Proveedores y encargados requieren evaluación periódica	Media	Falta mantener inventario actualizado de encargados, accesos de soporte y evaluación de garantías técnicas.	Actualizar inventario, contratos, confidencialidad, SLA de incidentes y accesos de soporte.
H-10	Capacitación requiere evidencia de ejecución	Media	Existe plan de capacitación, pero se requiere demostrar cobertura mediante listas, evaluaciones y material aplicado.	Ejecutar plan anual, registrar asistencia, evaluar comprensión y medir cobertura por rol.

8. Plan de acción priorizado

El plan de acción se ordena según criticidad, facilidad de verificación y urgencia operativa. Cada actividad debe cerrarse con evidencia formal: actas, matrices actualizadas, registros de logs, reportes, aprobaciones, bitácoras o resultados de pruebas.

Tabla 6. Plan de acción priorizado

N.º	Acción	Responsable sugerido	Plazo	Evidencia esperada	Prioridad
1	Depurar usuarios de empleados desvinculados, cuentas sin empleado asociado y accesos no justificados.	TI / Talento Humano / Jefaturas	30 días	Acta de bloqueo, matriz de usuarios depurada y aprobación de jefaturas.	Alta
2	Revisar usuarios db_owner y logins SQL con política incompleta.	TI / Seguridad de la Información	45 días	Cédula de privilegios DB, reporte de endurecimiento y justificación de cuentas técnicas.	Alta
3	Ejecutar recertificación RBAC/SoD del core y del flujo de crédito.	TI / Operaciones / Crédito / Talento Humano	Semestral	Matriz de roles, incompatibilidades, excepciones y usuarios recertificados.	Alta
4	Centralizar eventos críticos del core y definir catálogo de logs auditables.	TI / Seguridad / Auditoría Informática	120 días	Catálogo de eventos, reportes mensuales, política de retención y evidencia de revisión.	Alta
5	Realizar ejercicio de validación de brecha de datos personales.	DPD / Seguridad / TI / Operaciones	60 días	Acta de ejercicio, matriz de severidad, tiempos, responsables y lecciones aprendidas.	Alta
6	Completar la EIPD aplicada al core financiero.	DPD / Riesgos / TI / Seguridad	90 días	Informe EIPD, matriz de riesgos, controles, riesgo residual y plan de tratamiento.	Alta
7	Construir matriz campo-finalidad-base legal para formularios, reportes y exportaciones.	DPD / Legal / TI / Áreas propietarias	90 días	Matriz de minimización, reportes ajustados y criterios de enmascaramiento.	Alta
8	Formalizar tabla de retención, bloqueo, anonimización y eliminación segura.	DPD / Legal / TI / Archivo	120 días	Tabla de retención, procedimiento de borrado y actas de eliminación o bloqueo.	Alta

9	Validar exportación masiva con permisos, finalidad y evento de log.	TI / Auditoría Informática	60 días	Cédula de exportación, autorización y registro en bitácora.	Alta
10	Actualizar inventario de encargados y proveedores críticos.	Legal / Compras / TI / DPD	Semestral	Inventario, contratos, acuerdos de confidencialidad, evaluación y SLA de incidentes.	Media
11	Ejecutar plan anual de capacitación y concienciación.	Talento Humano / DPD / Seguridad	Anual	Material, listas de asistencia, evaluaciones y métricas de cobertura.	Media
12	Actualizar matriz de seguimiento LOPDP/ISO/NIST con resultados SQL.	DPD / Auditoría / Seguridad	Trimestral	Matriz con artículo/control, evidencia, responsable, estado y acción correctiva.	Media

9. Indicadores de seguimiento

Para asegurar que los hallazgos sean cerrados y no queden únicamente como recomendaciones, se proponen indicadores mínimos de seguimiento. Estos indicadores deben revisarse por lo menos de forma trimestral y documentarse en la matriz de seguimiento LOPDP/ISO/NIST.

Tabla 7. Indicadores de seguimiento propuestos

Indicador	Fórmula sugerida	Frecuencia	Responsable sugerido
Recertificación de usuarios	Usuarios recertificados / usuarios activos del core x 100	Semestral	TI / Talento Humano
Cuentas depuradas	Cuentas bloqueadas o regularizadas / cuentas observadas x 100	Mensual hasta cierre	TI
Cobertura de capacitación	Personas capacitadas / personas convocadas x 100	Trimestral / anual	Talento Humano / DPD
Revisión de logs críticos	Reportes de revisión emitidos / reportes planificados x 100	Mensual	Seguridad / TI

Avance de EIPD del core	Actividades EIPD completadas / actividades planificadas x 100	Mensual hasta cierre	DPD / Riesgos
Cierre de hallazgos	Hallazgos cerrados con evidencia / hallazgos totales x 100	Trimestral	DPD / Auditoría
Evaluación de proveedores	Proveedores críticos evaluados / proveedores críticos identificados x 100	Semestral	Legal / Compras / TI

10. Dictamen técnico y conclusión

10.1 Dictamen técnico

Con base en la evidencia revisada, se determina que la Cooperativa de Ahorro y Crédito Credi Ya Ltda. presenta un cumplimiento parcial frente a la Ley Orgánica de Protección de Datos Personales en los procesos asociados al core financiero Softbank. La institución cuenta con una estructura documental válida para iniciar y sostener la gestión de protección de datos personales; sin embargo, todavía debe fortalecer la evidencia operativa que demuestre que los controles funcionan de manera continua.

La opinión de cumplimiento parcial se sustenta en la existencia de políticas, manuales, formularios, subprocesos, metodología de riesgos, plan de capacitación y matrices; así como en la identificación de brechas técnicas relacionadas con accesos, segregación de funciones, trazabilidad, privilegios administrativos, retención, exposición de datos y ejecución periódica de controles.

10.2 Conclusión final

La Cooperativa no parte de cero en materia de protección de datos personales. Existe una base documental importante y un marco institucional que puede sostener un sistema de cumplimiento. No obstante, el mayor reto se encuentra en pasar de un cumplimiento principalmente documental a un cumplimiento demostrable, medible y sostenido mediante evidencias técnicas, bitácoras, reportes, recertificaciones y cierre formal de hallazgos.

Se recomienda atender de manera prioritaria los hallazgos de criticidad alta, especialmente aquellos relacionados con control de accesos, usuarios desvinculados, usuarios sin empleado asociado, privilegios administrativos, segregación de funciones, trazabilidad de eventos críticos, EIPD aplicada al core y minimización de datos en

reportes. El seguimiento de estas acciones permitirá reducir la exposición legal, operativa, tecnológica y reputacional de la Cooperativa.

El presente informe queda emitido para conocimiento de la alta gerencia, la Delegada de Protección de Datos Personales y las áreas responsables de implementar las acciones correctivas y preventivas correspondientes.

11. Firmas de entrega y recepción

Para constancia de la entrega del informe final de auditoría técnica, se registran las siguientes firmas:

Elaborado por	Recibido por
Nombre: Ezequiel Andrés Sánchez López	Nombre: Carmen Rocio Yanez Condor
Cargo: Tesistas	Cargo: Gerente Subrogante
Firma: Validar únicamente en FirmaEC. Firmado electrónicamente por: EZEQUIEL ANDRES SANCHEZ LOPEZ	Firma: Validar únicamente en FirmaEC. Firmado electrónicamente por: CARMEN ROCIO YANEZ CONDOR

Fecha de entrega: 05 / 06 / 2026