

UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

FACULTAD DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

PLAN DE CONTINUIDAD DE NEGOCIO PARA LOS SERVICIOS DIGITALES DE COAC YUYAY LTDA BASADO EN LA NORMA ISO 22301:2019

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

AUTOR: STEVE GEOVANNY DEFAS LUDIZACA

DIRECTORA: ING. FERNANDA MICHAELLE NARVÁEZ OCHOA

CAÑAR – ECUADOR

2026

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

FACULTAD DE INFORMATICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

PLAN DE CONTINUIDAD DE NEGOCIO PARA LOS SERVICIOS DIGITALES DE COAC YUYAY LTDA BASADO EN LA NORMA ISO 22301:2019

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

AUTOR: STEVE GEOVANNY DEFAS LUDIZACA

DIRECTORA: ING. FERNANDA MICHAELLE NARVÁEZ OCHOA

CAÑAR – ECUADOR

2026

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Steve Geovanny Defas Ludizaca, portador de la cédula de ciudadanía N.° 0302488846. Declaro ser el autor de la obra: "**Plan de Continuidad de negocio para los servicios digitales de COAC Yuyay Ltda basado en la norma ISO 22301:2019**" sobre la cual me hago responsable de las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cañar, 29 de octubre de 2026

F: .....

Steve Geovanny Defas Ludizaca
C.I. 0302488846

CERTIFICADO DEL TUTOR

Certifico que el presente trabajo denominado "**Plan de Continuidad de negocio para los servicios digitales de COAC Yuyay Ltda basado en la norma ISO 22301:2019** realizado por **Steve Geovanny Defas Ludizaca** con documento de identidad No.0302488846, previo a la obtención del título profesional de Ingeniero en Sistemas de Información, ha sido asesorado, supervisado y desarrollado bajo mi tutoría en todo su proceso, cumpliendo con la reglamentación pertinente que exige la Universidad Católica de Cuenca y los requisitos que determina la investigación científica.

Cañar, 29 de octubre 2026

Ing. Fernanda Michaelle Narváez Ochoa

DIRECTORA DEL TRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA EXTENSIÓN CAÑAR

DEDICATORIA

Dedico este trabajo, en primer lugar, a Dios, por brindarme la fortaleza, sabiduría y perseverancia necesarias para continuar avanzando a lo largo de mi formación académica y superar cada uno de los desafíos que se presentaron durante este proceso.

A mi familia, por ser un pilar fundamental en mi vida, por su apoyo incondicional, comprensión y confianza en cada etapa de este camino. Su esfuerzo, palabras de ánimo y acompañamiento han sido esenciales para alcanzar esta meta.

A mi novia, por su cariño, paciencia, comprensión y apoyo constante, especialmente en los momentos de mayor dificultad. Gracias por acompañarme durante este proceso, motivarme a seguir adelante y estar presente mientras trabajaba por alcanzar este objetivo.

A mi jefa de trabajo, por la confianza, comprensión y apoyo brindados durante el desarrollo de mi formación profesional, permitiéndome continuar creciendo tanto en el ámbito laboral como académico.

Steve Geovanny Defas Ludizaca

AGRADECIMIENTO

Agradezco a Dios por permitirme culminar esta etapa de formación académica y por brindarme la fortaleza necesaria para afrontar cada uno de los retos que surgieron durante el desarrollo de mi carrera universitaria.

A mi familia, por su apoyo constante, paciencia y confianza, quienes han sido una motivación fundamental para continuar esforzándome y alcanzar mis objetivos personales y profesionales.

De manera especial, agradezco a mi novia por acompañarme durante este proceso, por su paciencia, comprensión, cariño y por cada palabra de aliento en los momentos de cansancio y dificultad. Su apoyo ha sido muy importante para mantenerme enfocado y continuar hasta alcanzar esta meta.

También expreso mi agradecimiento a mi jefa de trabajo, por su confianza, consideración y apoyo durante este proceso académico, por comprender las responsabilidades que implicó el desarrollo de este trabajo de titulación y por contribuir a mi crecimiento profesional mediante las experiencias y oportunidades brindadas en el ámbito laboral.

A la Universidad Católica de Cuenca, a la Unidad Académica de Informática, Ciencias de la Computación e Innovación Tecnológica y a sus docentes, por los conocimientos, experiencias y orientación proporcionados durante mi formación profesional.

De manera particular, agradezco a mi director de trabajo de titulación, Mishel Narváez, por su orientación, tiempo y acompañamiento durante el desarrollo de la presente investigación.

Asimismo, agradezco a la Cooperativa de Ahorro y Crédito “Yuyay” Ltda. por facilitar el espacio y la información necesaria para el desarrollo del proyecto, permitiéndome aplicar los conocimientos adquiridos durante mi formación académica dentro de un contexto institucional real.

RESUMEN

La creciente dependencia de la tecnología digital en las corporaciones financieras ha generado una mayor necesidad de que las empresas cuenten con instrumentos para gestionar y restablecer las operaciones en caso de fallas tecnológicas, ciberataques, errores humanos, cortes de energía y otros eventos disruptivos. El propósito de esta investigación es crear un plan de continuidad del negocio para los servicios digitales de Cooperativa de Ahorro y Crédito "Yuyay" Ltda. utilizando el marco proporcionado por la norma ISO 22301:2019. La investigación se lleva a cabo mediante un método de investigación mixto, descriptivo y aplicado que utiliza análisis cualitativos de los procesos internos y capacidades de continuidad, así como una evaluación cuantitativa de vulnerabilidades. La investigación consiste en recopilar información institucional, identificar los procesos y tecnologías que se utilizan, realizar un análisis de impacto en el negocio, analizar riesgos y definir parámetros de restauración como MTPD, RTO y RPO. Con base en la información obtenida durante la investigación, se elegirán las prioridades de restauración y se desarrollarán las acciones de continuidad del negocio. La investigación se centra en el desarrollo de un plan de continuidad del negocio con directrices para la planificación de contingencias, la restauración y la mejora continua durante la implementación.

La investigación no incluirá la implementación completa de las estrategias proporcionadas ni la certificación de la organización según la norma ISO 22301: 2019.

Palabras clave: continuidad del negocio, ISO 22301, servicios digitales, análisis de impacto al negocio, gestión de riesgos.

ABSTRACT

The growing reliance on digital technology in financial institutions has increased the need for tools to manage and restore operations during technology failures, cyberattacks, human error, power outages, and other disruptive events. The purpose of this research is to develop a business continuity plan for the digital services of Cooperativa de Ahorro y Crédito "Yuyay" Ltda. using the framework provided by the ISO 22301:2019 standard. The research is conducted using a mixed-methods approach, descriptive and applied, which employs qualitative analyses of internal processes and business continuity capabilities, as well as a quantitative assessment of vulnerabilities. The investigation involves gathering institutional information, identifying the processes and technologies in use, conducting a business impact analysis, analyzing risks, and defining recovery parameters such as Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO). Based on the information obtained during the investigation, recovery priorities will be selected, and business continuity measures will be developed. The research focuses on developing a business continuity plan that includes guidelines for contingency planning, recovery, and continuous improvement during implementation. The research will not include the full implementation of the strategies provided or the organization's certification under the ISO 22301:2019 standard.

Keywords: business continuity, ISO 22301, digital services, business impact analysis, risk management.

ÍNDICE

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD I
CERTIFICADO DEL TUTOR II
DEDICATORIA III
AGRADECIMIENTO IV
RESUMEN V
ABSTRACT VI
ÍNDICE VII
ÍNDICE DE TABLAS XII
ÍNDICE DE ILUSTRACIONES XIV
INTRODUCCIÓN XV
CAPÍTULO I 1
1.1. Planteamiento del problema 1
1.1.1. Formulación del problema 2
1.2. Antecedentes de la investigación 3
1.3. Justificación de la investigación 4
1.4. Objetivos 6
1.4.1. Objetivo general 6
1.4.2. Objetivos específicos 6
1.5. Limitaciones 6
1.6. Delimitaciones 6
CAPÍTULO II 8
2. MARCO TEÓRICO 8
2.1. Sistemas de información y servicios digitales en el sector financiero cooperativo 8
2.1.1. Sistemas de información: concepto, componentes y dependencia organizacional 8
2.1.2. Servicios digitales financieros y canales electrónicos 9
2.1.3. Las cooperativas de ahorro y crédito en Ecuador: el sector financiero popular y solidario y la SEPS 10
2.1.4. Marco regulatorio aplicable: riesgo operativo, continuidad del negocio y protección de datos personales 11
2.2. Interrupciones y riesgos tecnológicos en los servicios digitales 13
2.2.1. Evento disruptivo, incidente e interrupción: definiciones normativas 13

2.2.2. Activos, amenazas y vulnerabilidades en infraestructuras de TI 14
2.2.3. El proceso de gestión del riesgo: identificación, análisis, evaluación y tratamiento; riesgo inherente y residual 16
2.2.4. Valoración del riesgo: escalas de probabilidad e impacto y matriz de riesgo 17
2.2.5. MAGERIT como técnica de análisis de riesgos de sistemas de información 19
2.3. Continuidad del negocio y resiliencia organizacional 20
2.3.1. Continuidad del negocio, resiliencia operativa y resiliencia organizacional: diferencias y relación 20
2.3.2. Sistema de Gestión de Continuidad del Negocio (SGCN) y Plan de Continuidad del Negocio (BCP) 22
2.3.3. Continuidad de los servicios TIC: preparación de las TIC para la continuidad 23
2.4. Análisis de Impacto al Negocio (BIA) 24
2.4.1. Finalidad y proceso del BIA según ISO/TS 22317:2021 24
2.4.2. Identificación de actividades prioritarias, recursos y dependencias 25
2.4.3. Tipos de impacto y su evolución en el tiempo 25
2.4.4. Parámetros de recuperación: MTPD, RTO, RPO y MBCO 26
2.4.5. Relación entre el BIA y la evaluación de riesgos en la definición de prioridades 27
2.5. Estrategias de continuidad, respuesta y recuperación 28
2.5.1. Selección de estrategias y soluciones de continuidad 28
2.5.2. Estructura de respuesta a incidentes, escalamiento y comunicación 29
2.5.3. Recuperación tecnológica: Plan de Recuperación ante Desastres (DRP) y su relación con el BCP 30
2.5.4. Respaldo, integridad y seguridad de la información durante la contingencia 31
2.5.5. Pruebas, ejercicios y mantenimiento del plan 31
2.6. La norma ISO 22301:2019 32
2.6.1. Alcance, propósito y vigencia 32
2.6.2. Estructura de alto nivel: cláusulas 4 a 10 33
2.6.3. Ciclo Planificar-Hacer-Verificar-Actuar en el SGCN 34
2.6.4. Requisitos operativos (cláusula 8) como columna vertebral del plan 35
2.7. Marcos complementarios y justificación metodológica 36
2.7.1. Cuadro comparativo de marcos de continuidad 36
2.7.2. Integración de ISO 22301 con MAGERIT 37

2.7.3. Aplicaciones de ISO 22301 y de la continuidad del negocio en instituciones ecuatorianas 38
2.8. Síntesis del capítulo 39
CAPÍTULO III 40
3. MARCO METODOLÓGICO 40
3.1. Enfoque de la investigación 40
3.2. Nivel y tipo de la investigación 41
3.3. Población y muestra 42
3.4. Técnicas e instrumentos de recolección de información 43
3.5. Tratamiento de la información 45
3.6. Resultados de la entrevista y de la revisión documental 47
3.6.1. Aplicación de los instrumentos 47
3.6.2. Contexto institucional y servicios digitales 48
3.6.3. Dependencias tecnológicas y proveedores 49
3.6.4. Historial de interrupciones 51
3.6.5. Controles de continuidad existentes 52
3.6.6. Respuesta a incidentes y comunicación 53
3.6.7. Tolerancia a la interrupción 54
3.6.8. Gobernanza, recursos y cultura 55
3.6.9. Resultados de las fichas de análisis de impacto 57
3.7. Análisis e interpretación de los resultados 59
3.7.1. Activos tecnológicos y su criticidad 59
3.7.2. Riesgos que afectan la continuidad 61
3.7.4. Situación frente a los requisitos de ISO 22301:2019 63
3.7.5. Síntesis de hallazgos e implicaciones para la propuesta 65
3.8. Fases de la metodología 66
CAPÍTULO IV 69
4. PROPUESTA 69
4.1. Título de la propuesta 69
4.2. Presentación 69
4.3. Objetivos de la propuesta 70
4.3.1. Objetivo general 70

4.3.2. Objetivos específicos....70
4.4. Justificación....70
4.5. Alcance y estructura de la propuesta....71
4.6. Fase 2: Contexto de la organización y alcance del plan....72
4.6.1. Caracterización de la organización....72
4.6.2. Partes interesadas y sus requisitos....74
4.6.3. Requisitos legales y regulatorios....74
4.6.4. Alcance del plan....75
4.7. Fase 3: Política, roles y responsabilidades....76
4.7.1. Política de continuidad del negocio....76
4.7.2. Objetivos de continuidad....77
4.7.3. Estructura de respuesta....77
4.7.4. Competencias, concienciación y documentación....81
4.8. Fase 4: Inventario y valoración de activos....81
4.8.1. Activos de soporte de los servicios digitales....81
4.8.2. Dependencias entre servicios y activos....83
4.9. Fase 5: Evaluación de riesgos....84
4.9.1. Criterios de valoración y de aceptación....84
4.9.2. Escenarios de interrupción....84
4.9.3. Valoración del riesgo inherente y residual....86
4.9.4. Plan de tratamiento de los riesgos....87
4.10. Fase 6: Análisis de impacto al negocio....89
4.10.1. Evolución del impacto y período máximo tolerable....89
4.10.2. Brechas entre los parámetros requeridos y la capacidad actual....90
4.10.3. Prioridades y secuencia de recuperación....92
4.11. Fase 7: Estrategias y soluciones de continuidad....93
4.11.1. Criterios de selección....93
4.11.2. Evaluación de alternativas para los servicios críticos....94
4.11.3. Estrategias seleccionadas....95
4.11.4. Hoja de ruta de implementación....96
4.12. Fase 8: Planes, ejercicios y mantenimiento....98
4.12.1. Niveles de activación....98

4.12.2. Procedimiento de activación y escalamiento 99
4.12.3. Plan de comunicación 100
4.12.4. Procedimientos de recuperación por escenario 102
4.12.5. Procedimientos de operación degradada 106
4.12.6. Retorno a la normalidad y cierre 107
4.12.7. Programa de ejercicios y pruebas 107
4.12.8. Evaluación del desempeño 108
4.12.9. Mantenimiento, revisión y mejora del plan 110
4.13. Correspondencia de la propuesta con los hallazgos del diagnóstico 111
Conclusiones 112
Recomendaciones 115
Referencias 117
Anexos 121
Anexo A: Guion de entrevista semiestructurada 138
Anexo B: Ficha de análisis de impacto al negocio (BIA) por servicio digital 145
Anexo C: Plan de Continuidad de Negocio para los servicios digitales de la COAC Yuyay Ltda. 1
Anexo D: Anteproyecto del trabajo de titulación 121

ÍNDICE DE TABLAS

Tabla 1 Familias de amenazas sobre activos de TI según MAGERIT y ejemplos aplicables a servicios digitales financieros 15
Tabla 2 Escala de probabilidad de ocurrencia 17
Tabla 3 Escala de impacto de una interrupción sobre los servicios digitales 17
Tabla 4 Pasos del análisis de riesgos según MAGERIT y su aplicación al diagnóstico de servicios digitales 20
Tabla 5 Cláusulas de requisitos de ISO 22301:2019 y su reflejo en el diseño de un plan de continuidad 33
Tabla 6 Comparación de marcos de referencia para la continuidad del negocio 36
Tabla 7 Población y muestra de la investigación 42
Tabla 8 Técnicas, instrumentos y fuentes de información 43
Tabla 9 Documentos institucionales analizados 44
Tabla 10 Categorías de análisis y criterios de tratamiento 45
Tabla 11 Informantes entrevistados 47
Tabla 12 Parámetros de recuperación por servicio digital 57
Tabla 13 Activos de soporte de los servicios digitales y su valoración de disponibilidad 60
Tabla 14 Riesgos identificados por ámbito y nivel 61
Tabla 15 Situación de la cooperativa frente a los requisitos de ISO 22301:2019 63
Tabla 16 Hallazgos del diagnóstico y fase de la propuesta que los atiende 65
Tabla 17 Fases de la metodología 67
Tabla 18 Componentes del Plan de Continuidad del Negocio 72
Tabla 19 Partes interesadas y requisitos para el plan de continuidad 74
Tabla 20 Requisitos legales y regulatorios aplicables al plan 74
Tabla 21 Alcance del Plan de Continuidad del Negocio 75
Tabla 22 Objetivos de continuidad del negocio 77
Tabla 23 Roles, titulares y suplentes del plan de continuidad 79
Tabla 24 Matriz RACI del plan de continuidad 80
Tabla 25 Activos de soporte de los servicios digitales valorados por dimensiones 81
Tabla 26 Matriz de dependencias entre servicios digitales y activos críticos 83
Tabla 27 Escenarios de interrupción de los servicios digitales 84
Tabla 28 Valoración del riesgo inherente y del riesgo residual actual de los escenarios (antes del plan) 86
Tabla 29 Plan de tratamiento y riesgo residual objetivo 87
Tabla 30 Impacto máximo según la duración de la interrupción 89
Tabla 31 Brecha entre los parámetros de recuperación requeridos y la capacidad actual 90
Tabla 32 Secuencia de recuperación y recursos mínimos por servicio 92
Tabla 33 Evaluación de alternativas para los recursos críticos 94
Tabla 34 Estrategias y soluciones de continuidad seleccionadas 95
Tabla 35 Hoja de ruta de implementación de las estrategias 96
Tabla 36 Niveles de activación del plan de continuidad 98
Tabla 37 Plan de comunicación durante una interrupción 100
Tabla 38 Mensajes predefinidos para los socios y el personal 101

Tabla 39 Procedimiento PR-01: interrupción del enlace de Internet (SD-07; RTO 4 h; objetivo técnico 2 h)..... 102
Tabla 40 Procedimiento PR-02: indisponibilidad del core financiero o de su base de datos (SD-01; RTO 4 h; RPO 1 h)..... 103
Tabla 41 Procedimiento PR-03: pérdida o corrupción de datos, incluido ransomware (SD-01 a SD-06)..... 104
Tabla 42 Procedimiento PR-04: indisponibilidad de la red de tarjetas (SD-05; RTO 4 h)..... 104
Tabla 43 Procedimiento PR-05: falla de un cajero automático (SD-04; RTO 8 h)..... 105
Tabla 44 Procedimiento PR-06: siniestro en el centro de datos o corte prolongado de energía..... 105
Tabla 45 Procedimientos de operación degradada..... 106
Tabla 46 Programa de ejercicios y pruebas del primer año..... 107
Tabla 47 Indicadores de desempeño del plan de continuidad..... 109
Tabla 48 Correspondencia entre los hallazgos del diagnóstico y los componentes del plan..... 111

ÍNDICE DE ILUSTRACIONES

Ilustración 1 Capas que componen un servicio digital financiero y relación de dependencia entre ellas 10
Ilustración 2 Matriz de nivel de riesgo (probabilidad × impacto) y zonas de tratamiento 19
Ilustración 3 Relación temporal entre RPO, RTO y MTPD ante una interrupción 26
Ilustración 4 Ciclo Planificar-Hacer-Verificar-Actuar y cláusulas de ISO 22301:2019 34
Ilustración 5 Distribución de los activos tecnológicos por categoría MAGERIT 59
Ilustración 6 Riesgos identificados por ámbito y nivel 61
Ilustración 7 Secuencia de las fases de la metodología 67
Ilustración 8 Estructura organizacional de la COAC Yuyay Ltda. 73
Ilustración 9 Estructura de respuesta del plan de continuidad 78
Ilustración 10 Ubicación de los escenarios en la matriz de riesgo: situación actual y objetivo 88
Ilustración 11 Evolución del impacto en el tiempo por perfil de servicio 90
Ilustración 12 RTO requerido, MTPD y capacidad actual de recuperación por servicio 91
Ilustración 13 Cronograma de implementación de las estrategias en los primeros 12 meses 97
Ilustración 14 Flujo de activación y escalamiento del plan 99

INTRODUCCIÓN

La dependencia de las instituciones financieras respecto de sus servicios digitales ha convertido la continuidad de dichos servicios en una condición de operación y en una exigencia regulatoria. Las cooperativas de ahorro y crédito del sector financiero popular y solidario ecuatoriano no son ajenas a esta realidad: sus canales electrónicos sostienen la atención a los socios y dependen de una infraestructura tecnológica expuesta a fallas, ataques, errores humanos y eventos externos. El presente trabajo de titulación desarrolla un Plan de Continuidad del Negocio para los servicios digitales de la Cooperativa de Ahorro y Crédito Yuyay Ltda., tomando como referencia los lineamientos de la norma ISO 22301:2019.

El documento se organiza en cuatro capítulos. El Capítulo I presenta el marco referencial: el planteamiento y la formulación del problema, los antecedentes, la justificación, los objetivos y las limitaciones y delimitaciones del estudio. El Capítulo II desarrolla el marco teórico, que fundamenta conceptualmente los sistemas de información y servicios digitales financieros, las interrupciones y riesgos tecnológicos, la continuidad del negocio y la resiliencia organizacional, el análisis de impacto al negocio, las estrategias de respuesta y recuperación, la norma ISO 22301:2019 y los marcos complementarios. El Capítulo III describe el marco metodológico y los resultados del diagnóstico de la cooperativa, y el Capítulo IV presenta la propuesta del plan de continuidad. Finalmente se exponen las conclusiones, las recomendaciones, las referencias y los anexos.

CAPÍTULO I

1.1. Planteamiento del problema

La proliferación de los servicios digitales impulsados por las instituciones financieras ha llevado implícito un aumento en la necesidad de disponer de infraestructura tecnológica adecuada que respalde los procesos institucionales a fin de lograr la continuidad operativa y la atención efectiva a socios y clientes (Gomber et al., 2018). En este contexto, las cooperativas de ahorro y crédito deben enfrentarse a distintos riesgos por falla tecnológica, ataques cibernéticos, errores humanos, fallos eléctricos y catástrofes naturales que pueden comprometer la disponibilidad, integridad y confidencialidad de la información institucional. La necesidad de un Plan de Continuidad de Negocio disminuye el impacto de dichos incidentes, mitigando problemas como, por ejemplo, la pérdida de operatividad de los servicios digitales, pérdida económica, efectos reputacionales y la disminución de la confianza de los usuarios (Buzzao & Rizzi, 2023).

La Cooperativa de Ahorro y Crédito “Yuyay” Ltda. (COAC Yuyay) no escapa ante esta realidad ya que sus procesos operativos y servicios digitales dependen de la infraestructura tecnológica para poder ejecutar actividades administrativas y financieras y, por lo tanto, se necesita establecer mecanismos y estrategias que permitan asegurar la continuidad de los servicios críticos ante posibles situaciones inesperadas que puedan afectar el desarrollo normal de las actividades. La norma ISO 22301:2019 establece una serie de lineamientos reconocidos a nivel internacional para ayudar a las organizaciones en el diseño e implementación de mecanismos que permitan mantener el funcionamiento de sus procesos esenciales, favoreciendo una mejor capacidad de respuesta y adaptación ante distintos escenarios (International Organization for Standardization [ISO], 2019).

Del mismo modo, dos investigaciones recientes enfatizan la necesidad de implementar modelos de continuidad del negocio bajo la norma ISO 22301, con el propósito de reducir

las consecuencias de los incidentes tecnológicos y de mejorar el nivel de la capacidad de respuesta organizativa de las entidades financieras y empresariales (Becerra Acevedo et al., 2021; Quituisaca-León et al., 2021). Atendiendo al precedente problema, aparece la necesidad de llevar a cabo un análisis sobre la posibilidad de que un Plan de Continuidad de Negocio contribuya a fortalecer el mantenimiento operativo de dicha entidad ante las posibles interrupciones en sus servicios digitales (Becerra Acevedo et al., 2021).

El planteamiento que será fundamentado en el transcurso de la presente investigación se encuentra enmarcado en el diseño de un Plan de Continuidad del Negocio, alineado a la norma ISO 22301 cuya orientación impere en la identificación de procesos críticos, así como en la evaluación de riesgos tecnológicos y el establecimiento de estrategias de recuperación, además de la resiliencia organizacional que debe tener la cooperativa ante cualquier posible incidente o evento disruptivo.

1.1.1. Formulación del problema

A pesar de la creciente dependencia de los servicios digitales dentro de las instituciones financieras, la continuidad de estas plataformas puede verse comprometida por diferentes eventos disruptivos, entre ellos fallas en la infraestructura técnica, ciberataques, errores humanos, interrupciones eléctricas y desastres naturales. En el caso de la cooperativa de ahorro y crédito Yuyay Ltda. sus procesos administrativos, financieros y de atención a los socios mantienen una dependencia directa de los recursos tecnológicos, por lo que una interrupción prolongada podría afectar la disponibilidad de los servicios, el desarrollo de las operaciones institucionales y la confianza de sus usuarios.

La ausencia de un análisis documentado que permita establecer la criticidad de los servicios digitales, sus dependencias, los impactos ocasionado por una interrupción y los tiempos aceptables para su recuperación dificulta la definición de prioridades y procedimientos de actuación ante posibles incidentes, En este contexto, resulta necesario identificar los

procesos y activos tecnológicos relacionados con los servicios digitales, desarrollar un Análisis del Impacto del negocio (BIA), evaluar los riesgos que puedan provocar interrupciones y establecer parámetros de recuperación como el RTO Y RPO, de manera que las acciones de continuidad respondan a las necesidades de la cooperativa.

En este sentido, resulta pertinente desarrollar un Plan de Continuidad del Negocio basado en los lineamientos de la norma ISO 22301:2019. Que permita establecer estrategias, responsabilidades y procedimientos orientados a fortalecer la capacidad de respuesta y recuperación de la cooperativa de ahorro y crédito Yuyay Ltda., ante situaciones que puedan afectar sus servicios digitales. Por lo tanto, la pregunta principal de esta investigación se formula de la siguiente manera: ¿De qué manera el desarrollo de un Plan de continuidad del Negocio basado en la norma ISO 22301:2019 permitirá fortalecer la capacidad de respuesta y recuperación de los servicios digitales de la Cooperativa de Ahorro y Crédito Yuyay Ltda., ante eventos disruptivos que pueden afectar a su continuidad operativa?

1.2. Antecedentes de la investigación

Corrales-Estrada et al. (2021), mediante una revisión de literatura, relacionan la continuidad con las capacidades de resiliencia y sostenibilidad. Sus resultados muestran que los conceptos se complementan, pero no deben asumirse como equivalentes. La continuidad se concentra en mantener o recuperar productos y servicios prioritarios; la resiliencia incorpora, además, la capacidad de adaptación y aprendizaje. Esta diferencia ayuda a evitar que el plan se reduzca a regresar exactamente al estado anterior, sin corregir las debilidades que favorecieron la interrupción.

En Ecuador, Quituisaca-León et al. (2021) analizaron la continuidad de las Mi Pymes de Cuenca bajo los criterios de ISO 22301. El estudio evidencia la necesidad de formalizar estrategias de respuesta y recuperación, especialmente en organizaciones donde la continuidad suele depender del conocimiento no documentado de unas pocas personas. Su aporte para

esta investigación radica en mostrar que un estándar internacional puede adaptarse a instituciones de menor tamaño, siempre que su aplicación responda al contexto y a los recursos disponibles.

En el ámbito cooperativo local, Buscán Pinguil et al. (2022) diseñaron un modelo de plan de continuidad de negocio basado en ISO 22301 para las cooperativas de ahorro y crédito del segmento B del cantón Cañar, que incorpora la identificación de procesos críticos y el análisis de riesgos tecnológicos como etapas previas a la definición de estrategias de mitigación. Este antecedente constituye una referencia metodológica relevante para la presente investigación; sin embargo, sus resultados no pueden ser aplicados directamente a la COAC Yuyay, debido a que cada organización presenta características particulares en cuanto a procesos, dependencias, recursos y niveles de tolerancia frente a una interrupción. Por esta razón, resulta necesario realizar un diagnóstico específico que responda a la realidad institucional de la cooperativa.

La revisión permite reconocer una brecha concreta. Existen propuestas generales y casos aplicados de continuidad, pero el anteproyecto no dispone todavía de un análisis documentado de los servicios digitales de COAC Yuyay, sus interdependencias, los impactos de una suspensión ni los tiempos aceptables de recuperación. El aporte del estudio será convertir esos elementos institucionales en prioridades y estrategias trazables, alineadas con ISO 22301:2019 y ajustadas a la realidad de la cooperativa.

1.3. Justificación de la investigación

La implantación de un Plan de Continuidad del Negocio (BCP) para los servicios digitales de la Cooperativa de Ahorro y Crédito COAC Yuyay Ltda. está justificada por el aumento del uso de las tecnologías de la información y comunicación por parte de las organizaciones financieras en la automatización de sus procesos de operación y la oferta de servicios

digitales. En la actualidad, el sector financiero se enfrenta a peligros tales como los ciberataques, las fallas en la infraestructura tecnológica, las interrupciones eléctricas, los errores humanos y las catástrofes naturales, los cuales pueden comprometer la estabilidad operativa, además de la seguridad depositada por los usuarios y sus miembros asociados.

Por eso, es preciso generar mecanismos que prevengan, respondan a y recuperen a partir de incidentes disruptivos y que minimicen su impacto. Desde la óptica técnica, el estudio posibilitará elaborar un conjunto ordenado de estrategias, procedimientos y controles dirigidos a asegurar la disponibilidad y la recuperación de los servicios críticos de la cooperativa, tomando como base los lineamientos del estándar internacional ISO 22301. Esta normativa proporciona una estructura global dirigida a fortalecer la capacidad de reacción interna, optimizar la administración de riesgos y garantizar la continuidad de las actividades más críticas ante las situaciones de emergencia. Al respecto, la propia norma establece que un sistema de gestión de la continuidad protege a la organización frente a las interrupciones, reduce su probabilidad y la prepara para responder y recuperarse (ISO, 2019), y la literatura sobre modelos de implementación confirma que su adopción fortalece la capacidad de reacción de las organizaciones y favorece su estabilidad a largo plazo (Becerra Acevedo et al., 2021).

La realización de esta investigación, en el ámbito académico, contribuirá a retornar información relacionada con la continuidad del negocio, gestión de riesgos y recuperación tecnológica dentro del entorno de las entidades financieras de la economía popular y solidaria, sirviendo de referencia en futuras investigaciones relacionadas con la seguridad y continuidad de los servicios digitales. Asimismo, servirá para integrar protocolos y buenas prácticas internacionales en el contexto ecuatoriano y en el sector cooperativo financiero (Buscán Pinguil et al., 2022).

1.4. Objetivos

1.4.1. Objetivo general

Desarrollar un Plan de Continuidad del Negocio para los servicios digitales pertenecientes a la Cooperativa de Ahorro y Crédito “Yuyay” Ltda., bajo los lineamientos que establece la norma ISO 22301:2019, que permita incrementar la eficacia en la recuperación y la respuesta ante incidentes que puedan comprometer la continuidad de los servicios digitales.

1.4.2. Objetivos específicos

- Elaborar el marco teórico y conceptual relacionado con continuidad del negocio, resiliencia organizacional, gestión del riesgo y la norma ISO 22301.
- Identificar y analizar los activos tecnológicos y procesos críticos asociados a las plataformas virtuales de la Cooperativa de Ahorro y Crédito "Yuyay" Ltda., mediante el levantamiento de información institucional.
- Elaborar el Plan de Continuidad del Negocio dirigido a los servicios digitales de la cooperativa mediante la ejecución de las fases establecidas en la metodología seleccionada.

1.5. Limitaciones

- Poco tiempo en recibir la información solicitada.
- Acceso restringido a cierta información confidencial.
- Las fichas de análisis de impacto se validaron en una sola sesión, a partir de valores propuestos por el investigador y sin acta firmada por los participantes, lo que limita la evidencia de la validación y puede introducir un sesgo de anclaje.

1.6. Delimitaciones

- El estudio estará enfocado en la continuidad del negocio de los servicios digitales y los recursos tecnológicos asociados a su funcionamiento.

- El desarrollo del Plan de Continuidad del Negocio se fundamentará principalmente en los lineamientos establecidos por la norma ISO 22301:2019, incorporando el Análisis de Impacto al Negocio (BIA), la evaluación de riesgos y la determinación de estrategias de continuidad y recuperación.
- La investigación comprenderá la identificación de procesos y recursos tecnológicos, análisis de impactos y riesgos, establecimiento de prioridades de recuperación y estructuración documental del Plan de Continuidad del Negocio.

CAPÍTULO II

2. MARCO TEÓRICO

El presente capítulo reúne los fundamentos conceptuales y normativos del diseño de planes de continuidad del negocio para servicios digitales en entidades financieras. Su organización sigue una secuencia lógica: primero se caracterizan los sistemas de información y los servicios digitales financieros, así como el contexto regulatorio del sector financiero popular y solidario ecuatoriano; luego se desarrollan los conceptos de interrupción y riesgo tecnológico que explican por qué dichos servicios pueden dejar de operar; a continuación se presentan la continuidad del negocio, el análisis de impacto y las estrategias de respuesta y recuperación como respuesta a ese problema; y finalmente se expone la norma ISO 22301:2019 junto con los marcos complementarios con los que suele combinarse.

2.1. Sistemas de información y servicios digitales en el sector financiero cooperativo

2.1.1. Sistemas de información: concepto, componentes y dependencia organizacional

Un sistema de información es un conjunto de componentes interrelacionados que recopilan, procesan, almacenan y distribuyen información para apoyar la toma de decisiones, la coordinación y el control de una organización (Laudon & Laudon, 2022). Desde la perspectiva de la gestión, el sistema no se reduce a la tecnología: integra tres dimensiones que deben entenderse conjuntamente, la organizacional (procesos, estructura, cultura), la humana (usuarios, competencias, roles) y la tecnológica (hardware, software, datos, redes y servicios contratados). Esta visión es relevante para la continuidad del negocio porque una interrupción puede originarse en cualquiera de las tres dimensiones y porque la recuperación exige actuar sobre todas ellas de forma coordinada.

En las entidades financieras la dependencia respecto de los sistemas de información es estructural: prácticamente ninguna operación de captación, colocación o pago se ejecuta hoy

sin la intervención de un sistema transaccional, una base de datos y una red de comunicaciones. El Comité de Supervisión Bancaria de Basilea (Basel Committee on Banking Supervision [BCBS], 2021) describe esta situación al señalar que las operaciones críticas de una institución financiera dependen de un entramado de personas, procesos, tecnología, instalaciones, información y proveedores cuya interconexión debe ser identificada y mapeada antes de poder protegerla. De ello se desprende que el inventario de activos tecnológicos y el mapa de dependencias constituyen el punto de partida obligado de cualquier plan de continuidad.

2.1.2. Servicios digitales financieros y canales electrónicos

Los servicios digitales financieros son aquellos productos y operaciones que la entidad presta a sus socios a través de canales electrónicos, sin necesidad de presencia física en una agencia. La literatura sobre la transformación digital del sector financiero los asocia a la convergencia de tecnologías de información, telecomunicaciones móviles y plataformas de pago que redefinieron la forma en que las instituciones interactúan con sus clientes (Gomber et al., 2018). En una cooperativa de ahorro y crédito los servicios digitales típicos incluyen la consulta de saldos y movimientos, las transferencias internas e interbancarias, el pago de servicios, la apertura de productos de ahorro y la atención de solicitudes de crédito, prestados mediante banca web, aplicación móvil, cajeros automáticos y corresponsales solidarios.

Un servicio digital no es un elemento aislado sino el resultado de una cadena de capas tecnológicas y organizacionales dependientes entre sí. La Ilustración 1 representa esa estructura: el socio accede mediante un canal, el canal invoca servicios y procesos, estos se ejecutan en aplicaciones (en particular el sistema central o core financiero), las aplicaciones corren sobre una infraestructura de servidores, bases de datos, redes y energía, y buena parte de esa infraestructura es provista o complementada por terceros, como operadores de telecomunicaciones, switches transaccionales o el Sistema de Pagos Interbancarios del Banco Central. La

falla de cualquiera de las capas inferiores se propaga hacia arriba hasta hacerse visible como indisponibilidad del servicio para el socio.

Ilustración 1

Capas que componen un servicio digital financiero y relación de dependencia entre ellas



Fuente: Elaboración propia a partir de Laudon y Laudon (2022) y BCBS (2021).

Esta descomposición por capas es la que permite, en el análisis de impacto, identificar qué recursos sostienen a cada servicio y, en la evaluación de riesgos, localizar en qué capa se concentran las amenazas más probables. Por ello conviene distinguir terminológicamente entre "servicios digitales", que designa el conjunto de prestaciones que la entidad ofrece a través de canales electrónicos, y "plataformas virtuales" o "activos tecnológicos", que se refiere a las capas de aplicaciones, infraestructura y terceros que los hacen posibles.

2.1.3. Las cooperativas de ahorro y crédito en Ecuador: el sector financiero popular y solidario y la SEPS

En Ecuador las cooperativas de ahorro y crédito forman parte del sector financiero popular y solidario, cuya organización, funcionamiento y control están definidos por la Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario

(Asamblea Nacional del Ecuador, 2011) y por el Código Orgánico Monetario y Financiero (Asamblea Nacional del Ecuador, 2014). Este último establece que las entidades del sector se someten a la regulación de la Junta de Política y Regulación Financiera y al control de la Superintendencia de Economía Popular y Solidaria (SEPS), y dispone que las normas que se emitan tengan en cuenta la naturaleza y las características propias del sector solidario. Las cooperativas se clasifican en segmentos según el volumen de sus activos, lo que determina la intensidad de los requisitos de supervisión que deben cumplir.

La condición cooperativa introduce dos particularidades relevantes para la continuidad de los servicios digitales. La primera es la relación de confianza con el socio: a diferencia del cliente de un banco, el socio es copropietario de la entidad, de modo que una interrupción prolongada de los servicios afecta no solo a la operación sino al vínculo asociativo que sostiene a la institución. La segunda es la limitación de recursos: las cooperativas de segmentos intermedios y pequeños operan con equipos de tecnología reducidos y con una alta dependencia de proveedores externos, lo que obliga a adaptar las normas internacionales a su escala en lugar de aplicarlas literalmente. Buscán Pinguil et al. (2022) documentan precisamente esa necesidad de adaptación al proponer un modelo de plan de continuidad para cooperativas del segmento B del cantón Cañar, y Quituisaca-León et al. (2021) constatan en Cuenca que las organizaciones de menor tamaño carecen de estrategias formales de continuidad pese a su exposición a interrupciones.

2.1.4. Marco regulatorio aplicable: riesgo operativo, continuidad del negocio y protección de datos personales

La continuidad del negocio no es, para una cooperativa ecuatoriana, una práctica voluntaria. La Superintendencia de Economía Popular y Solidaria expidió la Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del sector financiero popular y solidario (Superintendencia de Economía Popular y Solidaria [SEPS], 2018),

que exige a las entidades controladas identificar, medir, controlar y monitorear los eventos de riesgo operativo derivados de procesos, personas, tecnología de la información y eventos externos, y que incorpora disposiciones específicas sobre la continuidad del negocio y la información crítica que debe protegerse para garantizarla. Esa norma fue sustituida por la Resolución SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116, Norma de control para la administración del riesgo operativo en las entidades del sector financiero popular y solidario, publicada en el Registro Oficial Suplemento No. 606 de 23 de julio de 2024, que es la que rige al momento de esta investigación y la que la propia cooperativa cita como marco normativo (Anexo A, G4) (SEPS, 2024). La norma vigente toma como referencia la serie ISO 22301 y exige a las entidades un Comité de Continuidad del Negocio que sesione al menos trimestralmente; la determinación de los tiempos máximos de interrupción que soportan los procesos críticos y del RTO y el RPO de cada uno; un plan de recuperación de desastres con procedimientos de restauración en una ubicación remota; pruebas anuales de continuidad que incluyan a los proveedores críticos; y una disponibilidad anual del 99,99 % para los servicios críticos que se ofrecen a los usuarios financieros, sin considerar el mantenimiento programado de la plataforma. Estos requisitos fijan el mínimo que debe satisfacer el plan que se diseña en este trabajo.

Esta exigencia regulatoria coincide con la tendencia internacional. El BCBS (2021) formuló principios de resiliencia operativa para el sector bancario que consideran la gestión del riesgo operativo, la planificación de la continuidad, el mapeo de interconexiones, la gestión de terceros y la respuesta a incidentes como componentes inseparables de una misma capacidad. Aunque esos principios se dirigen a bancos internacionalmente activos, los supervisores nacionales los han ido trasladando al conjunto del sistema financiero, incluido el cooperativo.

A lo anterior se suma la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021), que obliga al responsable del tratamiento a adoptar medidas técnicas y organizativas que garanticen la seguridad de los datos, incluida su disponibilidad y la capacidad de restablecer el acceso a ellos tras un incidente. Dado que los servicios digitales de una cooperativa procesan datos financieros de sus socios, las estrategias de respaldo y recuperación del plan de continuidad deben diseñarse de modo que satisfagan también este deber legal. Su Reglamento General En conjunto, la norma de riesgo operativo de la SEPS, los principios de resiliencia operativa y la ley de datos personales configuran el marco de obligaciones que todo plan de continuidad de una cooperativa de ahorro y crédito ecuatoriana debe atender.(Presidencia de la República del Ecuador, 2023) desarrolla esas medidas de seguridad, y la Norma técnica de notificación de vulneraciones de la seguridad de los datos personales (Superintendencia de Protección de Datos Personales [SPDP], 2026) establece que el responsable notifique a la autoridad a través del Sistema Nacional de Registro de Datos Personales (SISPDP), dentro del plazo de cinco días que fija la ley, cualquier vulneración que afecte a la confidencialidad, integridad o disponibilidad de los datos; un incidente que active el plan de continuidad puede ser, al mismo tiempo, una vulneración notificable. Por último, la Norma de control respecto a la seguridad de la información en las entidades del sector financiero popular y solidario (SEPS, 2022) obliga a reportar de inmediato a la SEPS los eventos que afecten a la continuidad del negocio y a la prestación de los servicios financieros, y exige controles de respaldo de la información.

2.2. Interrupciones y riesgos tecnológicos en los servicios digitales

2.2.1. Evento disruptivo, incidente e interrupción: definiciones normativas

El vocabulario de la familia de normas de seguridad y resiliencia (ISO, 2021a) distingue tres nociones que con frecuencia se usan indistintamente. Un incidente es un suceso que puede constituir o conducir a una interrupción, pérdida, emergencia o crisis; una interrupción

(disruption) es un suceso, previsto o no, que provoca una desviación negativa no planificada en la entrega esperada de productos y servicios; y una crisis es una situación con un alto nivel de incertidumbre que afecta a las actividades centrales de la organización y requiere decisiones urgentes. La norma ISO 22301 utiliza el concepto de interrupción como eje: la continuidad del negocio se define como la capacidad de la organización para continuar entregando productos y servicios en plazos aceptables y a una capacidad predefinida durante una interrupción (ISO, 2019).

Trasladadas a los servicios digitales de una entidad financiera, estas definiciones permiten clasificar los sucesos por su gravedad. La caída momentánea de una aplicación móvil que se restablece en minutos es un incidente; la indisponibilidad del core financiero durante una jornada completa, que impide atender transacciones en todos los canales, es una interrupción; y la pérdida de la base de datos transaccional sin un respaldo íntegro constituye una crisis. El plan de continuidad se ocupa de las interrupciones y crisis, mientras que los incidentes menores se gestionan mediante los procedimientos ordinarios de soporte técnico. Esta distinción permite delimitar los escenarios de interrupción que un plan de continuidad debe considerar.

2.2.2. Activos, amenazas y vulnerabilidades en infraestructuras de TI

La metodología MAGERIT define un activo como cualquier componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización, e incluye en esa categoría la información, los servicios, las aplicaciones, los equipos, las comunicaciones, las instalaciones y las personas (Ministerio de Hacienda y Administraciones Públicas [MHAP], 2012a). Una amenaza es una causa potencial de un incidente no deseado que puede causar daño a un activo, y una vulnerabilidad es una debilidad del activo o de sus controles que puede ser explotada por una o más amenazas (International Organization for Standardization & International Electrotechnical

Commission [ISO/IEC], 2022b). El riesgo surge de la combinación de ambas: la probabilidad de que una amenaza explote una vulnerabilidad y la magnitud del daño resultante.

El catálogo de elementos de MAGERIT agrupa las amenazas en cuatro familias que resultan directamente aplicables a los servicios digitales de una cooperativa (MHAP, 2012b). La Tabla 1 las resume junto con ejemplos propios del contexto estudiado. Esta clasificación constituye la base habitual de los instrumentos de identificación de amenazas.

Tabla 1

Familias de amenazas sobre activos de TI según MAGERIT y ejemplos aplicables a servicios digitales financieros

Familia de amenaza	Descripción	Ejemplos en una cooperativa de ahorro y crédito
Desastres naturales	Sucesos de origen natural que afectan a las instalaciones y equipos	Sismos, inundaciones, tormentas eléctricas que dañan el centro de datos o las agencias
De origen industrial	Fallos de servicios básicos y de la infraestructura física	Cortes de energía eléctrica, fallas de climatización, incendio, interrupción del enlace de telecomunicaciones
Errores y fallos no intencionados	Acciones u omisiones involuntarias de usuarios, administradores o proveedores	Borrado accidental de datos, errores de configuración del core, respaldos no verificados, caída por actualización defectuosa
Ataques intencionados	Acciones deliberadas de agentes internos o externos	Ransomware, denegación de servicio sobre la banca web, suplantación de identidad, acceso no autorizado a bases de datos

Fuente: Elaboración propia a partir de MHAP (2012b).

Las vulnerabilidades más frecuentes en infraestructuras de TI de entidades pequeñas y medianas tienen un patrón reconocible: concentración de funciones críticas en un único servidor o en un único administrador, ausencia de redundancia en enlaces y energía, respaldos que se generan pero no se prueban, contratos con proveedores sin acuerdos de nivel de servicio que fijen tiempos de restablecimiento, y falta de procedimientos documentados para operar en modo degradado (NIST, 2010; Quituisaca-León et al., 2021). Identificarlas es tarea de la evaluación de riesgos; mitigarlas, de las estrategias de continuidad.

2.2.3. El proceso de gestión del riesgo: identificación, análisis, evaluación y tratamiento; riesgo inherente y residual

La norma ISO 31000 define el riesgo como el efecto de la incertidumbre sobre los objetivos y establece un proceso genérico de gestión que comprende el establecimiento del contexto, la apreciación del riesgo (identificación, análisis y evaluación), el tratamiento, el seguimiento y la revisión, y la comunicación y consulta con las partes interesadas (ISO, 2018). En el ámbito de la seguridad de la información, la norma ISO/IEC 27005 particulariza ese proceso para los riesgos que afectan a la confidencialidad, integridad y disponibilidad de la información (ISO/IEC, 2022b). La continuidad del negocio se interesa especialmente por la disponibilidad, pero no puede desatender las otras dos propiedades, porque una recuperación que restablece el servicio con datos corruptos o expuestos no es una recuperación aceptable.

Dentro del proceso resulta esencial distinguir el riesgo inherente del riesgo residual. El riesgo inherente es el nivel de riesgo que existe antes de considerar los controles vigentes; el riesgo residual es el que permanece después de aplicarlos (ISO, 2018). La diferencia entre ambos mide la eficacia de las salvaguardas existentes y permite decidir si es necesario tratamiento adicional. En la práctica esta distinción es operativa: primero se valora cada riesgo como si no existieran controles, luego se identifican los controles implementados y, finalmente, se recalcula el nivel residual, que es el que determina qué riesgos deben abordarse mediante estrategias de continuidad.

El tratamiento del riesgo admite cuatro opciones clásicas: evitar la actividad que lo genera, reducir su probabilidad o su impacto mediante controles, compartirlo con terceros (seguros, contratos de respaldo) o aceptarlo cuando su nivel es tolerable (ISO, 2018). El plan de continuidad se ubica principalmente en la opción de reducción del impacto: asume que ciertas interrupciones ocurrirán pese a los controles preventivos y se prepara para limitar sus consecuencias y acortar la recuperación.

2.2.4. Valoración del riesgo: escalas de probabilidad e impacto y matriz de riesgo

La técnica de la matriz consecuencia-probabilidad, descrita en la norma IEC 31010, consiste en valorar cada riesgo mediante dos escalas ordinales, una para la probabilidad de ocurrencia y otra para la gravedad de las consecuencias, y combinarlas en una matriz que clasifica el riesgo en niveles (International Electrotechnical Commission [IEC], 2019). MAGERIT emplea el mismo principio al estimar la frecuencia de materialización de cada amenaza y la degradación que produciría sobre el activo (MHAP, 2012a). Para que la valoración sea reproducible, las escalas deben definirse con criterios explícitos antes de aplicarse. Las Tablas 2 y 3 presentan un ejemplo de escalas de cinco niveles para servicios digitales financieros, construidas a partir de los criterios de las normas citadas.

Tabla 2

Escala de probabilidad de ocurrencia

Nivel	Denominación	Criterio de frecuencia
1	Muy baja	Podría ocurrir en circunstancias excepcionales; no se ha registrado en los últimos cinco años
2	Baja	Podría ocurrir alguna vez; aproximadamente una vez cada dos a cinco años
3	Media	Es posible que ocurra; aproximadamente una vez al año
4	Alta	Probablemente ocurrirá; varias veces al año
5	Muy alta	Se espera que ocurra; mensualmente o con mayor frecuencia

Fuente: Elaboración propia a partir de IEC (2019) y MHAP (2012a).

Tabla 3

Escala de impacto de una interrupción sobre los servicios digitales

Nivel	Denominación	Dimensión operativa (duración de la interrupción; un nivel más si afecta a varios canales o a toda la institución)	Dimensión financiera (pérdida estimada, como porcentaje del margen financiero mensual) y legal	Dimensión reputacional
1	Insignificante	Degradación sin interrupción, o interrupción de un servicio de hasta 1 h	Pérdida inferior al 1 % del margen financiero mensual; sin incumplimiento	Sin percepción por parte de los socios

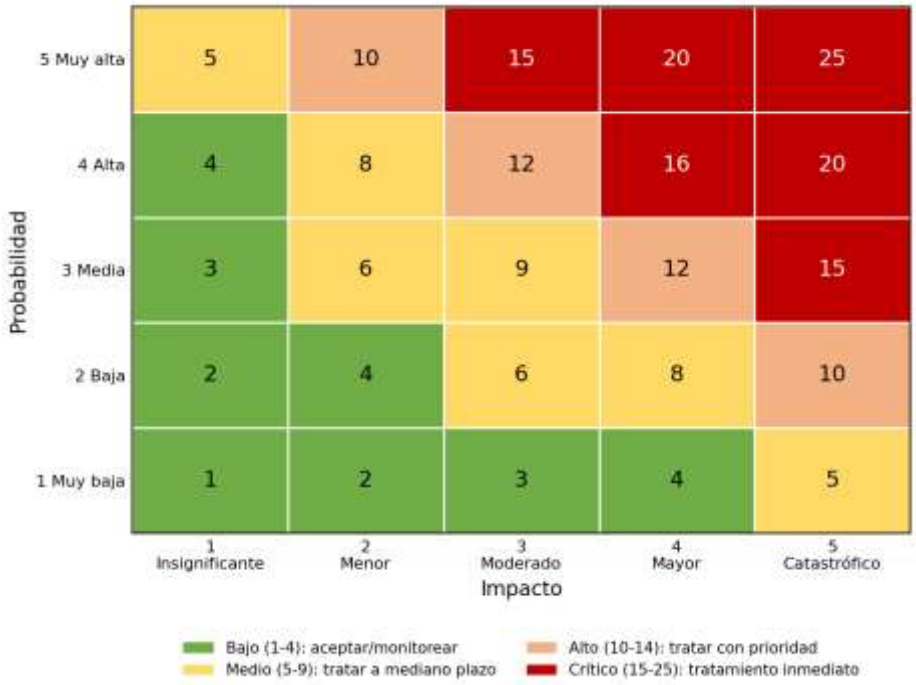
Nivel	Denominación	Dimensión operativa (duración de la interrupción; un nivel más si afecta a varios canales o a toda la institución)	Dimensión financiera (pérdida estimada, como porcentaje del margen financiero mensual) y legal	Dimensión reputacional
2	Menor	Interrupción de un servicio de 1 a 4 h; de varios canales o de toda la institución, de hasta 1 h	Pérdida del 1 % al 5 % del margen financiero mensual; sin incumplimiento regulatorio	Quejas aisladas
3	Moderado	Interrupción de un servicio de 4 a 8 h; de varios canales o de toda la institución, de 1 a 4 h	Pérdida del 5 % al 15 % del margen financiero mensual; posible observación del supervisor	Quejas generalizadas en el canal afectado
4	Mayor	Interrupción de un servicio de 8 a 24 h; de varios canales o de toda la institución, de 4 a 8 h	Pérdida del 15 % al 50 % del margen financiero mensual; incumplimiento regulatorio sancionable	Cobertura pública negativa; retiro de socios
5	Catastrófico	Interrupción de un servicio por más de 24 h o de toda la institución por más de 8 h; pérdida de datos transaccionales	Pérdida superior al 50 % del margen financiero mensual o afectación del patrimonio; riesgo para la viabilidad de la entidad	Pérdida de confianza en la institución

Nota: el nivel operativo se asigna por la duración de la interrupción del servicio y se incrementa un nivel, hasta el máximo de 5, cuando la interrupción afecta simultáneamente a varios canales o a toda la institución; los servicios de soporte sin operaciones propias se valoran por la pérdida de capacidad de detección y respuesta. La pérdida financiera comprende los ingresos no percibidos, los costos de recuperación y las sanciones, y se expresa como porcentaje del margen financiero mensual para que la valoración sea reproducible, como recomienda ISO/TS 22317. Fuente: Elaboración propia a partir de IEC (2019), ISO (2021b) y SEPS (2018).

El nivel de riesgo se obtiene como el producto de la probabilidad por el impacto, lo que genera valores entre 1 y 25. La Ilustración 2 presenta la matriz resultante con cuatro zonas de tratamiento. Los umbrales de cada zona expresan el apetito de riesgo de la organización y deben ser validados por su dirección; los que se muestran (bajo de 1 a 4, medio de 5 a 9, alto de 10 a 14 y crítico de 15 a 25) siguen la práctica habitual de las matrices de cinco por cinco (IEC, 2019; MHAP, 2012a).

Ilustración 2

Matriz de nivel de riesgo (probabilidad × impacto) y zonas de tratamiento



Fuente: Elaboración propia a partir de IEC (2019).

2.2.5. MAGERIT como técnica de análisis de riesgos de sistemas de información

MAGERIT es la metodología de análisis y gestión de riesgos de los sistemas de información elaborada por la administración pública española y de uso libre, cuya tercera versión está estructurada en un libro de método, un catálogo de elementos y una guía de técnicas (MHAP, 2012a, 2012b). Su propósito es ofrecer un procedimiento sistemático para conocer el riesgo al que están sometidos los activos de información y planificar su tratamiento. Tres características explican su amplia adopción en Iberoamérica: es gratuita y está documentada en español, lo que la hace accesible para organizaciones de recursos limitados; su catálogo de activos y amenazas está pensado para infraestructuras de TI; y es la metodología de referencia de la administración pública española, lo que explica su difusión en organizaciones públicas y privadas de habla hispana (MHAP, 2012a).

El método se desarrolla en una secuencia de pasos que la Tabla 4 resume y relaciona con las actividades típicas de un diagnóstico de continuidad de servicios digitales. El resultado final es un conjunto de riesgos valorados y priorizados que alimenta directamente la selección de estrategias de continuidad.

Tabla 4

Pasos del análisis de riesgos según MAGERIT y su aplicación al diagnóstico de servicios digitales

Paso MAGERIT	Descripción	Aplicación en un diagnóstico de servicios digitales
1. Identificación y valoración de activos	Inventariar los activos y valorarlos según las dimensiones de seguridad (disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad) y sus dependencias	Inventario de servicios digitales, aplicaciones, infraestructura y proveedores mediante fichas técnicas y entrevistas al área de TI
2. Identificación de amenazas	Determinar qué amenazas pueden afectar a cada activo	Selección de amenazas del catálogo (Tabla 1) aplicables a cada activo
3. Estimación de frecuencia y degradación	Valorar la probabilidad de cada amenaza y el daño que causaría	Aplicación de las escalas de las Tablas 2 y 3
4. Determinación del impacto y del riesgo	Calcular el impacto potencial y el riesgo combinando valor del activo, degradación y frecuencia	Cálculo del nivel de riesgo y ubicación en la matriz de la Figura 2
5. Identificación de salvaguardas	Reconocer los controles existentes y estimar su eficacia	Verificación de controles vigentes (respaldos, redundancia, contratos) y cálculo del riesgo residual
6. Priorización y tratamiento	Decidir qué riesgos requieren tratamiento y con qué prioridad	Lista priorizada de riesgos que orienta la selección de estrategias de continuidad

Fuente: Elaboración propia a partir de MHAP (2012a).

2.3. Continuidad del negocio y resiliencia organizacional

2.3.1. Continuidad del negocio, resiliencia operativa y resiliencia organizacional: diferencias y relación

La continuidad del negocio, la resiliencia operativa y la resiliencia organizacional son conceptos emparentados cuyo uso indistinto genera confusión en la literatura y en la práctica. Galaitsi et al. (2023) proponen diferenciarlos a partir de tres dicotomías: riesgo frente a resi-

liencia, procesos organizacionales frente a activos, y condiciones normales frente a condiciones de crisis. Según esa distinción, la gestión de la continuidad del negocio se centra en mantener la entrega de productos y servicios durante una interrupción, con un enfoque predominantemente orientado a los activos y procesos críticos y a escenarios previamente identificados; la resiliencia operativa amplía el foco hacia la capacidad de absorber perturbaciones y seguir prestando los servicios aun cuando los escenarios no hayan sido anticipados; y la resiliencia organizacional abarca la capacidad del conjunto de la organización para adaptarse, aprender y transformarse frente a cambios del entorno.

La revisión de Corrales-Estrada et al. (2021) confirma que la gestión de la continuidad y la resiliencia organizacional se relacionan de forma bidireccional: las prácticas de continuidad constituyen una capacidad que contribuye a la resiliencia, y las capacidades dinámicas de resiliencia, a su vez, mejoran la eficacia de los planes de continuidad. Buzzao y Rizzi (2023) aportan evidencia empírica en esa dirección al mostrar que el cumplimiento de los requisitos de continuidad expresados en ISO 22301 depende de capacidades organizacionales de detección, aprovechamiento de oportunidades y reconfiguración que van más allá de la dimensión técnica. En el sector financiero, el BCBS (2021) adopta explícitamente el término resiliencia operativa para designar la capacidad de la entidad de entregar sus operaciones críticas a través de una interrupción, y sitúa la continuidad del negocio como uno de los medios para alcanzarla.

La consecuencia práctica de esta distinción es doble. Por un lado, un plan de continuidad es un instrumento centrado en servicios críticos y escenarios definidos, lo que delimita su alcance. Por otro, el plan debe concebirse como un componente de la resiliencia operativa de la entidad, de modo que sus estrategias se evalúen también por su capacidad de responder a interrupciones no previstas y de incorporar el aprendizaje de los ejercicios y de los incidentes reales.

2.3.2. Sistema de Gestión de Continuidad del Negocio (SGCN) y Plan de Continuidad del Negocio (BCP)

La norma ISO 22301 define el sistema de gestión de la continuidad del negocio como la parte del sistema de gestión global que establece, implementa, opera, supervisa, revisa, mantiene y mejora la continuidad del negocio, e incluye la estructura organizativa, las políticas, la planificación, las responsabilidades, los procedimientos, los procesos y los recursos (ISO, 2019). El plan de continuidad del negocio, por su parte, es la información documentada que guía a la organización para responder a una interrupción y reanudar, recuperar y restaurar la entrega de productos y servicios de acuerdo con sus objetivos de continuidad (ISO, 2021a). La relación entre ambos es de parte a todo: el SGCN es el marco de gobierno que garantiza que exista un plan, que esté alineado con la estrategia, que se pruebe y que se mejore; el BCP es uno de sus productos operativos.

La guía de aplicación ISO 22313 precisa que un plan de continuidad debe contener, como mínimo, el propósito y alcance, los criterios de activación, los roles y responsabilidades, los procedimientos de respuesta y de comunicación, las estrategias y recursos para reanudar las actividades prioritarias, la información de contacto y los procedimientos de retorno a la normalidad (ISO, 2020). Niemimaa et al. (2019) advierten, además, que la continuidad no debe pensarse solo para la infraestructura tecnológica sino para el modelo de negocio en su conjunto, ya que una interrupción puede comprometer la propuesta de valor, los canales y las relaciones con los clientes aunque la tecnología se restablezca. Esta observación es especialmente pertinente para las cooperativas de ahorro y crédito, cuyos servicios digitales son, a la vez, canal de atención y elemento de la relación con el socio.

Cuando una organización no está en condiciones de implementar el sistema de gestión completo ni de certificarse, la guía de aplicación de la norma y la literatura recomiendan concentrarse en el plan de continuidad y en los elementos del SGCN que son indispensables para

que el plan sea viable (ISO, 2020; Sahebjamnia et al., 2015): la política, los roles, el análisis de impacto, la evaluación de riesgos, las estrategias, los procedimientos de respuesta y recuperación y el programa de ejercicios. Esta delimitación coincide con la de Păunescu y Argatu (2020), quienes identifican como funciones críticas de una gestión de continuidad eficaz el compromiso de la dirección, el análisis de impacto, la definición de estrategias y las pruebas periódicas.

2.3.3. Continuidad de los servicios TIC: preparación de las TIC para la continuidad

Cuando los productos y servicios de una organización dependen de las tecnologías de la información y la comunicación, la continuidad del negocio exige que las TIC estén preparadas para sostenerla. La norma ISO/IEC 27031 describe los conceptos y principios de la preparación de las TIC para la continuidad del negocio (ICT readiness for business continuity, IRBC) y proporciona un marco de métodos y procesos para identificar y especificar los aspectos que permiten mejorar esa preparación (ISO/IEC, 2025). Su segunda edición, publicada en 2025, incorpora explícitamente la dependencia de servicios externos como las plataformas en la nube y se concibe como complemento de ISO/IEC 27001 en materia de seguridad y de ISO 22301 en materia de continuidad.

La norma introduce, junto a los parámetros de tiempo y punto de recuperación que se desarrollan en la sección 2.4, el objetivo mínimo de continuidad del negocio (minimum business continuity objective, MBCO), que define el nivel mínimo de servicio aceptable durante una interrupción. Este concepto es especialmente útil para una cooperativa, porque permite diseñar modos de operación degradados, por ejemplo mantener consultas y transferencias internas aunque se interrumpan las transferencias interbancarias, en lugar de plantear la recuperación como una alternativa binaria entre servicio completo y ausencia de servicio.

En síntesis, la continuidad TIC es el componente del plan que traduce los objetivos de continuidad definidos por el negocio en requisitos concretos para la infraestructura: redundancia de componentes, respaldos con una frecuencia coherente con el punto de recuperación, sitios alternos, procedimientos de restauración y acuerdos de nivel de servicio con proveedores. La sección 2.5 desarrolla estas estrategias.

2.4. Análisis de Impacto al Negocio (BIA)

2.4.1. Finalidad y proceso del BIA según ISO/TS 22317:2021

El análisis de impacto al negocio es el proceso de analizar el efecto que una interrupción tendría sobre la organización a lo largo del tiempo, con el fin de identificar las actividades prioritarias, los recursos que las sostienen y los plazos dentro de los cuales deben ser reanudadas (ISO, 2021a). La especificación técnica ISO/TS 22317 desarrolla el procedimiento para llevarlo a cabo y lo presenta como el fundamento de todo el sistema de continuidad: sin un BIA, las estrategias se definen por intuición y los recursos se asignan sin relación con la criticidad real de los servicios (ISO, 2021b). La norma ISO 22301 lo exige en la cláusula 8.2.2 como requisito operativo del sistema de gestión (ISO, 2019).

El proceso del BIA comprende, de forma resumida, las siguientes etapas: definir el alcance y los productos y servicios que se analizarán; identificar las actividades que entregan esos productos y servicios; evaluar los impactos de no realizar cada actividad en función del tiempo transcurrido; determinar los plazos de reanudación y los niveles mínimos de servicio; identificar los recursos y dependencias necesarios para cada actividad; y consolidar los resultados en una priorización que la dirección aprueba (ISO, 2021b). En entidades pequeñas la información se obtiene predominantemente mediante entrevistas estructuradas con los responsables de cada proceso y con el área de tecnología, apoyadas en fichas de recolección que registran, para cada servicio, sus dependencias, su volumen de uso y los impactos esperados a distintas duraciones de interrupción.

2.4.2. Identificación de actividades prioritarias, recursos y dependencias

El BIA se construye sobre el inventario de servicios y activos descrito en la sección 2.1.2. Para cada servicio digital se identifican las actividades que lo entregan y, para cada actividad, los recursos de los que depende: personas con competencias específicas, aplicaciones, datos, infraestructura, instalaciones, proveedores y otras actividades internas. El BCBS (2021) insiste en que el mapeo de estas interconexiones e interdependencias, incluidas las que pasan por terceros, es una condición previa para cualquier estrategia de resiliencia, porque una operación crítica rara vez depende de un único recurso identificable.

La priorización resultante no coincide necesariamente con la importancia estratégica o comercial del servicio. Un servicio de uso masivo cuyos impactos crecen lentamente puede tolerar una interrupción más larga que un servicio de menor volumen pero sujeto a obligaciones regulatorias con plazos estrictos, como la liquidación de transferencias interbancarias. Por eso la priorización se fundamenta en la evolución temporal de los impactos y no en la percepción general de criticidad, lo que exige que los instrumentos de recolección del BIA indaguen explícitamente cómo cambia el daño a medida que la interrupción se prolonga.

2.4.3. Tipos de impacto y su evolución en el tiempo

La especificación ISO/TS 22317 recomienda evaluar los impactos en varias categorías, que suelen agruparse en financieras, operativas, legales o regulatorias y reputacionales, utilizando criterios cualitativos o cuantitativos previamente acordados (ISO, 2021b). En una cooperativa de ahorro y crédito los impactos financieros incluyen las comisiones no percibidas, los costos de recuperación y las eventuales sanciones; los operativos, la acumulación de transacciones pendientes y la sobrecarga de los canales presenciales; los legales, el incumplimiento de la normativa de riesgo operativo y de protección de datos; y los reputacionales, la pérdida de confianza de los socios y la cobertura pública negativa, que en el sector cooperativo pueden traducirse en retiros de depósitos.

La característica distintiva del BIA es que los impactos se evalúan en función del tiempo: una misma interrupción produce consecuencias leves durante las primeras horas y graves cuando se prolonga más allá de cierto umbral. La Tabla 3 de la sección 2.2.4 ya incorpora esta lógica al asociar los niveles de impacto a duraciones de interrupción, de modo que la misma escala sirve tanto para la valoración de riesgos como para el BIA. Esa convergencia es deliberada: Torabi et al. (2016) muestran que integrar el análisis de impacto con la evaluación de riesgos en un marco común evita incoherencias entre la prioridad asignada a un servicio y los recursos destinados a protegerlo.

2.4.4. Parámetros de recuperación: MTPD, RTO, RPO y MBCO

Del análisis de impacto se derivan los parámetros que gobiernan la planificación de la recuperación, cuyas definiciones normativas son las siguientes (ISO, 2021a; ISO/IEC, 2025). El período máximo tolerable de interrupción (maximum tolerable period of disruption, MTPD) es el tiempo que tardarían los impactos adversos de no entregar un producto o servicio en volverse inaceptables. El objetivo de tiempo de recuperación (recovery time objective, RTO) es el período, posterior a la interrupción, dentro del cual el producto, servicio o actividad debe reanudarse o los recursos recuperarse; por definición debe ser menor que el MTPD, de modo que exista un margen de seguridad. El objetivo de punto de recuperación (recovery point objective, RPO) es el punto en el tiempo hasta el cual los datos deben ser restaurados para que la actividad pueda operar tras la reanudación; equivale a la pérdida máxima de datos tolerable y determina la frecuencia de los respaldos. El objetivo mínimo de continuidad del negocio (MBCO) es el nivel mínimo de servicios o productos aceptable durante una interrupción. La Ilustración 3 representa la relación temporal entre los tres primeros.

Ilustración 3

Relación temporal entre RPO, RTO y MTPD ante una interrupción



Fuente: Elaboración propia a partir de ISO (2021a) e ISO/IEC (2025).

Estos parámetros son el principal resultado cuantitativo del BIA y el principal insumo de las estrategias de continuidad. Un RTO de dos horas para el core financiero implica, por ejemplo, disponer de infraestructura alterna lista para activarse, mientras que un RTO de dos días admite restaurar desde respaldos en equipos de reemplazo; un RPO de quince minutos exige replicación continua de la base de datos, mientras que un RPO de un día se satisface con un respaldo nocturno. Los valores de MTPD, RTO, RPO y MBCO se establecen para cada servicio a partir de la información aportada por los responsables de los procesos y del área de tecnología, y toda estrategia de continuidad debe verificarse frente a ellos.

2.4.5. Relación entre el BIA y la evaluación de riesgos en la definición de prioridades

El BIA y la evaluación de riesgos responden a preguntas distintas y complementarias. El primero responde qué servicios deben recuperarse primero y en cuánto tiempo, con independencia de la causa de la interrupción; la segunda responde qué amenazas tienen mayor probabilidad de provocar esa interrupción y con qué gravedad. La norma ISO 22301 exige ambos análisis en la cláusula 8.2 y dispone que las estrategias de continuidad se seleccionen a partir de sus resultados conjuntos (ISO, 2019). Sahebjamnia et al. (2015) formalizan esta integración en un marco que utiliza la priorización del BIA y los escenarios de la evaluación de

riesgos para asignar recursos limitados entre planes de continuidad y de recuperación, y Rezaei Soufi et al. (2019) muestran que la selección de planes puede modelarse como un problema de decisión que parte de los escenarios identificados en la evaluación de riesgos.

En términos prácticos, la combinación de ambos análisis produce una matriz de decisión: los servicios con MTPD corto y expuestos a riesgos de nivel alto o crítico reciben estrategias de alta disponibilidad y tratamiento inmediato; los servicios con MTPD largo y riesgos bajos pueden atenderse con procedimientos de restauración convencionales. Esta lógica es la que ordena la estructura de un plan de continuidad.

2.5. Estrategias de continuidad, respuesta y recuperación

2.5.1. Selección de estrategias y soluciones de continuidad

La cláusula 8.3 de ISO 22301 requiere que la organización identifique y seleccione estrategias y soluciones de continuidad basadas en los resultados del BIA y de la evaluación de riesgos, que permitan proteger las actividades prioritarias, estabilizar, continuar, reanudar y recuperar dichas actividades y sus dependencias, y mitigar, responder y gestionar los impactos (ISO, 2019). Las estrategias se refieren a los objetivos generales de continuidad y las soluciones a los medios concretos para alcanzarlos. La guía ISO 22313 sugiere evaluarlas considerando su costo, su capacidad de cumplir los RTO y RPO, sus consecuencias para otras actividades y la viabilidad de implementarlas (ISO, 2020).

Las estrategias se organizan habitualmente según el tipo de recurso que protegen. Para las personas, incluyen la definición de roles con suplentes, la documentación de procedimientos para que puedan ser ejecutados por personal distinto del habitual y la capacitación. Para la tecnología, la redundancia de componentes críticos, la replicación de datos, los sitios o servicios alternos y la virtualización. Para las instalaciones, la disponibilidad de energía de respaldo y de espacios alternativos de trabajo. Para los proveedores, los acuerdos de nivel de servicio con tiempos de restablecimiento comprometidos, la diversificación de proveedores

críticos y la verificación de sus propios planes de continuidad, aspecto en el que el BCBS (2021) insiste al tratar la dependencia de terceros como un riesgo que la entidad no puede transferir íntegramente. Para la información, los respaldos verificados y almacenados fuera del sitio principal. La selección final equilibra la reducción del tiempo de recuperación contra el costo de la solución, con el RTO y el RPO como restricciones que toda solución debe satisfacer.

2.5.2. Estructura de respuesta a incidentes, escalamiento y comunicación

La cláusula 8.4 de ISO 22301 establece que la organización debe implementar una estructura de respuesta que le permita alertar sobre la interrupción, evaluar sus efectos, activar la respuesta adecuada, planificar las acciones, coordinar los recursos y comunicarse con las partes interesadas (ISO, 2019). Esa estructura se concreta en equipos con roles definidos, típicamente un equipo de gestión de crisis que toma decisiones, un equipo de recuperación tecnológica que ejecuta la restauración y un responsable de comunicación que atiende a socios, empleados, proveedores y autoridades.

El escalamiento define cuándo un incidente deja de ser gestionado por el soporte ordinario y pasa a activar el plan de continuidad; los criterios de activación deben ser objetivos, por ejemplo la indisponibilidad de un servicio crítico por más de un tiempo determinado o la confirmación de un ataque que compromete la integridad de los datos. La comunicación durante la interrupción tiene un papel decisivo en el sector cooperativo, porque la incertidumbre de los socios sobre la seguridad de sus fondos puede amplificar el impacto reputacional más que la interrupción misma; por ello el plan debe prever mensajes predefinidos, canales alternativos de atención y la notificación oportuna al organismo de control conforme a la normativa de riesgo operativo (SEPS, 2018). La función Responder del marco de ciberseguridad del

NIST agrupa estos mismos elementos, gestión del incidente, análisis, comunicación y mitigación, y resulta útil como referencia para los incidentes de origen cibernético (National Institute of Standards and Technology [NIST], 2024).

2.5.3. Recuperación tecnológica: Plan de Recuperación ante Desastres (DRP) y su relación con el BCP

El plan de recuperación ante desastres es el componente del plan de continuidad que se ocupa específicamente de restaurar la infraestructura tecnológica, es decir, los sistemas, aplicaciones, datos y comunicaciones, tras una interrupción. La guía de planificación de contingencias del NIST lo define como un plan aplicable a eventos mayores que impiden el acceso a la instalación principal durante un período prolongado, orientado a restablecer la operatividad de los sistemas en un sitio alterno, y lo distingue del plan de continuidad del negocio, que se centra en sostener los procesos de negocio, y de los planes de contingencia de sistemas individuales (NIST, 2010). La misma guía propone un proceso de siete pasos, que comprende la política de contingencia, el análisis de impacto, la identificación de controles preventivos, la creación de estrategias de contingencia, el desarrollo del plan, las pruebas y la capacitación, y el mantenimiento, que coincide en lo esencial con el ciclo de ISO 22301.

La relación entre BCP y DRP es, por tanto, de inclusión: el BCP define qué servicios deben reanudarse, en qué orden y en qué plazos, y el DRP especifica cómo se recuperará la tecnología que los sostiene para cumplir esos plazos. Un DRP sin BCP recupera sistemas sin saber cuáles importan más; un BCP sin DRP fija objetivos de recuperación que nadie sabe cómo cumplir. Por ello, los procedimientos de recuperación de cada activo tecnológico crítico forman parte del plan, con la secuencia de restauración ordenada según los RTO definidos en el BIA.

2.5.4. Respaldo, integridad y seguridad de la información durante la contingencia

La recuperación de los servicios digitales depende de la existencia de copias de respaldo íntegras y restaurables. La norma ISO/IEC 27001 incluye entre sus controles de referencia el mantenimiento y la prueba de copias de respaldo de la información, el software y los sistemas, la planificación de la continuidad de la seguridad de la información durante las interrupciones y la redundancia de las instalaciones de procesamiento (ISO/IEC, 2022a). El marco de ciberseguridad del NIST, en su función Recuperar, añade un requisito con frecuencia descuidado: la integridad de los respaldos y de los demás activos de restauración debe verificarse antes de utilizarlos, para evitar restaurar datos corruptos o comprometidos (NIST, 2024).

Durante una contingencia las medidas de seguridad tienden a relajarse en favor de la rapidez, lo que abre vulnerabilidades: accesos de emergencia sin registro, equipos de reemplazo sin endurecimiento, datos restaurados en entornos no controlados. El plan debe prever que la confidencialidad y la integridad de la información se mantengan en el modo de operación degradado y durante la restauración, y que los accesos excepcionales queden documentados y se revoquen al retornar a la normalidad. Este requisito tiene además fundamento legal, puesto que la Ley Orgánica de Protección de Datos Personales no suspende las obligaciones del responsable del tratamiento durante un incidente (Asamblea Nacional del Ecuador, 2021).

2.5.5. Pruebas, ejercicios y mantenimiento del plan

Un plan de continuidad que no se prueba es una hipótesis no verificada. La cláusula 8.5 de ISO 22301 exige que la organización implemente y mantenga un programa de ejercicios y pruebas que sea coherente con el alcance y los objetivos del sistema, se base en escenarios adecuados, minimice el riesgo de incidentes derivados del propio ejercicio, produzca informes con resultados y recomendaciones y se revise en el contexto de la mejora continua

(ISO, 2019). Los ejercicios pueden graduarse desde revisiones de escritorio y simulaciones de mesa, en las que los equipos recorren un escenario sin afectar la operación, hasta pruebas técnicas de restauración de respaldos y simulacros de conmutación a sitio alterno.

El mantenimiento comprende la actualización del plan ante cambios en los servicios, la infraestructura, los proveedores o el personal, y la incorporación de las lecciones aprendidas de los ejercicios y de los incidentes reales, como dispone la cláusula 8.6 de la norma (ISO, 2019). Para una cooperativa que delega parte de su operación tecnológica en terceros, los ejercicios deben incluir a los proveedores críticos, de modo que se verifique que sus tiempos reales de respuesta son compatibles con los RTO comprometidos. Por ello, todo plan de continuidad debe incluir el programa de pruebas y el calendario de ejercicios que la organización deberá cumplir para que el plan conserve su validez.

2.6. La norma ISO 22301:2019

2.6.1. Alcance, propósito y vigencia

ISO 22301 es la norma internacional que especifica los requisitos para implementar, mantener y mejorar un sistema de gestión destinado a proteger a la organización frente a las interrupciones, reducir su probabilidad de ocurrencia, prepararse para ellas, responder y recuperarse cuando se presentan (ISO, 2019). Sus requisitos son genéricos y aplicables a organizaciones de cualquier tipo, tamaño y naturaleza, y el grado de aplicación depende del entorno operativo y de la complejidad de cada entidad, lo que legitima su adaptación a una cooperativa de escala media. Es la única norma de la familia que es certificable, mientras que ISO 22313 ofrece orientación sobre su uso e ISO/TS 22317 sobre el análisis de impacto (ISO, 2020, 2021b).

La edición vigente es la segunda, publicada en 2019 en sustitución de la de 2012, con un enfoque más simplificado y práctico. En febrero de 2024 se publicó la Enmienda 1, que incorpora la consideración del cambio climático como factor del contexto de la organización,

en línea con la actualización realizada a todas las normas de sistemas de gestión de ISO (ISO, 2024). Adicionalmente, el comité técnico ISO/TC 292 mantiene en elaboración una nueva edición, actualmente en fase de comité, que reemplazará a la de 2019 cuando se publique. La versión en vigor es, por tanto, ISO 22301:2019 con su Enmienda 1.

2.6.2. Estructura de alto nivel: cláusulas 4 a 10

La norma adopta la estructura armonizada común a los sistemas de gestión de ISO, lo que facilita su integración con ISO/IEC 27001 y otras normas de sistemas de gestión. Las cláusulas 1 a 3 corresponden al alcance, las referencias normativas y los términos; las cláusulas 4 a 10 contienen los requisitos. La Tabla 5 sintetiza cada una de ellas y señala de qué forma se refleja en el diseño de un plan de continuidad.

Tabla 5

Cláusulas de requisitos de ISO 22301:2019 y su reflejo en el diseño de un plan de continuidad

Cláusula	Contenido esencial	Reflejo en el diseño del plan
4. Contexto de la organización	Comprender la organización, su contexto y las partes interesadas; determinar el alcance del SGCN	Caracterización de la entidad, sus servicios digitales, socios, proveedores y obligaciones regulatorias
5. Liderazgo	Compromiso de la alta dirección; política de continuidad; roles, responsabilidades y autoridades	Política de continuidad y estructura de roles
6. Planificación	Acciones para abordar riesgos y oportunidades del sistema; objetivos de continuidad y planes para lograrlos	Objetivos de continuidad por servicio digital
7. Soporte	Recursos, competencias, toma de conciencia, comunicación e información documentada	Recursos y competencias mínimas; estructura documental del plan
8. Operación	Planificación operativa; BIA y evaluación de riesgos; estrategias y soluciones; planes y procedimientos; programa de ejercicios; evaluación de la documentación	Núcleo del plan: diagnóstico (BIA y riesgos) y desarrollo del plan
9. Evaluación del desempeño	Seguimiento, medición, análisis y evaluación; auditoría interna; revisión por la dirección	Indicadores de seguimiento del plan; auditoría interna y revisión por la dirección

Cláusula	Contenido esencial	Reflejo en el diseño del plan
10. Mejora	No conformidades y acciones correctivas; mejora continua	Mecanismo de actualización y mejora del plan

Fuente: Elaboración propia a partir de ISO (2019).

2.6.3. Ciclo Planificar-Hacer-Verificar-Actuar en el SGCN

La norma aplica el ciclo de mejora continua Planificar-Hacer-Verificar-Actuar a los procesos del sistema de gestión (ISO, 2019). En la fase de planificar se establecen la política, los objetivos, los controles y los procedimientos relevantes para mejorar la continuidad; en la fase de hacer se implementan y operan; en la de verificar se supervisa y revisa el desempeño frente a la política y los objetivos y se informa a la dirección; y en la de actuar se mantienen y mejoran las capacidades mediante acciones correctivas. La Ilustración 4 muestra la correspondencia entre las fases del ciclo y las cláusulas de la norma.

Ilustración 4

Ciclo Planificar-Hacer-Verificar-Actuar y cláusulas de ISO 22301:2019



Fuente: Elaboración propia a partir de ISO (2019).

La utilidad del ciclo es metodológica: ordena las fases del diseño de un plan de continuidad en una secuencia reconocible. El diagnóstico y la definición de política, objetivos y roles corresponden a planificar; el desarrollo del BIA, la evaluación de riesgos, las estrategias y los procedimientos corresponde a hacer; y los indicadores, el programa de ejercicios y el mecanismo de actualización corresponden a verificar y actuar.

2.6.4. Requisitos operativos (cláusula 8) como columna vertebral del plan

La cláusula 8 contiene los requisitos que dan forma al plan de continuidad propiamente dicho y, por esa razón, suele adoptarse como estructura de los planes de continuidad diseñados bajo la norma. Sus subcláusulas establecen una secuencia lógica que se corresponde con las secciones anteriores de este capítulo (ISO, 2019). La subcláusula 8.1 exige planificar y controlar los procesos necesarios para cumplir los requisitos; la 8.2 dispone realizar el análisis de impacto al negocio y la evaluación de riesgos (secciones 2.2 y 2.4); la 8.3 requiere identificar y seleccionar estrategias y soluciones de continuidad (sección 2.5.1); la 8.4 establece los planes y procedimientos de continuidad, con la estructura de respuesta, los procedimientos de alerta y comunicación y los planes de recuperación (secciones 2.5.2 a 2.5.4); la 8.5 exige el programa de ejercicios (sección 2.5.5); y la 8.6 dispone la evaluación de la documentación y las capacidades de continuidad.

Adoptar esta secuencia como columna vertebral tiene una ventaja adicional: garantiza que el plan resultante sea compatible con una eventual certificación futura de la organización y que su estructura sea reconocible para el organismo de control al verificar el cumplimiento de la normativa de riesgo operativo.

2.7. Marcos complementarios y justificación metodológica

2.7.1. Cuadro comparativo de marcos de continuidad

ISO 22301 no es el único referente disponible para planificar la continuidad. La Tabla 6 compara los marcos más utilizados con criterios homogéneos, a fin de fundamentar la elección de un marco principal y de sus complementos. Se incluyen la norma ISO/IEC 27031 de preparación de las TIC (ISO/IEC, 2025), la guía de planificación de contingencias del NIST (NIST, 2010), las Good Practice Guidelines del Business Continuity Institute (Business Continuity Institute [BCI], 2023) y las Prácticas Profesionales del DRI International (DRI International, 2017).

Tabla 6

Comparación de marcos de referencia para la continuidad del negocio

Criterio	ISO 22301:2019	ISO/IEC 27031:2025	NIST SP 800-34 Rev. 1	BCI Good Practice Guidelines	DRII Professional Practices
Naturaleza	Norma internacional de requisitos	Norma internacional de directrices	Guía técnica gubernamental (EE. UU.)	Guía de buenas prácticas profesionales	Guía de prácticas profesionales
Alcance	Toda la organización: productos y servicios	Tecnologías de la información y comunicación	Sistemas de información federales	Toda la organización	Toda la organización
Certificable	Sí	No	No	No (certificación de personas)	No (certificación de personas)
Enfoque de riesgos	Exige BIA y evaluación de riesgos; no prescribe método	Centrado en la preparación de las TIC	Incluye BIA de sistemas	Ciclo de gestión con BIA y evaluación	Ciclo de diez prácticas con BIA y evaluación
Relación con la regulación ecuatoriana	Reconocida como referente por la normativa de riesgo operativo	Complementaria	Referencial	Referencial	Referencial
Adaptabilidad a una cooperativa mediana	Alta: requisitos genéricos y escalables	Alta en el componente tecnológico	Media: orientada a entidades públicas de gran tamaño	Alta	Alta

Criterio	ISO 22301:2019	ISO/IEC 27031:2025	NIST SP 800-34 Rev. 1	BCI Good Practice Guidelines	DRII Professional Practices
Uso habitual	Marco principal	Complemento para la continuidad TIC y el MBCO	Referencia para el DRP	Referencia conceptual	Referencia conceptual

Fuente: Elaboración propia a partir de ISO (2019), ISO/IEC (2025), NIST (2010), BCI (2023) y DRI International (2017).

Del cuadro se desprende que ISO 22301 es el único marco que combina el carácter de norma internacional de requisitos, la aplicabilidad a toda la organización, la posibilidad de certificación y el reconocimiento regulatorio, mientras que los demás aportan profundidad en aspectos específicos: ISO/IEC 27031 en la preparación tecnológica, NIST SP 800-34 en los procedimientos de recuperación de sistemas y las guías profesionales en la práctica operativa. Esta complementariedad explica la práctica extendida de usar ISO 22301 como marco principal e incorporar los otros como referencias en las secciones del plan donde aportan precisión.

2.7.2. Integración de ISO 22301 con MAGERIT

ISO 22301 exige realizar una evaluación de riesgos pero no prescribe la técnica para hacerlo, de modo que la organización debe seleccionar un método reconocido y aplicarlo de manera consistente (ISO, 2019). La combinación de la norma con MAGERIT se fundamenta en cuatro razones. Primera, MAGERIT está diseñada específicamente para riesgos de sistemas de información, que es el ámbito de los servicios digitales. Segunda, su catálogo de activos y amenazas y sus escalas de frecuencia y degradación proporcionan exactamente los insumos que la cláusula 8.2 de ISO 22301 requiere, sin necesidad de construir un método propio. Tercera, es de acceso libre y está documentada en español, lo que facilita su adopción por organizaciones de recursos limitados y su comprensión por los organismos de control. Cuarta, es una metodología de auditoría y seguridad informática con aplicaciones previas en el país que permiten comparar resultados.

La integración opera en dos niveles. En el diagnóstico, MAGERIT aporta el inventario de activos, la identificación de amenazas y la valoración del riesgo que se combinan con el BIA para priorizar los servicios. En el diseño del plan, las salvaguardas identificadas con MAGERIT se traducen en estrategias y soluciones de continuidad según la cláusula 8.3, y los riesgos residuales que permanecen en zona alta o crítica determinan los escenarios para los que se desarrollan procedimientos de respuesta y recuperación según la cláusula 8.4. De este modo, la metodología resultante es la secuencia de la cláusula 8 de ISO 22301 alimentada por el análisis de riesgos de MAGERIT.

2.7.3. Aplicaciones de ISO 22301 y de la continuidad del negocio en instituciones ecuatorianas

La aplicación de ISO 22301 en organizaciones ecuatorianas cuenta con antecedentes documentados en la literatura nacional. Quituisaca-León et al. (2021) analizaron la situación de las micro, pequeñas y medianas empresas de Cuenca frente a la norma y propusieron componentes de un plan de continuidad adaptado a su escala, concluyendo que la ausencia de planificación formal es generalizada en las organizaciones de menor tamaño. En el ámbito cooperativo, Buscán Pinguil et al. (2022) diseñaron, desde la propia Universidad Católica de Cuenca, un modelo de plan de continuidad basado en ISO 22301 para las cooperativas de ahorro y crédito del segmento B del cantón Cañar, que incorpora el análisis de riesgos como etapa previa y confirma la pertinencia de adaptar la norma a entidades de este tipo. En el sector financiero, Rojas Bustamante (2017) propuso un plan de continuidad de negocio para una institución bancaria privada ecuatoriana mediante una metodología de cuatro fases que culmina en el mejoramiento continuo, lo que muestra que los parámetros descritos en la sección 2.4.4 y la secuencia de fases de la norma son transferibles a entidades financieras del país.

Estos trabajos muestran dos constantes: la necesidad de adaptar los requisitos de la norma a organizaciones con equipos de tecnología reducidos, y la conveniencia de anclar el

plan en un análisis de riesgos e impacto documentado en lugar de en percepciones generales de criticidad. También evidencian que el nivel de detalle que exige la normativa de riesgo operativo del sector, parámetros de recuperación y procedimientos específicos por servicio, solo se alcanza cuando el plan se diseña para una entidad concreta y sus servicios digitales.

2.8. Síntesis del capítulo

El marco teórico desarrollado establece la cadena conceptual del diseño de planes de continuidad para servicios digitales financieros. Los servicios digitales de una cooperativa de ahorro y crédito son el resultado de capas tecnológicas y organizacionales dependientes entre sí, cuya interrupción está sujeta a obligaciones regulatorias de continuidad. Esas interrupciones se explican mediante la relación entre activos, amenazas y vulnerabilidades, y se valoran con escalas y matrices que MAGERIT proporciona. La continuidad del negocio, entendida como componente de la resiliencia operativa, responde a ese problema mediante un plan que se fundamenta en el análisis de impacto, del que se derivan los parámetros MTPD, RTO, RPO y MBCO, y en estrategias de continuidad, respuesta y recuperación que deben probarse y mantenerse. ISO 22301:2019 organiza todo ello en un sistema de gestión cuya cláusula 8 proporciona la estructura habitual de los planes, y su combinación con MAGERIT queda fundamentada frente a los marcos alternativos.

CAPÍTULO III

3. MARCO METODOLÓGICO

En este capítulo se describe la estrategia metodológica seguida para cumplir el segundo objetivo específico identificar y analizar los activos tecnológicos y los procesos críticos asociados a los servicios digitales de la Cooperativa de Ahorro y Crédito Yuyay Ltda. y para establecer las bases del tercero, la elaboración del Plan de Continuidad del Negocio. Se exponen el enfoque y el nivel de la investigación, la población y la muestra, las técnicas e instrumentos de recolección, el tratamiento de la información, los resultados de la entrevista y de la revisión documental, su análisis e interpretación y, finalmente, las fases metodológicas que estructuran la propuesta del capítulo IV.

3.1. Enfoque de la investigación

La investigación adopta un enfoque mixto, que combina la recolección y el análisis de datos cualitativos y cuantitativos en un mismo estudio para obtener una comprensión más completa del fenómeno. Se emplea un diseño convergente, en el que ambos tipos de datos se recogen en la misma etapa, se analizan por separado y se integran en la interpretación de los resultados.

La vertiente cualitativa permite comprender cómo se gestiona actualmente la continuidad de los servicios digitales: los procesos operativos, los procedimientos de respaldo y contingencia, la estructura de respuesta ante incidentes, la relación con los proveedores tecnológicos y las directrices institucionales. Sus fuentes son la revisión de los documentos normativos y técnicos de la cooperativa y la entrevista semiestructurada a los responsables de tecnología y de seguridad de la información.

La vertiente cuantitativa permite medir la criticidad de los activos y de los riesgos, y expresar la tolerancia de la organización a la interrupción en magnitudes comparables. Se apoya en la valoración de los activos por dimensiones de seguridad en la escala de 0 a 10 de

MAGERIT (MHAP, 2012a), en el cálculo del nivel de riesgo como producto de la probabilidad por el impacto con las escalas de cinco niveles definidas en el capítulo II, y en la estimación de los parámetros de recuperación MTPD, RTO y RPO expresados en horas, conforme al procedimiento de análisis de impacto de la especificación ISO/TS 22317 (ISO, 2021b).

La integración de ambas vertientes se produce en el análisis e interpretación de los resultados (sección 3.7): los datos numéricos indican dónde se concentra la criticidad, y los datos cualitativos explican por qué y qué capacidades existen para responder a una interrupción.

3.2. Nivel y tipo de la investigación

Por su nivel, la investigación es descriptiva, porque busca especificar las propiedades y características de un fenómeno sin manipular variables (Hernández-Sampieri & Mendoza Torres, 2018). En este caso se describen los servicios digitales de la cooperativa, sus dependencias tecnológicas, los riesgos que pueden interrumpirlos, los controles existentes y la tolerancia institucional a su interrupción.

Por su finalidad, es una investigación aplicada, ya que el conocimiento generado se orienta a resolver un problema práctico de la organización: el diseño de un Plan de Continuidad del Negocio para sus servicios digitales conforme a la norma ISO 22301:2019. Por su diseño, es no experimental y transversal, pues los datos se recogen en un único período, el año 2026, sobre la situación existente. Por su producto, la investigación tiene además un carácter propositivo: el diagnóstico descriptivo sustenta el diseño de una propuesta de intervención, el plan de continuidad, cuya eficacia no se mide en este trabajo. La validación de la propuesta se realiza mediante la revisión de escritorio del plan con sus titulares y suplentes, programada como ejercicio EJ-04, y su aprobación corresponde al Consejo de Administración; el incremento de la eficacia en la recuperación que enuncia el objetivo general es un resultado esperado del diseño, que deberá comprobarse con los ejercicios y los indicadores del plan una vez implementado.

3.3. Población y muestra

La población está constituida por las personas que gestionan u operan los servicios digitales de la COAC Yuyay Ltda. o que son propietarias de los procesos que se prestan a través de ellos, y por la documentación institucional que regula la gestión tecnológica y la seguridad de la información. Según el manual de seguridad de la información y el inventario de activos de la cooperativa, el componente humano comprende los roles del área de Tecnologías de la Información y de Seguridad de la Información, los integrantes del Comité de Seguridad de la Información, los responsables de las áreas de negocio que prestan servicios por canales digitales y los proveedores tecnológicos externos (Cooperativa de Ahorro y Crédito Yuyay Ltda. [COAC Yuyay], s. f., 2024). La Tabla 7 resume la población y la muestra seleccionada.

Tabla 7

Población y muestra de la investigación

Estrato	Integrantes según los documentos	Muestra seleccionada	Criterio de selección
Roles de procesos operativos y técnicos	Personal de tecnologías de la información y de seguridad de la información	Dos informantes	Responsables directos de la operación tecnológica, los respaldos, los cambios, los proveedores y los incidentes
Rol directivo	Alta dirección y comité institucional que supervisa la seguridad de la información	Un informante	Define las prioridades del negocio y aprueba el plan
Propietarios de procesos de negocio	Responsables de las áreas que prestan servicios por canales digitales	Dos informantes	Propietarios de los servicios en las sesiones de análisis de impacto
Proveedores tecnológicos externos	Proveedores de software financiero, infraestructura en la nube, red de tarjetas, monitoreo de seguridad y mantenimiento de cajeros	No se incluyen como informantes	Su información se obtiene de los documentos y contratos de la cooperativa
Documentos institucionales	Manuales, procedimientos, informes y registros de gestión de TI y de seguridad de la información	Seis documentos	Vigentes y relacionados con continuidad, riesgos y activos

Fuente: Elaboración propia a partir de COAC Yuyay (s. f., 2024).

Dado que el diagnóstico requiere conocimiento técnico y estratégico específico, se optó por una muestra no probabilística intencional, en la que los participantes se eligen por su relación directa con el fenómeno estudiado y no por su representatividad estadística (Hernández-Sampieri & Mendoza Torres, 2018). La muestra está conformada por cinco informantes clave. Tres son entrevistados: dos pertenecen a los roles de procesos operativos y técnicos y uno al rol directivo. Los otros dos son propietarios de procesos de negocio que participaron en las sesiones de análisis de impacto. Al tratarse de una muestra intencional, los resultados describen solo la situación de la COAC Yuyay Ltda. y no se generalizan a otras cooperativas.

La unidad de análisis la constituyen ocho servicios digitales y los activos de los que dependen: el core financiero, la web transaccional, la aplicación móvil Yuyay Móvil, los cajeros automáticos, las tarjetas de débito, las transferencias electrónicas y recaudaciones, la infraestructura en la nube con el enlace de Internet, y el monitoreo de seguridad con las carpetas compartidas.

3.4. Técnicas e instrumentos de recolección de información

Se emplearon cuatro técnicas complementarias, cuya relación con los instrumentos, las fuentes y la información obtenida se presenta en la Tabla 8.

Tabla 8

Técnicas, instrumentos y fuentes de información

Técnica	Instrumento	Fuente o informante	Información que aporta	Ubicación
Revisión documental	Ficha de análisis documental	Seis documentos institucionales (Tabla 9)	Estructura, servicios, activos, procesos, políticas, riesgos y controles existentes	Sección 3.6
Entrevista semiestructurada	Guion de 31 preguntas en siete bloques	Coordinador de Sistemas, Oficial de Seguridad de la Información, Gerente General	Historial de interrupciones, controles, respuesta a incidentes, gobernanza y tolerancia a la interrupción	Anexo A

Técnica	Instrumento	Fuente o informante	Información que aporta	Ubicación
Análisis de impacto al negocio	Ficha BIA por servicio digital y matriz de consolidación	Propietarios de los servicios y responsable técnico	Dependencias, impacto en el tiempo, MTPD, RTO, RPO, MBCO y prioridad	Anexo B
Análisis de riesgos	Matriz de valoración MAGERIT con escala de 5 × 5	Inventario de activos e informe de riesgos	Riesgo inherente y residual por activo y amenaza	Capítulo IV

Fuente: Elaboración propia.

La revisión documental se aplicó a los seis documentos que la cooperativa mantiene vigentes sobre gestión tecnológica, seguridad de la información, riesgos y funciones del personal de TI (Tabla 9). Estos documentos permitieron levantar la mayor parte del contexto institucional antes de las entrevistas, de modo que estas se concentraran en confirmar la información documental y en obtener los datos que no constan por escrito.

Tabla 9

Documentos institucionales analizados

Documento	Tipo de documento	Año	Contenido utilizado
Manual institucional de seguridad de la información (2024)	Documento normativo aprobado por el órgano de gobierno	2024	Roles y responsabilidades, Comité de Seguridad de la Información, definiciones de plan de continuidad, RTO y RPO, políticas de respaldo, energía, incidentes y acuerdos de nivel de servicio
Manual institucional de procesos de TI (2026b)	Documento de procesos con actualización periódica	2025 y 2026	17 procesos y procedimientos, entre ellos la ejecución de planes operativos de contingencia, la gestión de riesgos, incidentes y cambios, el control de parches y el control de respaldos de la base de datos
Informe institucional de riesgos de seguridad de la información (2026a)	Informe técnico interno	2026	19 riesgos en canales electrónicos, core financiero, infraestructura y nube, cajeros automáticos y tarjetas de débito, con su nivel y tratamiento
Registro institucional de gestión de riesgos de TI (s. f.)	Libro de cálculo de trabajo	Sin fecha	Inventario de 68 activos valorados por dimensiones; valoraciones de riesgo
Manuales descriptivos de funciones del personal de TI (2019) y (2023)	Documentos de gestión del talento humano	2019 y 2023	Misión, procesos y funciones de los puestos de TI, facultades de decisión y respaldo (back up) designado

Fuente: Elaboración propia a partir de COAC Yuyay (s. f., 2019, 2023, 2024, 2026a, 2026b).

La entrevista semiestructurada (Anexo A) se organizó en siete bloques: contexto institucional y servicios digitales; dependencias tecnológicas y proveedores; historial de interrupciones; controles de continuidad existentes; respuesta a incidentes y comunicación; tolerancia a la interrupción; y gobernanza, recursos y cultura. La ficha de análisis de impacto (Anexo B) se aplica a cada servicio digital en una sesión conjunta con su propietario y con el responsable técnico, y recoge las actividades, las dependencias con su código de inventario, el impacto según la duración de la interrupción y los parámetros de recuperación.

La validez de contenido de ambos instrumentos se aseguró por dos vías: su construcción a partir de los requisitos de la cláusula 8.2 de ISO 22301:2019 (ISO, 2019) y del procedimiento de ISO/TS 22317 (ISO, 2021b); y la correspondencia explícita de cada bloque de preguntas con los objetivos específicos y con la norma (Anexo A, sección A.5).

La aplicación de los instrumentos contó con la autorización de la cooperativa y con el consentimiento informado de cada participante, garantizando la confidencialidad de la información y su uso exclusivamente académico.

3.5. Tratamiento de la información

La información cualitativa se trató mediante categorías de análisis definidas a priori, que corresponden a los bloques del guion de entrevista (Tabla 10). Las entrevistas se grabaron con autorización, se transcribieron y se codificaron según esas categorías; la evidencia documental se organizó con las mismas categorías, lo que permitió contrastar lo que establecen los documentos con lo que describen los informantes.

Tabla 10

Categorías de análisis y criterios de tratamiento

Categoría	Indicadores	Fuentes	Tratamiento
Servicios digitales y dependencias	Servicios, canales, activos de soporte y proveedores	Inventario, manual de procesos, entrevista (bloques A y B)	Descripción y mapa de dependencias
Riesgos de interrupción	Amenazas, nivel de riesgo, frecuencia de interrupciones	Informe de riesgos, inventario, entrevista (bloque C)	Conteo por nivel y ámbito; revaloración con escala de 5 × 5
Capacidades de continuidad	Respaldos, redundancias, DRP, pruebas, contingencia	Manual de procesos, manual de seguridad, entrevista (bloque D)	Contraste con las cláusulas 8.3 y 8.5 de ISO 22301
Respuesta y comunicación	Estructura de respuesta, escalamiento, comunicación	Manual de procesos, manual de seguridad, entrevista (bloque E)	Contraste con la cláusula 8.4
Tolerancia a la interrupción	MTPD, RTO, RPO, MBCO y prioridad	Fichas BIA, entrevista (bloque F)	Consolidación numérica y regla de determinación del MTPD
Gobernanza y recursos	Roles, comité, presupuesto, capacitación, capacidad de procesos	Manual de seguridad, inventario, entrevista (bloque G)	Contraste con las cláusulas 5 y 7

Fuente: Elaboración propia.

La información cuantitativa se tabuló en hojas de cálculo. Para cada servicio, el MTPD se determinó como la primera duración de interrupción en la que el impacto alcanza el nivel 4 (Mayor) de la Tabla 3, y se verificó que el RTO fuera menor que el MTPD y que el RPO fuera coherente con la frecuencia real de los respaldos.

El libro de gestión de riesgos de la cooperativa emplea dos escalas distintas de probabilidad una de cinco niveles y otra, asociada a MAGERIT, de tres y el informe de riesgos de 2026 utiliza niveles verbales (moderado, alto y extremo). Para garantizar la comparabilidad, los riesgos se revaloran en el capítulo IV con la escala única de cinco niveles de probabilidad e impacto y la matriz de cuatro zonas del capítulo II (Tablas 2 y 3, Ilustración 2) (IEC, 2019; MHAP, 2012a); las valoraciones institucionales se conservan como antecedente.

Finalmente, los resultados se triangularon entre fuentes documentos, entrevistas y fichas BIA, de modo que un hallazgo se considera confirmado cuando al menos dos fuentes lo sustentan (Creswell & Plano Clark, 2018).

3.6. Resultados de la entrevista y de la revisión documental

Esta sección presenta los resultados organizados según los bloques del guion de entrevista. En cada bloque se expone primero lo que establecen los documentos institucionales y después lo que aportan los informantes. Las respuestas completas constan en el Anexo A y las fichas de análisis de impacto en el Anexo B.

3.6.1. Aplicación de los instrumentos

Tabla 11

Informantes entrevistados

Código	Cargo	Fecha	Duración	Bloques aplicados
E1	Coordinador de Sistemas	24 de septiembre de 2026	45 min	A, B, C, D, E, F y G
E2	Oficial de Seguridad de la Información	24 de septiembre de 2026	45 min	B, C, D, E y G
E3	Gerente General	24 de septiembre de 2026	45 min	A, F y G
BIA	Propietarios de los servicios y Coordinador de Sistemas (responsable técnico)	1 de octubre de 2026	Sin dato	Fichas SD-01 a SD-08

Fuente: Elaboración propia.

La entrevista al Coordinador de Sistemas, informante principal por responder los siete bloques, se realizó el 24 de septiembre de 2026, a partir de las 08:44 y con una duración de 45 minutos; ese mismo día se entrevistó a la Oficial de Seguridad de la Información y al Gerente General. El 1 de octubre de 2026 se desarrolló la sesión de análisis de impacto, en la que los propietarios de los servicios y el Coordinador de Sistemas, como responsable técnico, completaron las ocho fichas del Anexo B. Para agilizar la sesión, cada ficha se presentó prellenada con la evidencia documental y con valores de MTPD, RTO, RPO, MBCO y prioridad propuestos como hipótesis de trabajo; los participantes valoraron el impacto por duración con la escala de la Tabla 3 y confirmaron o ajustaron cada valor. Esta forma de aplicación tiene dos limitaciones que se reconocen: los valores validados coincidieron en las ocho fichas con las hipótesis presentadas, lo que puede reflejar un sesgo de anclaje, y las fichas no cuentan

con la firma de los participantes ni con un acta de la sesión, por lo que la validación se sustenta en el registro del investigador. Por ello, el plan dispone que el Comité ratifique los parámetros del análisis de impacto y deje constancia en acta antes de la aprobación del plan. Las respuestas de los informantes se consolidaron por pregunta en el Anexo A, y en adelante se citan con el código de la pregunta.

3.6.2. Contexto institucional y servicios digitales

La COAC Yuyay Ltda. es una cooperativa de ahorro y crédito sujeta al control de la Superintendencia de Economía Popular y Solidaria, que opera en un entorno rural y agrícola del cantón Cañar. Su oficina matriz se ubica en la comunidad San Rafael y cuenta con oficinas en el Terminal Terrestre de Cañar, en El Tambo y en Suscal (COAC Yuyay, 2024). En su estructura organizacional, la unidad de Tecnologías de la Información y Comunicación se ubica dentro del área Financiera, junto a Tesorería, Contabilidad y Cajas, bajo la Gerencia General (COAC Yuyay, s. f.).

Los servicios digitales que la cooperativa presta a sus socios son la aplicación móvil Yuyay Móvil, la web transaccional y los cajeros virtuales agrupados como canales electrónicos, dos cajeros automáticos, las tarjetas de débito operadas sobre la red del proveedor COONECTA, la aplicación de recaudaciones y las transferencias electrónicas con autenticación de dos factores (COAC Yuyay, s. f., 2024).

Según el Coordinador de Sistemas, la cooperativa tiene alrededor de 9.800 socios activos y se ubica en el segmento 3 de la SEPS (Anexo A, A1). Los servicios digitales se incorporaron de forma progresiva: los cajeros automáticos y las tarjetas de débito en 2018, la web transaccional en 2019, las transferencias interbancarias por el Sistema de Pagos Interbancarios (SPI) en 2020 y la aplicación móvil en 2021; las transferencias y el pago de servicios se prestan desde la misma aplicación de recaudaciones, por lo que se tratan como un solo servi-

cio (Anexo A, A2). El core financiero concentra el mayor número de operaciones, porque registra las de todos los canales; entre los canales digitales, la aplicación móvil es el de mayor uso y la web transaccional el de menor uso. La demanda aumenta en las fechas de pago y en la temporada agrícola de la zona (Anexo A, A3). Las cifras de transacciones por canal y los horarios de mayor uso se omiten por confidencialidad institucional. Alrededor del 35 % de las operaciones se realiza por canales digitales, frente a cerca del 20 % hace dos años, crecimiento impulsado por la aplicación móvil (Anexo A, A4).

Estos datos tienen dos implicaciones para el plan. La creciente proporción digital eleva el impacto de una interrupción de los canales sobre la relación con los socios. Y el período de mayor uso de los canales digitales coincide con el momento en que se descarga el respaldo diario, de modo que las transacciones de ese período son las que más tiempo permanecen sin respaldo.

3.6.3. Dependencias tecnológicas y proveedores

Todos los servicios digitales dependen del core financiero Vimacoop/VimaSistem y de su base de datos Oracle, gestionados mediante la plataforma Vimagest y alojados en infraestructura de Oracle Cloud (OCI) administrada por el proveedor; los parches de estos componentes los ejecuta el contratista y la cooperativa los coordina mediante tickets (COAC Yuyay, 2026b). A ello se suman el enlace de Internet, que soporta los canales electrónicos, la nube y la red de pagos; el firewall perimetral; la red interna; el centro de datos con servidores locales, almacenamiento NAS, sistemas de alimentación ininterrumpida, generador y climatización; y el servicio externo de monitoreo de seguridad SOC/SIEM (COAC Yuyay, s. f.). Cinco proveedores externos sostienen componentes críticos: el del core financiero, el de la infraestructura en la nube, COONECTA para las tarjetas de débito, el del SOC y el de mantenimiento de los cajeros.

Aunque la política institucional exige que los contratos con terceros incluyan acuerdos de nivel de servicio (COAC Yuyay, 2024), el informe de riesgos de 2026 califica como extremos la falta de redundancia o de un DRP probado del core financiero y la ausencia de un plan de salida con su proveedor, y como altos la falta de certificaciones del proveedor de nube y la falta de un SLA en la red de tarjetas (COAC Yuyay, 2026a). La política exige además energía de respaldo con autonomía mínima de ocho horas, mientras que el inventario registra un único enlace de Internet (COAC Yuyay, s. f., 2024). Se observa también una discrepancia entre fuentes: el inventario ubica el core y el servidor de base de datos en el centro de datos propio, mientras el manual de procesos señala que operan en OCI bajo administración del proveedor; la entrevista permitió resolverla.

El Coordinador de Sistemas confirmó que el core y su base de datos operan en OCI administrados por el contratista, y que en el centro de datos local permanecen el almacenamiento NAS con los respaldos descargados, los servidores de dominio y de archivos y los equipos de comunicaciones (Anexo A, B1). Además de los cinco proveedores identificados en los documentos, el operador de telecomunicaciones del enlace de Internet es un sexto tercero crítico (Anexo A, B2). Los tiempos pactados no guardan relación con la criticidad de los servicios: el contrato del core fija un tiempo máximo de restablecimiento de 24 horas, sin penalizaciones ni plan de salida; el contratista de OCI tiene un tiempo de respuesta de 8 horas; el enlace de Internet, un tiempo de reparación de 6 horas; el SOC, 4 horas para alertas críticas; y COONECTA no tiene un acuerdo de disponibilidad. La cooperativa no ha revisado los planes de continuidad de ninguno de sus proveedores (Anexo A, B3). En cuanto a redundancia, existe un único enlace de Internet, aunque está en curso la contratación de un segundo enlace con otro operador; cinco UPS con autonomía aproximada de 30 minutos y un generador

con autonomía medida de 12 horas cubren el centro de datos y las áreas de atención de la Matriz, mientras que las agencias solo disponen de UPS; y no hay redundancia de servidores locales (Anexo A, B4).

3.6.4. Historial de interrupciones

Los documentos no contienen un registro de interrupciones de los servicios digitales. Los indicadores del manual de procesos ofrecen una aproximación: el tiempo promedio de resolución de incidentes tiene una línea base de 30 horas frente a una meta de 24, el tiempo de primera respuesta de 4 horas frente a una meta de 2, y el tiempo medio entre fallas de 120 horas frente a una meta de 200 (COAC Yuyay, 2026b). El ejercicio de *ethical hacking* de 2024 detectó y corrigió vulnerabilidades en la aplicación móvil instalación en versiones de Android sin soporte, tráfico en texto claro y cifrado vulnerable (COAC Yuyay, s. f.), sin que conste que hayan provocado interrupciones.

El Coordinador de Sistemas identificó en el gestor de incidentes cuatro eventos relevantes de los dos últimos años (Anexo A, C1). En marzo de 2025, un corte de fibra del operador dejó sin enlace de Internet a todos los canales electrónicos y al acceso al core durante unas 6 horas, y la ventanilla atendió con registro manual y digitación posterior. En agosto de 2025, una actualización fallida del proveedor dejó la aplicación móvil fuera de servicio unas 3 horas, hasta que se revirtió la versión. En enero de 2026, una falla del dispensador mantuvo fuera de servicio el cajero de la Matriz durante dos días. Y en julio de 2026, un corte eléctrico de 2 horas en la Matriz fue cubierto por las UPS y el generador sin afectar el servicio. El evento de marzo de 2025 fue el más largo y de mayor impacto: ocurrió en horario de atención, generó reclamos en las agencias y en redes sociales y obligó a una conciliación que tomó un día adicional, aunque no derivó en sanción ni requerimiento de la SEPS (Anexo A, C2). A ello se suman entre dos y tres caídas breves al mes, de 5 a 20 minutos, en la aplicación

móvil y la web, asociadas a mantenimientos del proveedor o a microcortes del enlace, y alrededor de una caída breve mensual en los cajeros (Anexo A, C3). No se ha producido ningún incidente de seguridad que interrumpa los servicios (Anexo A, C4).

El historial muestra que, hasta ahora, las interrupciones no se han originado en ciberataques, sino en la conectividad, en los cambios del proveedor y en fallas de equipos, que son precisamente los ámbitos donde los documentos registran un enlace único, una gestión de cambios débil y la ausencia de acuerdos de servicio.

3.6.5. Controles de continuidad existentes

El respaldo de la base de datos institucional se genera de forma automática y diaria mediante Vimagest; el Área de Sistemas verifica su estado cada día, lo descarga al cierre de la jornada, lo almacena en el repositorio institucional y conserva además un respaldo mensual y uno anual. El mismo procedimiento programa pruebas trimestrales de restauración y pruebas semestrales de sitios alternos y de enlaces de datos (COAC Yuyay, 2026b). Sin embargo, el inventario declara pendientes la prueba de restauración y la copia en sitio alterno, y el informe de riesgos registra la ausencia de copias fuera del sitio como un riesgo alto (COAC Yuyay, s. f., 2026a), pese a que la política exige el transporte seguro de los respaldos a un sitio alterno que no esté expuesto a los mismos riesgos del principal (COAC Yuyay, 2024).

Estas obligaciones no son nuevas. Desde 2019, el manual descriptivo de funciones asigna al Jefe de Sistemas denominación del cargo que los documentos posteriores y la entrevista llaman Coordinador de Sistemas instalar un servidor espejo dentro o fuera de la institución, generar respaldos de la base de datos en disco local, externo y en la nube, y contratar un respaldo de la comunicación de datos «para mantener la continuidad de negocio» (COAC Yuyay, 2019). Las brechas de respaldo y conectividad no se deben, por tanto, a la falta de definición de las tareas, sino a su falta de ejecución.

No existe un plan de continuidad del negocio integral y aprobado. Existen componentes dispersos: las definiciones de plan de continuidad, plan de contingencia, RTO y RPO, y el objetivo de disponer de un plan de contingencia de tecnología, en el manual de seguridad (COAC Yuyay, 2024); y el proceso de ejecución de los planes operativos de contingencia del centro de cómputo, en el manual de procesos (COAC Yuyay, 2026b).

La entrevista precisó la retención de los respaldos 30 diarios, 12 mensuales y los anuales de forma permanente, todos almacenados en el centro de datos de la Matriz y confirmó que no existe copia fuera del sitio (Anexo A, D1). La última restauración documentada se realizó en marzo de 2026 sobre el ambiente de pruebas y tomó alrededor de 3,5 horas hasta dejar operativo el core; desde entonces no se ha documentado otra y nunca se ha probado la recuperación en un sitio alterno, por lo que la periodicidad trimestral del procedimiento no se está cumpliendo (Anexo A, D2). El DRP del proveedor del core existe como anexo del contrato, pero la cooperativa nunca lo ha visto ejecutado (Anexo A, D3). Los modos de operación degradada consulta con el último saldo disponible, registro manual de depósitos y retiros de montos pequeños con digitación posterior, cajeros fuera de línea y transferencias diferidas al siguiente ciclo se aplican por práctica, sin estar documentados ni probados (Anexo A, D5).

3.6.6. Respuesta a incidentes y comunicación

El proceso de contingencia establece una secuencia: el Oficial de Seguridad Física y Electrónica notifica el incidente al Coordinador de TI y al Oficial de Seguridad de la Información; el Coordinador evalúa la gravedad y decide si se activa el plan de contingencia; el Oficial de Seguridad Física y Electrónica coordina la solución con las áreas y los proveedores, comunica el incidente al Comité de Continuidad, ejecuta el plan y remite un informe final con las causas, las acciones tomadas y las medidas de prevención (COAC Yuyay, 2026b). La gestión de incidentes y problemas añade clasificación, escalamiento y análisis de causa raíz.

No se documentan procedimientos de comunicación a los socios ni de notificación al organismo de control durante una interrupción.

En la práctica, la detección la realiza el personal de ventanilla o el monitoreo del SOC; el Coordinador de Sistemas decide y autoriza las acciones de recuperación, y la Gerencia General es informada cuando la interrupción supera una hora (Anexo A, E1). El Comité de Seguridad de la Información sesiona trimestralmente y de forma extraordinaria cuando se requiere; ha dispuesto la contratación del SOC y aprobado el procedimiento de respaldos, pero el desarrollo del plan de continuidad sigue pendiente en su plan de trabajo (Anexo A, E2). Los socios reciben avisos por el WhatsApp institucional, la página de Facebook y carteles en las agencias; el personal, por correo y por el grupo de WhatsApp de TI; y los proveedores, por contacto directo. No existen mensajes predefinidos ni un procedimiento de notificación a la SEPS, y hasta la fecha no se ha notificado formalmente ninguna interrupción al organismo de control (Anexo A, E3). Tras cada incidente se elabora un informe de ejecución con causas, acciones y medidas de prevención, que se registra en el gestor de incidentes y que revisan la Oficial de Seguridad de la Información y el Comité (Anexo A, E4). La práctica difiere de lo documentado en dos puntos: la detección, que el proceso asigna al Oficial de Seguridad Física y Electrónica, proviene de la ventanilla o del SOC; y el umbral de una hora para informar a la Gerencia no consta en ningún documento.

3.6.7. Tolerancia a la interrupción

Los documentos definen el RTO y el RPO, pero no fijan valores para ningún servicio (COAC Yuyay, 2024). La única magnitud que puede deducirse es la capacidad actual de recuperación de datos: al generarse un respaldo diario sin réplica documentada, la pérdida posible ante una falla de la base de datos es de hasta 24 horas de transacciones. Como referencia de criticidad, el inventario asigna el valor de disponibilidad 10 a los canales electrónicos, al servidor de base de datos, a la conexión a Internet, a la red interna, al firewall y al centro de

datos, y el valor 9 al core financiero, la nube, la web transaccional, las tarjetas de débito y los cajeros (COAC Yuyay, s. f.).

Los propietarios de los servicios fijaron el tiempo máximo tolerable de interrupción en 8 horas para el core financiero, la infraestructura en la nube con el enlace de Internet y las tarjetas de débito, porque una jornada sin core es inaceptable por el riesgo regulatorio y los reclamos, y porque los socios dependen de la tarjeta fuera del cantón; en 24 horas para la aplicación móvil, la web transaccional, las transferencias y recaudaciones y los cajeros automáticos, que pueden suplirse por la ventanilla o por el segundo cajero durante un día; y en 72 horas para el monitoreo de seguridad y las carpetas compartidas (Anexo A, F1). Los tiempos objetivo de recuperación son de 4, 8 y 24 horas para esos mismos grupos (Anexo A, F2). La cooperativa puede tolerar la pérdida de hasta 1 hora de transacciones del core y de los canales que dependen de él; las transacciones más difíciles de reconstruir serían las de cajeros y tarjetas no conciliadas con COONECTA y las transferencias SPI enviadas sin confirmación (Anexo A, F3). Durante una interrupción deben mantenerse, como mínimo, la consulta de saldos, los depósitos y retiros de montos pequeños con registro manual, el bloqueo de tarjetas por vía telefónica y la comunicación a los socios (Anexo A, F4). El orden de recuperación que proponen los informantes coincide con las dependencias técnicas: primero la infraestructura en la nube, el enlace y el core; luego las tarjetas de débito; después la aplicación móvil y la web; a continuación las transferencias y recaudaciones y los cajeros; y, al final, el monitoreo de seguridad y las carpetas compartidas (Anexo A, F5).

3.6.8. Gobernanza, recursos y cultura

El Comité de Seguridad de la Información, integrado por la presidenta del Comité, el Gerente General, el Coordinador de Sistemas, el Auditor Informático y la Oficial de Seguridad de la Información, tiene entre sus funciones supervisar el desarrollo y mantenimiento del

plan de continuidad, y el manual lo denomina también Comité de Seguridad de la Información y Continuidad del Negocio (COAC Yuyay, 2024). El inventario registra un titular por cada rol del área de TI, sin suplentes designados, y el informe de riesgos dirige recomendaciones a un Oficial de Continuidad del Negocio que no figura en la estructura documentada (COAC Yuyay, s. f., 2026a). Los recursos del procedimiento de respaldos se enumeran sin montos asignados (COAC Yuyay, 2026b).

No existen suplentes formales: el Ingeniero de Sistemas actúa de hecho como suplente del Coordinador de Sistemas y el Auditor Informático apoya a la Oficial de Seguridad de la Información; el rol de Oficial de Continuidad del Negocio no existe (Anexo A, G1). Tampoco hay una partida presupuestaria de continuidad: en el último año se aprobaron el segundo enlace de Internet y la renovación de las UPS, y se postergaron por costo el sitio alterno, la réplica de la base de datos y las pruebas de DRP con el proveedor (Anexo A, G2). El personal recibe una capacitación anual en seguridad de la información, pero no se han realizado simulacros ni pruebas de continuidad (Anexo A, G3). En su revisión de 2025, la SEPS observó la falta de un plan de contingencia probado y de respaldos fuera del sitio, observación que la auditoría interna reiteró en su informe anual y que se encuentra en proceso de atención (Anexo A, G4). Como obstáculos para implementar el plan, los informantes señalaron el presupuesto limitado, la dependencia de proveedores sin controles contractuales suficientes, un área de TI de solo tres personas y la debilidad de la gestión de acuerdos de servicio, proveedores, disponibilidad y cambios; y como apoyos necesarios, tiempo asignado al área de TI, presupuesto para el segundo enlace, la réplica de la base de datos y las pruebas de DRP, y la aprobación de la política y del plan por el Consejo de Administración (Anexo A, G5).

Los manuales descriptivos de funciones confirman y precisan estas carencias. El del Jefe de Sistemas define como misión del cargo «administrar y garantizar la continuidad y

buen funcionamiento de los recursos informáticos», le asigna la función de establecer los planes de continuidad de negocios, lo faculta para actuar de inmediato ante fallas tecnológicas que puedan frenar las operaciones y para verificar el cumplimiento normativo de los proveedores tecnológicos, y establece que supervisa a dos asistentes de TI; lo ubica, además, en el área Administrativa, mientras el organigrama sitúa a TIC en el área Financiera (COAC Yuyay, 2019). El del Asistente de Tecnologías de la Información le asigna el soporte al core financiero, la administración de los accesos a la base de datos y el monitoreo de vulnerabilidades en las consolas del firewall y del antivirus (COAC Yuyay, 2023). En ambos manuales el campo de respaldo (back up) del cargo está vacío, lo que confirma documentalmente la ausencia de suplentes designados, y ninguno menciona el rol de Oficial de Continuidad.

3.6.9. Resultados de las fichas de análisis de impacto

La Tabla 12 consolida los parámetros de recuperación obtenidos para los ocho servicios digitales en las sesiones de análisis de impacto (Anexo B). La última columna registra la capacidad actual que consta en los documentos, para contrastarla con los parámetros definidos por los propietarios de cada servicio.

Tabla 12

Parámetros de recuperación por servicio digital

Cód.	Servicio digital	MTPD (h)	RTO (h)	RPO (h)	MBCO	Prior.	Capacidad actual documentada
SD-01	Core financiero	8	4	1	Ventanilla con consultas y registro diferido de depósitos y retiros	1	RPO real ≤ 24 h; restauración en pruebas: 3,5 h; contrato: 24 h; DRP no probado
SD-02	Web transaccional	24	8	1*	Consultas de saldo	3	Depende de SD-01 y SD-07
SD-03	Aplicación móvil Yuyay Móvil	24	8	1*	Consultas de saldo	3	Depende de SD-01 y SD-07
SD-04	Cajeros automáticos	24	8	N/A	Un cajero operativo o retiro en ventanilla	5	Dos equipos; sin SLA de mantenimiento; falla de dos días en enero de 2026

Cód.	Servicio digital	MTPD (h)	RTO (h)	RPO (h)	MBCO	Prior.	Capacidad actual documentada
SD-05	Tarjetas de débito (COONECTA)	8	4	Según proveedor	Bloqueo de tarjetas y retiro en ventanilla	2	Sin SLA de disponibilidad con COONECTA
SD-06	Transferencias electrónicas y recaudaciones	24	8	1*	Depósitos en ventanilla con registro diferido	4	Depende de SD-01
SD-07	Infraestructura en la nube y enlace de Internet	8	4	N/A	Conectividad mínima para ventanilla y core	1	Enlace único (reparación: 6 h); OCI: respuesta en 8 h; generador: 12 h
SD-08	Monitoreo de seguridad y carpetas compartidas	72	24	24	Alertas críticas atendidas por TI	6	SOC: respuesta en 4 h; sin métricas de detección

Nota: * = hereda el RPO del core financiero; N/A = el servicio no almacena transacciones propias, que registra el core. Fuente: Elaboración propia a partir de las fichas BIA (Anexo B), de la entrevista (Anexo A) y de COAC Yuyay (s. f., 2026a, 2026b).

Los resultados distinguen tres grupos. El core financiero, la infraestructura en la nube con el enlace de Internet y las tarjetas de débito tienen el MTPD más corto, 8 horas, y un RTO de 4 horas; la aplicación móvil, la web transaccional, las transferencias y recaudaciones y los cajeros toleran hasta 24 horas, con un RTO de 8 horas; y el monitoreo de seguridad con las carpetas compartidas tolera 72 horas. En todos los casos el RTO es menor que el MTPD, como exige la definición de ambos parámetros. La dimensión operativa se valoró con los rangos de duración de la Tabla 3, que suman un nivel cuando la interrupción afecta a toda la institución o a varios canales; por eso el core, la nube con el enlace y las tarjetas de débito, cuya caída detiene todos los canales y la ventanilla, alcanzan el nivel 4 a las 8 horas, mientras que un canal aislado, como la web o la aplicación móvil, lo alcanza a las 24 horas. La dimensión financiera se valoró con los umbrales relativos de la misma tabla, expresados como porcentaje del margen financiero mensual, lo que permite reproducir la valoración sin divulgar cifras de la cooperativa.

El contraste con la capacidad actual revela tres brechas: un RPO requerido de 1 hora frente a una pérdida posible de hasta 24 horas con el respaldo diario; un tiempo de restablecimiento de 24 horas pactado con el proveedor del core, que triplica el MTPD de 8 horas; y un tiempo de reparación del enlace de 6 horas, superior al RTO de 4 horas del servicio del que dependen todos los demás. La restauración de 3,5 horas lograda en el ambiente de pruebas indica que el RTO del core de 4 horas solo es alcanzable si la detección del incidente y la decisión de activar la recuperación toman menos de 30 minutos y la falla no afecta antes a la conectividad; en cualquier otro caso, la recuperación completa queda entre el RTO y el MTPD de 8 horas, lo que exige una solución más rápida que la restauración, como una réplica en espera.

3.7. Análisis e interpretación de los resultados

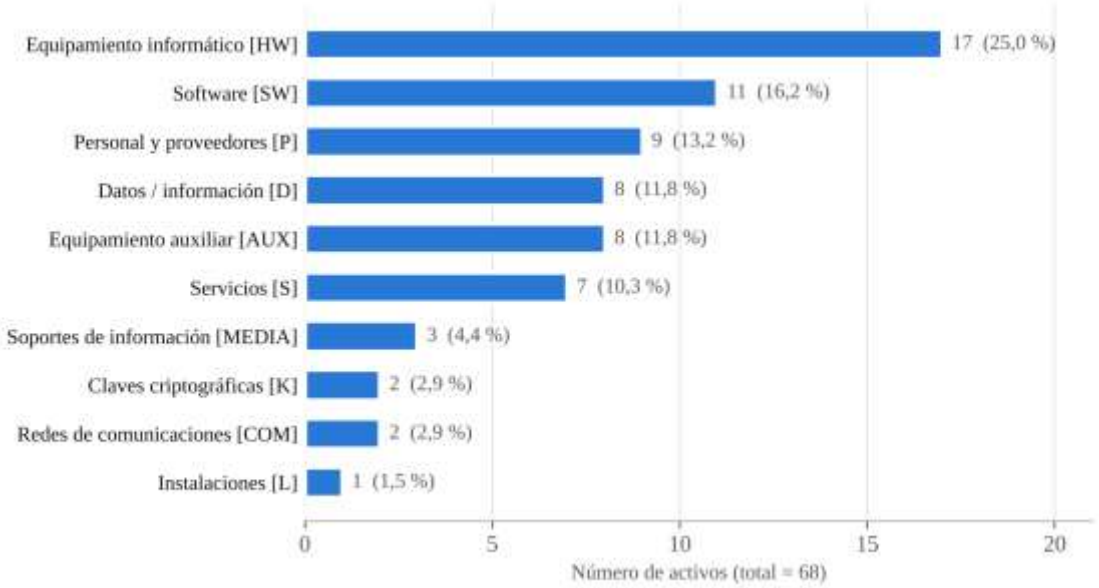
En esta sección se integran los resultados cuantitativos y cualitativos para caracterizar la criticidad de los activos, los riesgos que amenazan la continuidad y la situación de la cooperativa frente a los requisitos de ISO 22301:2019.

3.7.1. Activos tecnológicos y su criticidad

El inventario de la cooperativa identifica 68 activos clasificados según el catálogo de elementos de MAGERIT v3 (MHAP, 2012b). Predominan el equipamiento informático (17), el software (11), el personal y los proveedores (9), los datos y el equipamiento auxiliar (8 cada uno) y los servicios (7) (Ilustración 5). El 72,1 % de los activos (49) tiene un valor global muy alto o crítico (9 a 10), el 17,6 % (12) un valor alto y el 10,3 % (7) un valor medio; ninguno se valora como bajo o despreciable (COAC Yuyay, s. f.).

Ilustración 5

Distribución de los activos tecnológicos por categoría MAGERIT



Fuente: Elaboración propia a partir de COAC Yuyay (s. f.).

La concentración de valores críticos indica que la valoración institucional discrimina poco entre activos y que, por sí sola, no basta para priorizar la recuperación, puesto que casi todo aparece como crítico. Este resultado confirma la necesidad del análisis de impacto, que ordena los servicios según la evolución temporal del daño y no según una valoración estática (ISO, 2021b). Para el plan, el análisis se delimita a los servicios digitales y a los activos de los que dependen (Tabla 13).

Tabla 13

Activos de soporte de los servicios digitales y su valoración de disponibilidad

Código	Activo	Administración	D	Valor global
ACT-S-04	Canales electrónicos	Área de TI; nube y centro de datos	10	10
ACT-S-03	Web transaccional	Área de TI	9	9
ACT-SW-01	Aplicación móvil Yuyay Móvil	Área de TI; soporte del proveedor del core	8	10
ACT-SW-02	Core financiero (Vimacoop/VimaSistem)	Proveedor del core	9	9
ACT-SW-08	Servidor de base de datos	Proveedor del core	10	10
ACT-D-02	Bases de datos de los sistemas	Área de TI	9	10
ACT-D-04	Copias de respaldo de bases de datos	Coordinador de Sistemas	9	9
ACT-S-02	Servidores en la nube	Proveedor de nube	9	9

Código	Activo	Administración	D	Valor global
ACT-S-05	Servicio de tarjetas de débito	COONECTA	9	10
ACT-HW-15/16	Cajeros automáticos 1 y 2	Área de TI; mantenimiento externo	9	9
ACT-SW-06	Aplicación de recaudaciones	Área de TI	9	9
ACT-S-01	Orquestador de servicios	Área de TI	9	9
ACT-COM-02	Conexión a Internet	Área de TI (enlace único)	10	10
ACT-HW-13	Firewall perimetral	Área de TI	10	10
ACT-L-01	Centro de datos	Oficial de Seguridad Física y Electrónica	10	10
ACT-S-07	Monitoreo de seguridad (SOC/SIEM)	Proveedor del SOC	8	9

Nota: D = valoración de la dimensión de disponibilidad en escala de 0 a 10. Fuente: Elaboración propia a partir de COAC Yuyay (s. f.).

3.7.2. Riesgos que afectan la continuidad

El informe de riesgos de 2026 identifica 19 riesgos en cinco ámbitos: 5 de nivel extremo, 7 de nivel alto y 7 de nivel moderado (COAC Yuyay, 2026a), distribuidos como se muestra en la Tabla 14 y en la Ilustración 6.

Tabla 14

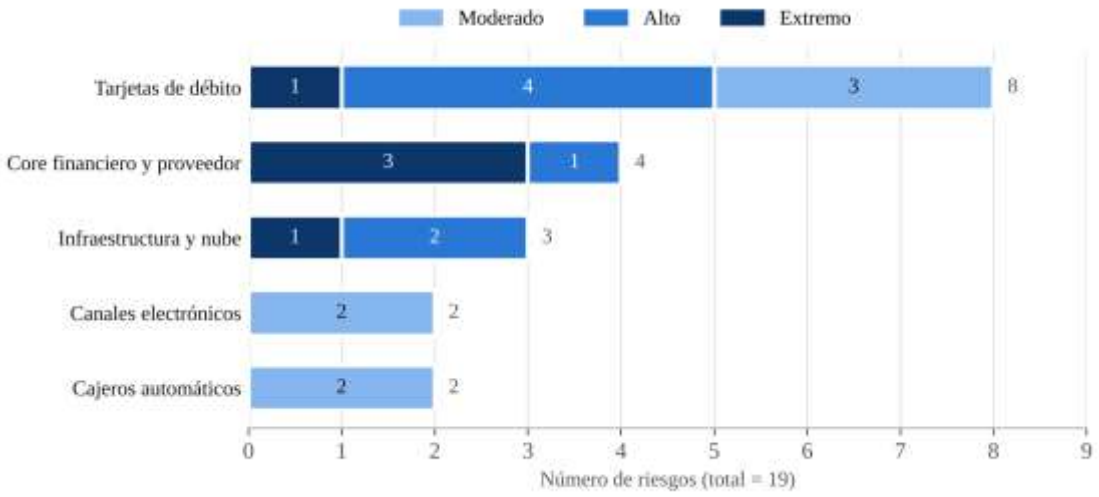
Riesgos identificados por ámbito y nivel

Ámbito	Extremo	Alto	Moderado	Total	Efecto directo sobre la disponibilidad
Canales electrónicos	0	0	2	2	
Core financiero y su proveedor	3	1	0	4	R23, R24, R26, R28
Infraestructura tecnológica y nube	1	2	0	3	
Cajeros automáticos	0	0	2	2	R32
Tarjetas de débito	1	4	3	8	TD-05
Total	**5**	**7**	**7**	**19**	**6 riesgos**

Fuente: Elaboración propia a partir de COAC Yuyay (2026a).

Ilustración 6

Riesgos identificados por ámbito y nivel



Fuente: Elaboración propia a partir de COAC Yuyay (2026a).

Seis de los 19 riesgos tienen un efecto directo sobre la disponibilidad de los servicios: la interrupción total de las operaciones financieras (R23), la pérdida o corrupción de datos (R24), el fallo por cambios no controlados (R26), la pérdida de acceso al sistema tras la terminación del contrato con el proveedor (R28), la falta de dispensación de efectivo (R32) y la indisponibilidad del servicio de tarjetas (TD-05). Tres de ellos son de nivel extremo y los tres se concentran en el core financiero y en la relación con su proveedor, lo que coincide con la conclusión del propio informe: la continuidad del core es el punto de mayor criticidad, porque su paralización arrastra a las tarjetas de débito, a los canales electrónicos y a los cajeros (COAC Yuyay, 2026a). Los otros dos riesgos extremos (R29 y TD-06) afectan sobre todo a la confidencialidad, por lo que corresponde tratarlos en el sistema de seguridad de la información más que en el plan de continuidad, salvo que deriven en una interrupción.

El libro de riesgos de la cooperativa contiene además una valoración por activo y amenaza con la codificación de MAGERIT para nueve activos; entre las amenazas de nivel crítico figuran la denegación de servicio y la difusión de software dañino sobre el core financiero, la avería de origen físico o lógico de los servidores en la nube y la indisponibilidad del sistema en las aplicaciones (COAC Yuyay, s. f.). Esa valoración presenta inconsistencias pro-

babilidades fuera de la escala declarada, productos mal calculados y amenazas sin denominación, por lo que se utiliza como antecedente y no como resultado; los riesgos se revaloran en el capítulo IV con la escala única descrita en la sección 3.5.

3.7.3. Situación frente a los requisitos de ISO 22301:2019

La Tabla 15 contrasta la evidencia obtenida con los requisitos de las cláusulas 4 a 10 de la norma (ISO, 2019). Se califica como «parcial» el requisito con evidencia incompleta y como «no evidenciado» el que carece de evidencia.

Tabla 15

Situación de la cooperativa frente a los requisitos de ISO 22301:2019

Cláusula	Evidencia en la cooperativa	Estado	Brecha principal
4. Contexto de la organización	Estructura organizacional, marco normativo (SEPS, LOPDP) y proveedores identificados en el manual de seguridad y el inventario	Parcial	No se ha definido el alcance del sistema de continuidad ni los requisitos de las partes interesadas
5. Liderazgo	Comité de Seguridad de la Información y Continuidad del Negocio con función de supervisar el plan, que sesiona trimestralmente; manual aprobado por el Consejo de Administración; manual de funciones que asigna al Jefe de Sistemas establecer el plan de continuidad	Parcial	Sin política de continuidad; desarrollo del plan pendiente; rol de Oficial de Continuidad no formalizado; sin suplentes
6. Planificación	Sin evidencia de objetivos de continuidad	No evidenciado	Definir objetivos de continuidad por servicio
7. Soporte	Recursos enumerados sin montos en el procedimiento de respaldos; capacitación anual en seguridad de la información; control de versiones de los manuales	Parcial	Sin presupuesto de continuidad; inversiones clave postergadas; área de TI de tres personas; sin simulacros
8.2.2 Análisis de impacto	Sin BIA institucional; RTO y RPO definidos solo conceptualmente; los parámetros de la Tabla 12 se obtuvieron en esta investigación	No evidenciado	Formalizar el BIA y aprobar MTPD, RTO, RPO y MBCO
8.2.3 Evaluación de riesgos	Informe de riesgos 2026 y libro de riesgos con valoraciones MAGERIT	Parcial	Enfoque en seguridad de la información; escalas heterogéneas

Cláusula	Evidencia en la cooperativa	Estado	Brecha principal
8.3 Estrategias y soluciones	Respaldo diario, UPS y generador de 12 h, dos cajeros, SOC externo; segundo enlace en contratación	Parcial	Sin copia fuera del sitio ni réplica; enlace único; contratos no alineados con el RTO; DRP del core no probado
8.4 Planes y procedimientos	Proceso de ejecución de planes operativos de contingencia; gestión de incidentes y problemas; informes de ejecución tras cada incidente	Parcial	Sin plan integral; operación degradada no documentada; sin procedimientos de comunicación a socios ni a la SEPS
8.5 Programa de ejercicios	Restauración en ambiente de pruebas en marzo de 2026 (3,5 h); pruebas trimestrales y semestrales programadas en el procedimiento	Parcial	Pruebas esporádicas; sin prueba de sitio alterno, de DRP ni simulacros
8.6 Evaluación de la documentación	Sin evidencia	No evidenciado	Establecer revisión periódica de las capacidades de continuidad
9. Evaluación del desempeño	Indicadores de respaldos, tiempo de resolución y tiempo entre fallas; auditoría informática; revisión de la SEPS de 2025	Parcial	Sin indicadores específicos de continuidad
10. Mejora	Informes de ejecución con medidas de prevención; análisis de causa raíz en la gestión de problemas	Parcial	Observación de la SEPS en proceso de atención; sin acciones correctivas de continuidad cerradas

Fuente: Elaboración propia a partir de ISO (2019), COAC Yuyay (s. f., 2024, 2026a, 2026b) y la entrevista (Anexo A).

Ningún requisito se cumple plenamente y tres carecen de evidencia: los objetivos de continuidad, el análisis de impacto al negocio y la evaluación de la documentación de continuidad. Las entrevistas confirmaron la calificación documental y aportaron evidencia en dos cláusulas: la prueba de restauración de marzo de 2026 constituye evidencia parcial de ejercicios (8.5), y la observación de la SEPS de 2025 muestra que la falta de un plan probado ya ha sido señalada por el organismo de control (9). Los requisitos parciales comparten un patrón: existen políticas o procedimientos aprobados, pero su ejecución es esporádica una prueba de restauración, ninguna copia en sitio alterno, ningún ejercicio del DRP del proveedor y no están orientados específicamente a la continuidad de los servicios digitales.

3.7.4. Síntesis de hallazgos e implicaciones para la propuesta

La triangulación de las fuentes permite establecer los hallazgos de la Tabla 16, cada uno vinculado con la fase de la propuesta que lo atiende.

Tabla 16

Hallazgos del diagnóstico y fase de la propuesta que los atiende

N.º	Hallazgo	Fuentes	Fase de la propuesta (cláusula)
H1	No existe un plan de continuidad integral aprobado, aunque el manual de funciones asigna esa tarea al Jefe de Sistemas desde 2019; las piezas existentes están dispersas y el desarrollo del plan sigue pendiente en el Comité, pese a la observación de la SEPS de 2025.	MSI, MP, IR, MF, ENT	Planes y procedimientos de continuidad (8.4)
H2	El RPO requerido de 1 hora contrasta con una pérdida posible de hasta 24 horas; los respaldos no tienen copia fuera del sitio ni servidor espejo, aunque la política y el manual de funciones los exigen, y la prueba de restauración de marzo de 2026 (3,5 h) no se ha repetido.	MSI, MP, INV, MF, ENT, BIA	Estrategias de respaldo y recuperación de datos (8.3)
H3	Los contratos con los proveedores críticos no están alineados con los tiempos requeridos: restablecimiento del core en 24 h frente a un MTPD de 8 h, reparación del enlace en 6 h frente a un RTO de 4 h y COONECTA sin SLA; no hay plan de salida ni revisión de sus planes de continuidad.	IR, INV, ENT, BIA	Estrategias para proveedores (8.3)
H4	El core financiero y la conectividad concentran los riesgos de disponibilidad: de ellos dependen todos los canales y la ventanilla, y ambos tienen un MTPD de 8 horas.	IR, INV, BIA	Evaluación de riesgos (8.2.3) y prioridades de recuperación (8.2.2)
H5	La conectividad depende de un único enlace de Internet, cuya caída en marzo de 2025 provocó la interrupción más larga del período (6 h); el respaldo de la comunicación de datos figura en el manual de funciones desde 2019 y el segundo enlace está en contratación.	INV, MF, ENT	Estrategias tecnológicas (8.3)
H6	La gestión de cambios del proveedor es débil: riesgo R26 extremo y una actualización fallida que detuvo la aplicación móvil 3 h en agosto de 2025.	IR, INV, ENT	Controles preventivos asociados a las estrategias (8.3)
H7	La operación degradada en ventanilla existe por práctica, pero no está documentada ni probada; tras la interrupción de 2025 la conciliación tomó un día adicional.	ENT	Procedimientos de operación degradada (8.4)

N.º	Hallazgo	Fuentes	Fase de la propuesta (cláusula)
H8	El Comité existe y sesiona, pero no se ha formalizado el rol de Oficial de Continuidad ni se han designado suplentes en un área de TI de tres personas: el campo de respaldo de los manuales de funciones de TI está vacío.	MSI, INV, IR, MF, ENT	Política, roles y responsabilidades (5; 7)
H9	No hay mensajes predefinidos ni procedimiento de notificación a la SEPS; ninguna interrupción ha sido notificada formalmente.	MSI, MP, ENT	Estructura de respuesta y comunicación (8.4)
H10	No se han realizado simulacros ni pruebas del DRP, y las pruebas programadas se ejecutan de forma esporádica.	MP, INV, ENT	Programa de ejercicios y pruebas (8.5)
H11	Las valoraciones de riesgo institucionales emplean escalas heterogéneas.	INV, IR	Revaloración con escala única (8.2.3)
H12	No existe presupuesto de continuidad; el sitio alterno, la réplica de la base de datos y las pruebas de DRP se postergaron por costo.	ENT	Hoja de ruta y recursos de las estrategias (7.1; 8.3)

Nota: MSI = manual de seguridad de la información (COAC Yuyay, 2024); MP = manual de procesos de TI (COAC Yuyay, 2026b); IR = informe de riesgos (COAC Yuyay, 2026a); INV = libro de gestión de riesgos e inventario (COAC Yuyay, s. f.); MF = manuales descriptivos de funciones (COAC Yuyay, 2019, 2023); ENT = entrevista (Anexo A); BIA = fichas de análisis de impacto (Anexo B). Fuente: Elaboración propia.

En conjunto, el diagnóstico muestra que la COAC Yuyay Ltda. dispone de una base documental y de gestión de riesgos sobre la cual construir el plan, pero carece de los elementos que convierten esa base en capacidad de continuidad: prioridades de recuperación basadas en el impacto, parámetros de recuperación definidos, estrategias verificadas y un plan que articule la respuesta. Estos son los contenidos que desarrolla el capítulo IV.

3.8. Fases de la metodología

La propuesta se desarrolla en ocho fases que siguen la secuencia del ciclo Planificar-Hacer-Verificar-Actuar y de la cláusula 8 de ISO 22301:2019, con el análisis de riesgos de MAGERIT integrado en la evaluación de riesgos (ISO, 2019; MHAP, 2012a). La primera fase corresponde al diagnóstico presentado en este capítulo; las siete restantes se desarrollan en el capítulo IV (Tabla 17; Ilustración 7).

Tabla 17

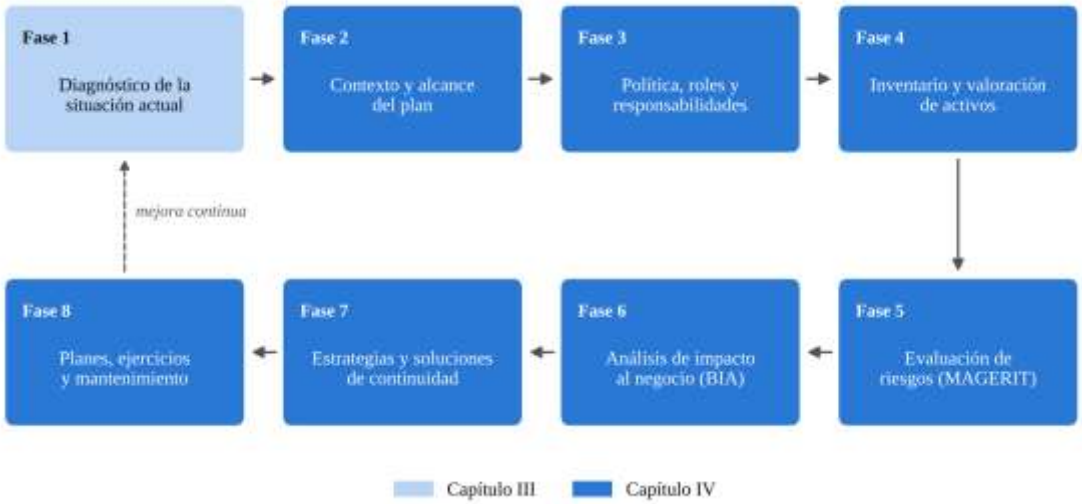
Fases de la metodología

Fase	Actividades	Técnica o instrumento	Producto	Cláusula	Cap.
1. Diagnóstico de la situación actual	Revisión documental, entrevistas y aplicación de fichas BIA	Ficha documental; guion (Anexo A); ficha BIA (Anexo B)	Resultados y hallazgos (3.6 y 3.7)	4.1; 8.2	III
2. Contexto y alcance del plan	Caracterización de la organización, partes interesadas, requisitos legales y servicios incluidos	Revisión documental	Contexto y alcance del plan	4	IV
3. Política, roles y responsabilidades	Política de continuidad, estructura de roles y suplentes, funciones del comité	Revisión documental; entrevista (bloque G)	Política y matriz de roles	5; 7	IV
4. Inventario y valoración de activos	Identificación y valoración por dimensiones de los activos de los servicios digitales	MAGERIT, paso 1	Inventario valorado	8.2.3	IV
5. Evaluación de riesgos	Amenazas, probabilidad, impacto, riesgo inherente, salvaguardas y riesgo residual	MAGERIT, pasos 2 a 6; escala de 5 × 5	Matriz de riesgos priorizada	8.2.3	IV
6. Análisis de impacto al negocio	Impactos en el tiempo; MTPD, RTO, RPO y MBCO; prioridades	Fichas BIA; matriz de consolidación	Prioridades y parámetros de recuperación	8.2.2	IV
7. Estrategias y soluciones de continuidad	Selección por tipo de recurso frente a RTO, RPO y riesgos	Matriz de decisión BIA-riesgos	Estrategias seleccionadas	8.3	IV
8. Planes, ejercicios y mantenimiento	Estructura de respuesta, comunicación, procedimientos de recuperación, programa de pruebas, indicadores y actualización	Procedimientos documentados	Plan de Continuidad del Negocio	8.4 a 8.6; 9; 10	IV

Fuente: Elaboración propia a partir de ISO (2019) y MHAP (2012a).

Ilustración 7

Secuencia de las fases de la metodología



Fuente: Elaboración propia.

La secuencia es cíclica: los resultados de los ejercicios y de los incidentes reales de la fase 8 alimentan la actualización del diagnóstico, en coherencia con el principio de mejora continua de la norma. De este modo, el marco metodológico enlaza el diagnóstico de la situación actual con el diseño del plan, que se presenta en el capítulo siguiente.

CAPÍTULO IV

4. PROPUESTA

Este capítulo desarrolla el tercer objetivo específico de la investigación: elaborar el Plan de Continuidad del Negocio para los servicios digitales de la COAC Yuyay Ltda. mediante la ejecución de las fases de la metodología seleccionada. Se parte del diagnóstico del capítulo III fase 1 de la metodología y se desarrollan, en el orden de la Tabla 17, las siete fases restantes: contexto y alcance, política y roles, inventario de activos, evaluación de riesgos, análisis de impacto, estrategias y, finalmente, planes, ejercicios y mantenimiento. Cada fase produce un componente del plan, de modo que el conjunto constituye el documento que la cooperativa puede aprobar e implementar.

4.1. Título de la propuesta

Plan de Continuidad de negocio para los servicios digitales de COAC Yuyay Ltda basado en la norma ISO 22301:2019.

4.2. Presentación

La COAC Yuyay Ltda. presta ocho servicios digitales que, en conjunto, canalizan alrededor del 35 % de sus operaciones y dependen de un core financiero alojado en la nube, de un único enlace de Internet y de seis proveedores externos. El diagnóstico mostró que la cooperativa dispone de políticas de seguridad aprobadas, de un análisis de riesgos actualizado y de un procedimiento de respaldos, pero no de un plan que establezca qué recuperar primero, en cuánto tiempo, con qué recursos y bajo la dirección de quién. La SEPS observó esa carencia en su revisión de 2025 (Anexo A, G4).

El plan que se presenta responde a esa necesidad. Está construido sobre los requisitos operativos de la cláusula 8 de ISO 22301:2019 análisis de impacto, evaluación de riesgos, estrategias, procedimientos y ejercicios y sobre los requisitos de liderazgo, planificación, soporte, evaluación y mejora de las cláusulas 5 a 10 (ISO, 2019). La evaluación de riesgos

aplica el método de MAGERIT con la escala de 5 × 5 definida en el capítulo II (MHAP, 2012a), y el análisis de impacto sigue el procedimiento de ISO/TS 22317 (ISO, 2021b). El plan se dimensiona para una organización con un área de TI de tres personas: privilegia soluciones contractuales y procedimentales de bajo costo, y reserva las inversiones mayores para los servicios cuyo MTPD lo exige.

4.3. Objetivos de la propuesta

4.3.1. Objetivo general

Establecer la capacidad de la COAC Yuyay Ltda. para responder a una interrupción de sus servicios digitales y recuperarlos dentro de los tiempos que la organización puede tolerar, conforme a los requisitos de la norma ISO 22301:2019.

4.3.2. Objetivos específicos

- Definir el contexto, el alcance, la política y la estructura de roles del plan de continuidad.
- Determinar los activos, los riesgos y las prioridades de recuperación de los servicios digitales mediante la evaluación de riesgos y el análisis de impacto.
- Seleccionar las estrategias y soluciones de continuidad que permitan cumplir los parámetros de recuperación definidos.
- Documentar los procedimientos de respuesta, comunicación, recuperación y operación degradada, así como el programa de ejercicios, los indicadores y el mantenimiento del plan.

4.4. Justificación

La propuesta se justifica, en primer lugar, por los hallazgos del diagnóstico. La cooperativa puede perder hasta 24 horas de transacciones cuando su tolerancia es de 1 hora, los contratos con sus proveedores críticos admiten tiempos de restablecimiento que triplican el MTPD del core financiero, y la interrupción de marzo de 2025 demostró que una sola falla

del enlace de Internet detiene todos los canales y la ventanilla (sección 3.7.5). Ninguna de estas brechas se resuelve con más controles de seguridad de la información; requieren decisiones de continuidad: prioridades, parámetros, estrategias y procedimientos.

En segundo lugar, por el marco regulatorio. La norma de control del riesgo operativo para el sector financiero popular y solidario exigía desde 2018 que las entidades cuenten con planes de continuidad que aseguren su capacidad para operar y limitar las pérdidas ante interrupciones (SEPS, 2018), y la norma vigente de 2024 precisa esos planes con un comité de continuidad, tiempos objetivo de recuperación, un plan de recuperación de desastres en sitio remoto, pruebas anuales con proveedores y una disponibilidad anual del 99,99 % para los servicios críticos (SEPS, 2024), y la observación de la SEPS de 2025 convierte esa exigencia en un compromiso pendiente de atención. A ello se suma la Ley Orgánica de Protección de Datos Personales, que mantiene las obligaciones del responsable del tratamiento durante un incidente (Asamblea Nacional del Ecuador, 2021).

En tercer lugar, por su utilidad práctica. El plan traduce en tareas, responsables y plazos lo que hoy depende de la experiencia de tres personas, y la estructura empleada fases de ISO 22301 con evaluación de riesgos MAGERIT puede replicarse en otras cooperativas del segmento con servicios digitales y dependencia de proveedores semejantes.

4.5. Alcance y estructura de la propuesta

El plan cubre los ocho servicios digitales identificados en el diagnóstico (SD-01 a SD-08), los activos y proveedores de los que dependen y las cuatro oficinas de la cooperativa Matriz, Terminal Terrestre, El Tambo y Suscal, en la medida en que la ventanilla depende del core financiero y de la conectividad. La Tabla 18 presenta los componentes del plan, la fase de la metodología que los produce y la cláusula de la norma que atienden. El plan resultante, redactado como documento institucional listo para su revisión y aprobación por la cooperativa, consta en el Anexo C.

Tabla 18

Componentes del Plan de Continuidad del Negocio

Componente	Contenido	Sección	Cláusula ISO 22301
Contexto y alcance	Partes interesadas, requisitos legales y regulatorios, servicios, sedes y exclusiones	4.6	4.1 a 4.4
Política, objetivos y roles	Política de continuidad, objetivos medibles, estructura de respuesta, roles con suplentes, matriz RACI y competencias	4.7	5; 6.2; 7.2 y 7.3
Activos y dependencias	Activos de soporte valorados por dimensiones y matriz de dependencias servicio-activo	4.8	8.2.2; 8.2.3
Evaluación de riesgos	Escenarios de interrupción, riesgo inherente y residual, plan de tratamiento	4.9	8.2.3
Análisis de impacto	Evolución del impacto, brechas de recuperación y secuencia de recuperación	4.10	8.2.2
Estrategias y soluciones	Alternativas evaluadas, estrategias seleccionadas y hoja de ruta	4.11	8.3
Planes y procedimientos	Niveles de activación, comunicación, procedimientos de recuperación, operación degradada y retorno a la normalidad	4.12.1 a 4.12.6	8.4
Ejercicios, desempeño y mejora	Programa de ejercicios, indicadores, revisión y mantenimiento del plan	4.12.7 a 4.12.9	8.5; 8.6; 9; 10

Fuente: Elaboración propia a partir de ISO (2019).

4.6. Fase 2: Contexto de la organización y alcance del plan

4.6.1. Caracterización de la organización

La COAC Yuyay Ltda. es una cooperativa del segmento 3, controlada por la SEPS, con alrededor de 9.800 socios activos y 45 usuarios internos del core financiero, que opera en un entorno rural y agrícola del cantón Cañar desde una matriz y tres agencias (Anexo A, A1). La unidad de Tecnologías de la Información y Comunicación pertenece al área Financiera y está integrada por tres personas el Coordinador de Sistemas, el Ingeniero de Sistemas y la Oficial de Seguridad de la Información, con el apoyo del Oficial de Seguridad Física y Electrónica y del Auditor Informático (COAC Yuyay, s. f.). El core financiero y su base de datos

operan en Oracle Cloud (OCI) bajo administración del contratista, y en el centro de datos local permanecen el almacenamiento de respaldos, los servidores de dominio y de archivos y los equipos de comunicaciones (Anexo A, B1).

La Ilustración 8 presenta la estructura organizacional de la cooperativa: bajo la Gerencia General se ubican las áreas de Negocios, Administración y Gestión, y Financiero, y esta última agrupa las unidades de TIC, Tesorería, Contabilidad y Cajas (COAC Yuyay, s. f.). El manual descriptivo de funciones denomina Jefe de Sistemas al responsable de TI, que reporta a la Gerencia General y supervisa a dos asistentes de TI (COAC Yuyay, 2019); los documentos más recientes y la entrevista lo llaman Coordinador de Sistemas, denominación que se usa en este plan.

Ilustración 8

Estructura organizacional de la COAC Yuyay Ltda.



Fuente: Elaboración propia a partir de COAC Yuyay (s. f.).

4.6.2. Partes interesadas y sus requisitos

La cláusula 4.2 de la norma exige identificar a las partes interesadas pertinentes para la continuidad y sus requisitos (ISO, 2019). La Tabla 19 las resume y señala qué exige cada una al plan.

Tabla 19

Partes interesadas y requisitos para el plan de continuidad

Parte interesada	Necesidades y expectativas respecto a la continuidad	Requisito para el plan
Socios	Acceso a sus fondos, información oportuna durante la interrupción y exactitud de sus saldos	MBCO por servicio, mensajes predefinidos y conciliación tras la interrupción
Consejo de Administración y Gerencia General	Proteger la viabilidad, la reputación y el cumplimiento regulatorio con recursos limitados	Prioridades basadas en el BIA, estrategias de costo proporcional e informes periódicos
Personal de agencias y de TI	Saber qué hacer, quién decide y cómo registrar las operaciones durante la interrupción	Roles con suplentes, procedimientos documentados y capacitación
SEPS	Gestión del riesgo operativo y continuidad probada; atención de la observación de 2025	Plan aprobado, ejercicios documentados y notificación de eventos
Autoridad de protección de datos y titulares	Protección de los datos personales durante la contingencia	Controles de seguridad en la operación degradada y notificación de vulneraciones
Proveedores críticos (core, nube, operador, COONECTA, SOC, cajeros)	Reglas claras de escalamiento y coordinación	Contactos, SLA alineados con el RTO y participación en los ejercicios
Banco Central y red de pagos	Integridad de las transferencias y de las transacciones con tarjeta	Procedimientos de conciliación y verificación antes de reenviar operaciones

Fuente: Elaboración propia a partir de la entrevista (Anexo A) y de ISO (2019).

4.6.3. Requisitos legales y regulatorios

Tabla 20

Requisitos legales y regulatorios aplicables al plan

Norma	Requisito relacionado con la continuidad	Implicación para el plan
Código Orgánico Monetario y Financiero (Asamblea Nacional del Ecuador, 2014)	Las entidades del sistema financiero deben administrar sus riesgos y proteger los depósitos del público	Prioridad de los servicios que dan acceso a los fondos de los socios
Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario (Asamblea Nacional del Ecuador, 2011)	Las cooperativas están sujetas al control de la SEPS	El plan forma parte de la gestión supervisada por la SEPS
Norma de control para la administración del riesgo operativo (SEPS, 2024), que sustituye a la norma de 2018	Comité de Continuidad del Negocio; tiempos máximos de interrupción, RTO y RPO por proceso crítico; DRP con restauración en sitio remoto; pruebas anuales que incluyan a proveedores; disponibilidad anual del 99,99 % de los servicios críticos	Plan aprobado, probado anualmente y actualizado; parámetros por servicio; estrategia de recuperación remota; meta de disponibilidad; notificación de eventos de riesgo operativo
Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021)	Seguridad del tratamiento y notificación de vulneraciones de datos personales a la SPDP por el SISPDP en un plazo máximo de cinco días (Reglamento General, Presidencia de la República del Ecuador, 2023; Norma técnica SPDP, 2026)	Controles en la operación degradada y procedimiento de notificación
Norma de control respecto a la seguridad de la información (SEPS, 2022)	Reporte inmediato a la SEPS de los eventos que afecten a la continuidad del negocio y a la prestación de servicios financieros; controles de respaldo de la información	Notificación a la SEPS en la matriz de comunicación y en la declaratoria de nivel 3; estrategia de respaldos E-01
Manual de seguridad de la información (COAC Yuyay, 2024)	Respaldo en sitio alterno, energía con autonomía de 8 h, SLA con terceros, supervisión del plan por el Comité	Estrategias de respaldo, energía y proveedores; rol del Comité

Fuente: Elaboración propia a partir de las normas citadas.

4.6.4. Alcance del plan

Tabla 21

Alcance del Plan de Continuidad del Negocio

Elemento	Incluye	Excluye
Servicios	SD-01 a SD-08 y la atención en ventanilla en cuanto depende del core y de la conectividad	Servicios no digitales que no dependen de la tecnología (asesoría, cobranza en campo)
Sedes	Matriz (con su centro de datos), Terminal Terrestre, El Tambo y Suscal	Instalaciones de los proveedores, salvo su obligación contractual de continuidad

Elemento	Incluye	Excluye
Activos	Activos de soporte de los servicios digitales (sección 4.8) y personal de TI	Activos administrativos sin relación con los servicios digitales
Escenarios	Pérdida de conectividad, del core o de los datos, falla de proveedores, cajeros, energía, personal clave y siniestro en el centro de datos	Pandemias y conflictos sociales prolongados, que requieren un plan institucional más amplio
Alcance temporal	Respuesta, recuperación y retorno a la normalidad	Investigación forense detallada de ciberincidentes, que corresponde al proceso de gestión de incidentes de seguridad

Fuente: Elaboración propia.

4.7. Fase 3: Política, roles y responsabilidades

4.7.1. Política de continuidad del negocio

La cláusula 5.2 exige una política de continuidad aprobada por la alta dirección, apropiada al propósito de la organización y que incluya el compromiso de cumplir los requisitos aplicables y de mejorar continuamente (ISO, 2019). Se propone el siguiente texto para aprobación del Consejo de Administración:

La Cooperativa de Ahorro y Crédito Yuyay Ltda. se compromete a proteger la continuidad de los servicios digitales que presta a sus socios y a recuperarlos dentro de los tiempos que la institución puede tolerar. Para ello, mantendrá un Plan de Continuidad del Negocio basado en el análisis de impacto y en la evaluación de riesgos; asignará los recursos y las responsabilidades necesarios para su funcionamiento; exigirá a sus proveedores críticos niveles de servicio coherentes con sus objetivos de recuperación; probará periódicamente su capacidad de respuesta; cumplirá la normativa de la SEPS y de protección de datos personales; y mejorará el plan a partir de los ejercicios y de los incidentes reales.

La política se complementa con los siguientes principios de actuación:

- La seguridad de las personas prevalece sobre la recuperación de cualquier servicio.
- Los servicios se recuperan en el orden que fija el análisis de impacto, no en el orden en que se reportan.

- Ninguna operación registrada manualmente se da por concluida hasta su digitación y conciliación con doble control.
- Los controles de seguridad de la información se mantienen durante la contingencia; los accesos excepcionales se registran y se revocan al retornar a la normalidad.
- Los socios reciben información veraz y oportuna sobre la interrupción y las alternativas disponibles.

4.7.2. Objetivos de continuidad

La cláusula 6.2 requiere objetivos de continuidad medibles, con responsables, recursos y plazos (ISO, 2019). La Tabla 22 los establece a partir de los parámetros del análisis de impacto y de las brechas del diagnóstico.

Tabla 22

Objetivos de continuidad del negocio

Cód.	Objetivo	Indicador	Meta	Plazo	Responsable
OC-1	Recuperar los servicios de prioridad 1 y 2 (SD-01, SD-05, SD-07) dentro de su RTO	Tiempo de recuperación en ejercicios e incidentes	≤ 4 h	12 meses	Coordinador de Sistemas
OC-2	Limitar la pérdida de datos del core financiero	RPO alcanzado en la prueba de restauración	≤ 1 h	3 meses	Coordinador de Sistemas
OC-3	Disponer de copias de respaldo íntegras fuera del sitio principal	Respaldos diarios replicados y verificados fuera del sitio	100 %	3 meses	Coordinador de Sistemas
OC-4	Alinear los contratos de los proveedores críticos con los parámetros de recuperación	Proveedores críticos con SLA coherente con el RTO	6 de 6	12 meses	Gerente General
OC-5	Ejecutar el programa anual de ejercicios	Ejercicios ejecutados sobre los programados	≥ 90 %	Anual	Oficial de Continuidad
OC-6	Capacitar a quienes tienen un rol en el plan	Titulares y suplentes capacitados	100 %	6 meses	Talento Humano
OC-7	Atender la observación de la SEPS de 2025	Observación cerrada con evidencia de plan aprobado y probado	Cerrada	12 meses	Gerente General

Fuente: Elaboración propia a partir de las Tablas 12 y 16.

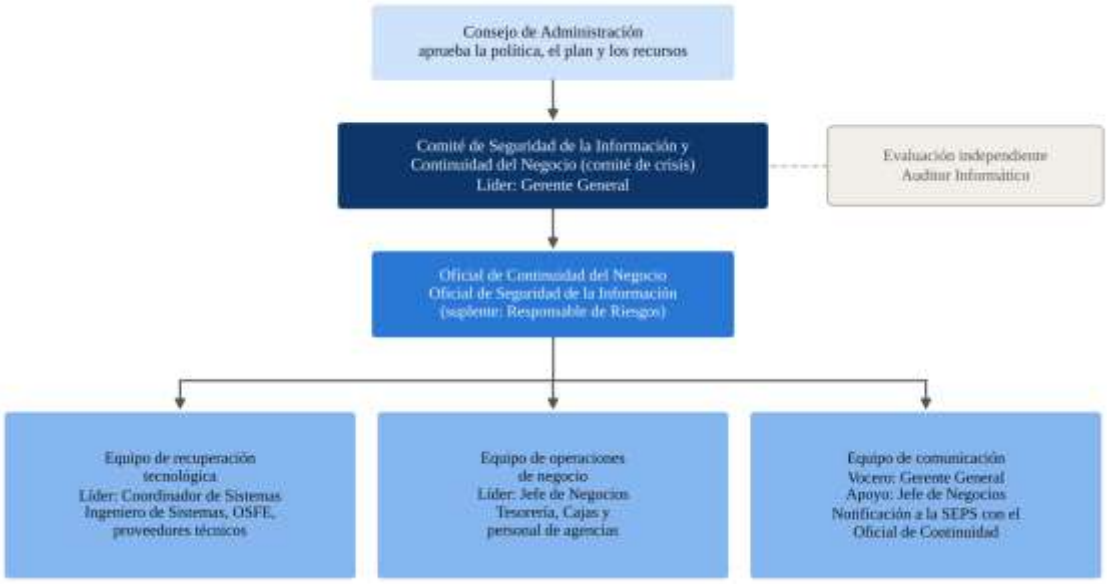
4.7.3. Estructura de respuesta

La estructura de respuesta se apoya en los órganos existentes para no crear instancias que una organización pequeña no pueda sostener. El Comité de Seguridad de la Información

y Continuidad del Negocio actúa como comité de crisis; se crea el rol de Oficial de Continuidad del Negocio, que asume la Oficial de Seguridad de la Información porque el manual de seguridad de la información ya le asigna la función de garantizar la continuidad (COAC Yuyay, 2024); y se organizan tres equipos operativos: recuperación tecnológica, operaciones de negocio y comunicación (Ilustración 9). Esta asignación concentra en una misma persona la seguridad y la continuidad, dentro de un área de TI de tres personas, y la Oficial de Seguridad de la Información participa además en las tareas operativas de PR-03 y PR-04. Para evitar que en un ciberincidente coincidan en ella la contención técnica y la coordinación del plan, el procedimiento establece que, al activarse PR-03 o PR-04, la coordinación del plan pasa al suplente del rol, el Auditor Informático, mientras la titular dirige la contención; el Comité debe revisar esta carga en la primera evaluación anual del plan y, si la cooperativa formaliza una función de riesgos, valorar el traslado del rol a esa función. La asignación es coherente con el manual descriptivo de funciones, que encarga al Jefe de Sistemas establecer los planes de continuidad de negocios (COAC Yuyay, 2019): el Coordinador de Sistemas conserva la elaboración y actualización de los componentes tecnológicos del plan procedimientos de recuperación y coordinación del DRP con los proveedores, y el Oficial de Continuidad coordina el plan en su conjunto.

Ilustración 9

Estructura de respuesta del plan de continuidad



Fuente: Elaboración propia a partir de ISO (2019) y COAC Yuyay (2024).

La Tabla 23 asigna cada rol a un titular y a un suplente. Los suplentes son una exigencia práctica antes que formal: con tres personas en el área de TI, la ausencia de una sola puede dejar sin quien ejecute la recuperación.

Tabla 23

Roles, titulares y suplentes del plan de continuidad

Rol	Titular	Suplente	Responsabilidades principales
Aprobación y recursos	Presidente del Consejo de Administración	Vicepresidente del Consejo	Aprobar la política y el plan, asignar recursos y conocer el informe anual de continuidad
Líder de crisis (Comité)	Gerente General	Gerente subrogante	Declarar el nivel 3, priorizar la recuperación, autorizar gastos de emergencia y aprobar las comunicaciones externas y la notificación a la SEPS
Oficial de Continuidad del Negocio	Oficial de Seguridad de la Información	Auditor Informático	Mantener el plan, coordinar la respuesta, llevar la bitácora de decisiones, organizar los ejercicios e informar al Comité
Líder de recuperación tecnológica	Coordinador de Sistemas	Ingeniero de Sistemas	Diagnosticar, declarar el nivel 2, ejecutar los procedimientos de recuperación, coordinar a los proveedores técnicos y mantener los procedimientos técnicos y el DRP
Equipo técnico	Ingeniero de Sistemas; Oficial de Seguridad Física y Electrónica	Personal de los proveedores	Restaurar, conmutar y verificar los servicios; atender energía, climatización e instalaciones

Rol	Titular	Suplente	Responsabilidades principales
Líder de operaciones de negocio	Jefe de Negocios	Responsable de Tesorería	Activar la operación degradada en las agencias, coordinar la digitación y la conciliación
Comunicación	Gerente General (vocero)	Jefe de Negocios	Emitir los mensajes a socios, personal y medios; preparar con el Oficial de Continuidad la notificación a la SEPS
Evaluación independiente	Auditor Informático	Auditoría interna	Evaluar los ejercicios y el cumplimiento del plan, sin ejecutar tareas de recuperación

Fuente: Elaboración propia a partir de COAC Yuyay (s. f., 2024) y de la entrevista (Anexo A).

La Tabla 24 precisa la participación de cada rol en las actividades del plan con la notación RACI: responsable de ejecutar (R), responsable último que rinde cuentas (A), consultado (C) e informado (I).

Tabla 24

Matriz RACI del plan de continuidad

Actividad	CA	GG	OCN	CS	ET	JN	AI
Aprobar la política y el plan	A	R	C	C		C	C
Detectar y evaluar la interrupción		I	I	A	R	R	
Declarar el nivel 2 (contingencia)		I	C	R/A	C	I	
Declarar el nivel 3 (crisis)	I	R/A	C	C		C	
Ejecutar la recuperación tecnológica		I	C	A	R	I	
Activar la operación degradada		I	C	C		R/A	
Comunicar a socios y personal		A	C	I		R	
Notificar a la SEPS	I	A	R	C			I
Coordinar a los proveedores		I	C	R/A	R		
Declarar el retorno a la normalidad		A	R	R	C	R	
Elaborar el informe posterior		I	A	R	C	C	I
Planificar y ejecutar los ejercicios	I	A	R	R	R	R	C
Revisar y actualizar el plan	A	R	R	R		C	C

Nota: CA = Consejo de Administración; GG = Gerente General y Comité de crisis; OCN = Oficial de Continuidad del Negocio; CS = Coordinador de Sistemas; ET = equipo técnico; JN = Jefe de Negocios; AI = Auditor Informático. Fuente: Elaboración propia.

4.7.4. Competencias, concienciación y documentación

Para cumplir las cláusulas 7.2 a 7.5 (ISO, 2019), el plan establece tres medidas. Primera, una capacitación inicial de cuatro horas para titulares y suplentes sobre el plan, sus niveles de activación y sus procedimientos, y una actualización anual que se integra a la capacitación en seguridad de la información que ya imparten Talento Humano y la Oficial de Seguridad de la Información (Anexo A, G3). Segunda, una sesión anual de concienciación para todo el personal de agencias sobre la operación degradada y los mensajes a los socios. Tercera, el control de la documentación: el plan se codifica y versiona como los demás manuales de la cooperativa, y se mantiene una copia digital fuera de la red institucional y una copia impresa en cada oficina, porque un plan que solo existe en el servidor afectado no puede consultarse durante la interrupción.

4.8. Fase 4: Inventario y valoración de activos

4.8.1. Activos de soporte de los servicios digitales

Siguiendo el primer paso de MAGERIT, se seleccionaron del inventario institucional los activos de los que dependen los servicios digitales, según las dependencias registradas en las fichas BIA, y se conservó su valoración en las cinco dimensiones de seguridad en la escala de 0 a 10 (MHAP, 2012a, 2012b). La Tabla 25 presenta los 28 activos resultantes; el valor del activo es el máximo de sus dimensiones.

Tabla 25

Activos de soporte de los servicios digitales valorados por dimensiones

Código	Activo	Servicios	D	I	C	A	T	Valor
ACT-S-02	Servidores en la nube (OCI)	SD-01 a SD-07	9	9	9	9	9	9
ACT-COM-02	Conexión a Internet	Todos	10	8	8	6	6	10
ACT-HW-13	Firewall perimetral	Todos	10	10	10	10	10	10
ACT-COM-01	Red interna (LAN)	Todos	10	8	8	6	6	10
ACT-SW-02	Core financiero (Vimacoop/VimaSistem)	SD-01 a SD-06	9	9	9	9	9	9

Código	Activo	Servicios	D	I	C	A	T	Valor
ACT-SW-08	Servidor de base de datos (SGBD)	SD-01 a SD-06	10	10	9	8	8	10
ACT-D-02	Bases de datos de los sistemas	SD-01 a SD-06	9	10	10	9	9	10
ACT-D-04	Copias de respaldo de bases de datos	SD-01	9	9	9	6	6	9
ACT-ME-DIA-02	Almacenamiento en red (NAS)	SD-01, SD-08	9	9	8	6	6	9
ACT-S-04	Canales electrónicos	SD-02, SD-03	10	10	9	10	9	10
ACT-S-03	Web transaccional	SD-02	9	9	9	9	9	9
ACT-SW-01	Aplicación móvil Yuyay Móvil	SD-03	8	10	8	8	8	10
ACT-K-01	Certificado digital SSL/TLS	SD-02, SD-03	8	9	9	10	6	10
ACT-HW-15/16	Cajeros automáticos 1 y 2	SD-04	9	9	9	9	9	9
ACT-S-05	Servicio de tarjetas de débito	SD-04, SD-05	9	9	9	10	9	10
ACT-SW-06	Aplicación de recaudaciones	SD-06	9	9	6	8	9	9
ACT-S-01	Orquestador de servicios	SD-06	9	9	6	8	9	9
ACT-S-07	Monitoreo de seguridad (SOC/SIEM)	SD-08	8	8	8	7	9	9
ACT-S-06	Carpetas compartidas (NAS y SharePoint)	SD-08	8	8	8	6	6	8
ACT-L-01	Centro de datos	Todos	10	8	8	6	6	10
ACT-AUX-03	UPS y reguladores de voltaje	Todos	10	8	4	2	4	10
ACT-AUX-08	Planta eléctrica (generador)	Todos	9	4	2	2	2	9
ACT-P-04	Coordinador de Sistemas	Todos	8	10	10	10	10	10
ACT-P-05	Proveedor del core financiero	SD-01 a SD-06	10	9	9	8	8	10
ACT-P-06	Proveedor de servicios en la nube	SD-01 a SD-07	9	9	10	8	8	10
ACT-P-07	Proveedor de red de tarjetas (COONECTA)	SD-04, SD-05	9	9	9	8	8	9
ACT-P-08	Proveedor del SOC	SD-08	8	8	9	8	8	9
ACT-P-09	Proveedor de mantenimiento de cajeros	SD-04	8	6	6	6	6	8

Nota: D = disponibilidad; I = integridad; C = confidencialidad; A = autenticidad; T = trazabilidad.

Fuente: Elaboración propia a partir de COAC Yuyay (s. f.) y de las fichas BIA (Anexo B).

Dos ajustes al inventario institucional se derivan de esta fase. El operador de telecomunicaciones del enlace de Internet, identificado en la entrevista como proveedor crítico (Anexo A, B2), no figura en el inventario y debe incorporarse en la categoría de personal y proveedores, con su valoración a cargo del Coordinador de Sistemas. Y la ubicación del core

financiero y del servidor de base de datos debe corregirse de «centro de datos» a «nube (OCI)», conforme a lo confirmado en la entrevista (Anexo A, B1).

4.8.2. Dependencias entre servicios y activos

La Tabla 26 cruza los servicios con los activos que comparten. Su lectura por filas identifica los puntos únicos de falla: un activo del que dependen muchos servicios y que no tiene alternativa.

Tabla 26

Matriz de dependencias entre servicios digitales y activos críticos

Activo	SD-01	SD-02	SD-03	SD-04	SD-05	SD-06	SD-07	SD-08	N.º de servicios
Conexión a Internet (enlace único)	●	●	●	●	●	●	●	●	8
Firewall perimetral y LAN	●	●	●	●	●	●	●	●	8
Centro de datos, energía y climatización	●	●	●	●	●	●	●	●	8
Coordinador de Sistemas	●	●	●	●	●	●	●	●	8
Servidores en la nube (OCI) y su proveedor	●	●	●	●	●	●	●		7
Core financiero, SGBD y bases de datos	●	●	●	●	●	●			6
Proveedor del core financiero	●	●	●	●	●	●			6
Servicio de tarjetas y COOPNECTA				●	●				2
Canales electrónicos y certificado TLS		●	●						2
Recaudaciones y orquestador						●			1
Cajeros automáticos y su mantenimiento				●					1
SOC/SIEM y carpetas compartidas								●	1

Fuente: Elaboración propia a partir de las fichas BIA (Anexo B) y de COAC Yuyay (s. f.).

Cuatro elementos sostienen los ocho servicios: el enlace de Internet, el firewall con la red interna, el centro de datos con su energía y el Coordinador de Sistemas. De ellos, el enlace es el único que no tiene ninguna alternativa hoy el generador respalda la energía y el Ingeniero de Sistemas suple de hecho al Coordinador, y su falla ya produjo la interrupción más

larga del período. Le siguen la infraestructura en la nube, de la que dependen siete servicios, y el core financiero con su proveedor, del que dependen seis. Estos activos concentran la evaluación de riesgos y las estrategias de las fases siguientes.

4.9. Fase 5: Evaluación de riesgos

4.9.1. Criterios de valoración y de aceptación

Los riesgos se valoran con la escala única de cinco niveles de probabilidad (Tabla 2) y de impacto (Tabla 3), y el nivel de riesgo se obtiene como su producto, ubicado en las cuatro zonas de la Ilustración 2: bajo (1 a 4), medio (5 a 9), alto (10 a 14) y crítico (15 a 25) (IEC, 2019; MHAP, 2012a). La probabilidad se estimó con el historial de interrupciones de la entrevista y los antecedentes del informe de riesgos; el impacto, con la escala de la Tabla 3 aplicada a los servicios afectados y a la duración probable de la interrupción. Se calculan dos valores: el riesgo inherente, sin considerar salvaguardas, y el riesgo residual, con las salvaguardas que existen hoy.

Como criterio de aceptación, que deberá aprobar la Gerencia General, se propone que, una vez aplicado el tratamiento del plan, ningún riesgo residual permanezca en las zonas alta o crítica. Por eso, los riesgos actuales con valor de 10 o más requieren tratamiento en el plan, los de nivel medio se tratan cuando la solución es de bajo costo o se monitorean, y los de nivel bajo se aceptan.

4.9.2. Escenarios de interrupción

Se identificaron 13 escenarios de interrupción de los servicios digitales, que combinan los riesgos de disponibilidad del informe institucional, las amenazas valoradas en el libro de riesgos y los eventos relatados en la entrevista (Tabla 27). Las amenazas se codifican según el catálogo de MAGERIT (MHAP, 2012b).

Tabla 27

Escenarios de interrupción de los servicios digitales

ID	Escenario	Activos	Amenaza MAGERIT	Vulnerabilidad principal	Servicios	Antecedentes
RC-01	Interrupción del enlace de Internet	ACT-COM-02	[I.8] Fallo de servicios de comunicaciones	Enlace único; reparación contractual de 6 h	Todos	Caída de 6 h (marzo 2025); 2–3 microcortes al mes
RC-02	Indisponibilidad del core financiero o de su base de datos	ACT-SW-02, ACT-SW-08	[I.5] Avería de origen físico o lógico	DRP no probado; sin réplica; restablecimiento contractual de 24 h	SD-01 a SD-06	R23 (extremo)
RC-03	Falla por cambios o actualizaciones del proveedor	ACT-SW-02, ACT-SW-01	[E.21] Errores de mantenimiento o actualización de programas	Gestión de cambios del proveedor sin control formal de la cooperativa	SD-01 a SD-06	App fuera de servicio 3 h (agosto 2025); R26 (extremo)
RC-04	Pérdida o corrupción de datos, incluido cifrado por ransomware	ACT-D-02, ACT-D-04	[E.18] Destrucción de información; [A.8] Difusión de software dañino	Respaldos solo en el sitio principal; RPO real de 24 h	SD-01 a SD-06	R24 (alto); amenaza E.8 crítica en el libro de riesgos
RC-05	Terminación o incumplimiento del contrato del proveedor del core	ACT-P-05	Dependencia de terceros (sin código en el catálogo)	Sin plan de salida ni respaldo del código fuente	SD-01 a SD-06	R28 (extremo)
RC-06	Indisponibilidad de la red de tarjetas	ACT-S-05, ACT-P-07	[I.8] Fallo de servicios de comunicaciones	Sin SLA de disponibilidad ni alternativa	SD-04, SD-05	TD-05 (alto)
RC-07	Falla de un cajero automático	ACT-HW-15/16, ACT-P-09	[I.5] Avería de origen físico o lógico	Sin SLA de mantenimiento	SD-04	Cajero fuera 2 días (enero 2026); 1 caída breve al mes; R32
RC-08	Corte prolongado de energía eléctrica	ACT-AUX-03, ACT-AUX-08	[I.6] Corte del suministro eléctrico	Agencias solo con UPS de 30 min	Todos	Corte de 2 h sin afectación (julio 2026)
RC-09	Denegación de servicio sobre los canales	ACT-S-04, ACT-COM-02	[A.24] Denegación de servicio	Sin protección específica frente a ataques volumétricos	SD-02, SD-03, SD-06	A.24 crítica sobre el core en el libro de riesgos
RC-10	Falla de la infraestructura del proveedor de nube	ACT-S-02, ACT-P-06	[I.5] Avería de origen físico o lógico	Respuesta contractual de 8 h; certificaciones no verificadas	SD-01 a SD-07	I.5 crítica en el libro de riesgos; R31 (alto)
RC-11	Ausencia del personal clave de TI	ACT-P-04, ACT-P-01	[E.28] Indisponibilidad del personal	Tres personas; sin suplentes formales ni procedimientos documentados	Todos	Entrevista (G1, G5)
RC-12	Falla del monitoreo de seguridad	ACT-S-07, ACT-P-08	[I.8] Fallo de servicios de comunicaciones	Sin métricas de detección del SOC	SD-08	R30 (alto)

ID	Escenario	Activos	Amenaza MAGERIT	Vulnerabilidad principal	Servicios	Antecedentes
RC-13	Siniestro en el centro de datos (incendio o inundación)	ACT-L-01, ACT-ME-DIA-02	[N.1] Fuego; [N.2] Daños por agua	Respaldos almacenados en el mismo sitio	Todos	Sin antecedentes

Fuente: Elaboración propia a partir de COAC Yuyay (s. f., 2026a), MHAP (2012b) y la entrevista (Anexo A).

4.9.3. Valoración del riesgo inherente y residual

Tabla 28

Valoración del riesgo inherente y del riesgo residual actual de los escenarios (antes del plan)

ID	P	I	Riesgo inherente	Salvaguardas existentes	P	I	Riesgo residual actual
RC-01	4	5	20 Crítico	Monitoreo de enlaces; pruebas semestrales; atención manual en ventanilla no documentada	4	4	16 Crítico
RC-02	3	5	15 Crítico	Redundancia interna del proveedor de nube; respaldo diario; restauración probada en 3,5 h; DRP contractual no probado	3	4	12 Alto
RC-03	4	4	16 Crítico	Ambientes de producción, contingencia y pruebas; reversión de versiones; parches por tickets	3	4	12 Alto
RC-04	3	5	15 Crítico	Respaldo diario con retención; antimalware; SOC; archivos de registro de Oracle en OCI	2	5	10 Alto
RC-05	2	5	10 Alto	Ninguna efectiva: contrato vigente sin plan de salida ni compromisos de recuperación	2	5	10 Alto
RC-06	3	4	12 Alto	Monitoreo transaccional del proveedor; bloqueo telefónico; retiro en ventanilla	3	3	9 Medio
RC-07	4	3	12 Alto	Segundo cajero; ventanilla; mantenimiento externo sin SLA	4	2	8 Medio
RC-08	3	4	12 Alto	Generador de 12 h y UPS en la Matriz; UPS de 30 min en agencias	3	2	6 Medio
RC-09	3	4	12 Alto	Firewall perimetral; monitoreo del SOC 24/7	2	4	8 Medio
RC-10	2	5	10 Alto	Ninguna efectiva: la redundancia interna del proveedor ya está considerada en el riesgo inherente y los respaldos locales no permiten operar sin la nube	2	5	10 Alto
RC-11	3	3	9 Medio	Suplencia de hecho del Ingeniero de Sistemas	3	3	9 Medio
RC-12	3	2	6 Medio	Revisión de alertas por el área de TI	3	2	6 Medio

ID	P	I	Riesgo inherente	Salvaguardas existentes	P	I	Riesgo residual actual
RC-13	1	5	5 Medio	Climatización; detección de humo; control de acceso	1	5	5 Medio

Nota: P = probabilidad (Tabla 2); I = impacto (Tabla 3). Fuente: Elaboración propia.

Sin salvaguardas, cuatro escenarios son críticos, seis altos y tres medios. Las salvaguardas existentes reducen el riesgo de forma desigual: bajan a nivel medio los escenarios de tarjetas, cajeros, energía y denegación de servicio, pero dejan en zona alta o crítica los seis que tienen que ver con la conectividad, el core financiero, los datos y los proveedores. El enlace de Internet (RC-01) se mantiene crítico porque la única salvaguarda que reduce su impacto, la atención manual en ventanilla, no está documentada ni probada. Su valor actual de 16 supera el criterio de aceptación y lo convierte en la primera prioridad de tratamiento: con las estrategias E-03, E-09 y E-12, su riesgo objetivo baja a 6, nivel medio (Tabla 29). Los escenarios de terminación del contrato del core (RC-05) y de falla del proveedor de nube (RC-10) no se reducen en absoluto, porque la cooperativa no tiene hoy salvaguardas efectivas sobre ellos: el contrato del core carece de plan de salida y la continuidad de la nube depende por completo del proveedor. Las estrategias E-04 (RC-05) y E-02 con E-05 (RC-10) los llevan a nivel medio. El resultado coincide con el informe de riesgos institucional, que califica como extremos los riesgos del core y de su proveedor (COAC Yuyay, 2026a), y lo precisa con el historial real de interrupciones.

4.9.4. Plan de tratamiento de los riesgos

La Tabla 29 define la opción de tratamiento de cada escenario, las estrategias de la sección 4.11 que lo atienden y el riesgo residual objetivo, es decir, el que se espera una vez implementadas. La Ilustración 10 compara la situación actual con la objetivo.

Tabla 29

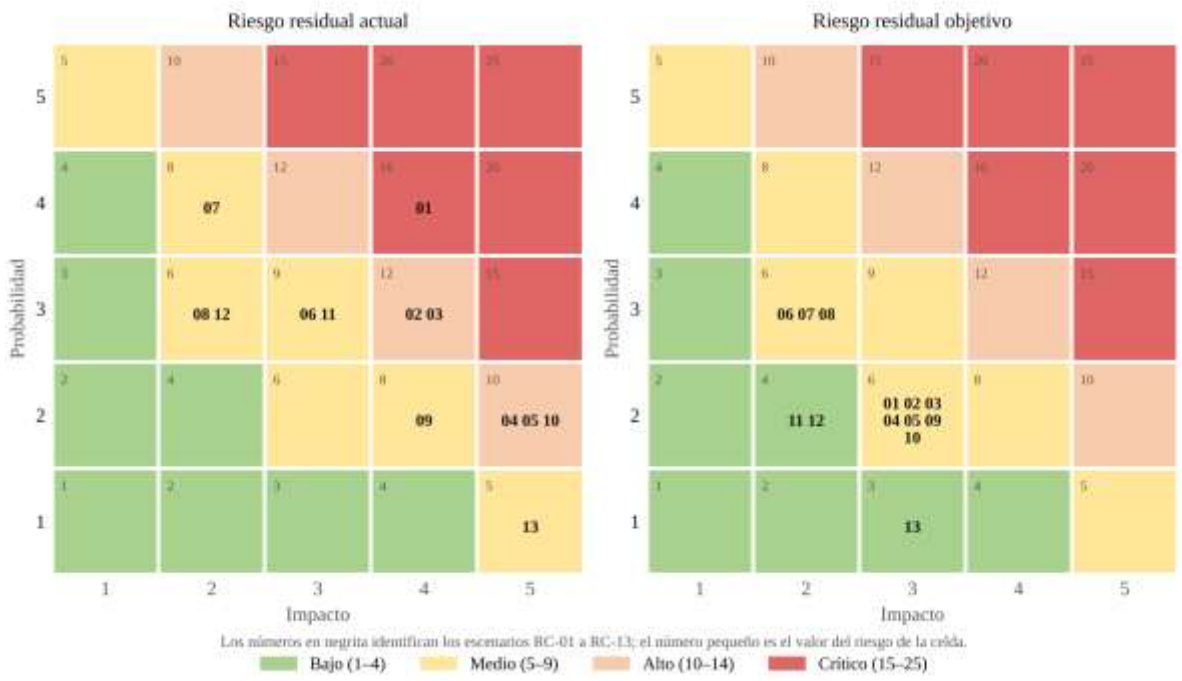
Plan de tratamiento y riesgo residual objetivo

ID	Opción	Estrategias (sección 4.11)	P	I	Riesgo objetivo	Riesgo residual actual
RC-01	Reducir	E-03, E-09, E-12	2	3	6 Medio	16 Crítico
RC-02	Reducir	E-02, E-04, E-09	2	3	6 Medio	12 Alto
RC-03	Reducir	E-07	2	3	6 Medio	12 Alto
RC-04	Reducir	E-01, E-02	2	3	6 Medio	10 Alto
RC-05	Reducir	E-04	2	3	6 Medio	10 Alto
RC-06	Reducir	E-06, E-09	3	2	6 Medio	9 Medio
RC-07	Reducir	E-06	3	2	6 Medio	8 Medio
RC-08	Aceptar y monitorear	E-11 (complementaria)	3	2	6 Medio	6 Medio
RC-09	Reducir	E-08, E-12	2	3	6 Medio	8 Medio
RC-10	Reducir	E-02, E-05	2	3	6 Medio	10 Alto
RC-11	Reducir	E-10	2	2	4 Bajo	9 Medio
RC-12	Reducir	E-12	2	2	4 Bajo	6 Medio
RC-13	Reducir	E-01, E-11	1	3	3 Bajo	5 Medio

Fuente: Elaboración propia.

Ilustración 10

Ubicación de los escenarios en la matriz de riesgo: situación actual y objetivo



Fuente: Elaboración propia con la matriz de la Ilustración 2.

Con el tratamiento propuesto, ningún escenario queda en las zonas alta o crítica: diez se ubican en nivel medio y tres en nivel bajo, lo que satisface el criterio de aceptación. Los

riesgos medios remanentes reflejan una realidad que el plan no puede eliminar la cooperativa seguirá dependiendo de un proveedor de core, de una red de tarjetas y de la nube, pero sí acotar: lo que cambia es que, cuando el evento ocurra, existirán una alternativa técnica, un compromiso contractual y un procedimiento probado.

4.10. Fase 6: Análisis de impacto al negocio

4.10.1. Evolución del impacto y período máximo tolerable

El análisis de impacto se aplicó a los ocho servicios en la sesión del 1 de octubre de 2026, con las fichas del Anexo B y el procedimiento de ISO/TS 22317 (ISO, 2021b). Para cada servicio se valoró el impacto operativo, financiero, legal y reputacional en seis horizontes de interrupción, y se tomó el máximo de las cuatro dimensiones como impacto del período (Tabla 30). El MTPD es la primera duración en la que ese impacto alcanza el nivel 4 (Mayor).

Tabla 30

Impacto máximo según la duración de la interrupción

Cód.	Servicio digital	1 h	4 h	8 h	24 h	72 h	1 sem.	MTPD
SD-01	Core financiero	2	3	4	5	5	5	8 h
SD-02	Web transaccional	1	2	3	4	5	5	24 h
SD-03	Aplicación móvil Yuyay Móvil	1	2	3	4	5	5	24 h
SD-04	Cajeros automáticos	1	2	3	4	5	5	24 h
SD-05	Tarjetas de débito (COONECTA)	2	3	4	5	5	5	8 h
SD-06	Transferencias electrónicas y recaudaciones	1	2	3	4	5	5	24 h
SD-07	Infraestructura en la nube y enlace de Internet	2	3	4	5	5	5	8 h
SD-08	Monitoreo de seguridad y carpetas compartidas	1	1	2	2	4	5	72 h

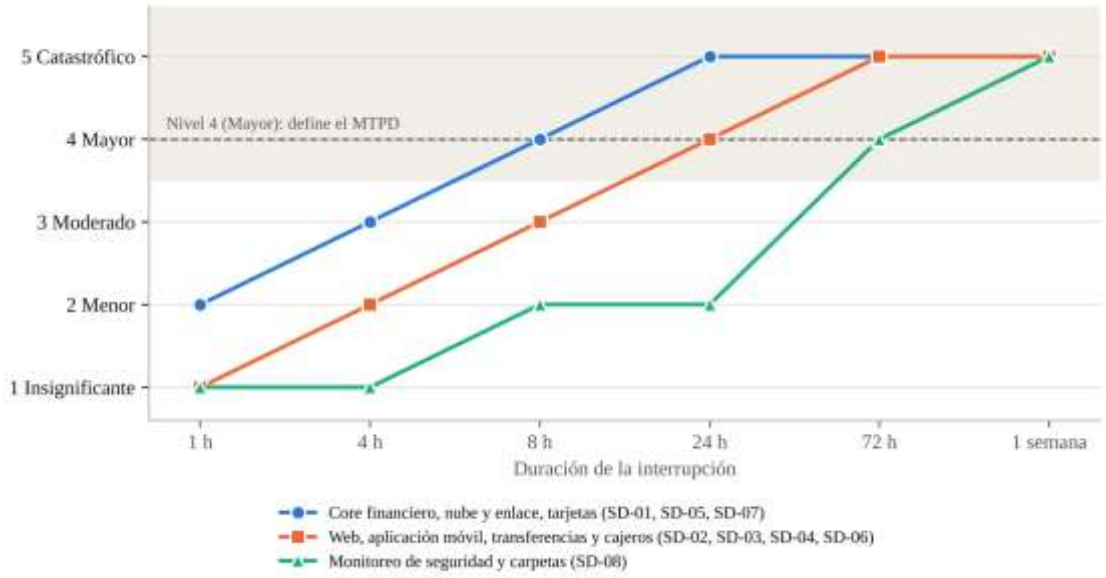
Nota: escala de impacto de la Tabla 3 (1 = insignificante; 5 = catastrófico). Fuente: Fichas BIA (Anexo B).

Los ocho servicios se agrupan en tres perfiles de impacto (Ilustración 11). El core financiero, la infraestructura en la nube con el enlace y las tarjetas de débito alcanzan el nivel 4 a las 8 horas, porque de ellos depende la atención en ventanilla o el acceso de los socios a su

dinero fuera del cantón. Los canales digitales, las transferencias y los cajeros lo alcanzan a las 24 horas, gracias a que la ventanilla y el segundo cajero absorben la demanda durante una jornada. El monitoreo de seguridad y las carpetas compartidas solo producen un impacto mayor a partir de las 72 horas, cuando la falta de detección empieza a exponer a la cooperativa a incidentes no atendidos.

Ilustración 11

Evolución del impacto en el tiempo por perfil de servicio



Fuente: Elaboración propia a partir de las fichas BIA (Anexo B).

4.10.2. Brechas entre los parámetros requeridos y la capacidad actual

Los parámetros validados en el análisis de impacto (Tabla 12) se contrastaron con la capacidad de recuperación que hoy puede demostrarse: los tiempos comprometidos en los contratos, los resultados de la prueba de restauración y los eventos reales del historial (Tabla 31; Ilustración 12).

Tabla 31

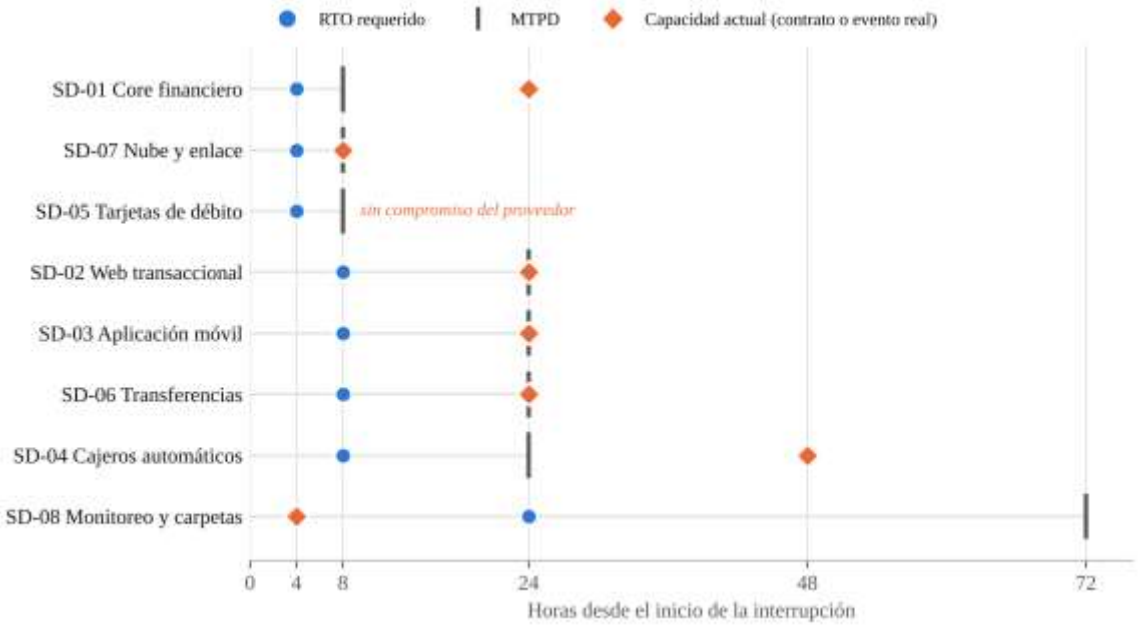
Brecha entre los parámetros de recuperación requeridos y la capacidad actual

Cód.	Servicio	RTO	Capacidad actual de recuperación	RPO	RPO actual	Brecha principal
SD-01	Core financiero	4 h	24 h según contrato; 3,5 h en la prueba de restauración	1 h	24 h	Contrato y RPO
SD-02	Web transaccional	8 h	Hereda SD-01 y SD-07 (hasta 24 h)	1 h	24 h	Dependencia del core
SD-03	Aplicación móvil	8 h	Hereda SD-01 y SD-07 (hasta 24 h)	1 h	24 h	Dependencia del core
SD-04	Cajeros automáticos	8 h	Sin SLA; 48 h en la falla de enero de 2026	N/A	N/A	Mantenimiento
SD-05	Tarjetas de débito	4 h	Sin compromiso del proveedor	Según proveedor	Sin dato	SLA inexistente
SD-06	Transferencias y recaudaciones	8 h	Hereda SD-01 (hasta 24 h)	1 h	24 h	Dependencia del core
SD-07	Nube y enlace de Internet	4 h (objetivo técnico: 2 h)	6 h (reparación del enlace); 8 h (respuesta del contratista de OCI); ninguna de las dos cabe en el objetivo de 2 h sin el enlace secundario	N/A	N/A	Enlace único y SLA
SD-08	Monitoreo y carpetas	24 h	4 h (respuesta del SOC a alertas críticas)	24 h	24 h	Sin brecha

Fuente: Elaboración propia a partir de las fichas BIA (Anexo B) y de la entrevista (Anexo A).

Ilustración 12

RTO requerido, MTPD y capacidad actual de recuperación por servicio



Fuente: Elaboración propia a partir de las fichas BIA (Anexo B) y de la entrevista (Anexo A).

Siete de los ocho servicios no pueden demostrar hoy que se recuperarían dentro de su RTO, y seis alcanzarían o superarían su MTPD si el evento se resolviera en el plazo máximo que admiten los contratos o que se observó en la falla de enero de 2026. La causa es común: los servicios digitales heredan el tiempo de recuperación del core financiero y de la conectividad, cuyos compromisos contractuales 24 y 6 horas exceden el RTO de 4 horas. Solo el monitoreo de seguridad tiene una capacidad superior a la requerida. La prueba de restauración de 3,5 horas demuestra que la recuperación técnica del core es viable dentro del RTO, pero la cooperativa no puede exigirla mientras el contrato admita 24 horas.

4.10.3. Prioridades y secuencia de recuperación

La secuencia de recuperación combina la prioridad de negocio fijada por los informantes con las dependencias técnicas: un servicio no puede recuperarse antes que aquellos de los que depende (Tabla 32). Los RTO de la Tabla 12 son los tiempos que el negocio tolera para cada servicio; como las dependencias se recuperan en serie, el RTO de un servicio dependiente incluye el tiempo de recuperación de sus dependencias. Por ello, el plan fija para SD-07 un objetivo técnico de 2 horas, la mitad del RTO del core, de modo que, cuando la interrupción comience en la nube o en el enlace, al core le queden 2 horas netas para restaurarse; las tarjetas de débito se recuperan en paralelo con el core, y los servicios de prioridad 3 a 5 disponen de 4 horas netas una vez recuperado el core. Este ajuste hace más exigente la brecha del core, porque la restauración probada de 3,5 horas supera las 2 horas netas: hasta que opere la réplica en espera (E-02 B), una interrupción que afecte primero a SD-07 solo puede resolverse dentro del MTPD de 8 horas, no dentro del RTO.

Tabla 32

Secuencia de recuperación y recursos mínimos por servicio

Orden	Servicio	RTO	Requiere previamente	Recursos mínimos para reanudar
1	SD-07 Nube y enlace de Internet	4 h (objetivo técnico: 2 h)	Energía, firewall y LAN	Enlace operativo (principal o secundario); Coordinador o Ingeniero de Sistemas; operador y contratista de OCI
1	SD-01 Core financiero	4 h (2 h netas si falló antes SD-07)	SD-07	Base de datos íntegra (réplica o respaldo físico RMAN con archivos de registro); proveedor del core; Coordinador de Sistemas
2	SD-05 Tarjetas de débito	4 h (en paralelo con SD-01)	SD-01 y SD-07	Conexión con COONECTA; Oficial de Seguridad de la Información; Jefe de Negocios
3	SD-02 Web y SD-03 Aplicación móvil	8 h (4 h netas tras SD-01)	SD-01 y SD-07	Canales electrónicos, certificado TLS y claves de cifrado; Ingeniero de Sistemas; soporte del proveedor de la aplicación
4	SD-06 Transferencias y recaudaciones	8 h (4 h netas tras SD-01)	SD-01	Aplicación de recaudaciones y orquestador; Tesorería; verificación de transferencias SPI pendientes
5	SD-04 Cajeros automáticos	8 h (4 h netas tras SD-01)	SD-01, SD-05 y energía	Al menos un cajero operativo; proveedor de mantenimiento; Tesorería y Cajas
6	SD-08 Monitoreo y carpetas	24 h	SD-07	Servicio del SOC; NAS o SharePoint; Oficial de Seguridad de la Información

Fuente: Elaboración propia a partir de las fichas BIA (Anexo B) y de la entrevista (Anexo A, F5).

4.11. Fase 7: Estrategias y soluciones de continuidad

4.11.1. Criterios de selección

Las estrategias se seleccionaron con los cuatro criterios que recomienda la guía ISO 22313: capacidad de cumplir el RTO y el RPO, costo, efectos sobre otras actividades y viabilidad de implementación (ISO, 2020). Se añadió un quinto criterio derivado del diagnóstico, la capacidad del área de TI para operar la solución, y se privilegiaron las soluciones que trasladan obligaciones a los proveedores mediante contrato antes que las que exigen infraestruc-

tura propia. Los costos se expresan en términos relativos (bajo, medio o alto) porque su cuantificación requiere cotizaciones que la cooperativa deberá solicitar antes de aprobar el presupuesto.

4.11.2. Evaluación de alternativas para los servicios críticos

Tabla 33

Evaluación de alternativas para los recursos críticos

Necesidad	Alternativa	¿Cumple el parámetro?	Costo relativo	Decisión
Datos del core (RPO 1 h)	Mantener solo el respaldo diario	No (24 h)		Descartada
	Respaldo físico con RMAN en modo ARCHIVELOG y copia horaria de los archivos de registro (archive logs) a un almacenamiento externo	Sí (RPO ≤ 1 h)	Bajo	Seleccionada (corto plazo)
	Réplica de la base de datos en espera en una segunda región de la nube	Sí (RPO de minutos; RTO < 1 h)	Medio a alto	Seleccionada (mediano plazo)
Infraestructura del core (RTO 4 h)	Depender del DRP contractual vigente	No (24 h; sin prueba)		Descartada
	Adenda con RTO de 4 h, RPO de 1 h y ejecución anual del DRP	Sí, si se prueba	Bajo a medio	Seleccionada
	Sitio alterno físico propio	Sí	Alto	Descartada: el core ya opera en la nube
Conectividad (RTO 4 h)	Enlace único con reparación en 6 h	No		Descartada
	Segundo enlace con otro operador y ruta física distinta, con conmutación automática	Sí	Medio	Seleccionada (en contratación)
	Enlace móvil 4G de contingencia para la ventanilla de cada oficina	Parcial (garantiza el MBCO)	Bajo	Seleccionada como complemento
Tarjetas (RTO 4 h)	SLA con COONECTA con restablecimiento ≤ 4 h	Sí	Bajo	Seleccionada
	Contratar una segunda red de pagos	Sí	Alto	Descartada por costo
Cajeros (RTO 8 h)	SLA de mantenimiento con atención ≤ 8 h y repuestos críticos	Sí	Bajo	Seleccionada
Personas	Suplentes formales, procedimientos documentados y capacitación cruzada	Sí	Bajo	Seleccionada
	Contratar personal adicional de TI	Sí	Alto	Diferida a la revisión anual

Fuente: Elaboración propia a partir de ISO (2020) y de la entrevista (Anexo A).

La decisión central es la estrategia de datos del core en dos etapas. El respaldo físico con RMAN en modo ARCHIVELOG, con copia horaria de los archivos de registro a un almacenamiento externo, cumple el RPO de 1 hora a bajo costo y en pocas semanas. El respaldo lógico actual con Data Pump no sirve para este fin, porque los archivos de registro no pueden aplicarse sobre una importación lógica: la recuperación a un punto en el tiempo exige respaldos físicos de la base de datos (Anexo A, D1). Aun con RMAN, la recuperación sigue dependiendo de una restauración que tomó 3,5 horas en la prueba, apenas dentro del RTO. La réplica en espera en una segunda región elimina esa dependencia y reduce la recuperación a minutos, pero su costo justifica implementarla después de la renegociación del contrato, cuando el proveedor quede obligado a operarla y probarla.

4.11.3. Estrategias seleccionadas

La Tabla 34 reúne las 13 estrategias seleccionadas, organizadas por tipo de recurso conforme a la cláusula 8.3.2 de la norma (ISO, 2019), con los escenarios de riesgo y los hallazgos que atienden.

Tabla 34

Estrategias y soluciones de continuidad seleccionadas

Cód.	Estrategia o solución	Recurso	Escenarios	Hallazgos
E-01	Copia de los respaldos fuera del sitio principal según la regla 3-2-1, con una copia inmutable o desconectada, y prueba mensual de restauración	Información	RC-04, RC-13	H2
E-02	Respaldo físico con RMAN en modo ARCHIVELOG y copia horaria de los archivos de registro a almacenamiento externo (etapa A), y réplica en espera en una segunda región de la nube (etapa B)	Información y tecnología	RC-02, RC-04, RC-10	H2, H4
E-03	Segundo enlace de Internet con otro operador y ruta física distinta, con conmutación automática, y enlace 4G de contingencia para la ventanilla	Tecnología	RC-01	H4, H5
E-04	Adenda con el proveedor del core: RTO de 4 h, RPO de 1 h, ejecución anual del DRP con presencia de la cooperativa, penalizaciones, plan de salida y custodia del código fuente	Proveedores	RC-02, RC-05	H3

Cód.	Estrategia o solución	Recurso	Escenarios	Hallazgos
E-05	SLA con el contratista de OCI: respuesta de 1 h a incidentes críticos y evidencia anual de certificaciones ISO/IEC 27001 y 27017	Proveedores	RC-10	H3
E-06	SLA con COONECTA (restablecimiento ≤ 4 h y notificación de incidentes) y con el proveedor de mantenimiento de cajeros (atención ≤ 8 h)	Proveedores	RC-06, RC-07	H3
E-07	Gestión formal de cambios del proveedor: ventanas fuera de horas pico y días de pago, prueba previa, plan de reversión y aprobación	Procesos	RC-03	H6
E-08	Protección frente a denegación de servicio con el operador o mediante un cortafuegos de aplicaciones web	Tecnología	RC-09	H4
E-09	Procedimientos documentados de operación degradada con formularios prenumerados, montos máximos, doble control y conciliación	Personas y procesos	RC-01, RC-02, RC-06	H7
E-10	Designación del Oficial de Continuidad y de suplentes, registrados en el campo de respaldo de los manuales de funciones; procedimientos técnicos escritos y capacitación cruzada en el área de TI	Personas	RC-11	H8
E-11	Sitio alterno de trabajo en la agencia Terminal Terrestre con acceso a OCI, renovación de UPS en agencias y contrato de suministro de combustible	Instalaciones	RC-08, RC-13	H4
E-12	Monitoreo de disponibilidad de los servicios con alertas y SLA del SOC con métricas de detección	Tecnología y proveedores	RC-01, RC-09, RC-12	H3
E-13	Plan de comunicación con mensajes predefinidos y procedimiento de notificación a la SEPS	Personas	Todos	H9

Fuente: Elaboración propia.

4.11.4. Hoja de ruta de implementación

Las estrategias se ordenan en tres horizontes según su urgencia, su costo y su dependencia de otras decisiones (Tabla 35; Ilustración 13). El primer trimestre concentra las medidas de bajo costo que cierran las brechas más graves copia fuera del sitio, RPO de 1 hora, roles y operación degradada; el segundo y tercer trimestres, la renegociación de contratos, que puede coincidir con sus renovaciones; y el último, la réplica en espera y la protección frente a denegación de servicio, que requieren presupuesto aprobado.

Tabla 35

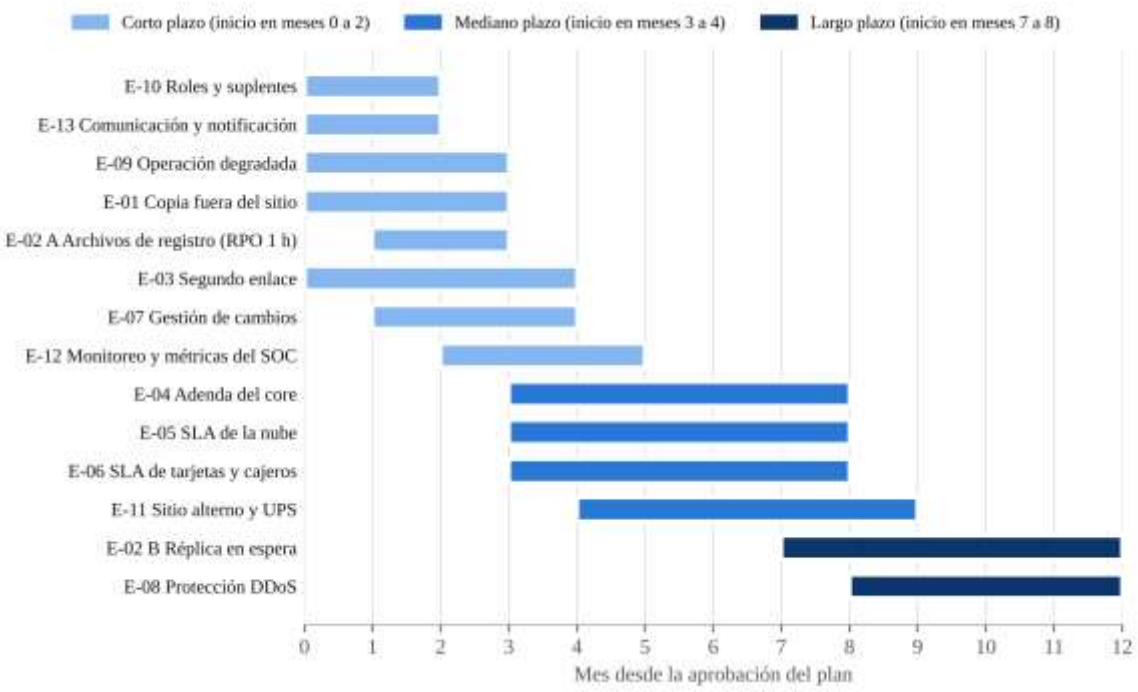
Hoja de ruta de implementación de las estrategias

Cód.	Acción principal	Responsable	Plazo (meses)	Costo	Evidencia de cumplimiento
E-10	Designar al Oficial de Continuidad y a los suplentes, y registrarlos en los manuales de funciones; documentar procedimientos técnicos	Gerente General	0–2	Bajo	Resolución de designación
E-13	Aprobar mensajes predefinidos y procedimiento de notificación a la SEPS	Oficial de Continuidad	0–2	Bajo	Procedimiento aprobado
E-09	Documentar la operación degradada e imprimir formularios	Jefe de Negocios	0–3	Bajo	Procedimiento y formularios
E-01	Implementar la copia fuera del sitio y la prueba mensual de restauración	Coordinador de Sistemas	0–3	Bajo	Acta de la primera prueba
E-02 A	Migrar el respaldo a RMAN en modo ARCHIVELOG y copiar cada hora los archivos de registro a almacenamiento externo	Coordinador de Sistemas	1–3	Bajo	Prueba con RPO ≤ 1 h
E-03	Completar la contratación del segundo enlace y la conmutación automática	Coordinador de Sistemas	0–4	Medio	Prueba de conmutación
E-07	Acordar con el proveedor el procedimiento de cambios	Coordinador de Sistemas	1–4	Bajo	Procedimiento firmado
E-12	Configurar el monitoreo de disponibilidad y las métricas del SOC	Oficial de Seguridad de la Información	2–5	Bajo	Reporte mensual
E-04	Negociar la adenda con el proveedor del core	Gerente General	3–8	Bajo a medio	Adenda firmada
E-05	Negociar el SLA con el contratista de OCI	Gerente General	3–8	Bajo	SLA firmado
E-06	Negociar los SLA con COONECTA y con el mantenimiento de cajeros	Gerente General	3–8	Bajo	SLA firmados
E-11	Habilitar el sitio alterno de trabajo y renovar las UPS de agencias	Oficial de Seguridad Física y Electrónica	4–9	Medio	Prueba de operación desde el sitio alterno
E-02 B	Implementar la réplica en espera en una segunda región	Coordinador de Sistemas y proveedor	7–12	Medio a alto	Ejercicio de conmutación
E-08	Contratar la protección frente a denegación de servicio	Coordinador de Sistemas	8–12	Medio	Servicio activo

Fuente: Elaboración propia.

Ilustración 13

Cronograma de implementación de las estrategias en los primeros 12 meses



Fuente: Elaboración propia.

4.12. Fase 8: Planes, ejercicios y mantenimiento

4.12.1. Niveles de activación

La cláusula 8.4.2 exige una estructura de respuesta con criterios para activar los planes (ISO, 2019). Se definen tres niveles con criterios objetivos, derivados del RTO de cada servicio: la contingencia se declara cuando una interrupción consume la mitad del RTO sin solución a la vista, de modo que quede tiempo para recuperar el servicio antes de alcanzarlo (Tabla 36).

Tabla 36

Niveles de activación del plan de continuidad

Nivel	Criterios de activación	Declara	Respuesta
1. Incidente	Falla de un servicio con restablecimiento estimado menor a 1 h; caídas breves de los canales	Ingeniero de Sistemas	Gestión ordinaria de incidentes; registro en el gestor de incidentes
2. Contingencia	Indisponibilidad de un servicio de prioridad 1 o 2 por más de 30 min, o de prioridad 3 a 6 por más de 2 h; o restablecimiento estimado superior a la mitad del RTO	Coordinador de Sistemas	Equipo de recuperación tecnológica; operación degradada; mensaje inicial a los socios; aviso al Oficial de Continuidad y al Gerente

Nivel	Criterios de activación	Declara	Respuesta
3. Crisis	Indisponibilidad de SD-01 o SD-07 por más de 30 min sin solución confirmada en sitio; riesgo de superar el MTPD de cualquier servicio; pérdida o corrupción de datos; ciberataque confirmado; siniestro en una oficina	Gerente General	Comité de crisis; activación de estrategias alternas; notificación inmediata a la SEPS y, si aplica, a la SPDP en un plazo máximo de cinco días

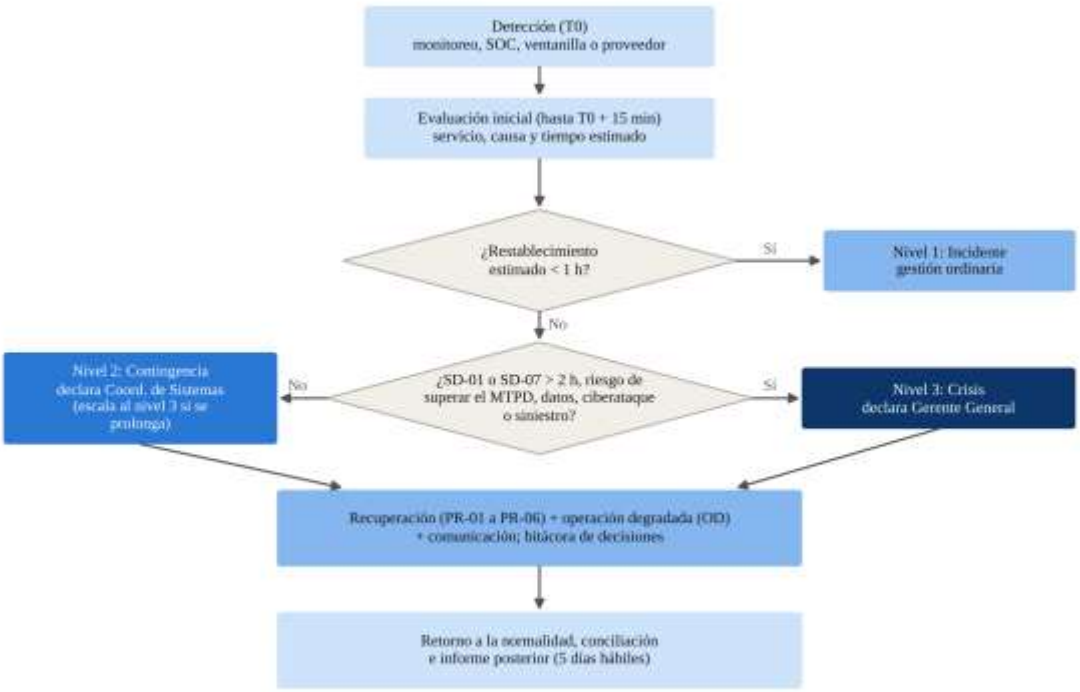
Fuente: Elaboración propia a partir de ISO (2019) y de las fichas BIA (Anexo B).

4.12.2. Procedimiento de activación y escalamiento

La Ilustración 14 representa el flujo desde la detección hasta el cierre. Las decisiones de escalamiento se registran en una bitácora con la hora de cada evento, que constituye la evidencia para medir los tiempos de activación y de recuperación.

Ilustración 14

Flujo de activación y escalamiento del plan



Fuente: Elaboración propia.

- Detección: el monitoreo de disponibilidad, el SOC, el personal de ventanilla o un proveedor reporta la falla al Ingeniero de Sistemas, que registra la hora de inicio (T0).

- Evaluación inicial (hasta T0 + 15 min): el Ingeniero de Sistemas identifica el servicio afectado, la causa probable y el tiempo estimado de restablecimiento, y consulta al proveedor si corresponde.
- Clasificación: con los criterios de la Tabla 36, el Coordinador de Sistemas declara el nivel 2 o propone al Gerente General el nivel 3.
- Activación: se ejecuta el procedimiento de recuperación del escenario (sección 4.12.4), el Jefe de Negocios activa la operación degradada y se emite el mensaje inicial a los socios.
- Seguimiento: el Oficial de Continuidad actualiza la bitácora y el Comité, en el nivel 3, se reúne cada dos horas hasta el restablecimiento.
- Cierre: se declara el retorno a la normalidad, se concilian las operaciones manuales y se elabora el informe posterior.

4.12.3. Plan de comunicación

La comunicación es la parte de la respuesta que el diagnóstico encontró más débil: no hay mensajes predefinidos ni procedimiento de notificación al organismo de control (Anexo A, E3). La Tabla 37 establece qué se comunica, a quién, cuándo y por qué medio, y la Tabla 38 propone los mensajes modelo.

Tabla 37

Plan de comunicación durante una interrupción

Audiencia	Contenido	Momento	Canal	Responsable
Personal de la cooperativa	Nivel declarado, servicio afectado e instrucciones de operación degradada	Al declarar el nivel 2 o 3 y en cada cambio	Grupo de WhatsApp institucional, llamada y correo	Oficial de Continuidad
Socios	Servicio afectado, alternativas disponibles y hora estimada de restablecimiento	Hasta 30 min después de declarar el nivel 2; actualización cada 2 h	WhatsApp institucional, Facebook, carteles en agencias y aviso en la aplicación y la web	Jefe de Negocios, con aprobación del Gerente

Audiencia	Contenido	Momento	Canal	Responsable
Proveedores críticos	Reporte técnico y solicitud de escalamiento	Inmediato	Ticket y teléfono del contacto de emergencia	Coordinador de Sistemas
Consejo de Administración	Situación, impacto y decisiones tomadas	Al declarar el nivel 3 y al cierre	Llamada e informe escrito	Gerente General
SEPS	Evento, servicios afectados, impacto y acciones	De inmediato al declarar el nivel 3, con un reporte inicial el mismo día por el canal oficial, conforme a la norma de seguridad de la información (SEPS, 2022); informe de cierre al retornar a la normalidad	Oficio o canal oficial del organismo	Gerente General y Oficial de Continuidad
Autoridad de protección de datos y titulares	Vulneración de datos personales, alcance y medidas adoptadas	A la SPDP, por el SISPDP, en un plazo máximo de cinco días desde que se conozca la vulneración (LOPDP, art. 43; SPDP, 2026); a los titulares, en el término de tres días cuando exista riesgo para sus derechos (LOPDP, art. 44)	Canal oficial de la autoridad; comunicación directa a los titulares	Oficial de Seguridad de la Información
Medios y redes sociales	Posición oficial de la cooperativa	Cuando la interrupción tenga repercusión pública	Comunicado oficial	Gerente General

Fuente: Elaboración propia a partir de la entrevista (Anexo A), SEPS (2018, 2022), Asamblea Nacional del Ecuador (2021) y SPDP (2026).

Tabla 38

Mensajes predefinidos para los socios y el personal

Momento	Mensaje modelo
Inicio (socios)	Estimado socio: en este momento el servicio de [servicio] presenta una interrupción. Sus fondos están seguros. Puede realizar depósitos y retiros en nuestras oficinas de Cañar, Terminal Terrestre, El Tambo y Suscal. Le informaremos cuando el servicio se restablezca. COAC Yuyay Ltda.
Actualización (socios)	Seguimos trabajando para restablecer [servicio]. Hora estimada: [hora]. Nuestras oficinas atienden con normalidad. Gracias por su comprensión.
Restablecimiento (socios)	El servicio de [servicio] se encuentra restablecido desde las [hora]. Si realizó una operación durante la interrupción y observa alguna diferencia en su cuenta, acérquese a cualquiera de nuestras oficinas.

Momento	Mensaje modelo
Activación (personal)	Se declara nivel [2/3] por [evento]. Aplicar el procedimiento [OD-xx]: registrar las operaciones en los formularios prenumerados, respetar los montos máximos autorizados y entregar los formularios al cierre a Tesorería. No emitir declaraciones a terceros.

Fuente: Elaboración propia.

4.12.4. Procedimientos de recuperación por escenario

Se documentan seis procedimientos de recuperación para los escenarios que afectan a los servicios de mayor prioridad o que concentran el riesgo residual. Cada procedimiento indica los pasos, el responsable y el tiempo objetivo medido desde la detección (T0), de forma coherente con el RTO del servicio. Donde una estrategia aún no se ha implementado, el procedimiento indica la alternativa vigente, de modo que el plan sea aplicable desde su aprobación. Los procedimientos técnicos detallados de cada proveedor por ejemplo, los comandos de restauración de la base de datos se mantienen como anexos operativos bajo custodia del Coordinador de Sistemas, conforme a la relación entre el plan de continuidad y el plan de recuperación ante desastres (NIST, 2010).

Tabla 39

Procedimiento PR-01: interrupción del enlace de Internet (SD-07; RTO 4 h; objetivo técnico 2 h)

Paso	Acción	Responsable	Tiempo objetivo
1	Confirmar la pérdida del enlace y descartar una falla del firewall o de la red interna	Ingeniero de Sistemas	T0 + 15 min
2	Verificar la conmutación automática al enlace secundario (E-03) y el acceso a OCI, a la red de pagos y a los canales	Ingeniero de Sistemas	T0 + 30 min
3	Si no hay enlace secundario disponible: activar el enlace 4G de contingencia para la ventanilla y declarar el nivel 2	Coordinador de Sistemas	T0 + 30 min
4	Activar la operación degradada OD-01 y emitir el mensaje inicial a los socios	Jefe de Negocios	T0 + 45 min
5	Abrir el reclamo con el operador y escalar a su nivel gerencial si el tiempo estimado supera 2 h; en ese caso, proponer el nivel 3	Coordinador de Sistemas	T0 + 2 h

Paso	Acción	Responsable	Tiempo objetivo
6	Al restablecerse el enlace (objetivo: 2 h con el enlace secundario; 4 h como máximo): verificar los servicios en el orden de la Tabla 32 y retirar la operación degradada	Ingeniero de Sistemas	≤ T0 + 4 h
7	Digitar y conciliar las operaciones manuales con doble control	Tesorería y Cajas	Mismo día

Fuente: Elaboración propia.

Tabla 40

Procedimiento PR-02: indisponibilidad del core financiero o de su base de datos (SD-01; RTO 4 h; RPO 1 h)

Paso	Acción	Responsable	Tiempo objetivo
1	Confirmar la falla y abrir el ticket de prioridad crítica con el proveedor del core, con llamada al contacto de emergencia	Ingeniero de Sistemas	T0 + 15 min
2	Determinar con el proveedor si la falla es recuperable en sitio (reinicio, reversión de un cambio) y el tiempo estimado	Coordinador de Sistemas	T0 + 30 min
3	Declarar el nivel 2, activar la operación degradada OD-01 y comunicar a los socios	Coordinador de Sistemas; Jefe de Negocios	T0 + 45 min
4	Si la falla no es recuperable en sitio en menos de 30 min: declarar el nivel 3 y ordenar la ejecución del DRP del proveedor (conmutación a la réplica, E-02 B, o restauración RMAN del último respaldo físico íntegro con aplicación de los archivos de registro, E-02 A)	Gerente General	T0 + 30 min
5	Validar la integridad de los datos restaurados: totales de control, saldos de cuentas de muestra y número de la última transacción	Coordinador de Sistemas; Contabilidad	T0 + 4 h con restauración RMAN (3,5 h); T0 + 1 h 30 min con la réplica E-02 B
6	Habilitar la ventanilla y luego los canales en el orden de la Tabla 32	Ingeniero de Sistemas	≤ T0 + 4 h 30 min hasta que opere la réplica; ≤ T0 + 2 h con la réplica
7	Conciliar con COONECTA y verificar las transferencias SPI pendientes antes de reenviarlas	Tesorería	Mismo día

Fuente: Elaboración propia.

Con la capacidad actual, el procedimiento PR-02 no alcanza el RTO de 4 horas: aun declarando el nivel 3 a los 30 minutos, la restauración RMAN de 3,5 horas y la validación de integridad llevan la reanudación hacia T0 + 4 h 30 min, dentro del MTPD de 8 horas pero fuera del RTO. El RTO solo se cumple con la réplica en espera (E-02 B, meses 7 a 12), que reduce la recuperación a menos de 1 hora; por eso el objetivo OC-1 fija un plazo de 12 meses y la Tabla 31 registra esta brecha.

Tabla 41

Procedimiento PR-03: pérdida o corrupción de datos, incluido ransomware (SD-01 a SD-06)

Paso	Acción	Responsable	Tiempo objetivo
1	Aislar los equipos y segmentos afectados y preservar la evidencia, con apoyo del SOC	Oficial de Seguridad de la Información	T0 + 30 min
2	Declarar el nivel 3 y convocar al Comité de crisis; no negociar ni pagar rescates	Gerente General	T0 + 1 h
3	Identificar el último respaldo íntegro, verificando su integridad antes de usarlo, a partir de la copia fuera del sitio (E-01)	Coordinador de Sistemas	T0 + 2 h
4	Restaurar con RMAN en un entorno limpio y aplicar los archivos de registro hasta el punto más reciente sin compromiso	Proveedor del core; Coordinador de Sistemas	T0 + 4 h
5	Cambiar las credenciales privilegiadas y revisar los accesos antes de reconectar los servicios	Oficial de Seguridad de la Información	Antes de reconectar
6	Notificar a la SEPS y, si hubo datos personales comprometidos, a la autoridad de protección de datos y a los titulares	Gerente General; Oficial de Seguridad de la Información	Según la Tabla 37

Fuente: Elaboración propia.

Tabla 42

Procedimiento PR-04: indisponibilidad de la red de tarjetas (SD-05; RTO 4 h)

Paso	Acción	Responsable	Tiempo objetivo
1	Confirmar la indisponibilidad con el centro de operaciones de COONECTA y obtener el tiempo estimado	Oficial de Seguridad de la Información	T0 + 30 min
2	Declarar el nivel 2 y emitir el mensaje a los socios con la alternativa de retiro en ventanilla	Coordinador de Sistemas; Jefe de Negocios	T0 + 45 min
3	Habilitar el retiro en ventanilla con cédula (OD-02) y mantener el bloqueo de tarjetas por vía telefónica	Jefe de Negocios	T0 + 1 h

Paso	Acción	Responsable	Tiempo objetivo
4	Si la interrupción supera 2 h en día de pago o fin de mes: extender el horario de atención de las agencias	Gerente General	T0 + 2 h
5	Al restablecerse: conciliar las transacciones con CONECTA y registrar los débitos no reconocidos	Tesorería	Siguiente día hábil

Fuente: Elaboración propia.

Tabla 43

Procedimiento PR-05: falla de un cajero automático (SD-04; RTO 8 h)

Paso	Acción	Responsable	Tiempo objetivo
1	Retirar el cajero de servicio, colocar el aviso con la ubicación del otro cajero y de la ventanilla	Tesorería y Cajas	T0 + 30 min
2	Reportar la falla al proveedor de mantenimiento con la prioridad del SLA (E-06)	Coordinador de Sistemas	T0 + 30 min
3	Verificar el efectivo y cuadrar el cajero; registrar los débitos sin entrega de efectivo	Tesorería y Cajas	T0 + 2 h
4	Si ambos cajeros están fuera de servicio: declarar el nivel 2 y aplicar OD-03	Coordinador de Sistemas	T0 + 2 h
5	Verificar el funcionamiento tras la reparación y reponer el servicio	Tesorería y Cajas	≤ T0 + 8 h

Fuente: Elaboración propia.

Tabla 44

Procedimiento PR-06: siniestro en el centro de datos o corte prolongado de energía

Paso	Acción	Responsable	Tiempo objetivo
1	Evacuar y proteger a las personas; activar a los organismos de emergencia si corresponde	Oficial de Seguridad Física y Electrónica	Inmediato
2	En corte de energía: verificar el arranque del generador y la autonomía disponible; solicitar combustible si el corte supera 6 h	Oficial de Seguridad Física y Electrónica	T0 + 15 min
3	En agencias sin generador: cerrar las sesiones del core de forma ordenada antes de agotar las UPS y aplicar OD-01	Jefe de Negocios	T0 + 20 min
4	Si el centro de datos queda inutilizable: declarar el nivel 3 y trasladar la administración al sitio alterno de trabajo (E-11)	Gerente General; Coordinador de Sistemas	T0 + 2 h
5	Restablecer la conectividad de las agencias con OCI desde el sitio alterno y recuperar los respaldos de la copia fuera del sitio (E-01)	Coordinador de Sistemas	T0 + 4 h

Paso	Acción	Responsable	Tiempo objetivo
6	Evaluar los daños, gestionar el seguro y planificar la reconstrucción	Gerente General	Siguiente día hábil

Fuente: Elaboración propia.

4.12.5. Procedimientos de operación degradada

La operación degradada mantiene el MBCO de cada servicio mientras dura la recuperación. Formaliza lo que hoy se hace por práctica (Anexo A, D5) y le añade los controles que exige la seguridad de la información durante la contingencia: registro prenumerado, límites, doble control y conciliación (Tabla 45).

Tabla 45

Procedimientos de operación degradada

Cód.	Servicio afectado	Nivel mínimo (MBCO)	Procedimiento manual	Controles
OD-01	Core financiero o conectividad (SD-01, SD-07)	Consultas, depósitos y retiros de montos pequeños en ventanilla	Consulta con el reporte de saldos del cierre anterior; depósitos y retiros en formularios prenumerados; digitación al restablecerse	Monto máximo de retiro fijado por la Gerencia; verificación de identidad y firma; doble control en la digitación; cuadre de caja
OD-02	Tarjetas de débito (SD-05)	Bloqueo de tarjetas y retiro en ventanilla	Bloqueo por vía telefónica; retiro con cédula en ventanilla; registro de reclamos	Registro de cada bloqueo; conciliación con COONECTA
OD-03	Cajeros automáticos (SD-04)	Un cajero operativo o retiro en ventanilla	Aviso en el cajero; redirección al otro cajero o a la ventanilla	Registro de débitos sin entrega; cuadre del cajero
OD-04	Web y aplicación móvil (SD-02, SD-03)	Consultas de saldo por la ventanilla	Mensaje a los socios; atención en ventanilla; extensión de horario si la interrupción coincide con días pico	Registro de los reclamos recibidos
OD-05	Transferencias y recaudaciones (SD-06)	Recepción de depósitos con registro diferido	Comprobante manual prenumerado; transferencias SPI diferidas al siguiente ciclo	Verificar que la transferencia no se haya ejecutado antes de reenviarla
OD-06	Monitoreo y carpetas (SD-08)	Atención de alertas críticas por el área de TI	Revisión diaria de alertas del firewall y del antivirus; uso de la ubicación alterna de archivos (NAS o SharePoint)	Registro de alertas revisadas

Fuente: Elaboración propia a partir de las fichas BIA y de la entrevista (Anexos A y B).

El reporte de saldos del cierre anterior, imprescindible para la consulta en ventanilla, se genera y resguarda cada día al cierre como parte de E-09, y su acceso queda restringido al

personal de cajas. Como establece el capítulo II, los accesos excepcionales concedidos durante la contingencia se registran y se revocan al retornar a la normalidad (NIST, 2024).

4.12.6. Retorno a la normalidad y cierre

El retorno a la normalidad lo declara quien declaró el nivel, una vez cumplidas las siguientes condiciones:

- Los servicios afectados operan con normalidad durante al menos 30 minutos y se ha verificado la integridad de los datos.
- Las operaciones registradas manualmente han sido digitadas y conciliadas con doble control, y las diferencias se han resuelto o documentado.
- Los accesos excepcionales y las configuraciones temporales se han revocado.
- Se ha emitido el mensaje de restablecimiento a los socios y al personal.

Dentro de los cinco días hábiles siguientes, el Oficial de Continuidad elabora el informe posterior a partir del informe de ejecución que ya exige el proceso de contingencia (COAC Yuyay, 2026b), con la cronología de la bitácora, los tiempos alcanzados frente al RTO y al RPO, las causas, las lecciones aprendidas y las acciones correctivas, y lo presenta al Comité.

4.12.7. Programa de ejercicios y pruebas

La cláusula 8.5 exige un programa de ejercicios basado en escenarios, que valide las estrategias y los procedimientos y produzca informes con recomendaciones (ISO, 2019). El programa del primer año combina pruebas técnicas frecuentes y de bajo costo con ejercicios de mesa y simulacros que involucran a toda la estructura de respuesta (Tabla 46). Su ejecución atiende además la recomendación del informe de riesgos de realizar pruebas mensuales de restauración (COAC Yuyay, 2026a).

Tabla 46

Programa de ejercicios y pruebas del primer año

Cód.	Ejercicio	Tipo	Procedimiento	Participantes	Frecuencia o mes
EJ-01	Restauración del respaldo del core en el ambiente de pruebas, midiendo el tiempo y el RPO	Prueba técnica	PR-02, PR-03	Coordinador de Sistemas; proveedor	Mensual
EJ-02	Verificación de la integridad de la copia fuera del sitio	Prueba técnica	PR-03	Coordinador de Sistemas	Mensual
EJ-03	Prueba del árbol de llamadas y de los contactos de proveedores	Prueba de comunicación	Todos	Oficial de Continuidad	Trimestral
EJ-04	Revisión de escritorio del plan con titulares y suplentes	Revisión	Todos	Comité y equipos	Meses 2 y 8
EJ-05	Conmutación al enlace secundario en horario de baja demanda	Prueba técnica	PR-01	Equipo técnico; operador	Meses 4 y 10
EJ-06	Simulación de mesa: caída del core en día de pago	Ejercicio de mesa	PR-02	Comité y tres equipos	Mes 5
EJ-07	Simulacro de operación degradada en una agencia	Simulacro	OD-01	Negocios, Cajas, Tesorería	Mes 6
EJ-08	Ejecución del DRP del proveedor del core con presencia de la cooperativa	Prueba técnica	PR-02	Proveedor; Coordinador de Sistemas; Auditor	Mes 7
EJ-09	Simulación de mesa: ransomware en la base de datos	Ejercicio de mesa	PR-03	Comité; SOC; equipo técnico	Mes 9
EJ-10	Simulacro integral: pérdida del enlace con operación degradada y comunicación	Simulacro	PR-01, OD-01, comunicación	Toda la estructura de respuesta	Mes 11

Fuente: Elaboración propia a partir de ISO (2019) y COAC Yuyay (2026a).

Los ejercicios se programan fuera de las horas pico y de los días de pago, y las pruebas técnicas se ejecutan en el ambiente de pruebas o con plan de reversión, para que el propio ejercicio no provoque una interrupción. El Auditor Informático observa los ejercicios EJ-06 a EJ-10 y emite un informe con los resultados frente a los tiempos objetivo y las recomendaciones de mejora.

4.12.8. Evaluación del desempeño

El desempeño del plan se mide con los indicadores de la Tabla 47, que el Oficial de Continuidad reporta trimestralmente al Comité, en cumplimiento de la cláusula 9.1 (ISO, 2019).

Tabla 47

Indicadores de desempeño del plan de continuidad

Indicador	Fórmula o medición	Meta	Frecuencia	Fuente
Tiempo de activación	Minutos entre T0 y la declaratoria del nivel	≤ 30 min	Por evento	Bitácora
Cumplimiento del RTO	Servicios recuperados dentro de su RTO / servicios interrumpidos	100 %	Por evento y ejercicio	Bitácora e informes
RPO alcanzado	Horas de transacciones perdidas en la restauración	≤ 1 h	Mensual	EJ-01
Pruebas de restauración exitosas	Pruebas exitosas / pruebas programadas	100 %	Mensual	EJ-01 y EJ-02
Disponibilidad de los canales digitales	Tiempo disponible / tiempo total, sin contar el mantenimiento programado	Meta regulatoria: ≥ 99,99 % anual para los servicios críticos (SD-01, SD-05, SD-07), conforme a la Resolución SEPS 0116. Meta transitoria del primer año: ≥ 99,5 % mensual para todos los canales, hasta que operen el enlace secundario (E-03) y la réplica (E-02 B)	Mensual	Monitoreo de disponibilidad
Ejercicios ejecutados	Ejercicios ejecutados / ejercicios programados	≥ 90 %	Trimestral	Programa de ejercicios
Acciones correctivas cerradas a tiempo	Acciones cerradas en plazo / acciones abiertas	≥ 90 %	Trimestral	Registro de acciones
Personal capacitado	Titulares y suplentes capacitados / total de roles	100 %	Semestral	Talento Humano

Fuente: Elaboración propia a partir de ISO (2019).

La meta regulatoria del 99,99 % anual equivale a unos 53 minutos de indisponibilidad al año. El historial de la cooperativa no la cumple: las dos o tres caídas breves al mes, de 5 a 20 minutos, suman entre 2 y 12 horas al año, y la interrupción de 6 horas de marzo de 2025 la superó por sí sola, lo que sitúa la disponibilidad actual por debajo del 99,9 %. Una sola interrupción recuperada dentro del RTO (4 horas para el core, 8 para los canales) también incumple la meta anual, porque el RTO acota la duración de un evento, no su frecuencia: ambos parámetros se complementan, el RTO limita el peor caso y la disponibilidad limita la suma de todas las interrupciones. Por eso el plan fija una meta transitoria del 99,5 % mensual para el

primer año, medible con la arquitectura actual, y reconoce de forma explícita la brecha frente al mínimo regulatorio. La meta regulatoria pasa a ser exigible a partir del segundo año, cuando operen el enlace secundario (E-03), la réplica en espera (E-02 B) y la protección frente a denegación de servicio (E-08), que eliminan las causas de las caídas registradas; mientras tanto, el Oficial de Continuidad reporta la brecha al Comité y la cooperativa la comunica a la SEPS en su plan de acción.

4.12.9. Mantenimiento, revisión y mejora del plan

El plan se revisa al menos una vez al año, en la sesión del Comité que precede a la aprobación del presupuesto, y además cuando ocurre alguno de los siguientes eventos:

- Una activación real del nivel 2 o 3, o un ejercicio con resultados por debajo de las metas.
- La incorporación o el retiro de un servicio digital, o un cambio de proveedor crítico o de sus contratos.
- Un cambio en la infraestructura por ejemplo, la entrada en operación del segundo enlace o de la réplica o en el personal con roles en el plan.
- Una nueva disposición de la SEPS o de la normativa de protección de datos, o una observación de auditoría.

La revisión actualiza el análisis de impacto y la evaluación de riesgos, verifica que las estrategias sigan cumpliendo los parámetros y registra las acciones correctivas, con lo que se cumplen las cláusulas 8.6, 9.3 y 10 de la norma (ISO, 2019). La auditoría interna incluye el plan en su programa anual y verifica la ejecución de los ejercicios y el cierre de las acciones correctivas (cláusula 9.2). Cada versión aprobada se registra en el control de cambios del documento y se distribuye a los titulares y suplentes, retirando las versiones anteriores.

4.13. Correspondencia de la propuesta con los hallazgos del diagnóstico

La Tabla 48 verifica que cada hallazgo del capítulo III tiene una respuesta en el plan, lo que cierra el ciclo entre el diagnóstico y la propuesta.

Tabla 48

Correspondencia entre los hallazgos del diagnóstico y los componentes del plan

Hallazgo	Síntesis	Respuesta en el plan	Sección
H1	Sin plan de continuidad integral aprobado	Plan completo con política aprobable por el Consejo	4.6 a 4.12
H2	RPO de 1 h frente a 24 h; sin copia fuera del sitio	E-01, E-02; OC-2 y OC-3; EJ-01 y EJ-02	4.11; 4.12.7
H3	Contratos no alineados con los tiempos requeridos	E-04, E-05, E-06; OC-4	4.11
H4	Core y conectividad concentran el riesgo	Secuencia de recuperación; PR-01 y PR-02	4.10; 4.12.4
H5	Enlace único de Internet	E-03; EJ-05	4.11; 4.12.7
H6	Gestión de cambios del proveedor débil	E-07	4.11
H7	Operación degradada no documentada	E-09; OD-01 a OD-06; EJ-07	4.12.5
H8	Sin Oficial de Continuidad ni suplentes	Estructura de respuesta, roles con suplentes y RACI; E-10	4.7
H9	Sin mensajes predefinidos ni notificación a la SEPS	Plan de comunicación y mensajes modelo; E-13	4.12.3
H10	Sin simulacros ni pruebas del DRP	Programa de ejercicios EJ-01 a EJ-10	4.12.7
H11	Escalas de riesgo heterogéneas	Revaloración con escala única de 5 × 5	4.9
H12	Sin presupuesto de continuidad	Hoja de ruta con costos relativos y plazos	4.11.4

Fuente: Elaboración propia.

Con estas fases, la cooperativa dispone de un plan que define qué recuperar primero, en cuánto tiempo, con qué recursos y bajo la dirección de quién. Su eficacia, sin embargo, depende de dos decisiones que están fuera del alcance de este trabajo y en manos de la dirección: aprobar la política y el plan, y asignar los recursos de la hoja de ruta, empezando por las medidas de bajo costo del primer trimestre.

CONCLUSIONES

Respecto al objetivo general. Se desarrolló el Plan de Continuidad del Negocio para los servicios digitales de la COAC Yuyay Ltda. siguiendo la estructura de las cláusulas 4 a 10 de la norma ISO 22301:2019, con la evaluación de riesgos de MAGERIT integrada en la cláusula 8. Los requisitos que presuponen un sistema en operación, como la auditoría interna (9.2), la revisión por la dirección (9.3) y el tratamiento de no conformidades (10.1), quedan previstos en el plan, pero solo podrán cumplirse cuando la cooperativa lo apruebe y lo ejecute, como refleja la Tabla 15. El plan cubre los ocho servicios digitales de la cooperativa y sustituye la respuesta actual, que depende de la experiencia de tres personas y carece de criterios escritos, por una estructura con niveles de activación objetivos, roles con suplentes, procedimientos de recuperación con tiempos medidos desde la detección y un programa de ejercicios. Su aporte a la eficacia de la recuperación se expresa en tres cambios verificables: el riesgo residual de los escenarios de interrupción pasa de un escenario crítico y cinco altos a ninguno por encima del nivel medio; la pérdida de datos tolerable del core financiero baja de hasta 24 horas a 1 hora; y el tiempo de recuperación exigible a los proveedores del core y de la conectividad se alinea con un RTO de 4 horas. Estos resultados son proyectados: se alcanzarán en la medida en que la cooperativa apruebe el plan, ejecute la hoja de ruta y compruebe los tiempos en los ejercicios programados.

Respecto al primer objetivo específico. La revisión de la literatura y de las normas permitió construir la cadena conceptual que sustenta el plan: los servicios digitales dependen de capas de infraestructura, aplicaciones, datos y proveedores; su interrupción se analiza como un riesgo que combina probabilidad e impacto; y la continuidad se gestiona fijando, mediante el análisis de impacto, el período máximo tolerable de interrupción, el tiempo y el punto objetivo de recuperación y el nivel mínimo de servicio, antes de seleccionar estrategias. La comparación de los marcos de referencia justificó la elección de ISO 22301:2019 como

columna vertebral, por ser certificable y estructurar el ciclo completo de la continuidad, complementada con MAGERIT, que aporta un catálogo de activos y amenazas en español adecuado a infraestructuras de TI. El marco teórico produjo además la escala única de cinco niveles de probabilidad e impacto y la matriz de cuatro zonas que, aplicadas en los capítulos III y IV, resolvieron la heterogeneidad de las escalas que utilizaba la cooperativa.

Respecto al segundo objetivo específico. El diagnóstico identificó 68 activos tecnológicos, de los cuales el 72,1 % tiene una valoración muy alta o crítica, lo que demuestra que la valoración estática no basta para priorizar la recuperación. El análisis de impacto aportó esa priorización: el core financiero, la infraestructura en la nube con el enlace de Internet y las tarjetas de débito son los servicios críticos, con un MTPD de 8 horas, un RTO de 4 horas y, en el caso del core, un RPO de 1 hora. El análisis de dependencias mostró que cuatro elementos sostienen los ocho servicios y que uno de ellos, el enlace de Internet, no tiene alternativa y causó la interrupción más larga del período, de 6 horas en marzo de 2025. Las brechas principales son la pérdida posible de hasta 24 horas de transacciones frente a una tolerancia de 1 hora, la ausencia de copia de respaldo fuera del sitio, los contratos que admiten 24 horas de restablecimiento del core frente a un MTPD de 8 horas y la falta de un acuerdo de servicio con la red de tarjetas; como consecuencia, siete de los ocho servicios no pueden demostrar hoy que se recuperarían dentro de su RTO. Estas brechas obedecen a la falta de ejecución más que de definición: desde 2019 el manual de funciones asigna al Jefe de Sistemas el plan de continuidad, el servidor espejo, el respaldo externo y en la nube y el respaldo de la comunicación de datos. Frente a la norma, ningún requisito se cumple plenamente y tres carecen de evidencia, lo que coincide con la observación de la SEPS de 2025.

Respecto al tercer objetivo específico. El plan se elaboró mediante la ejecución de las ocho fases de la metodología y está compuesto por una política de continuidad con siete objetivos medibles; una estructura de respuesta que aprovecha el Comité existente y crea el

rol de Oficial de Continuidad; la valoración de 28 activos de soporte y su matriz de dependencias; la evaluación de 13 escenarios de interrupción con su plan de tratamiento; 13 estrategias organizadas en una hoja de ruta de 12 meses, que concentra en el primer trimestre las medidas de bajo costo que cierran las brechas más graves; tres niveles de activación; un plan de comunicación que incluye la notificación a la SEPS; seis procedimientos de recuperación y seis de operación degradada; un programa de diez ejercicios; y ocho indicadores de desempeño. Cada uno de los doce hallazgos del diagnóstico tiene una respuesta en el plan, lo que asegura la correspondencia entre el problema identificado y la solución propuesta.

RECOMENDACIONES

A la Universidad Católica de Cuenca. Se recomienda a la carrera de Ingeniería en Sistemas de Información dar continuidad a esta línea de trabajo mediante proyectos de titulación que implementen y validen el plan en la COAC Yuyay Ltda., midiendo los indicadores de desempeño propuestos tras los primeros ejercicios, y que repliquen la metodología fases de ISO 22301 con evaluación de riesgos MAGERIT y análisis de impacto por servicio en otras cooperativas de ahorro y crédito de la provincia con servicios digitales y dependencia de proveedores semejantes. Para facilitar el acceso a la información institucional, limitación enfrentada en esta investigación, se sugiere formalizar convenios de cooperación con estas entidades que establezcan la confidencialidad de los datos y los plazos de entrega. Asimismo, se recomienda incorporar a las asignaturas de seguridad y gobierno de TI casos prácticos de análisis de impacto y ejercicios de continuidad basados en escenarios reales como los documentados en este trabajo.

A la COAC Yuyay Ltda. Se recomienda que el Consejo de Administración apruebe la política y el Plan de Continuidad del Negocio, y que la Gerencia General designe formalmente al Oficial de Continuidad y a los suplentes de cada rol. En el primer trimestre, la cooperativa debería ejecutar las medidas de bajo costo de la hoja de ruta copia de los respaldos fuera del sitio, respaldo físico con RMAN y copia horaria de los archivos de registro de la base de datos para alcanzar el RPO de 1 hora, documentación de la operación degradada y aprobación de los mensajes y del procedimiento de notificación a la SEPS y concluir la contratación del segundo enlace de Internet. En las próximas renovaciones contractuales debería exigir al proveedor del core un tiempo de restablecimiento de 4 horas, la ejecución anual de su plan de recuperación ante desastres y un plan de salida, y establecer acuerdos de servicio con COONECTA y con el proveedor de mantenimiento de cajeros. Por último, se recomienda

iniciar el programa de ejercicios con la prueba mensual de restauración, utilizar sus resultados como evidencia para cerrar la observación de la SEPS y revisar el plan al menos una vez al año.

REFERENCIAS

Asamblea Nacional del Ecuador. (2011). Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario. Registro Oficial No. 444, 10 de mayo de 2011.

Asamblea Nacional del Ecuador. (2014). Código Orgánico Monetario y Financiero. Registro Oficial Segundo Suplemento No. 332, 12 de septiembre de 2014.

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Quinto Suplemento No. 459, 26 de mayo de 2021.

Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.pdf

Becerra Acevedo, R., Benavides Muñoz, J. R., Camacho Camacho, H., & Obando, C. J. (2021). Evolución y modelos de implementación de sistemas de gestión de continuidad del negocio. SIGNOS – Investigación en Sistemas de Gestión, 13(2). https://doi.org/10.15332/24631140.6669

Buscán Pinguil, P. C., Flores Urgilés, C. H., Pinos Castillo, L. F., & Flores Urgilés, C. M. (2022). Modelo de plan de continuidad de negocio de las cooperativas segmento B del cantón Cañar. Pro Sciences: Revista de Producción, Ciencias e Investigación, 6(43), 59-70. https://doi.org/10.29018/issn.2588-1000vol6iss43.2022pp59-70

Business Continuity Institute. (2023). Good practice guidelines (Edition 7.0). The Business Continuity Institute.

Buzzao, G., & Rizzi, F. (2023). The role of dynamic capabilities for resilience in pursuing business continuity: An empirical study. Total Quality Management & Business Excellence, 34(11-12), 1353-1385. https://doi.org/10.1080/14783363.2023.2174427

Cooperativa de Ahorro y Crédito Yuyay Ltda. (s. f.). *Gestión de riesgos de TI: inventario de activos MAGERIT y matrices de riesgo* [Libro de cálculo; documento interno no publicado].

Cooperativa de Ahorro y Crédito Yuyay Ltda. (2019). Manual descriptivo de funciones [Documento interno no publicado].

Cooperativa de Ahorro y Crédito Yuyay Ltda. (2023). Manual descriptivo de funciones del área de TI [Documento interno no publicado].

Cooperativa de Ahorro y Crédito Yuyay Ltda. (2024). Manual de seguridad de la información [Documento interno no publicado].

Cooperativa de Ahorro y Crédito Yuyay Ltda. (2026a). Informe de riesgos de seguridad de la información [Documento interno no publicado].

Cooperativa de Ahorro y Crédito Yuyay Ltda. (2026b). Manual de procesos de TI [Documento interno no publicado].

Corrales-Estrada, A. M., Gómez-Santos, L. L., Bernal-Torres, C. A., & Rodriguez-López, J. E. (2021). Sustainability and resilience organizational capabilities to enhance business continuity management: A literature review. Sustainability, 13(15), 8196. https://doi.org/10.3390/su13158196

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3.ª ed.). SAGE Publications.

DRI International. (2017). The professional practices for business continuity management. DRI International.

Galaitsi, S. E., Pinigina, E., Keisler, J. M., Pescaroli, G., Keenan, J. M., & Linkov, I. (2023). Business continuity management, operational resilience, and organizational resilience: Commonalities, distinctions, and synthesis. International Journal of Disaster Risk Science, 14(5), 713-721. https://doi.org/10.1007/s13753-023-00494-x

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. Journal of Management Information Systems, 35(1), 220-265. https://doi.org/10.1080/07421222.2018.1440766

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

International Electrotechnical Commission. (2019). Risk management Risk assessment techniques (IEC Standard No. 31010:2019). IEC.

International Organization for Standardization. (2018). Risk management Guidelines (ISO Standard No. 31000:2018). ISO.

International Organization for Standardization. (2019). Security and resilience Business continuity management systems Requirements (ISO Standard No. 22301:2019). ISO. https://www.iso.org/standard/75106.html

International Organization for Standardization. (2020). Security and resilience Business continuity management systems Guidance on the use of ISO 22301 (ISO Standard No. 22313:2020). ISO.

International Organization for Standardization. (2021a). Security and resilience Vocabulary (ISO Standard No. 22300:2021). ISO.

International Organization for Standardization. (2021b). Security and resilience Business continuity management systems Guidelines for business impact analysis (ISO Technical Specification No. 22317:2021). ISO.

International Organization for Standardization. (2024). Security and resilience Business continuity management systems Requirements Amendment 1: Climate action changes (ISO Standard No. 22301:2019/Amd 1:2024). ISO.

International Organization for Standardization & International Electrotechnical Commission. (2022a). Information security, cybersecurity and privacy protection Information security management systems Requirements (ISO/IEC Standard No. 27001:2022). ISO.

International Organization for Standardization & International Electrotechnical Commission. (2022b). Information security, cybersecurity and privacy protection Guidance on managing information security risks (ISO/IEC Standard No. 27005:2022). ISO.

International Organization for Standardization & International Electrotechnical Commission. (2025). Cybersecurity Information and communication technology readiness for business continuity (ISO/IEC Standard No. 27031:2025). ISO.

Laudon, K. C., & Laudon, J. P. (2022). Management information systems: Managing the digital firm (17.ª ed.). Pearson.

Ministerio de Hacienda y Administraciones Públicas. (2012a). MAGERIT – versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I: Método. Gobierno de España.

Ministerio de Hacienda y Administraciones Públicas. (2012b). MAGERIT – versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II: Catálogo de elementos. Gobierno de España.

National Institute of Standards and Technology. (2010). Contingency planning guide for federal information systems (NIST Special Publication 800-34 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-34r1

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. International Journal of Information Management, 49, 208-216. https://doi.org/10.1016/j.ijinfomgt.2019.04.010

Păunescu, C., & Argatu, R. (2020). Critical functions in ensuring effective business continuity management. Evidence from Romanian companies. Journal of Business Economics and Management, 21(2), 497-520. https://doi.org/10.3846/jbem.2020.12205

Presidencia de la República del Ecuador. (2023). *Reglamento General a la Ley Orgánica de Protección de Datos Personales* (Decreto Ejecutivo No. 904). Registro Oficial Tercer Suplemento No. 435, 13 de noviembre de 2023.

Quituisaca-León, A. K., Ruilova-Morocho, R. A., & Araujo-Ochoa, G. I. (2021). Propuesta de la gestión de la continuidad de las MiPymes bajo la norma ISO 22301 en la ciudad de Cuenca – Azuay. 593 Digital Publisher CEIT, 6(2), 30-42. https://doi.org/10.33386/593dp.2021.2.441

Rezaei Soufi, H., Torabi, S. A., & Sahebjamnia, N. (2019). Developing a novel quantitative framework for business continuity planning. International Journal of Production Research, 57(3), 779-800. https://doi.org/10.1080/00207543.2018.1483586

Rojas Bustamante, J. D. (2017). Propuesta de un plan de continuidad de negocio para una institución financiera del sector privado bancario del Ecuador [Tesis de maestría, Universidad de Las Américas]. Repositorio UDLA.

https://dspace.udla.edu.ec/jspui/bitstream/33000/7531/1/UDLA-EC-TMGSTI-2017-08.pdf

Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. European Journal of Operational Research, 242(1), 261-273. https://doi.org/10.1016/j.ejor.2014.09.055

Superintendencia de Economía Popular y Solidaria. (2018). Resolución No. SEPS-IGT-IR-IGJ-2018-0279. Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del sector financiero popular y solidario bajo el control de la Superintendencia de Economía Popular y Solidaria. SEPS. https://www.seps.gob.ec/wp-content/uploads/Resolucio%CC%81n-No.-SEPS-IGT-IR-IGJ-2018-0279.pdf

Superintendencia de Economía Popular y Solidaria. (2022). *Resolución No. SEPS-IGS-IGT-IGJ-INGINT-INTIC-INSESF-INR-DNSI-2022-002. Norma de control respecto a la seguridad de la información en las entidades del sector financiero popular y solidario*. SEPS.

Superintendencia de Economía Popular y Solidaria. (2024). *Resolución No. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116. Norma de control para la administración del riesgo operativo en las entidades del sector financiero popular y solidario*. Registro Oficial Suplemento No. 606, 23 de julio de 2024. https://www.seps.gob.ec/wp-content/uploads/NORMA-DE-RIESGO-OPERATIVO.pdf

Superintendencia de Protección de Datos Personales. (2026). *Resolución No. SPDP-SPD-2026-0040-R. Norma técnica de notificación de vulneraciones de la seguridad de los datos personales*. SPDP.

Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. Safety Science, 89, 201-218. https://doi.org/10.1016/j.ssci.2016.06.015

ANEXOS

Anexo 1: Protocolo de Investigación

Anexo: Formato del Anteproyecto.

A. TÍTULO
Plan de Continuidad de Negocio para los servicios digitales de la COAC Yuyay Ltda. Basado en la norma ISO 22301:2019.

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Energía eléctrica y tecnologías de la información para la innovación y el desarrollo sostenible	**Ciencias de los ordenadores, Analítica de datos y Algoritmos computacionales**	Analítica de datos	
		Ingeniera de software	
		Algoritmos computacionales	
		Inteligencia de negocios	
		Gobierno de TI	
		Auditoría y seguridad informática	
		Simulación	

C. PLANTEAMIENTO DEL PROBLEMA
La proliferación de los servicios digitales impulsados por las instituciones financieras ha llevado implícita aumentar también la necesidad de disponer de infraestructura tecnológica adecuada que respalde los procesos institucionales a fin de lograr la continuidad operativa y la atención efectiva a socios y clientes. En este contexto, las cooperativas de ahorro y crédito deben enfrentarse a distintos riesgos por falla tecnológica, ataques cibernéticos, errores humanos, fallos eléctricos y catástrofes naturales que pueden

comprometer la disponibilidad, integridad y confidencialidad de la información institucional. La necesidad de un Plan de Continuidad de Negocio disminuye el impacto de dichos incidentes, mitigando problemas como por ejemplo, la pérdida de operatividad de los servicios digitales, pérdida económica, efectos reputacionales y la disminución de la confianza de los usuarios. (Buzzao & Rizzi, 2023).

La Cooperativa de Ahorro y Crédito "Yuyay" Ltda. (COAC Yuyay) no escapa ante esta realidad ya que sus procesos operativos y servicios digitales dependen de la infraestructura tecnológica para poder ejecutar actividades administrativas y financieras y por lo tanto, se necesita establecer mecanismos y estrategias que permitan asegurar la continuidad de los servicios críticos ante posibles situaciones inesperadas que puedan afectar el desarrollo normal de las actividades. La norma ISO 22301:2019 establece una serie de lineamientos reconocidos a nivel internacional para ayudar a las organizaciones en el diseño e implementación de mecanismos que permitan mantener el funcionamiento de sus procesos esenciales, favoreciendo una mejor capacidad de respuesta y adaptación ante distintos escenarios.

Del mismo modo, una pluralidad de investigaciones recientes enfatiza implementar modelos de continuidad del negocio bajo la norma ISO 22301, con el propósito de reducir las consecuencias de los incidentes tecnológicos y de mejorar el nivel de la capacidad de respuesta organizativa de las entidades financieras y empresariales. Atendiendo al precedente problema, aparece la necesidad de llevar a cabo un análisis sobre la posibilidad de que un Plan de Continuidad de Negocio contribuya a fortalecer el mantenimiento operativo de dicha entidad ante las posibles interrupciones en sus servicios digitales (Puspitaningrum, 2022).

El planteamiento que será fundamentado en el transcurso de la presente investigación se encuentra enmarcado en el diseño de un Plan de Continuidad del Negocio, alineado a la norma ISO 22301 cuya orientación impere en la identificación de procesos críticos, así como en la evaluación de riesgos tecnológicos y el establecimiento de estrategias de recuperación, además de la resiliencia organizacional que debe tener la cooperativa ante cualquier posible incidente o evento disruptivo.

D. OBJETIVO GENERAL

Desarrollar un Plan de Continuidad del Negocio para los servicios digitales pertenecientes a la Cooperativa de Ahorro y Crédito “Yuyay” Ltda., bajo los lineamientos que establece la norma ISO 22301:2019, que permita incrementar la eficacia en la recuperación y la respuesta ante incidentes que puedan comprometer la continuidad de los servicios digitales.

E. OBJETIVOS ESPECÍFICOS

1. Elaborar el marco teórico y conceptual relacionado con continuidad del negocio, resiliencia organizacional, gestión del riesgo y la norma ISO 22301.
2. Identificar y analizar los activos tecnológicos y procesos críticos asociados a las plataformas virtuales de la Cooperativa de Ahorro y Crédito "Yuyay" Ltda., mediante el levantamiento de información institucional.
3. Elaborar el Plan de Continuidad del Negocio dirigida a los servicios digitales de la cooperativa mediante la ejecución de las fases establecidas en la metodología seleccionada.

F. JUSTIFICACIÓN

La implantación de un Plan de Continuidad del Negocio (BCP) para los servicios digitales de la Cooperativa de Ahorro y Crédito COAC Yuyay Ltda. está justificada por el aumento del uso de las tecnologías de la información y comunicación por parte de las organizaciones financieras en la automatización de sus procesos de operación y la oferta de servicios digitales. En la actualidad, el sector financiero se enfrenta a peligros tales como los ciberataques, las fallas en la infraestructura tecnológica, las interrupciones eléctricas, los errores humanos y las catástrofes naturales, los cuales pueden comprometer la estabilidad operativa, además de la seguridad depositada por los usuarios y sus miembros asociados.

Por eso, es preciso generar mecanismos que prevengan, respondan a y recuperen a partir de incidentes disruptivos y que minimicen su impacto. Desde la óptica técnica, el estudio posibilitará elaborar un conjunto ordenado de estrategias, procedimientos y controles dirigidos a asegurar la disponibilidad y la recuperación de los servicios críticos de la cooperativa, tomando como base los lineamientos del estándar internacional ISO 22301. Esta normativa proporciona una estructura global dirigida a fortalecer la capacidad de reacción interna, optimizar la administración de riesgos y garantizar la continuidad de las actividades más críticas ante las situaciones de emergencia. Al respecto, Morrison (2024) señala que aplicar modelos de continuidad del negocio apoyados en la norma ISO 22301 fortalece la capacidad de reacción de las organizaciones y favorece su estabilidad a largo plazo.

La realización de esta investigación, en el ámbito académico, contribuirá a retornar información relacionada con la continuidad del negocio, gestión de riesgos y recuperación tecnológica dentro del entorno de las entidades financieras de la economía popular y solidaria, sirviendo de referencia en futuras investigaciones relacionadas con la seguridad y continuidad de los servicios digitales. Para la misma también sirve para integrar

protocolos y buenas prácticas internacionales en el contexto ecuatoriano y en el sector cooperativo financiero (Toledo, 2025).

G. ALCANCE

Este estudio busca analizar el desarrollo de un Plan de Continuidad del Negocio (BCP) enfocada a la administración de las plataformas tecnológicas de la Cooperativa de Ahorro y Crédito COAC Yuyay Ltda. Siguiendo las directrices de la norma ISO 22301, el análisis se enfoca en los elementos esenciales para la operación institucional y de esta manera poder identificar los riesgos, paradigmas o escenarios que podrían causar una interrupción.

Para alcanzar esto, se considera necesario realizar primero una evaluación del impacto en el negocio (BIA) junto con un estudio de riesgos tecnológicos para definir las prioridades de recuperación y a partir de ahí, las estrategias y los procedimientos de continuidad que permitirán mejorar la capacidad de respuesta y recuperación ante un evento que afecte a la prestación de los servicios digitales.

El alcance del trabajo abarca de igual manera la estructuración documental de dicha planificación de continuidad, definiendo las pautas de contingencia, recuperación y mejora continua; aunque la implementación de las estrategias propuestas queda fuera del alcance, así como la certificación institucional en base a la norma ISO 2230.

H. CONCEPTOS RELACIONADOS

El Plan de Continuidad del Negocio

Se entiende por El Plan de Continuidad del Negocio (BCP) al esquema integrado por directrices, acciones operativas, recursos y líneas de acción orientadas a salvaguardar

la estabilidad de las operaciones esenciales dentro de una empresa frente a eventos que pongan en riesgo su actividad ordinaria (ISO 22301:2019, s.f.)

La finalidad de esta planificación radica en minimizar el impacto operativo, financiero y reputacional por causa el de incidentes tecnológicos, desastres naturales, ciberataques o fallos en la operación y asegure la recuperación de los servicios críticos.

Hoy en día, el BCP, forma parte de una de las bases más importantes de los sistemas de resiliencia organizacional, ya que permite a las organizaciones anticipar que el contexto puede cambiar y fortalecer la respuesta y recuperación. Los estudios actuales afirman que los modelos modernos de continuidad del negocio para fortalecer la estabilidad de la organización, así como de la continuidad operativa incluye procesos de gestión de riesgo, análisis de impacto y la recuperación con modelos acordes a estándares internacionales como ISO 22301. (Funcia, 2024).

Continuidad del Negocio

Esta disciplina se entiende como la capacidad institucional para continuar ofreciendo productos o brindando servicios en condiciones aceptables, incluso durante y después de una interrupción. Esta noción tiene en cuenta también la descripción de los diferentes procesos de prevención, contestación y recobro de las dificultades que afectan a las operaciones críticas de las propias instituciones.

Para las organizaciones financieras y cooperativas, la continuidad del negocio tiene un sentido estratégico debido a que existe un grado elevado de dependencia de la prestación de servicios digitales, de las plataformas para las transacciones y del uso de información sensible. Los resultados conseguidos mediante trabajos recientes sugieren también que la continuidad del negocio es, para la propia organización, un recurso para mejorar la resiliencia, haciendo que la capacidad de respuesta institucional permaneciera adecuada frente a la génesis de riesgos y crisis de nueva. La literatura científica incluso

avala que la continuidad del negocio ha pasado a ser un elemento crítico para la viabilidad operativa y la sostenibilidad de las instituciones como entidades en el entorno. (Buzzao & Rizzi, 2023).

ISO 22301

Este estándar internacional establece una serie de lineamientos que orientan el diseño, la implementación y la mejora de un Sistema de Gestión de Continuidad del Negocio (SGCN), con el fin de que las organizaciones puedan gestionar de manera más ordenada sus procesos ante posibles interrupciones. La nueva versión de 2024 incorpora los criterios relacionados con las amenazas climáticas, así como el alcance de análisis de los contextos y las amenazas, ampliando así la aplicación de esta norma en las instituciones gubernamentales y municipales (Loyarte, 2024).

Análisis de Impacto al Negocio

El análisis orientado a la elaboración del Impacto en el Negocio (Business Impact Analysis – BIA) es una metodología que sirve para identificar y valorar cuánto puede afectar la interrupción de procesos críticos de una organización. El BIA identifica el grado de criticidad de los servicios, los impactos más relevantes que esto podría suponer en los aspectos financieros y operacionales, así como también las prioridades de recuperación institucional.

El BIA es uno de los instrumentos que se consideran imprescindibles en la continuidad del negocio ya que, nos ayuda a la toma de decisiones estratégicamente necesarias en cuanto a la recuperación de los servicios y la disponibilidad de recursos. Recientes investigaciones sociales demuestran que, la introducción del BIA en los sistemas de continuidad de una organización permite mejorar la operación efectiva y consolidar con ello la

resiliencia ante un evento disruptivo. Además, estudios recientes señalan que la investigación del impacto permite fijar parámetros de recuperación que resulten más precisos y alineados con las necesidades de la organización (Zanni, 2024).

Gestión de Riesgos

La administración tecnológica del riesgo corporativo incluye dentro del proceso sistemático de identificar, analizar, evaluar y tratar las amenazas que pueden comprometer los activos tecnológicos junto con las plataformas de información institucionales incluyéndose en este proceso las vulnerabilidades, la probabilidad de ser atacados y la forma que tendrá este impacto para la operación de una entidad; así como también la posibilidad de establecer controles y la forma en desarrollar estrategias que logren mitigar los impactos de los incidentes tecnológicos sufridos.

Dentro del marco de la resiliencia operativa, el control de las amenazas tecnológicas tiene un papel clave, ya que permite prevenir interrupciones y potenciar la reacción de las organizaciones frente a eventos causantes de interrupciones en su funcionamiento normal, contribuyendo a la disponibilidad de la información y asegurando la integridad y la fiabilidad de los servicios digitales críticos que tienen las entidades financieras. Múltiples estudios han evidenciado que la adecuada interrelación e integración de los procesos de gestión de la tecnología de riesgos y continuidad del negocio mejora significativamente la resiliencia de las organizaciones en el ámbito digital, y de este modo puede favorecer la sostenibilidad operacional en los contextos digitales.

Recuperación ante desastres

La recuperación ante desastres (Disaster Recovery Plan - DRP) consiste en un conjunto de procedimientos técnicos destinados a recuperar la infraestructura, sistemas, aplicaciones y datos después de un incidente severo. En este sentido, el DRP es un elemento auxiliar al BCP que tiene como objetivo la recuperación tecnológica. Al respecto,

Nikolovski y Pece (2025) destacan que los DRP actuales tienen que ser integrados con simulaciones y pruebas periódicas para contar con tiempos de recuperación eficientes.

Objetivos de recuperación (RTO y RPO)

El RPO, se define como el máximo una organización puede permitirse perder como consecuencia de un determinado tipo de incidente. Se establece hacia atrás desde el tiempo del incidente y refleja la periodicidad con la que se deben realizar las copias de seguridad o replicaciones con la finalidad de cumplir su propia tolerancia frente a la pérdida de datos. Cuanto más corto el RPO, más frecuentemente habrá que realizar copias de seguridad, utilizar replicación continua o emplear tecnologías que hagan que la pérdida de datos esté prácticamente eliminada.

Estos indicadores permiten determinar los niveles de servicio y ayudar a establecer las actividades de recuperación alineadas con las exigencias de la organización. La correcta definición de los objetivos RTO y RPO es necesaria para garantizar la eficacia del Plan de Continuidad del Negocio y minimizar las afectaciones. Además, una adecuada gestión de estos indicadores contribuye a optimizar los procesos de recuperación y fortalecer la resiliencia organizacional, (Jurgens, 2024).

I. TRABAJOS RELACIONADOS

A nivel internacional, diversos estudios han demostrado la importancia de implementar sistemas y planes enfocados en la preservación de operaciones bajo las directrices del estándar ISO 22301, orientados a fortalecer la capacidad de adaptación de las organizaciones y a disminuir el impacto que pueden generar los incidentes operativos y tecnológicos. La adopción de prácticas de continuidad del negocio en organizaciones modernas, concluyendo que la implementación de modelos alineados con ISO 22301

mejora significativamente la capacidad de respuesta, recuperación y sostenibilidad operativa frente a eventos disruptivos.

Este estudio aporta a la presente investigación debido a que proporciona fundamentos metodológicos relacionados con la gestión de continuidad y resiliencia organizacional aplicables al entorno financiero. (Sawalha et al. 2021).

En el contexto latinoamericano, Quituisaca León et al. (2021), desarrollaron una investigación enfocada en el mantenimiento operativo en diferentes organizaciones tomando como base la norma ISO 22301 dentro del contexto de Cuenca (Azuay). Dicha investigación identificó deficiencias relacionadas con la ausencia de estrategias de continuidad y propuso mecanismos orientados al fortalecimiento de la resiliencia organizacional mediante gestión de riesgos y procedimientos de recuperación. Este antecedente aporta a la investigación porque permite tomar como referencia estrategias aplicadas en organizaciones ecuatorianas con características similares.

A nivel nacional, Iza (2021) desarrollo un Plan de Continuidad del Negocio basado en ISO 22301 para la empresa Airmax Telecom Soluciones Tecnológicas S.A., con el propósito de mejorar la capacidad de respuesta de la organización ante situaciones que puedan afectar la prestación de servicios tecnológicos. Este estudio resulta relevante para la presente investigación, ya que aporta lineamientos orientados a la identificación de amenazas y al diseño de estrategias de resiliencia en el ámbito tecnológico.

Asimismo, Picay (2021), elaboró un Plan de Continuidad de Negocio dirigido a la firma Construproyec S.A., identificando riesgos operacionales y estableciendo estrategias de recuperación para garantizar la continuidad de las actividades críticas ante incidentes tecnológicos y desastres naturales. Este estudio contribuye a la presente investigación porque evidencia la importancia de integrar análisis de riesgos y procedimientos de recuperación dentro de un modelo de continuidad organizacional.

En el área de la cooperación, Moya (2020) estructuró una planificación de continuidad operativa destinada al departamento de servicio al usuario de la Cooperativa de Ahorro y Crédito "San Antonio" Ltda. Tomando como base la versión ISO 22301, este estudio incluyó un análisis de impacto al negocio, identificación de las actividades importantes y la recuperación de procedimientos a utilizar para garantizar la operatividad tanto del servicio financiero. Este antecedente retoma la presente investigación, ya que es una referencia metodológica que fue concretada a la actividad cooperativa financiera.

J. METODOLOGÍA

Este estudio se sustenta metodológicamente bajo un modelo de tipo mixto, el cual articula el análisis cualitativo de los procesos críticos y las estrategias de la continuidad del negocio con la evaluación cuantitativa de los riesgos e impactos potenciales de la interrupción de los servicios digitales. El enfoque de la investigación cualitativa permitirá evaluar el estado actual de la gestión de la continuidad, procedimientos operativos, capacidad de respuesta y directrices institucionales con el carácter de resiliencia organizacional de la Cooperativa de Ahorro y Crédito COAC Yuyay Ltda. En equilibrio, el enfoque de la investigación cuantitativa permitirá valorar los riesgos técnicos valorar las repercusiones sobre los procesos comerciales (BIA) y jerarquizar las prestaciones esenciales con base en las métricas relacionadas con el tiempo de recuperación y con los niveles de afectación operativa.

La investigación tiene un nivel descriptivo – puesto que se examinará el estado contemporáneo de los canales virtuales junto con las medidas de continuidad existentes en la cooperativa, posibles vulnerabilidades, amenazas y riesgos que puedan afectar la operatividad institucional. Del mismo modo, se tratará de una investigación aplicada

porque mediante ella será posible el diseño de un Plan de Continuidad del Negocio según la norma ISO 22301:2019, para reforzar la capacidad de respuesta a los incidentes tecnológicos, o algunos eventos disruptivos.

K. CRONOGRAMA DE ACTIVIDADES

°	ACTIVIDAD	MES						MEDIOS DE VERIFICACIÓN
			I	II	V		I	
	Definición del tema de investigación							Aprobación del tema
	Elaboración del planteamiento del problema							Documento elaborado
	Desarrollo del marco teórico y conceptual							Revisión bibliográfica
	Recopilación de información científica							Artículos y tesis analizadas
	Levantamiento de información institucional							Entrevistas y fichas técnicas
	Identificación y observación de riesgos							Matriz e identificación de riesgos

	Desarrollo un BIA (análisis de Impacto al Neogocio)							Informe
	Diseño del Plan de Continuidad del Negocio							Documento del BCP
	Elaboración de estrategias de continuidad y recuperación							Estrategias documentadas
0	Redacción del documento final							Documento final
1	Revisión y correcciones							Informe corregido
2	Presentación de la investigación							Presentación final

L. DECLARACIÓN FINAL

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

M. PARTICIPANTES

DIRECTOR:	Ing. Mishel Narvaez

ESTUDIANTE:	Steve Geovanny Defas Ludizaca

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	
Fecha:	

Firmas:

Nombre: Mishel Narvaez	Nombre: Steve Geovanny Defas Ludizaca
CC:	C.C.: 0302488846
Director del Proyecto	**Estudiante / Egresado**

O. APROBACIÓN

Firmas:

P. REFERENCIAS

Alexandra Katherine Quituisaca Leon, R. A. (2021). Propuesta de la Gestión de la Continuidad de las Mipymes Bajo la Norma Iso 22301 en la Ciudad de Cuenca. *PURE UPS*.

Alraja, M. N. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, 103744.

Buzzao & Rizzi. (2023). The role of dynamic capabilities for resilience in pursuing business continuity: An empirical study. *Cogent Business & Managemen*.

Cahaya Puspitaningrum, A. (2022). Proposed Business Continuity Plan Information Technology using ISO 22301 And ISO 27031. *ResearchGate Logo*, 601-613.

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). he ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, 76-105.

Fuentes, I. (2021). Propuesta de la Gestión de la Continuidad de las Mipymes Bajo la Norma Iso 22301 en la Ciudad de Cuenca. *PURE UPS*.

Funcia. (2024). Modelo de gobernanza de la continuidad: una nueva etapa del proceso en la gestión de la continuidad del negocio (BCM).sistema que sustenta la resiliencia organizacio. *Taylor & Francis Online*.

ISO. (2022). *ISO/IEC 27001:2022 Information Security Management*. Obtenido de https://www.iso.org/isoiec-27001-information-security.html

ISO 22301:2019. (s.f.). *ISO*. Obtenido de ISO: https://www.iso.org/standard/75106.html

Iza, F. (2021). Plan de Continuidad del Negocio basado en ISO 22301.

Jurgens, T. (2024). RTO vs RPO: ¿Cuál es la diferencia? *Veeam*. Obtenido de https://www.veeam.com/blog/recovery-time-recovery-point-objectives.html

Loyarte, E. (2024). Modelo de gobernanza de la continuidad: una nueva etapa del proceso en el sistema BCM que sustenta la resiliencia organizacional. *Cogent Business & Management, 11*(1), Consultar edición publicada. doi:https://www.tandfonline.com/doi/full/10.1080/23311975.2024.2434731

Medina, M. (2020). *Diseño de un plan de continuidad de negocio en el área de atención al cliente.* Ibarra, Ecuador. Obtenido de https://repositorio.utn.edu.ec/bitstream/123456789/10633/2/04%20IND%20268%20TRABAJO%20GRADO.pdf

Morrison, R. (2024). *Bacula*. Obtenido de Bacula: https://www.baculasystems.com/es/el-blog/iso-22301-marco-de-gestion-de-la-continuidad-de-las-actividades/

Moya, M. (2020). *Diseño de un plan de continuidad de negocio en el área de atención al cliente para la cooperativa de ahorro y crédito san antonio ltda. basado en la norma iso 22301:2012* .

Nikolovski, S., & Mitrevski, P. (2025). *Modelado y simulación de sistemas de protección de datos para la continuidad del negocio y la recuperación ante desastres.* Obtenido de Conell University: https://arxiv.org/abs/2512.01477

Picay Ronquillo, J. (2021). Plan de continuidad del negocio para la empresa Construproyec S.A.

Puspitaningrum, C. (2022). Proposed Business Continuity Plan Information Technology using ISO 22301 and ISO 27031. *International Journal of Computer and Information System, 3(5), 601–613.*

Quituisaca León, A., Ruilova Morocho, R., & Araujo-Ochoa, G. (2021). Continuidad de las MiPymes bajo la norma ISO 22301. *Caso Cuenca–Azuay. 593 Digital Publisher CEIT, 6(2), 30–42.* Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7897398

Robayo Jácome, D. J., Aguilar-Molina, P., & Chiliquinga Véjar, L. C. (2023). Seguridad de la información mediante la norma ISO/IEC 27001:2013. *Medwave*, e275.

Sawalha, I. H., Anchor, J. R., & Meaton, J. (2021). Cultura de continuidad: un factor clave para desarrollar resiliencia y sólidas capacidades de recuperación. *International Journal of Disaster Risk Science*. Obtenido de https://link.springer.com/article/10.1007/s13753-015-0070-5

Toledo, M. N. (2025). Diseño de un sistema de gestión de continuidad de negocio basado en la norma ISO 22301 para entidades financieras. *Univesidad de Guayaquil*.

Villarreal Morales, V., Coro Villarreal, K. E., Fernández Sánchez, E. G., & Cueva Martinez, J. P. (2024). Sistema Gestión de Seguridad de la Información y su impacto en el Gobierno y Gestión de las Tecnologías de la Información. *Ciencia Latina Revista Científica Multidisciplinar*, 1250-1268.

Zanni, M. (2024). Business continuity plan in the management and operations of hospitals: First experience to certify the PDTA processes with the requirements defined by ISO 22301:2019 in emergency medical services. *Journal of EMERGENCY MANAGEMENT*.

Anexo A: Guion de entrevista semiestructurada

Proyecto: Plan de Continuidad de negocio para los servicios digitales de COAC Yuyay Ltda basado en la norma ISO 22301:2019

Investigador: Steve Geovanny Defas Ludizaca · **Directora:** Ing. Fernanda Michaelle Narváez Ochoa

A.1 Objetivo del instrumento

Recabar, de los responsables de la gestión tecnológica de la cooperativa, información sobre los servicios digitales que presta la institución, sus dependencias tecnológicas, el historial de interrupciones, los controles de continuidad existentes, la estructura de respuesta ante incidentes y la tolerancia de la organización a la interrupción de cada servicio. La información obtenida alimenta las secciones 3.6 y 3.7 del marco metodológico y las fases de inventario, evaluación de riesgos y análisis de impacto al negocio (BIA) de la propuesta (capítulo IV).

A.2 Ficha técnica

Elemento	Descripción
Técnica	Entrevista semiestructurada, individual, presencial o por videollamada
Informantes clave	Coordinador de Sistemas (bloques A–G); Oficial de Seguridad de la Información (bloques B, C, D, E, G); Gerente General (bloques A, F y G, en versión abreviada)
Duración estimada	60 a 75 minutos por informante
Documentos de apoyo	Inventario de activos MAGERIT, manual de procesos de TI, manual de seguridad de la información e informe de riesgos de seguridad de la información
Tratamiento	Codificación temática por bloque; las respuestas cuantificables (tiempos, frecuencias, volúmenes) se trasladan a la ficha BIA (Anexo B) y a la matriz de riesgos

A.3 Consentimiento informado (leer al inicio)

La presente entrevista forma parte de un trabajo de titulación de la carrera de Ingeniería en Sistemas de Información de la Universidad Católica de Cuenca, extensión Cañar, cuyo objetivo es diseñar un Plan de Continuidad de Negocio para los servicios digitales de la cooperativa. La información proporcionada se utilizará exclusivamente con fines académicos, se tratará de forma confidencial y los resultados se presentarán de manera agregada o con la autorización expresa de la institución. La participación es voluntaria y puede interrumpirse en cualquier momento. ¿Autoriza la grabación de la entrevista? Sí ___ No ___

Nombre del entrevistado: Coordinador de Sistemas de la COAC Yuyay Ltda. Cargo: Coordinador de Sistemas Fecha: 24/09/2026 Hora de inicio: 08:44 Hora de fin: 09:29

A.4 Preguntas por bloque

Bloque A. Contexto institucional y servicios digitales

N.º	Pregunta	Respuesta / notas del entrevistador
A1	¿Cuántos socios activos, agencias y puntos de atención tiene actualmente la cooperativa, y en qué segmento de la SEPS se ubica?	Cuatro oficinas: Matriz (Comuna San Rafael, a 200 m de la Organización Tucayta, Cañar), Terminal Terrestre (Cañar), El Tambo (Panamericana Norte) y Suscal. La cooperativa cuenta con alrededor de 9.800 socios activos y se ubica en el segmento 3 de la SEPS. Entidad bajo control de la SEPS, en entorno rural y agrícola del cantón Cañar. RUC 0391005664001.
A2	¿Qué servicios digitales ofrece la cooperativa a sus socios (banca web, aplicación móvil, cajeros automáticos, tarjetas de débito, transferencias interbancarias, pago de servicios, otros)? ¿Desde cuándo opera cada uno?	Aplicación móvil Yuyay Móvil (en operación desde 2021); web transaccional (desde 2019); cajeros virtuales (agrupados como canales electrónicos); dos cajeros automáticos (ATM, desde 2018); tarjetas de débito sobre la red COONECTA (desde 2018); aplicación de recaudaciones; transferencias electrónicas interbancarias (SPI, desde 2020) con autenticación de dos factores y OTP. Las transferencias interbancarias y el pago de servicios se prestan desde la misma aplicación de recaudaciones, por lo que se tratan como un solo servicio (SD-06).
A3	Para cada servicio digital, ¿cuál es el volumen aproximado de transacciones por día y en qué horarios se concentra el uso? ¿Existen días o fechas de mayor demanda (fin de mes, pago de bono, cosechas)?	Volumen por canal: el core financiero concentra el mayor número de operaciones; entre los canales digitales, la aplicación móvil registra el mayor uso, seguida por las tarjetas de débito, las transferencias y recaudaciones, los cajeros automáticos y la web transaccional. La demanda aumenta en las fechas de pago y en la temporada agrícola. Las cifras por canal y los horarios de mayor uso se reservan por confidencialidad institucional. La descarga del respaldo diario se realiza al cierre de la jornada operativa.
A4	¿Qué porcentaje de las operaciones de la cooperativa se realiza hoy por canales digitales frente a ventanilla? ¿Cómo ha evolucionado en los últimos dos años?	Aproximadamente el 35 % de las operaciones se realiza hoy por canales digitales (aplicación móvil, web, cajeros y tarjetas) y el 65 % en ventanilla. Hace dos años la proporción digital era cercana al 20 %, de modo que ha crecido unos 15 puntos porcentuales, impulsada principalmente por la aplicación móvil.

Bloque B. Dependencias tecnológicas y proveedores

N.º	Pregunta	Respuesta / notas del entrevistador
B1	¿Qué componentes tecnológicos sostienen cada servicio digital (core financiero, base de datos, servidores en nube, enlaces de Internet, firewall, switch transaccional, pasarela de tarjetas)? Validar contra el inventario de activos.	Core financiero Vimacoop/VimaSistem sobre base de datos Oracle y SGBD, gestionado con la plataforma Vimagest; infraestructura en la nube Oracle Cloud (OCI) administrada por el contratista; conexión a Internet que soporta los canales electrónicos, la nube y la red de pagos; firewall perimetral; red LAN; centro de datos con servidores locales, NAS, UPS, generador y aire acondicionado; SOC/SIEM externo. Se aclara la inconsistencia del inventario: el core y el SGBD operan en OCI administrado por el contratista; en el centro de datos local quedan el NAS, los respaldos descargados, los servidores de dominio y archivos, y los equipos de comunicaciones.
B2	¿Qué servicios están provistos o administrados por terceros (proveedor del core Vimacoop/VimaSistem, infraestructura OCI, red COONECTA, SOC gestionado, operador de telecomunicaciones, mantenimiento de ATM)? ¿Qué parte de la operación queda bajo control directo de la cooperativa?	Terceros: proveedor del core Vimacoop/VimaSistem (actualizaciones, parches, DRP, soporte del core y de la app móvil); contratista de la infraestructura OCI; COONECTA (red de pagos y monitoreo transaccional de tarjetas); proveedor de SOCaaS; proveedor de mantenimiento de cajeros; operador de telecomunicaciones del enlace de Internet. Bajo control de la cooperativa: sistemas, equipos, redes, endpoints y entornos propios. Los parches del servicio administrado se coordinan mediante tickets en Vimagest.

N.º	Pregunta	Respuesta / notas del entrevistador
B3	¿Los contratos con esos proveedores incluyen acuerdos de nivel de servicio con tiempos máximos de restablecimiento, penalizaciones y planes de salida? ¿Se han verificado sus propios planes de continuidad?	La política exige que los contratos con terceros incluyan niveles de servicio, monitoreo del desempeño y mitigación de riesgos del proveedor, y asigna a TI la negociación de ANS. En la práctica: el contrato con el proveedor del core fija un tiempo máximo de restablecimiento de 24 horas, sin penalizaciones ni plan de salida; el contratista de OCI tiene un tiempo de respuesta de 8 horas; el enlace de Internet tiene un tiempo de reparación de 6 horas; COONECTA no tiene SLA de disponibilidad; el SOC tiene tiempo de respuesta de 4 horas para alertas críticas. La cooperativa no ha revisado los planes de continuidad de sus proveedores. El informe de riesgos identifica falta de DRP probado del proveedor del core (R23, Extremo), ausencia de plan de salida y de respaldo del código fuente (R28, Extremo), ausencia de certificaciones y auditorías del proveedor cloud (R31, Alto), falta de SLA en la red de tarjetas (TD-05, Alto) y no exigencia contractual de certificaciones (TD-07, Alto).
B4	¿Existe redundancia en los enlaces de Internet, en la energía eléctrica (UPS, generador) y en los servidores críticos? ¿Qué autonomía real tiene el centro de datos ante un corte de energía?	Existe un único enlace de Internet; está en proceso la contratación de un segundo enlace con otro operador. Energía: cinco UPS con autonomía de unos 30 minutos y un generador con autonomía medida de 12 horas con el tanque lleno, que cubre el centro de datos y las áreas de atención de la Matriz; las agencias cuentan solo con UPS. No hay redundancia de servidores locales; el core en OCI depende de la redundancia del proveedor cloud. La política exige energía de respaldo con autonomía mínima de 8 horas y estándar del área de servidores con climatización, detección de humo, UPS y generador. El informe de riesgos señala "falta de redundancia" en el core (R23). El procedimiento de respaldos programa pruebas semestrales de enlaces de datos.

Bloque C. Historial de interrupciones

N.º	Pregunta	Respuesta / notas del entrevistador
C1	En los últimos dos años, ¿qué interrupciones han afectado a los servicios digitales? Para cada una: fecha aproximada, servicio afectado, causa, duración y cómo se resolvió.	Interrupciones relevantes registradas en el gestor de incidentes: (1) marzo de 2025, caída del enlace de Internet por corte de fibra del operador, afectó a todos los canales electrónicos y al acceso al core, duración aproximada de 6 horas, se atendió en ventanilla con registro manual y digitación posterior; (2) agosto de 2025, aplicación móvil fuera de servicio unas 3 horas por una actualización fallida del proveedor, se revirtió la versión; (3) enero de 2026, cajero automático de la Matriz fuera de servicio dos días por falla del dispensador, los socios usaron el segundo cajero y la ventanilla; (4) julio de 2026, corte eléctrico de 2 horas en la Matriz cubierto por UPS y generador sin afectación al servicio. Indicadores de mesa de ayuda y de incidentes: tiempo promedio de resolución con línea base de 30 h (meta ≤ 24 h), tiempo de primera respuesta 4 h (meta ≤ 2 h), tiempo medio entre fallas 120 h (meta ≥ 200 h).
C2	¿Cuál ha sido la interrupción más larga y cuál la de mayor impacto? ¿Qué consecuencias tuvo para los socios, para la operación y ante el organismo de control?	La interrupción más larga y de mayor impacto fue la caída del enlace de Internet de marzo de 2025, de unas 6 horas en horario de atención: la aplicación móvil, la web, las transferencias y los cajeros quedaron fuera de servicio y la ventanilla no tuvo acceso al core, por lo que se registraron depósitos y retiros en formularios manuales y se digitaron al restablecerse el servicio. Hubo reclamos de socios en las agencias y en redes sociales, y la conciliación posterior tomó un día adicional. No se recibió sanción ni requerimiento de la SEPS; el incidente quedó registrado en el gestor de incidentes con su informe de ejecución.
C3	¿Con qué frecuencia se presentan caídas breves (minutos) de la aplicación móvil, la banca web o los cajeros? ¿Se registran en el gestor de incidentes?	Se presentan entre dos y tres caídas breves al mes, de 5 a 20 minutos, principalmente en la aplicación móvil y la web, asociadas a mantenimientos del proveedor o a microcortes del enlace; los cajeros presentan una caída breve al mes aproximadamente. Los incidentes se reportan por correo, personalmente o mediante el HelpDesk y se registran en el gestor de incidentes; se envían estadísticas mensuales al Oficial de SI y trimestrales desde Riesgos.

N.º	Pregunta	Respuesta / notas del entrevistador
C4	¿Se ha presentado algún incidente de seguridad (ransomware, fraude en canales, denegación de servicio) que haya interrumpido servicios? ¿Cómo se gestionó?	No se ha presentado ningún incidente de seguridad (ransomware, fraude en canales o denegación de servicio) que haya interrumpido los servicios. El Ethical Hacking 2024 detectó y corrigió vulnerabilidades en la app móvil (instalación en Android sin soporte, tráfico en texto claro, cifrado CBC vulnerable), gestionadas con el proveedor sin afectación al servicio. Los riesgos de fuga de información, manipulación de transacciones, clonación de tarjetas y denegación de servicio están identificados en la matriz de riesgos, pero no se han materializado.

Bloque D. Controles de continuidad existentes

N.º	Pregunta	Respuesta / notas del entrevistador
D1	Describa el esquema actual de respaldos de la base de datos: frecuencia, horario, medio, lugar de almacenamiento, retención y responsable. ¿Existe copia fuera del sitio principal o en otra región de la nube?	Respaldo automático diario de la base de datos Oracle mediante Vimagest (Data Pump); verificación diaria del estado; descarga al cierre de la jornada y almacenamiento en el repositorio institucional (centro de datos/NAS); respaldo mensual (último día del mes) y anual (último día del año). Retención: 30 respaldos diarios, 12 mensuales y los anuales de forma permanente. Responsable: Coordinador de Sistemas. No existe copia fuera del sitio: la política la exige, el inventario la declara pendiente y el informe de riesgos registra "ausencia de copias fuera del sitio" (R24, Alto).
D2	¿Con qué frecuencia se prueba la restauración de un respaldo? ¿Cuándo fue la última prueba documentada y cuánto tiempo tomó restaurar el core financiero?	El procedimiento fija pruebas de restauración de copias de BD trimestrales y pruebas de sitios alternos semestrales, ambas con seguimiento de Seguridad de la Información. La última restauración documentada se realizó en marzo de 2026 sobre el ambiente de pruebas y tomó alrededor de 3,5 horas para dejar operativo el core; no se ha realizado una prueba en sitio alterno. El informe recomienda pruebas mensuales.
D3	¿El proveedor del core financiero dispone de un plan de recuperación ante desastres (DRP) y de un sitio alterno? ¿La cooperativa ha presenciado o exigido su ejecución?	El proveedor del core es responsable del DRP, que existe por escrito como anexo del contrato de servicio, pero nunca se ha ejecutado ni presenciado por la cooperativa. El informe califica como Extremo la "falta de redundancia o DRP probado" y recomienda exigir su ejecución anual y la réplica de la base de datos en sitio alterno. El procedimiento de parches distingue ambientes de producción, contingencia y pruebas.
D4	¿Existe un plan de contingencia o de continuidad documentado y aprobado por el Consejo de Administración? Si la respuesta es parcial, ¿qué documentos lo sustituyen en la práctica (proceso 5 del Manual de Procesos de TI, procedimientos operativos)?	No existe un BCP integral aprobado por el Consejo de Administración. Existen piezas: definiciones de BCP, DRP, plan de contingencia, RTO y RPO; objetivo de "disponer de un plan de contingencia de TI"; el Comité de SI debe supervisar el desarrollo y mantenimiento del BCP; el proceso 5 regula la ejecución de planes operativos de contingencia del centro de cómputo. El informe recomienda al "Oficial de Continuidad / DRP" que BCP y DRP incluyan escenarios de ciberincidentes y fallas de proveedores.
D5	¿Qué modos de operación degradada existen cuando falla un componente (atención manual en ventanilla, cajeros fuera de línea, transferencias diferidas)? ¿Están documentados y el personal los conoce?	Cuando cae el core o el enlace, la ventanilla atiende consultas con el último saldo disponible y registra depósitos y retiros en formularios manuales que se digitan al restablecerse el servicio; los retiros se limitan a montos pequeños; los cajeros quedan fuera de línea; las transferencias se difieren al siguiente ciclo. Estos modos de operación degradada se aplican por práctica y no están documentados ni probados. La política dispone que la continuidad de los sistemas de transferencias electrónicas cubra eventos fortuitos con equipo de respaldo y procedimientos de contingencia, y que la continuidad de la operación de sistemas se asegure con un plan de contingencias.

Bloque E. Respuesta a incidentes y comunicación

N.º	Pregunta	Respuesta / notas del entrevistador
E1	Cuando ocurre una interrupción, ¿quién la detecta, quién decide que es grave y quién autoriza las acciones de recuperación? Describa la secuencia real desde la alerta hasta la restauración.	Proceso 5: el Oficial de Seguridad Física y Electrónica (OSFE) notifica al Coordinador de TI y al Oficial de SI; el Coordinador evalúa la gravedad y decide si se activa el plan de contingencia; el OSFE coordina y soluciona el incidente con apoyo de áreas y proveedores, lo comunica al Comité de Continuidad, ejecuta el plan y remite el informe final al Coordinador. En la práctica, la detección la realiza el personal de ventanilla o el monitoreo del SOC, el Coordinador de Sistemas decide y autoriza las acciones y la Gerencia General se informa cuando la interrupción supera una hora. Los incidentes se clasifican, escalan y se someten a análisis de causa raíz.
E2	¿Está conformado y operativo el Comité de Seguridad de la Información y Continuidad del Negocio? ¿Con qué frecuencia se reúne y qué decisiones ha tomado sobre continuidad?	Comité de Seguridad de la Información integrado por la presidenta, el Gerente General, el Coordinador de Sistemas, el Auditor Informático y la Oficial de SI (secretaria); se reúne trimestralmente y de forma extraordinaria cuando se requiere. Revisó el manual de seguridad en octubre de 2024, dispuso la contratación del SOC gestionado y aprobó el procedimiento de respaldos; el desarrollo del BCP está pendiente en su plan de trabajo. Entre sus funciones: supervisar el desarrollo y mantenimiento del BCP y validar el mapa de riesgos. El manual lo nombra también "Comité de Seguridad de la Información y Continuidad del Negocio".
E3	¿Cómo se comunica una interrupción a los socios, al personal, a los proveedores y a la SEPS? ¿Existen mensajes o canales predefinidos?	A los socios se les comunica mediante el WhatsApp institucional, la página de Facebook y avisos en las agencias; al personal, por correo y grupo de WhatsApp de TI; a los proveedores, por contacto inmediato ante pérdida de enlace o falla del core. No existen mensajes predefinidos ni un procedimiento de notificación a la SEPS, y hasta la fecha no se ha notificado formalmente ninguna interrupción al organismo de control. Acuse de recibo al usuario que reporta un incidente; estadísticas internas mensuales y trimestrales; la información de incidentes es confidencial.
E4	¿Se elabora un informe posterior a cada incidente con causas, acciones y lecciones aprendidas? ¿Dónde se registra y quién lo revisa?	Sí. El plan de contingencia genera un "informe de ejecución" con causas, acciones y medidas de prevención; la gestión de problemas exige análisis de causa raíz, registro de errores conocidos y base de conocimiento; el Oficial de SI documenta los incidentes relevantes. Los informes se registran en el gestor de incidentes y en el repositorio de TI, y los revisan el Oficial de SI y el Comité de SI en su sesión trimestral.

Bloque F. Tolerancia a la interrupción (insumo del BIA)

N.º	Pregunta	Respuesta / notas del entrevistador
F1	Para cada servicio digital, ¿cuánto tiempo puede estar fuera de servicio antes de que las consecuencias sean inaceptables para la cooperativa (horas, un día, varios días)? Justifique con el efecto sobre socios, ingresos, obligaciones regulatorias y reputación.	Tiempo máximo tolerable de interrupción por servicio: core financiero e infraestructura en la nube/enlace de Internet, 8 horas (una jornada de atención sin core es inaceptable por el riesgo regulatorio y de reclamos); tarjetas de débito, 8 horas (los socios dependen del retiro con tarjeta fuera del cantón); aplicación móvil, web transaccional, transferencias y recaudaciones, 24 horas (pueden suplirse por ventanilla durante un día); cajeros automáticos, 24 horas (existe el segundo cajero y la ventanilla); SOC/SIEM y carpetas compartidas, 72 horas. Valoración de disponibilidad (D) del inventario MAGERIT: canales electrónicos, SGBD, Internet, LAN, firewall y centro de datos D = 10; core, nube, web, tarjetas y ATM D = 9.
F2	¿En qué plazo debería estar reanudado cada servicio para operar con seguridad (tiempo objetivo de recuperación)? ¿Es menor que el tiempo máximo tolerable indicado en F1?	Tiempo objetivo de recuperación: 4 horas para el core, la infraestructura en la nube/enlace y las tarjetas de débito; 8 horas para la aplicación móvil, la web, las transferencias y los cajeros; 24 horas para el SOC/SIEM y carpetas compartidas. En todos los casos el RTO es menor que el MTPD indicado. La política define el RTO como el período para reanudar antes de que la entidad genere pérdidas significativas, sin fijar valores.

N.º	Pregunta	Respuesta / notas del entrevistador
F3	¿Cuántas horas de transacciones podría perder la cooperativa sin que la pérdida sea inaceptable (punto objetivo de recuperación)? ¿Qué transacciones son irrecuperables manualmente?	La cooperativa puede tolerar la pérdida de hasta 1 hora de transacciones (RPO objetivo de 1 hora para el core y los canales que dependen de él). Capacidad actual (no objetivo): con un respaldo diario, la pérdida posible es de hasta 24 horas de transacciones si falla la base de datos y no hay réplica; el proveedor mantiene los archivos de registro (archive logs) de Oracle en OCI, lo que permitiría reducir la pérdida solo si el respaldo fuera físico (RMAN), pues el respaldo actual con Data Pump es lógico y no admite la aplicación de archivos de registro (Anexo A, D1); tampoco existe réplica en sitio alterno. Las transacciones irrecuperables serían las de cajeros y tarjetas que no se hubieran conciliado con COONECTA y las transferencias SPI enviadas sin confirmación. La política define el RPO sin fijar valores.
F4	Durante una interrupción, ¿cuál es el nivel mínimo de servicio que debe mantenerse (por ejemplo, consultas y retiros en ventanilla aunque fallen las transferencias interbancarias)?	Durante una interrupción debe mantenerse, como mínimo: consulta de saldos, depósitos y retiros de montos pequeños en ventanilla con registro manual y digitación posterior; bloqueo de tarjetas por vía telefónica; y comunicación a los socios por WhatsApp y Facebook. Las transferencias interbancarias y el pago de servicios pueden diferirse al siguiente ciclo.
F5	¿Qué servicio debería recuperarse primero si todos cayeran a la vez y por qué? Ordene los servicios digitales por prioridad de recuperación.	Orden de prioridad de recuperación desde la perspectiva del negocio: (1) infraestructura en la nube y enlace de Internet, y core financiero, porque de ellos dependen todos los demás canales y la ventanilla; (2) tarjetas de débito, por el volumen de socios que las usan fuera del cantón; (3) aplicación móvil y web transaccional; (4) transferencias electrónicas y recaudaciones; (5) cajeros automáticos; (6) SOC/SIEM y carpetas compartidas. Por dependencias técnicas, todos los canales dependen del core y de la base de datos, y estos de la nube y del enlace de Internet.

Bloque G. Gobernanza, recursos y cultura

N.º	Pregunta	Respuesta / notas del entrevistador
G1	¿Qué roles del Manual de Seguridad de la Información (Oficial de SI, Coordinador de TI, OSFE, Auditoría Interna) intervienen en la continuidad y cuáles tienen suplente designado?	Consejo de Administración, Gerencia, Comité de SI, Oficial de SI (entre sus funciones "garantizar la continuidad del negocio"), Coordinador de TI, OSFE, Talento Humano, Auditoría Interna y personal. No existen suplentes formales designados: el Ingeniero de Sistemas actúa como suplente de hecho del Coordinador de Sistemas y el Auditor Informático apoya a la Oficial de SI. No existe el rol de Oficial de Continuidad del Negocio; el informe alude a un "Oficial de Continuidad del Negocio/DRP" que no figura en el inventario de personal. El inventario registra un titular por rol; la política exige administrador principal y de respaldo para servidores.
G2	¿Existe presupuesto asignado a continuidad y recuperación (sitio alterno, redundancias, pruebas)? ¿Qué inversiones se han aprobado o postergado en el último año?	No existe una partida específica de continuidad. En el último año se aprobó la contratación de un segundo enlace de Internet (en ejecución) y la renovación de las UPS; se postergaron el sitio alterno, la réplica de la base de datos y las pruebas de DRP con el proveedor por costo. El procedimiento de respaldos enumera recursos financieros (almacenamiento, licencias y soporte de Vimagest, infraestructura, mantenimiento) sin montos. El informe recomienda al Directorio asignar recursos priorizando riesgos Alto y Extremo.
G3	¿El personal ha recibido capacitación o ha participado en simulacros de continuidad? ¿Con qué frecuencia?	El personal recibe una capacitación anual en seguridad de la información a cargo de Talento Humano y la Oficial de SI; no se han realizado simulacros ni pruebas de continuidad con participación del personal.
G4	¿Qué observaciones ha recibido la cooperativa de la SEPS o de auditoría interna sobre continuidad del negocio y riesgo operativo tecnológico?	En la revisión de la SEPS de 2025 se recibió una observación sobre la falta de un plan de contingencia probado y de respaldos fuera del sitio, que se encuentra en proceso de atención; auditoría interna reiteró la observación en su informe anual. Marco normativo interno citado: Resolución SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116 (riesgo operativo y legal), Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSEF-INR-DNSI-2022-002 (seguridad de la información) y LOPDP.

N.º	Pregunta	Respuesta / notas del entrevistador
G5	¿Qué obstáculos prevé para implementar un plan de continuidad formal y qué apoyo necesitaría del área de TI, de la gerencia y del Consejo de Administración?	Obstáculos previstos: presupuesto limitado para sitio alterno y redundancias; alta dependencia del proveedor del core y del SOC externo sin controles contractuales suficientes; personal de TI reducido (tres personas) para documentar y probar el plan. Apoyo requerido: de TI, tiempo asignado para documentar y ejecutar las pruebas; de la Gerencia, presupuesto para el segundo enlace, la réplica de base de datos y las pruebas de DRP; del Consejo de Administración, aprobación de la política de continuidad y del BCP, y exigencia de SLA en la renovación de contratos.

A.5 Correspondencia de las preguntas con los objetivos y el marco normativo

Bloque	Objetivo específico que alimenta	Cláusula ISO 22301:2019	Fase MAGERIT / BIA
A. Contexto y servicios	OE2 – identificar activos y procesos críticos	4.1 Contexto; 8.2.2 BIA	Identificación de servicios
B. Dependencias y proveedores	OE2	8.2.2 dependencias; 8.3 estrategias	Paso 1 inventario y valoración de activos
C. Historial de interrupciones	OE2 – riesgos tecnológicos	8.2.3 evaluación de riesgos	Paso 3 frecuencia de amenazas
D. Controles existentes	OE2 – riesgo residual	8.2.3; 8.3.3 recursos	Paso 5 salvaguardas
E. Respuesta y comunicación	OE3 – elaboración del plan	8.4 estructura de respuesta y comunicación	Procedimientos de respuesta
F. Tolerancia a la interrupción	OE2 y OE3 – BIA, prioridades	8.2.2 MTPD, RTO, RPO, MBCO	Ficha BIA (Anexo B)
G. Gobernanza y cultura	OE3 – política, roles, ejercicios	5 Liderazgo; 7 Soporte; 8.5 ejercicios	Plan de tratamiento

Firma del entrevistado: _____ Firma del investigador:

_____

Anexo B: Ficha de análisis de impacto al negocio (BIA) por servicio digital

B.1 Instrucciones de aplicación

- Se completa una ficha por cada servicio digital de la lista B.2, en sesión conjunta con el propietario del servicio (negocio) y el responsable técnico (TI), tomando como base las respuestas del bloque F de la entrevista y la información del inventario de activos.
- Las dependencias (sección 3 de la ficha) se validan contra el inventario MAGERIT, indicando el código de cada activo (p. ej., ACT-SW-02 Core Financiero, ACT-COM-02 Conexión a Internet).
- Los impactos (sección 4) se valoran con la escala de 1 a 5 de la Tabla 3 del marco teórico para cada duración de interrupción; la casilla en la que el impacto alcanza el nivel 4 (Mayor) determina el período máximo tolerable de interrupción (MTPD).
- El RTO debe ser menor que el MTPD; el RPO expresa la pérdida máxima de datos tolerable en horas y se contrasta con la frecuencia real de respaldos (actualmente diaria).
- El MBCO describe en palabras el nivel mínimo de servicio aceptable durante la interrupción (qué operaciones deben mantenerse y por qué medio).
- Al terminar, los valores de MTPD, RTO, RPO y prioridad de todas las fichas se consolidan en la matriz B.4, que es el insumo directo de la fase de estrategias de continuidad del capítulo IV.

B.2 Servicios digitales a evaluar

Código	Servicio digital	Activo principal (inventario)	Propietario sugerido
SD-01	Core financiero (transacciones, cuentas, reportes)	ACT-SW-02 / ACT-SW-08	Gerencia / Coordinador de Sistemas
SD-02	Web transaccional (banca por Internet)	ACT-S-03	Jefe de Negocios
SD-03	Aplicación móvil Yuyay Móvil	ACT-SW-01 / ACT-S-04	Jefe de Negocios
SD-04	Cajeros automáticos (ATM)	ACT-HW-15 / ACT-HW-16	Tesorería / Cajas
SD-05	Tarjetas de débito (red COONECTA)	ACT-S-05 / ACT-P-07	Jefe de Negocios
SD-06	Transferencias interbancarias y pago de servicios	ACT-S-01 / ACT-SW-06	Tesorería
SD-07	Infraestructura en la nube (OCI) y enlaces de Internet	ACT-S-02 / ACT-COM-02	Coordinador de Sistemas
SD-08	Monitoreo de seguridad (SOC/SIEM) y carpetas compartidas	ACT-S-07 / ACT-S-06	Oficial de SI

Nota: la lista se confirmó con las respuestas de las preguntas A2 y F5 de la entrevista; las transferencias interbancarias y el pago de servicios se mantienen como un solo servicio (SD-06).

B.3 Fichas BIA por servicio digital

Las fichas se completaron con la información disponible en los documentos institucionales y se validaron en la sesión BIA con los propietarios de cada servicio y el responsable técnico. Los valores de MTPD, RTO, RPO, MBCO y prioridad propuestos como hipótesis de trabajo fueron confirmados y constan en la columna "Valor validado"; los impactos por duración se valoraron con la escala de la Tabla 3 del marco teórico.

Ficha SD-01 – Core financiero (transacciones, cuentas, reportes)

1. Identificación del servicio

Campo	Registro
Código y nombre del servicio	SD-01 – Core financiero (transacciones, cuentas, reportes)
Descripción breve	Registro de transacciones; conciliaciones; saldos; productos financieros; reportes regulatorios [IR 2]
Propietario del servicio / responsable técnico	Gerencia / Coordinador de Sistemas; proveedor Vimacoop/VimaSistem
Canales por los que se presta	Ventanilla, y como back-end de app, web, ATM y tarjetas
Horario de operación	Ventanilla: lunes a viernes 08:00–17:00 y sábados 08:00–13:00; como back-end de los canales digitales, 24/7
Usuarios / socios que lo utilizan	Todo el personal operativo (45 usuarios internos) y los 9.800 socios a través de ventanilla y canales
Transacciones por día (promedio y pico)	Dato reservado por confidencialidad institucional
Fuentes documentales	[INV] inventario de activos; [MP] manual de procesos de TI; [MSI] manual de seguridad de la información; [IR] informe de riesgos de seguridad de la información
Fecha de la ficha y participantes	Sesión BIA del 1 de octubre de 2026. Participantes: propietario del servicio, Coordinador de Sistemas (responsable técnico) e investigador.

2. Actividades que entrega el servicio

N.º	Actividad o proceso	Área responsable
1	Registro de transacciones	Gerencia / Coordinador de Sistemas
2	Conciliaciones	Gerencia / Coordinador de Sistemas
3	Saldos	Gerencia / Coordinador de Sistemas
4	Productos financieros	Gerencia / Coordinador de Sistemas
5	Reportes regulatorios	Gerencia / Coordinador de Sistemas

3. Dependencias

Recurso / activo (código de inventario)	Interno / tercero	Alternativa existente
ACT-SW-02 Core	Tercero	Ambiente de contingencia mencionado en [MP] 16.3 sin evidencia de prueba; sin réplica en sitio alterno [IR R23]
ACT-SW-08 SGBD Oracle	Tercero	Sin alternativa en operación; restauración desde el respaldo diario (prueba de 3,5 h)
ACT-D-02 Bases de datos	Interno	Respaldo diario restaurable (prueba de 3,5 h); sin réplica en espera
ACT-D-04 Respaldos	Interno	Sin copia fuera del sitio: los respaldos se guardan en el mismo centro de datos
ACT-S-02 Nube OCI	Tercero	Redundancia interna del proveedor; sin réplica en otra región
ACT-COM-02 Internet	Interno	Sin enlace alterno; segundo enlace con otro operador en contratación
ACT-P-04 Coordinador de Sistemas	Interno	Suplencia de hecho del Ingeniero de Sistemas, sin designación formal
ACT-P-05 Proveedor del core	Tercero	Sin alternativa: no existe plan de salida ni custodia del código fuente

4. Impacto según la duración de la interrupción (escala 1 a 5 de la Tabla 3)

Dimensión de impacto	1 hora	4 horas	8 horas	24 horas	72 horas	1 semana
Operativa	2	3	4	5	5	5
Financiera	1	2	3	4	5	5
Legal / regulatoria	1	1	2	3	4	5
Reputacional	1	2	3	4	5	5
Impacto máximo del período	2	3	4	5	5	5

Referencia para la valoración: criticidad MAGERIT Core D = 9; SGBD D = 10; BD D = 9. Riesgos asociados: R23 interrupción total por falta de redundancia o DRP probado (Extremo); R24 pérdida o corrupción de datos (Alto); R26 cambios no controlados (Extremo); R28 pérdida de acceso tras terminación del contrato (Extremo); MAGERIT: denegación de servicio 15 y software dañino 15 (Crítico).

5. Parámetros de recuperación

Parámetro	Hipótesis de trabajo	Valor validado	Justificación
MTPD (horas)	8 h	8 h	Primera duración con impacto ≥ 4
RTO (horas)	4 h	4 h	Menor que el MTPD
RPO (horas)	1 h	1 h	Capacidad actual: RPO real ≤ 24 h; RTO no documentado; DRP no probado

Parámetro	Hipótesis de trabajo	Valor validado	Justificación
MBCO	Ventanilla con consultas y registro diferido de depósitos y retiros	Ventanilla con consultas y registro diferido de depósitos y retiros	Nivel mínimo durante la interrupción
Prioridad de recuperación	1	1	Dependencias técnicas; confirmado en entrevista (F5)

6. Controles existentes y recursos mínimos para recuperar

Controles o alternativas existentes hoy	Recursos mínimos necesarios para reanudar en el RTO
Respaldo diario Vimagest con verificación diaria, mensual y anual [MP 17]; gestión de parches vía Vimagest [MP 16]; gestión de cambios [MP 11]	ACT-SW-02, ACT-SW-08, ACT-D-02, ACT-D-04, ACT-S-02, ACT-COM-02, ACT-P-04, ACT-P-05

7. Observaciones y validación

Observaciones
Capacidad actual documentada: RPO real ≤ 24 h; RTO no documentado; DRP no probado. Hipótesis de MTPD, RTO, RPO, MBCO y prioridad validadas en la sesión BIA con el propietario del servicio y el responsable técnico; impactos por duración valorados con la escala de la Tabla 3. Valores incorporados a la matriz B.4.

Propietario del servicio: _____ Responsable técnico: _____ Investigador: _____

Ficha SD-02 – Web transaccional (banca por Internet)

1. Identificación del servicio

Campo	Registro
Código y nombre del servicio	SD-02 – Web transaccional (banca por Internet)
Descripción breve	Consultas de saldos y movimientos; transferencias; operaciones en línea [INV ACT-S-03]
Propietario del servicio / responsable técnico	Jefe de Negocios; Ingeniero de Sistemas
Canales por los que se presta	Internet
Horario de operación	24/7; mantenimientos programados del proveedor fuera del horario de atención
Usuarios / socios que lo utilizan	Alrededor de 1.500 socios registrados en la banca por Internet
Transacciones por día (promedio y pico)	Dato reservado por confidencialidad institucional
Fuentes documentales	[INV] inventario de activos; [MP] manual de procesos de TI; [MSI] manual de seguridad de la información; [IR] informe de riesgos de seguridad de la información

Campo	Registro
Fecha de la ficha y participantes	Sesión BIA del 1 de octubre de 2026. Participantes: propietario del servicio, Coordinador de Sistemas (responsable técnico) e investigador.

2. Actividades que entrega el servicio

N.º	Actividad o proceso	Área responsable
1	Consultas de saldos y movimientos	Jefe de Negocios
2	Transferencias	Jefe de Negocios
3	Operaciones en línea	Jefe de Negocios

3. Dependencias

Recurso / activo (código de inventario)	Interno / tercero	Alternativa existente
ACT-S-03 Web transaccional	Interno	Sin alterno documentado
ACT-SW-02 Core	Tercero	Ambiente de contingencia del proveedor sin evidencia de prueba; sin réplica en sitio alterno
ACT-K-01 Certificado TLS	Interno	Sin alternativa documentada
ACT-COM-02 Internet	Interno	Sin enlace alterno; segundo enlace con otro operador en contratación
ACT-HW-13 Firewall	Interno	Sin alternativa documentada
ACT-S-02 Nube	Tercero	Redundancia interna del proveedor; sin réplica en otra región

4. Impacto según la duración de la interrupción (escala 1 a 5 de la Tabla 3)

Dimensión de impacto	1 hora	4 horas	8 horas	24 horas	72 horas	1 semana
Operativa	1	2	3	4	5	5
Financiera	1	1	2	3	4	5
Legal / regulatoria	1	1	1	2	3	4
Reputacional	1	2	2	4	4	5
Impacto máximo del período	1	2	3	4	5	5

Referencia para la valoración: criticidad MAGERIT D = 9. Riesgos asociados: R1 fuga de información (Moderado); R2 manipulación de transacciones (Moderado); MAGERIT: robo 8, errores 8 (Medio).

5. Parámetros de recuperación

Parámetro	Hipótesis de trabajo	Valor validado	Justificación
MTPD (horas)	24 h	24 h	Primera duración con impacto ≥ 4
RTO (horas)	8 h	8 h	Menor que el MTPD
RPO (horas)	1 h (hereda del core)	1 h (hereda del core)	Capacidad actual: Depende de SD-01 y SD-07

Parámetro	Hipótesis de trabajo	Valor validado	Justificación
MBCO	Consultas de saldo	Consultas de saldo	Nivel mínimo durante la interrupción
Prioridad de recuperación	3	3	Dependencias técnicas; confirmado en entrevista (F5)

6. Controles existentes y recursos mínimos para recuperar

Controles o alternativas existentes hoy	Recursos mínimos necesarios para reanudar en el RTO
HTTPS; bloqueo tras 3 intentos fallidos; autenticación de dos factores con OTP [MSI 7.6.9 y 7.20]; SOC/SIEM	ACT-S-03, ACT-SW-02, ACT-K-01, ACT-COM-02, ACT-HW-13, ACT-S-02

7. Observaciones y validación

Observaciones
Capacidad actual documentada: Depende de SD-01 y SD-07. Hipótesis de MTPD, RTO, RPO, MBCO y prioridad validadas en la sesión BIA con el propietario del servicio y el responsable técnico; impactos por duración valorados con la escala de la Tabla 3. Valores incorporados a la matriz B.4.

Propietario del servicio: _____ Responsable técnico: _____ Investigador: _____

Ficha SD-03 – Aplicación móvil Yuyay Móvil

1. Identificación del servicio

Campo	Registro
Código y nombre del servicio	SD-03 – Aplicación móvil Yuyay Móvil
Descripción breve	Consultas, transferencias y operaciones de banca móvil [INV ACT-SW-01]
Propietario del servicio / responsable técnico	Jefe de Negocios; proveedor del core (soporte de la app)
Canales por los que se presta	Teléfono móvil
Horario de operación	24/7; mantenimientos programados del proveedor fuera del horario de atención
Usuarios / socios que lo utilizan	Alrededor de 3.200 socios activos en la aplicación
Transacciones por día (promedio y pico)	Dato reservado por confidencialidad institucional
Fuentes documentales	[INV] inventario de activos; [MP] manual de procesos de TI; [MSI] manual de seguridad de la información; [IR] informe de riesgos de seguridad de la información
Fecha de la ficha y participantes	Sesión BIA del 1 de octubre de 2026. Participantes: propietario del servicio, Coordinador de Sistemas (responsable técnico) e investigador.

2. Actividades que entrega el servicio

N.º	Actividad o proceso	Área responsable
1	Consultas, transferencias y operaciones de banca móvil	Jefe de Negocios

3. Dependencias

Recurso / activo (código de inventario)	Interno / tercero	Alternativa existente
ACT-SW-01 App móvil	Interno	Sin alterno documentado
ACT-K-02 Cifrado de comunicaciones	Interno	Sin alternativa documentada
ACT-SW-02 Core	Tercero	Ambiente de contingencia del proveedor sin evidencia de prueba; sin réplica en sitio alterno
ACT-S-04 Canales electrónicos	Interno	Atención en ventanilla, sin procedimiento documentado
ACT-COM-02 Internet	Interno	Sin enlace alterno; segundo enlace con otro operador en contratación
ACT-P-05 Proveedor	Tercero	Sin alternativa: no existe plan de salida ni custodia del código fuente

4. Impacto según la duración de la interrupción (escala 1 a 5 de la Tabla 3)

Dimensión de impacto	1 hora	4 horas	8 horas	24 horas	72 horas	1 semana
Operativa	1	2	3	4	5	5
Financiera	1	1	2	3	4	5
Legal / regulatoria	1	1	1	2	3	4
Reputacional	1	2	2	4	4	5
Impacto máximo del período	1	2	3	4	5	5

Referencia para la valoración: criticidad MAGERIT App D = 8; canales electrónicos D = 10. Riesgos asociados: R1 (Moderado); R2 (Moderado); vulnerabilidades del Ethical Hacking 2024 corregidas.

5. Parámetros de recuperación

Parámetro	Hipótesis de trabajo	Valor validado	Justificación
MTPD (horas)	24 h	24 h	Primera duración con impacto ≥ 4
RTO (horas)	8 h	8 h	Menor que el MTPD
RPO (horas)	1 h (hereda del core)	1 h (hereda del core)	Capacidad actual: Depende de SD-01 y SD-07
MBCO	Consultas de saldo	Consultas de saldo	Nivel mínimo durante la interrupción
Prioridad de recuperación	3	3	Dependencias técnicas; confirmado en entrevista (F5)

6. Controles existentes y recursos mínimos para recuperar

Controles o alternativas existentes hoy	Recursos mínimos necesarios para reanudar en el RTO
Cifrado robusto tras Ethical Hacking 2024; MFA; antimalware en canales [MSI 7.8.5]	ACT-SW-01, ACT-K-02, ACT-SW-02, ACT-S-04, ACT-COM-02, ACT-P-05

7. Observaciones y validación

Observaciones
Capacidad actual documentada: Depende de SD-01 y SD-07. Hipótesis de MTPD, RTO, RPO, MBCO y prioridad validadas en la sesión BIA con el propietario del servicio y el responsable técnico; impactos por duración valorados con la escala de la Tabla 3. Valores incorporados a la matriz B.4.

Propietario del servicio: _____ Responsable técnico: _____ Investigador: _____

Ficha SD-04 – Cajeros automáticos (ATM 1 y ATM 2)

1. Identificación del servicio

Campo	Registro
Código y nombre del servicio	SD-04 – Cajeros automáticos (ATM 1 y ATM 2)
Descripción breve	Retiro de efectivo; consulta de saldos; conciliación de transacciones [INV ACT-HW-15/16; IR 4.4]
Propietario del servicio / responsable técnico	Tesorería / Cajas; proveedor de mantenimiento
Canales por los que se presta	Autoservicio en oficinas y puntos estratégicos
Horario de operación	24/7 (ATM Matriz y ATM Terminal Terrestre)
Usuarios / socios que lo utilizan	Alrededor de 4.000 socios tarjetahabientes
Transacciones por día (promedio y pico)	Dato reservado por confidencialidad institucional
Fuentes documentales	[INV] inventario de activos; [MP] manual de procesos de TI; [MSI] manual de seguridad de la información; [IR] informe de riesgos de seguridad de la información
Fecha de la ficha y participantes	Sesión BIA del 1 de octubre de 2026. Participantes: propietario del servicio, Coordinador de Sistemas (responsable técnico) e investigador.

2. Actividades que entrega el servicio

N.º	Actividad o proceso	Área responsable
1	Retiro de efectivo	Tesorería / Cajas
2	Consulta de saldos	Tesorería / Cajas
3	Conciliación de transacciones	Tesorería / Cajas

3. Dependencias

Recurso / activo (código de inventario)	Interno / tercero	Alternativa existente
ACT-HW-15/16 ATM	Interno	Dos cajeros (redundancia parcial entre sí); retiro en ventanilla
ACT-S-05 Red de tarjetas	Interno	Sin alterno: depende de la red del proveedor
ACT-SW-02 Core	Tercero	Ambiente de contingencia del proveedor sin evidencia de prueba; sin réplica en sitio alterno
ACT-COM-02 Internet	Interno	Sin enlace alterno; segundo enlace con otro operador en contratación
ACT-AUX-03/08 energía	Interno	Generador de 12 h y UPS en la Matriz; UPS de 30 min en agencias
ACT-P-09 mantenimiento	Interno	Sin alternativa: mantenimiento externo sin SLA

4. Impacto según la duración de la interrupción (escala 1 a 5 de la Tabla 3)

Dimensión de impacto	1 hora	4 horas	8 horas	24 horas	72 horas	1 semana
Operativa	1	2	3	4	5	5
Financiera	1	1	2	3	4	5
Legal / regulatoria	1	1	1	2	3	4
Reputacional	1	2	2	4	4	5
Impacto máximo del período	1	2	3	4	5	5

Referencia para la valoración: criticidad MAGERIT D = 9. Riesgos asociados: R32 no dispensación (Moderado); R33 débito sin entrega (Moderado); MAGERIT: acceso no autorizado 15 y manipulación 12 (Crítico).

5. Parámetros de recuperación

Parámetro	Hipótesis de trabajo	Valor validado	Justificación
MTPD (horas)	24 h	24 h	Primera duración con impacto ≥ 4
RTO (horas)	8 h	8 h	Menor que el MTPD
RPO (horas)	N/A (transacciones en el core)	N/A (transacciones en el core)	Capacidad actual: SLA de mantenimiento no definido [IR R32]
MBCO	Al menos un cajero operativo o retiro en ventanilla	Al menos un cajero operativo o retiro en ventanilla	Nivel mínimo durante la interrupción
Prioridad de recuperación	5	5	Dependencias técnicas; confirmado en entrevista (F5)

6. Controles existentes y recursos mínimos para recuperar

Controles o alternativas existentes hoy	Recursos mínimos necesarios para reanudar en el RTO
Mantenimiento por proveedor externo; antimalware; conciliación (manual, se recomienda automatizar) [IR R33]	ACT-HW-15/16, ACT-S-05, ACT-SW-02, ACT-COM-02, ACT-AUX-03/08, ACT-P-09

7. Observaciones y validación

Observaciones
Capacidad actual documentada: SLA de mantenimiento no definido [IR R32]. Hipótesis de MTPD, RTO, RPO, MBCO y prioridad validadas en la sesión BIA con el propietario del servicio y el responsable técnico; impactos por duración valorados con la escala de la Tabla 3. Valores incorporados a la matriz B.4.

Propietario del servicio: _____ Responsable técnico: _____ Inves-

tigador: _____

Ficha SD-05 – Tarjetas de débito (red COONECTA)

1. Identificación del servicio

Campo	Registro
Código y nombre del servicio	SD-05 – Tarjetas de débito (red COONECTA)
Descripción breve	Uso de tarjeta; autorización; procesamiento y conciliación; atención de reclamos [IR 4.5]
Propietario del servicio / responsable técnico	Jefe de Negocios; Oficial de SI
Canales por los que se presta	POS, ATM propios y de la red, comercio electrónico
Horario de operación	24/7 a través de la red COONECTA
Usuarios / socios que lo utilizan	Alrededor de 4.000 socios tarjetahabientes
Transacciones por día (promedio y pico)	Dato reservado por confidencialidad institucional
Fuentes documentales	[INV] inventario de activos; [MP] manual de procesos de TI; [MSI] manual de seguridad de la información; [IR] informe de riesgos de seguridad de la información
Fecha de la ficha y participantes	Sesión BIA del 1 de octubre de 2026. Participantes: propietario del servicio, Coordinador de Sistemas (responsable técnico) e investigador.

2. Actividades que entrega el servicio

N.º	Actividad o proceso	Área responsable
1	Uso de tarjeta	Jefe de Negocios
2	Autorización	Jefe de Negocios
3	Procesamiento y conciliación	Jefe de Negocios

N.º	Actividad o proceso	Área responsable
4	Atención de reclamos	Jefe de Negocios

3. Dependencias

Recurso / activo (código de inventario)	Interno / tercero	Alternativa existente
ACT-S-05 Servicio de tarjetas	Tercero	Sin alterno: depende de la red del proveedor
ACT-P-07 COONECTA	Tercero	Sin alternativa: no existe acuerdo de disponibilidad con COONECTA
ACT-D-08 Datos de tarjetas	Interno	Sin alternativa documentada
ACT-MEDIA-03 Plásticos	Interno	Sin alternativa documentada
ACT-SW-02 Core	Tercero	Ambiente de contingencia del proveedor sin evidencia de prueba; sin réplica en sitio alterno
ACT-COM-02 Internet	Interno	Sin enlace alterno; segundo enlace con otro operador en contratación

4. Impacto según la duración de la interrupción (escala 1 a 5 de la Tabla 3)

Dimensión de impacto	1 hora	4 horas	8 horas	24 horas	72 horas	1 semana
Operativa	2	3	4	5	5	5
Financiera	1	2	3	4	5	5
Legal / regulatoria	1	1	2	3	4	5
Reputacional	1	2	3	4	5	5
Impacto máximo del período	2	3	4	5	5	5

Referencia para la valoración: criticidad MAGERIT D = 9. Riesgos asociados: TD-05 indisponibilidad del servicio (Alto); TD-06 fuga de datos (Extremo); TD-01 clonación (Alto); TD-07 incumplimiento del proveedor (Alto).

5. Parámetros de recuperación

Parámetro	Hipótesis de trabajo	Valor validado	Justificación
MTPD (horas)	8 h	8 h	Primera duración con impacto ≥ 4
RTO (horas)	4 h	4 h	Menor que el MTPD
RPO (horas)	Según proveedor	Según proveedor	Capacidad actual: Sin SLA de disponibilidad con el proveedor [IR TD-05]
MBCO	Bloqueo de tarjetas y retiro en ventanilla	Bloqueo de tarjetas y retiro en ventanilla	Nivel mínimo durante la interrupción
Prioridad de recuperación	2	2	Dependencias técnicas; confirmado en entrevista (F5)

6. Controles existentes y recursos mínimos para recuperar

Controles o alternativas existentes hoy	Recursos mínimos necesarios para reanudar en el RTO
Monitoreo transaccional del proveedor; bloqueo de tarjeta; cifrado [IR 4.5]	ACT-S-05, ACT-P-07, ACT-D-08, ACT-MEDIA-03, ACT-SW-02, ACT-COM-02

7. Observaciones y validación

Observaciones
Capacidad actual documentada: Sin SLA de disponibilidad con el proveedor [IR TD-05]. Hipótesis de MTPD, RTO, RPO, MBCO y prioridad validadas en la sesión BIA con el propietario del servicio y el responsable técnico; impactos por duración valorados con la escala de la Tabla 3. Valores incorporados a la matriz B.4.

Propietario del servicio: _____ Responsable técnico: _____ Investigador: _____

Ficha SD-06 – Transferencias electrónicas y recaudaciones

1. Identificación del servicio

Campo	Registro
Código y nombre del servicio	SD-06 – Transferencias electrónicas y recaudaciones
Descripción breve	Transferencias electrónicas con límites y comprobantes [MSI 7.20]; recaudación de depósitos [INV ACT-SW-06]
Propietario del servicio / responsable técnico	Tesorería
Canales por los que se presta	App, web y ventanilla
Horario de operación	Transferencias SPI en los ciclos del Banco Central (días hábiles); recaudaciones 24/7
Usuarios / socios que lo utilizan	Alrededor de 2.000 socios y los convenios de recaudación
Transacciones por día (promedio y pico)	Dato reservado por confidencialidad institucional
Fuentes documentales	[INV] inventario de activos; [MP] manual de procesos de TI; [MSI] manual de seguridad de la información; [IR] informe de riesgos de seguridad de la información
Fecha de la ficha y participantes	Sesión BIA del 1 de octubre de 2026. Participantes: propietario del servicio, Coordinador de Sistemas (responsable técnico) e investigador.

2. Actividades que entrega el servicio

N.º	Actividad o proceso	Área responsable
1	Transferencias electrónicas con límites y comprobantes	Tesorería
2	Recaudación de depósitos	Tesorería

3. Dependencias

Recurso / activo (código de inventario)	Interno / tercero	Alternativa existente
ACT-SW-06 App de recaudaciones	Interno	Equipo de respaldo exigido por política [MSI 7.20], sin evidencia
ACT-S-01 Orquestador de servicios	Interno	Sin alternativa documentada
ACT-SW-02 Core	Tercero	Ambiente de contingencia del proveedor sin evidencia de prueba; sin réplica en sitio alterno
ACT-COM-02 Internet	Interno	Sin enlace alterno; segundo enlace con otro operador en contratación

4. Impacto según la duración de la interrupción (escala 1 a 5 de la Tabla 3)

Dimensión de impacto	1 hora	4 horas	8 horas	24 horas	72 horas	1 semana
Operativa	1	2	3	4	5	5
Financiera	1	1	2	3	4	5
Legal / regulatoria	1	1	1	2	3	4
Reputacional	1	2	2	4	4	5
Impacto máximo del período	1	2	3	4	5	5

Referencia para la valoración: criticidad MAGERIT Recaudaciones D = 9; orquestador D = 9. Riesgos asociados: R2 manipulación (Moderado); MAGERIT orquestador: amenaza A.4 12 (Crítico).

5. Parámetros de recuperación

Parámetro	Hipótesis de trabajo	Valor validado	Justificación
MTPD (horas)	24 h	24 h	Primera duración con impacto ≥ 4
RTO (horas)	8 h	8 h	Menor que el MTPD
RPO (horas)	1 h (hereda del core)	1 h (hereda del core)	Capacidad actual: Depende de SD-01
MBCO	Recepción de depósitos en ventanilla con registro diferido	Recepción de depósitos en ventanilla con registro diferido	Nivel mínimo durante la interrupción
Prioridad de recuperación	4	4	Dependencias técnicas; confirmado en entrevista (F5)

6. Controles existentes y recursos mínimos para recuperar

Controles o alternativas existentes hoy	Recursos mínimos necesarios para reanudar en el RTO
Doble factor, límites por transferencia, bloqueo tras 3 intentos, registro para auditoría [MSI 7.20]	ACT-SW-06, ACT-S-01, ACT-SW-02, ACT-COM-02

7. Observaciones y validación

Observaciones
Capacidad actual documentada: Depende de SD-01. Hipótesis de MTPD, RTO, RPO, MBCO y prioridad validadas en la sesión BIA con el propietario del servicio y el responsable técnico; impactos por duración valorados con la escala de la Tabla 3. Valores incorporados a la matriz B.4.

Propietario del servicio: _____ Responsable técnico: _____ Investigador: _____

Ficha SD-07 – Infraestructura en la nube (OCI) y enlace de Internet

1. Identificación del servicio

Campo	Registro
Código y nombre del servicio	SD-07 – Infraestructura en la nube (OCI) y enlace de Internet
Descripción breve	Alojamiento del core y servicios; conectividad de canales y red de pagos [INV ACT-S-02, ACT-COM-02; MP 16]
Propietario del servicio / responsable técnico	Coordinador de Sistemas; contratista OCI
Canales por los que se presta	Soporte de todos los servicios
Horario de operación	24/7; soporta el core, los canales digitales y la operación de las cuatro oficinas
Usuarios / socios que lo utilizan	Toda la institución (personal y socios de forma indirecta)
Transacciones por día (promedio y pico)	No aplica; soporta el tráfico de todos los servicios
Fuentes documentales	[INV] inventario de activos; [MP] manual de procesos de TI; [MSI] manual de seguridad de la información; [IR] informe de riesgos de seguridad de la información
Fecha de la ficha y participantes	Sesión BIA del 1 de octubre de 2026. Participantes: propietario del servicio, Coordinador de Sistemas (responsable técnico) e investigador.

2. Actividades que entrega el servicio

N.º	Actividad o proceso	Área responsable
1	Alojamiento del core y servicios	Coordinador de Sistemas
2	Conectividad de canales y red de pagos	Coordinador de Sistemas

3. Dependencias

Recurso / activo (código de inventario)	Interno / tercero	Alternativa existente
ACT-S-02 Servidores en la nube	Tercero	Enlace único registrado; energía de respaldo con autonomía exigida de 8 h [MSI 7.10]
ACT-P-06 proveedor cloud	Tercero	Sin proveedor sustituto; respuesta contractual de 8 h

Recurso / activo (código de inventario)	Interno / tercero	Alternativa existente
ACT-COM-02 Internet	Interno	Sin enlace alterno; segundo enlace con otro operador en contratación
ACT-HW-13 Firewall	Interno	Sin alternativa documentada
ACT-COM-01 LAN	Interno	Sin alternativa documentada
ACT-L-01 Centro de datos	Interno	Sin sitio alterno de trabajo
ACT-AUX-03/08 energía	Interno	Generador de 12 h y UPS en la Matriz; UPS de 30 min en agencias

4. Impacto según la duración de la interrupción (escala 1 a 5 de la Tabla 3)

Dimensión de impacto	1 hora	4 horas	8 horas	24 horas	72 horas	1 semana
Operativa	2	3	4	5	5	5
Financiera	1	2	3	4	5	5
Legal / regulatoria	1	1	2	3	4	5
Reputacional	1	2	3	4	5	5
Impacto máximo del período	2	3	4	5	5	5

Referencia para la valoración: criticidad MAGERIT Nube D = 9; Internet, LAN, firewall y centro de datos D = 10. Riesgos asociados: R29 exposición de datos en la nube (Extremo); R31 incumplimiento del proveedor (Alto); MAGERIT nube: avería 15 (Crítico).

5. Parámetros de recuperación

Parámetro	Hipótesis de trabajo	Valor validado	Justificación
MTPD (horas)	8 h	8 h	Primera duración con impacto ≥ 4
RTO (horas)	4 h	4 h	Menor que el MTPD
RPO (horas)	N/A	N/A	Capacidad actual: Sin redundancia de enlace documentada
MBCO	Conectividad mínima para ventanilla y core	Conectividad mínima para ventanilla y core	Nivel mínimo durante la interrupción
Prioridad de recuperación	1	1	Dependencias técnicas; confirmado en entrevista (F5)

6. Controles existentes y recursos mínimos para recuperar

Controles o alternativas existentes hoy	Recursos mínimos necesarios para reanudar en el RTO
Firewall perimetral; monitoreo 24/7 de enlaces y equipos; pruebas semestrales de enlaces [MSI 7.8.11; MP 17]	ACT-S-02, ACT-P-06, ACT-COM-02, ACT-HW-13, ACT-COM-01, ACT-L-01, ACT-AUX-03/08

7. Observaciones y validación

Observaciones
Capacidad actual documentada: Sin redundancia de enlace documentada. Hipótesis de MTPD, RTO, RPO, MBCO y prioridad validadas en la sesión BIA con el propietario del servicio y el responsable técnico; impactos por duración valorados con la escala de la Tabla 3. Valores incorporados a la matriz B.4.

Propietario del servicio: _____ Responsable técnico: _____ Investigador: _____

Ficha SD-08 – Monitoreo de seguridad (SOC/SIEM) y carpetas compartidas

1. Identificación del servicio

Campo	**Registro**
Código y nombre del servicio	SD-08 – Monitoreo de seguridad (SOC/SIEM) y carpetas compartidas
Descripción breve	Detección y respuesta a incidentes; resguardo de archivos institucionales [INV ACT-S-07, ACT-S-06]
Propietario del servicio / responsable técnico	Oficial de SI; Coordinador de Sistemas
Canales por los que se presta	Interno
Horario de operación	24/7 (monitoreo del SOC); carpetas compartidas en horario laboral
Usuarios / socios que lo utilizan	Área de TI (3 personas) y Oficial de SI; carpetas compartidas: todo el personal
Transacciones por día (promedio y pico)	No aplica; alertas del SOC revisadas diariamente
Fuentes documentales	[INV] inventario de activos; [MP] manual de procesos de TI; [MSI] manual de seguridad de la información; [IR] informe de riesgos de seguridad de la información
Fecha de la ficha y participantes	Sesión BIA del 1 de octubre de 2026. Participantes: propietario del servicio, Coordinador de Sistemas (responsable técnico) e investigador.

2. Actividades que entrega el servicio

N.º	**Actividad o proceso**	**Área responsable**
1	Detección y respuesta a incidentes	Oficial de SI
2	Resguardo de archivos institucionales	Oficial de SI

3. Dependencias

Recurso / activo (código de inventario)	**Interno / tercero**	**Alternativa existente**
ACT-S-07 SOCaaS	Tercero	NAS y SharePoint como doble ubicación de archivos
ACT-P-08 proveedor SOC	Tercero	Revisión de alertas por el área de TI
ACT-S-06 NAS y SharePoint	Interno	Doble ubicación de archivos entre NAS y SharePoint

Recurso / activo (código de inventario)	Interno / tercero	Alternativa existente
ACT-MEDIA-02 NAS	Interno	SharePoint como segunda ubicación de archivos; sin copia de los respaldos fuera del sitio
ACT-HW-17 Servidores locales	Interno	Sin redundancia de servidores locales

4. Impacto según la duración de la interrupción (escala 1 a 5 de la Tabla 3)

Dimensión de impacto	1 hora	4 horas	8 horas	24 horas	72 horas	1 semana
Operativa	1	1	2	2	4	5
Financiera	1	1	1	2	3	4
Legal / regulatoria	1	1	1	2	4	5
Reputacional	1	1	1	2	3	4
Impacto máximo del período	1	1	2	2	4	5

Referencia para la valoración: criticidad MAGERIT SOC D = 8; carpetas D = 8. Riesgos asociados: R30 falta de detección oportuna por dependencia del SOC (Alto).

5. Parámetros de recuperación

Parámetro	Hipótesis de trabajo	Valor validado	Justificación
MTPD (horas)	72 h	72 h	Primera duración con impacto ≥ 4
RTO (horas)	24 h	24 h	Menor que el MTPD
RPO (horas)	24 h	24 h	Capacidad actual: Sin métricas de detección [IR R30]
MBCO	Alertas críticas atendidas por TI	Alertas críticas atendidas por TI	Nivel mínimo durante la interrupción
Prioridad de recuperación	6	6	Dependencias técnicas; confirmado en entrevista (F5)

6. Controles existentes y recursos mínimos para recuperar

Controles o alternativas existentes hoy	Recursos mínimos necesarios para reanudar en el RTO
Monitoreo 24/7; reportes al Oficial de SI [MSI 7.8.11]	ACT-S-07, ACT-P-08, ACT-S-06, ACT-MEDIA-02, ACT-HW-17

7. Observaciones y validación

Observaciones
Capacidad actual documentada: Sin métricas de detección [IR R30]. Hipótesis de MTPD, RTO, RPO, MBCO y prioridad validadas en la sesión BIA con el propietario del servicio y el responsable técnico; impactos por duración valorados con la escala de la Tabla 3. Valores incorporados a la matriz B.4.

Propietario del servicio: _____ Responsable técnico: _____ Investigador: _____

B.4 Matriz de consolidación del BIA

Valores validados en la sesión BIA con los propietarios de servicio; constituyen el insumo directo de la fase de estrategias de continuidad del capítulo IV.

Código	Servicio digital	MTPD (h)	RTO (h)	RPO (h)	MBCO (resumen)	Prioridad
SD-01	Core financiero (transacciones, cuentas, reportes)	8 h	4 h	1 h	Ventanilla con consultas y registro diferido de depósitos y retiros	1
SD-02	Web transaccional (banca por Internet)	24 h	8 h	1 h (hereda del core)	Consultas de saldo	3
SD-03	Aplicación móvil Yuyay Móvil	24 h	8 h	1 h (hereda del core)	Consultas de saldo	3
SD-04	Cajeros automáticos (ATM 1 y ATM 2)	24 h	8 h	N/A (transacciones en el core)	Al menos un cajero operativo o retiro en ventanilla	5
SD-05	Tarjetas de débito (red COONECTA)	8 h	4 h	Según proveedor	Bloqueo de tarjetas y retiro en ventanilla	2
SD-06	Transferencias electrónicas y recaudaciones	24 h	8 h	1 h (hereda del core)	Recepción de depósitos en ventanilla con registro diferido	4
SD-07	Infraestructura en la nube (OCI) y enlace de Internet	8 h	4 h	N/A	Conectividad mínima para ventanilla y core	1
SD-08	Monitoreo de seguridad (SOC/SIEM) y carpetas compartidas	72 h	24 h	24 h	Alertas críticas atendidas por TI	6

Escala de referencia (Tabla 3 del marco teórico)	Criterio
1 Insignificante	Degradación sin interrupción o interrupción de un servicio de hasta 1 h; pérdida inferior al 1 % del margen financiero mensual
2 Menor	Interrupción de un servicio de 1 a 4 h (de varios canales o de toda la institución, hasta 1 h); pérdida del 1 % al 5 % del margen financiero mensual; quejas aisladas
3 Moderado	Interrupción de un servicio de 4 a 8 h (de varios canales o de toda la institución, de 1 a 4 h); pérdida del 5 % al 15 %; posible observación del supervisor
4 Mayor	Interrupción de un servicio de 8 a 24 h (de varios canales o de toda la institución, de 4 a 8 h); pérdida del 15 % al 50 %; incumplimiento regulatorio sancionable; retiro de socios
5 Catastrófico	Interrupción de un servicio por más de 24 h o de toda la institución por más de 8 h, o pérdida de datos transaccionales; pérdida superior al 50 % del margen financiero mensual; riesgo para la viabilidad

Anexo C: Plan de Continuidad de Negocio para los servicios digitales de la COAC Yu-yay Ltda.

YUYAY Ltda.

PLAN

PLAN DE CONTINUIDAD DE NEGOCIO PARA LOS SERVICIOS DIGITALES

Basado en la norma ISO 22301:2019

Código:	PCN-TI-001
Versión:	1.00
Fecha de la versión:	Octubre de 2026
Clasificación de la información:	Interna
Estado:	Propuesta pendiente de aprobación

Registro de firmas

Creado por/ Modificado por	Revisado por	Aprobado por
Steve Geovanny Defas Ludizaca Autor de la propuesta (trabajo de titulación, UCACUE)	Oficial de Seguridad de la Información Oficial de Continuidad del Negocio	Consejo de Administración
	Coordinador de Sistemas	
	Comité de Seguridad de la Información y Continuidad del Negocio	
	Gerente General	
Octubre de 2026	____/____/_____	____/____/_____

Historial de modificaciones

Fecha	Versión	Creado por/ Modificado por	Descripción de la modificación
10/2026	1.00	Steve Geovanny Defas Ludizaca Autor de la propuesta	Creación del documento como producto del trabajo de titulación «Plan de Continuidad de negocio para los servicios digitales de COAC Yuyay Ltda basado en la norma ISO 22301:2019». Pendiente de revisión y aprobación.

Índice

1. Objetivo **5**
2. Alcance **5**
3. Usuarios **5**
4. Terminología **6**
5. Lineamientos del plan **6**

5.1. Política de continuidad del negocio 6

5.2. Organización para la continuidad 7

5.3. Servicios críticos y parámetros de recuperación 9

5.4. Riesgos de interrupción y tratamiento 10

5.5. Estrategias de continuidad y hoja de ruta 11

5.6. Activación y respuesta 11

5.7. Comunicación 13

5.8. Procedimientos de recuperación 14

5.9. Operación degradada 17

5.10. Retorno a la normalidad y cierre 18

5.11. Ejercicios y pruebas 18

5.12. Capacitación y concienciación 19

5.13. Evaluación del desempeño 19

5.14. Mantenimiento, revisión y mejora 20

6. Documentos de referencia **20**
7. Normativa interna **20**
8. Anexos **21**

8.1. Directorio de contactos de emergencia 21

8.2. Bitácora del incidente 21

8.3. Declaratoria de activación 22

8.4. Formulario de registro manual de operaciones (OD-01) 22

8.5. Informe posterior al incidente 22

8.6. Lista de verificación para el retorno a la normalidad 23

8.7. Informe de ejercicio 23

1. Objetivo

Establecer las directrices, responsabilidades y procedimientos que permiten a la Cooperativa de Ahorro y Crédito Yuyay Ltda. (en adelante, «la Cooperativa») responder a una interrupción de sus servicios digitales y recuperarlos dentro de los tiempos que la institución puede tolerar, protegiendo los fondos y los datos de los socios y el cumplimiento de la normativa de la Superintendencia de Economía Popular y Solidaria (SEPS).

Asimismo, el plan busca que la recuperación no dependa de la experiencia individual de las personas del área de TI, sino de criterios, roles y procedimientos documentados, probados y conocidos por quienes deben aplicarlos.

2. Alcance

Este plan se aplica a los ocho servicios digitales de la Cooperativa, a los activos tecnológicos y proveedores de los que dependen y a las cuatro oficinas Matriz, Terminal Terrestre, El Tambo y Suscal, en la medida en que la atención en ventanilla depende del core financiero y de la conectividad. Cubre la respuesta, la recuperación y el retorno a la normalidad ante la pérdida de conectividad, del core financiero o de los datos; la falla de proveedores, cajeros, energía o personal clave; y un siniestro en el centro de datos.

Código	Servicio digital	Propietario del servicio
SD-01	Core financiero (transacciones, cuentas, reportes)	Gerente General
SD-02	Web transaccional	Jefe de Negocios
SD-03	Aplicación móvil Yuyay Móvil	Jefe de Negocios
SD-04	Cajeros automáticos (ATM 1 y ATM 2)	Responsable de Tesorería y Cajas
SD-05	Tarjetas de débito (red COONECTA)	Jefe de Negocios
SD-06	Transferencias electrónicas y recaudaciones	Responsable de Tesorería
SD-07	Infraestructura en la nube (OCI) y enlace de Internet	Coordinador de Sistemas
SD-08	Monitoreo de seguridad (SOC/SIEM) y carpetas compartidas	Oficial de Seguridad de la Información

Quedan fuera del alcance los servicios que no dependen de la tecnología (asesoría y cobranza en campo), las instalaciones de los proveedores salvo sus obligaciones contractuales de continuidad, las pandemias y conflictos sociales prolongados, que requieren un plan institucional más amplio, y la investigación forense de ciberincidentes, que corresponde al proceso de gestión de incidentes de seguridad.

3. Usuarios

Los usuarios de este documento son el Consejo de Administración, la Gerencia General, el Comité de Seguridad de la Información y Continuidad del Negocio, el Oficial de Continuidad del Negocio, el área de Tecnologías de la Información, los responsables de Negocios, Tesorería, Contabilidad y Cajas, y el personal de las cuatro oficinas. Su aplicación es obligatoria para todo el personal con un rol asignado en el plan, titular o suplente, y sus disposiciones se trasladan a los proveedores críticos mediante los acuerdos de nivel de servicio.

4. Terminología

- **Análisis de impacto al negocio (BIA):** análisis de cómo crece con el tiempo el daño de interrumpir cada servicio, que determina sus prioridades y parámetros de recuperación.
- **Contingencia (nivel 2):** interrupción que activa el equipo de recuperación tecnológica y la operación degradada.
- **Crisis (nivel 3):** interrupción que amenaza el MTPD de un servicio, los datos o las instalaciones, y activa el Comité de crisis.
- **DRP:** plan de recuperación ante desastres: procedimientos técnicos para restaurar la tecnología que sostiene un servicio.
- **Incidente (nivel 1):** falla con restablecimiento estimado menor a 1 hora, atendida por la gestión ordinaria de incidentes.
- **MBCO:** objetivo mínimo de continuidad del negocio: nivel mínimo de servicio aceptable mientras dura la interrupción.
- **MTPD:** período máximo tolerable de interrupción: tiempo después del cual el impacto se vuelve inaceptable (nivel 4, Mayor).
- **Operación degradada:** atención manual con controles que mantiene el MBCO mientras se recupera el servicio.
- **Plan de continuidad del negocio (PCN):** información documentada que guía a la Cooperativa para responder a una interrupción y reanudar sus servicios.
- **RPO:** punto objetivo de recuperación: pérdida máxima de datos tolerable, expresada en horas de transacciones.
- **RTO:** tiempo objetivo de recuperación: plazo en que el servicio debe reanudarse; siempre menor que el MTPD.
- **Sitio alterno de trabajo:** oficina desde la que el personal de TI administra los servicios si la Matriz queda inutilizable.
- **SLA:** acuerdo de nivel de servicio con un proveedor, con tiempos de respuesta y restablecimiento comprometidos.
- **T0:** hora en que se detecta la interrupción; los tiempos objetivo de los procedimientos se cuentan desde ella.

5. Lineamientos del plan

5.1. Política de continuidad del negocio

La Cooperativa de Ahorro y Crédito Yuyay Ltda. se compromete a proteger la continuidad de los servicios digitales que presta a sus socios y a recuperarlos dentro de los tiempos que la institución puede tolerar. Para ello mantendrá este plan basado en el análisis de impacto y en la evaluación de riesgos; asignará los recursos y las responsabilidades necesarios; exigirá a sus proveedores críticos niveles de servicio coherentes con sus objetivos de recuperación; probará periódicamente su capacidad de respuesta; cumplirá la normativa de la SEPS y de

protección de datos personales; y mejorará el plan a partir de los ejercicios y de los incidentes reales.

5.1.1. Principios de actuación

- La seguridad de las personas prevalece sobre la recuperación de cualquier servicio.
- Los servicios se recuperan en el orden que fija la sección 5.3, no en el orden en que se reportan.
- Ninguna operación registrada manualmente se da por concluida hasta su digitación y conciliación con doble control.
- Los controles de seguridad se mantienen durante la contingencia; los accesos excepcionales se registran y se revocan al retornar a la normalidad.
- Los socios reciben información veraz y oportuna sobre la interrupción y sus alternativas.

5.1.2. Objetivos de continuidad

Cód.	Objetivo	Indicador	Meta	Plazo	Responsable
OC-1	Recuperar los servicios de prioridad 1 y 2 (SD-01, SD-05, SD-07) dentro de su RTO	Tiempo de recuperación en ejercicios e incidentes	≤ 4 h	12 meses	Coordinador de Sistemas
OC-2	Limitar la pérdida de datos del core financiero	RPO alcanzado en la prueba de restauración	≤ 1 h	3 meses	Coordinador de Sistemas
OC-3	Disponer de copias de respaldo íntegras fuera del sitio principal	Respaldos diarios replicados y verificados fuera del sitio	100 %	3 meses	Coordinador de Sistemas
OC-4	Alinear los contratos de los proveedores críticos con los parámetros de recuperación	Proveedores críticos con SLA coherente con el RTO	6 de 6	12 meses	Gerente General
OC-5	Ejecutar el programa anual de ejercicios	Ejercicios ejecutados sobre los programados	≥ 90 %	Anual	Oficial de Continuidad
OC-6	Capacitar a quienes tienen un rol en el plan	Titulares y suplentes capacitados	100 %	6 meses	Talento Humano
OC-7	Atender la observación de la SEPS de 2025	Observación cerrada con evidencia de plan aprobado y probado	Cerrada	12 meses	Gerente General

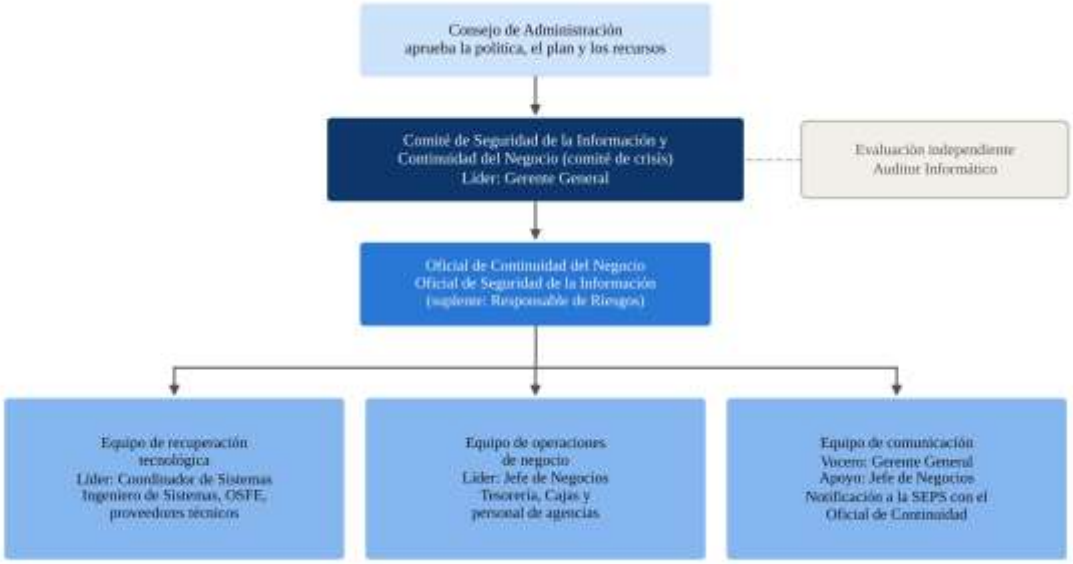
Los plazos se cuentan desde la aprobación del plan.

5.2. Organización para la continuidad

5.2.1. Estructura de respuesta

La respuesta la dirige el Comité de Seguridad de la Información y Continuidad del Negocio como comité de crisis, la coordina el Oficial de Continuidad del Negocio y la ejecutan tres equipos: recuperación tecnológica, operaciones de negocio y comunicación. El rol de Oficial de Continuidad lo asume la Oficial de Seguridad de la Información, a quien el manual de seguridad asigna la función de garantizar la continuidad del negocio. El Coordinador de Sistemas, denominado Jefe de Sistemas en el manual descriptivo de funciones que le encarga

establecer los planes de continuidad, elabora y actualiza los componentes tecnológicos del plan.



Estructura de respuesta del plan de continuidad

5.2.2. Roles, titulares y suplentes

Rol	Titular	Suplente	Responsabilidades principales
Aprobación y recursos	Presidente del Consejo de Administración	Vicepresidente del Consejo	Aprobar la política y el plan, asignar recursos y conocer el informe anual de continuidad
Líder de crisis (Comité)	Gerente General	Gerente subrogante	Declarar el nivel 3, priorizar la recuperación, autorizar gastos de emergencia y aprobar las comunicaciones externas y la notificación a la SEPS
Oficial de Continuidad del Negocio	Oficial de Seguridad de la Información	Auditor Informático	Mantener el plan, coordinar la respuesta, llevar la bitácora de decisiones, organizar los ejercicios e informar al Comité
Líder de recuperación tecnológica	Coordinador de Sistemas	Ingeniero de Sistemas	Diagnosticar, declarar el nivel 2, ejecutar los procedimientos de recuperación, coordinar a los proveedores técnicos y mantener los procedimientos técnicos y el DRP
Equipo técnico	Ingeniero de Sistemas; Oficial de Seguridad Física y Electrónica	Personal de los proveedores	Restaurar, conmutar y verificar los servicios; atender energía, climatización e instalaciones
Líder de operaciones de negocio	Jefe de Negocios	Responsable de Tesorería	Activar la operación degradada en las agencias, coordinar la digitación y la conciliación
Comunicación	Gerente General (vocero)	Jefe de Negocios	Emitir los mensajes a socios, personal y medios; preparar con el Oficial de Continuidad la notificación a la SEPS
Evaluación independiente	Auditor Informático	Auditoría interna	Evaluar los ejercicios y el cumplimiento del plan, sin ejecutar tareas de recuperación

Los suplentes se registran en el campo de respaldo (back up) del manual descriptivo de funciones de cada cargo. Sus datos de contacto constan en el Anexo 8.1 y se actualizan cada trimestre.

5.2.3. Matriz de responsabilidades (RACI)

R = ejecuta; A = rinde cuentas; C = consultado; I = informado. CA = Consejo de Administración; GG = Gerente General y Comité de crisis; OCN = Oficial de Continuidad del Negocio; CS = Coordinador de Sistemas; ET = equipo técnico; JN = Jefe de Negocios; AI = Auditor Informático.

Actividad	CA	GG	OCN	CS	ET	JN	AI
Aprobar la política y el plan	A	R	C	C		C	C
Detectar y evaluar la interrupción		I	I	A	R	R	
Declarar el nivel 2 (contingencia)		I	C	R/A	C	I	
Declarar el nivel 3 (crisis)	I	R/A	C	C		C	
Ejecutar la recuperación tecnológica		I	C	A	R	I	
Activar la operación degradada		I	C	C		R/A	
Comunicar a socios y personal		A	C	I		R	
Notificar a la SEPS	I	A	R	C			I
Coordinar a los proveedores		I	C	R/A	R		
Declarar el retorno a la normalidad		A	R	R	C	R	
Elaborar el informe posterior		I	A	R	C	C	I
Planificar y ejecutar los ejercicios	I	A	R	R	R	R	C
Revisar y actualizar el plan	A	R	R	R		C	C

5.3. Servicios críticos y parámetros de recuperación

El core financiero, la infraestructura en la nube con el enlace de Internet y las tarjetas de débito deben recuperarse en 4 horas, porque su impacto llega al nivel Mayor a las 8 horas; los demás servicios toleran 24 o 72 horas. Un servicio no se recupera antes que aquellos de los que depende: todos los canales dependen del core, y el core depende de la nube y del enlace de Internet. Como las dependencias se recuperan en serie, el objetivo técnico de la nube y el enlace es de 2 horas, para que al core le queden 2 horas netas cuando la interrupción empiece en la conectividad; las tarjetas se recuperan en paralelo con el core y los demás servicios disponen de 4 horas netas después del core. Los valores fueron validados por los propietarios de cada servicio en la sesión de análisis de impacto del 1 de octubre de 2026.

Orden	Servicio	MTPD	RTO	RPO	MBCO (nivel mínimo durante la interrupción)
1	SD-07 Infraestructura en la nube y enlace de Internet	8 h	4 h (objetivo técnico: 2 h)	No aplica	Conectividad mínima para ventanilla y core
1	SD-01 Core financiero	8 h	4 h (2 h netas si falló antes SD-07)	1 h	Ventanilla con consultas y registro diferido de depósitos y retiros
2	SD-05 Tarjetas de débito (COONECTA)	8 h	4 h	Según proveedor	Bloqueo de tarjetas y retiro en ventanilla
3	SD-02 Web transaccional	24 h	8 h	1 h (del core)	Consultas de saldo
3	SD-03 Aplicación móvil Yuyay Móvil	24 h	8 h	1 h (del core)	Consultas de saldo
4	SD-06 Transferencias electrónicas y recaudaciones	24 h	8 h	1 h (del core)	Depósitos en ventanilla con registro diferido
5	SD-04 Cajeros automáticos	24 h	8 h	No aplica	Un cajero operativo o retiro en ventanilla
6	SD-08 Monitoreo de seguridad y carpetas compartidas	72 h	24 h	24 h	Alertas críticas atendidas por TI

5.4. Riesgos de interrupción y tratamiento

El riesgo se calcula como probabilidad × impacto en escalas de 1 a 5, con cuatro zonas: bajo (1 a 4), medio (5 a 9), alto (10 a 14) y crítico (15 a 25). Una vez aplicadas las estrategias de la sección 5.5, ningún riesgo residual debe permanecer en zona alta o crítica; con ellas, todos los escenarios quedan en nivel medio o bajo.

ID	Escenario de interrupción	Riesgo residual actual	Estrategias	Riesgo objetivo
RC-01	Interrupción del enlace de Internet	16 Crítico	E-03, E-09, E-12	6 Medio
RC-02	Indisponibilidad del core o de su base de datos	12 Alto	E-02, E-04, E-09	6 Medio
RC-03	Falla por cambios o actualizaciones del proveedor	12 Alto	E-07	6 Medio
RC-04	Pérdida o corrupción de datos, incluido ransomware	10 Alto	E-01, E-02	6 Medio
RC-05	Terminación o incumplimiento del contrato del core	10 Alto	E-04	6 Medio
RC-10	Falla de la infraestructura del proveedor de nube	10 Alto	E-02, E-05	6 Medio
RC-06	Indisponibilidad de la red de tarjetas	9 Medio	E-06, E-09	6 Medio
RC-11	Ausencia del personal clave de TI	9 Medio	E-10	4 Bajo
RC-07	Falla de un cajero automático	8 Medio	E-06	6 Medio
RC-09	Denegación de servicio sobre los canales	8 Medio	E-08, E-12	6 Medio
RC-08	Corte prolongado de energía	6 Medio	E-11 (aceptar y monitorear)	6 Medio

ID	Escenario de interrupción	Riesgo residual actual	Estrategias	Riesgo objetivo
RC-12	Falla del monitoreo de seguridad	6 Medio	E-12	4 Bajo
RC-13	Siniestro en el centro de datos	5 Medio	E-01, E-11	3 Bajo

5.5. Estrategias de continuidad y hoja de ruta

Las estrategias cierran las brechas entre los parámetros de la sección 5.3 y la capacidad actual. El primer trimestre concentra las medidas de bajo costo que corrigen las brechas más graves; los costos son relativos y se cuantifican con cotizaciones antes de aprobar el presupuesto. Mientras una estrategia no esté implementada, los procedimientos de la sección 5.8 indican la alternativa vigente.

Cód.	Acción principal	Responsable	Plazo (meses)	Costo	Evidencia de cumplimiento
E-10	Designar al Oficial de Continuidad y a los suplentes, y registrarlos en los manuales de funciones; documentar procedimientos técnicos	Gerente General	0–2	Bajo	Resolución de designación
E-13	Aprobar mensajes predefinidos y procedimiento de notificación a la SEPS	Oficial de Continuidad	0–2	Bajo	Procedimiento aprobado
E-09	Documentar la operación degradada e imprimir formularios	Jefe de Negocios	0–3	Bajo	Procedimiento y formularios
E-01	Implementar la copia fuera del sitio y la prueba mensual de restauración	Coordinador de Sistemas	0–3	Bajo	Acta de la primera prueba
E-02 A	Migrar el respaldo a RMAN en modo ARCHIVELOG y copiar cada hora los archivos de registro a almacenamiento externo	Coordinador de Sistemas	1–3	Bajo	Prueba con RPO ≤ 1 h
E-03	Completar la contratación del segundo enlace y la conmutación automática	Coordinador de Sistemas	0–4	Medio	Prueba de conmutación
E-07	Acordar con el proveedor el procedimiento de cambios	Coordinador de Sistemas	1–4	Bajo	Procedimiento firmado
E-12	Configurar el monitoreo de disponibilidad y las métricas del SOC	Oficial de Seguridad de la Información	2–5	Bajo	Reporte mensual
E-04	Negociar la adenda con el proveedor del core	Gerente General	3–8	Bajo a medio	Adenda firmada
E-05	Negociar el SLA con el contratista de OCI	Gerente General	3–8	Bajo	SLA firmado
E-06	Negociar los SLA con COONECTA y con el mantenimiento de cajeros	Gerente General	3–8	Bajo	SLA firmados
E-11	Habilitar el sitio alterno de trabajo y renovar las UPS de agencias	Oficial de Seguridad Física y Electrónica	4–9	Medio	Prueba de operación desde el sitio alterno
E-02 B	Implementar la réplica en espera en una segunda región	Coordinador de Sistemas y proveedor	7–12	Medio a alto	Ejercicio de conmutación
E-08	Contratar la protección frente a denegación de servicio	Coordinador de Sistemas	8–12	Medio	Servicio activo

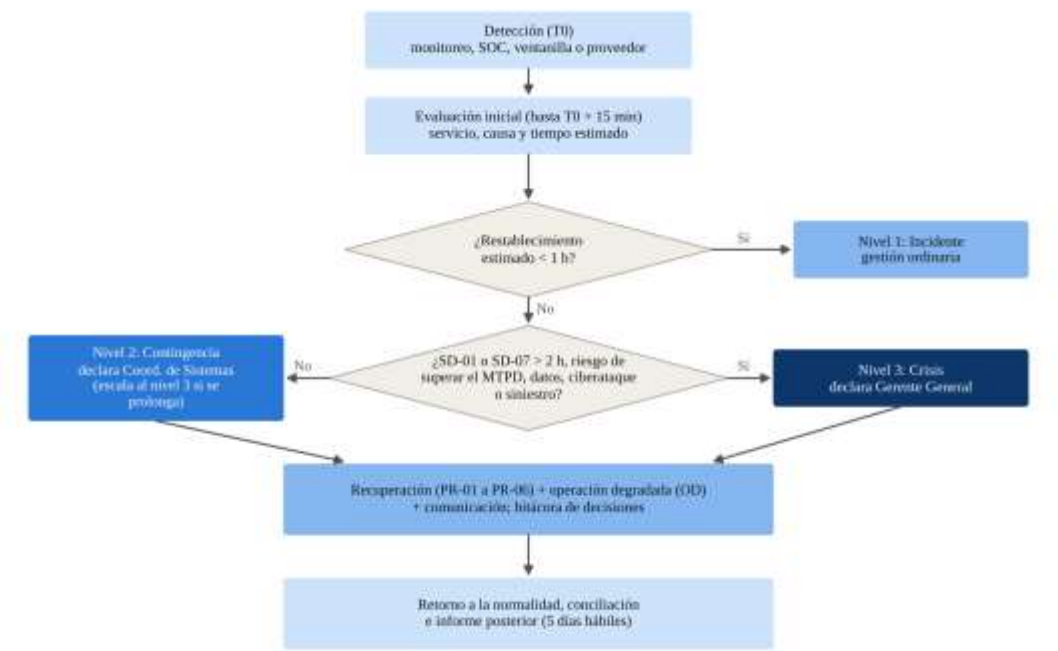
5.6. Activación y respuesta

5.6.1. Niveles de activación

La contingencia se declara cuando una interrupción consume la mitad del RTO sin solución a la vista, de modo que quede tiempo para recuperar el servicio antes de alcanzarlo.

Nivel	Criterios de activación	Declara	Respuesta
1. Incidente	Falla de un servicio con restablecimiento estimado menor a 1 h; caídas breves de los canales	Ingeniero de Sistemas	Gestión ordinaria de incidentes; registro en el gestor de incidentes
2. Contingencia	Indisponibilidad de un servicio de prioridad 1 o 2 por más de 30 min, o de prioridad 3 a 6 por más de 2 h; o restablecimiento estimado superior a la mitad del RTO	Coordinador de Sistemas	Equipo de recuperación tecnológica; operación degradada; mensaje inicial a los socios; aviso al Oficial de Continuidad y al Gerente
3. Crisis	Indisponibilidad de SD-01 o SD-07 por más de 30 min sin solución confirmada en sitio; riesgo de superar el MTPD de cualquier servicio; pérdida o corrupción de datos; ciberataque confirmado; siniestro en una oficina	Gerente General	Comité de crisis; activación de estrategias alternas; notificación inmediata a la SEPS y, si aplica, a la SPDP en un plazo máximo de cinco días

5.6.2. Procedimiento de activación y escalamiento



Flujo de activación y escalamiento

1. Detección. El monitoreo de disponibilidad, el SOC, la ventanilla o un proveedor reporta la falla al Ingeniero de Sistemas, que registra la hora de inicio (T0) en la bitácora (Anexo 8.2).

2. Evaluación inicial (hasta T0 + 15 min). El Ingeniero de Sistemas identifica el servicio afectado, la causa probable y el tiempo estimado de restablecimiento, y consulta al proveedor si corresponde.

3. Clasificación. Con los criterios de la sección 5.6.1, el Coordinador de Sistemas declara el nivel 2 o propone al Gerente General el nivel 3, y lo registra en la declaratoria (Anexo 8.3).

4. Activación. Se ejecuta el procedimiento de recuperación del escenario (sección 5.8); el Jefe de Negocios activa la operación degradada (sección 5.9) y se emite el mensaje inicial a los socios (sección 5.7).

5. Seguimiento. El Oficial de Continuidad actualiza la bitácora; en el nivel 3, el Comité se reúne cada 2 horas hasta el restablecimiento.

6. Escalamiento. Un nivel 2 que se prolonga y cumple un criterio de nivel 3 se escala al Gerente General sin esperar la siguiente reunión.

7. Cierre. Se declara el retorno a la normalidad (sección 5.10) y se elabora el informe posterior (Anexo 8.5).

Fuera del horario laboral, el Ingeniero de Sistemas de turno o el SOC llaman al Coordinador de Sistemas; si no responde en 15 minutos, al Oficial de Continuidad y luego al Gerente General.

5.7. Comunicación

5.7.1. Matriz de comunicación

Los socios reciben el primer mensaje hasta 30 minutos después de declarado el nivel 2, y la SEPS es notificada de inmediato al declarar el nivel 3, conforme a la norma de control de seguridad de la información (Resolución SEPS 2022-002), y, cuando la interrupción implique una vulneración de datos personales, la SPDP es notificada por el SISPDP en un plazo máximo de cinco días y los titulares en tres días si existe riesgo para sus derechos (LOPDP, arts. 43 y 44). Ningún empleado emite declaraciones a terceros fuera de este plan.

Audiencia	Contenido	Momento	Canal	Responsable
Personal de la cooperativa	Nivel declarado, servicio afectado e instrucciones de operación degradada	Al declarar el nivel 2 o 3 y en cada cambio	Grupo de WhatsApp institucional, llamada y correo	Oficial de Continuidad
Socios	Servicio afectado, alternativas disponibles y hora estimada de restablecimiento	Hasta 30 min después de declarar el nivel 2; actualización cada 2 h	WhatsApp institucional, Facebook, carteles en agencias y aviso en la aplicación y la web	Jefe de Negocios, con aprobación del Gerente
Proveedores críticos	Reporte técnico y solicitud de escalamiento	Inmediato	Ticket y teléfono del contacto de emergencia	Coordinador de Sistemas
Consejo de Administración	Situación, impacto y decisiones tomadas	Al declarar el nivel 3 y al cierre	Llamada e informe escrito	Gerente General

Audiencia	Contenido	Momento	Canal	Responsable
SEPS	Evento, servicios afectados, impacto y acciones	De inmediato al declarar el nivel 3, con un reporte inicial el mismo día por el canal oficial, conforme a la norma de seguridad de la información (SEPS, 2022); informe de cierre al retornar a la normalidad	Oficio o canal oficial del organismo	Gerente General y Oficial de Continuidad
Autoridad de protección de datos y titulares	Vulneración de datos personales, alcance y medidas adoptadas	A la SPDP, por el SISPDP, en un plazo máximo de cinco días desde que se conozca la vulneración (LOPDP, art. 43; SPDP, 2026); a los titulares, en el término de tres días cuando exista riesgo para sus derechos (LOPDP, art. 44)	Canal oficial de la autoridad; comunicación directa a los titulares	Oficial de Seguridad de la Información
Medios y redes sociales	Posición oficial de la cooperativa	Cuando la interrupción tenga repercusión pública	Comunicado oficial	Gerente General

5.7.2. Mensajes predefinidos

Momento	Mensaje modelo
Inicio (socios)	Estimado socio: en este momento el servicio de [servicio] presenta una interrupción. Sus fondos están seguros. Puede realizar depósitos y retiros en nuestras oficinas de Cañar, Terminal Terrestre, El Tambo y Suscal. Le informaremos cuando el servicio se restablezca. COAC Yuyay Ltda.
Actualización (socios)	Seguimos trabajando para restablecer [servicio]. Hora estimada: [hora]. Nuestras oficinas atienden con normalidad. Gracias por su comprensión.
Restablecimiento (socios)	El servicio de [servicio] se encuentra restablecido desde las [hora]. Si realizó una operación durante la interrupción y observa alguna diferencia en su cuenta, acérquese a cualquiera de nuestras oficinas.
Activación (personal)	Se declara nivel [2/3] por [evento]. Aplicar el procedimiento [OD-xx]: registrar las operaciones en los formularios prenumerados, respetar los montos máximos autorizados y entregar los formularios al cierre a Tesorería. No emitir declaraciones a terceros.
Notificación (SEPS)	La COAC Yuyay Ltda. informa que el [fecha] a las [hora] se produjo [evento], que afectó [servicios] durante [duración]. Se activó el Plan de Continuidad del Negocio en nivel 3. Impacto estimado: [socios y operaciones afectados]. Acciones: [resumen]. Se remitirá el informe posterior en [plazo].

5.8. Procedimientos de recuperación

Cada procedimiento cuenta sus tiempos desde la detección (T0) y termina dentro del RTO del servicio. Los comandos técnicos de cada proveedor, como la restauración de la base de datos, se mantienen como anexos operativos bajo custodia del Coordinador de Sistemas.

5.8.1. PR-01: interrupción del enlace de Internet (SD-07; RTO 4 h; objetivo técnico 2 h)

Paso	Acción	Responsable	Tiempo objetivo
1	Confirmar la pérdida del enlace y descartar una falla del firewall o de la red interna	Ingeniero de Sistemas	T0 + 15 min
2	Verificar la conmutación automática al enlace secundario (E-03) y el acceso a OCI, a la red de pagos y a los canales	Ingeniero de Sistemas	T0 + 30 min
3	Si no hay enlace secundario disponible: activar el enlace 4G de contingencia para la ventanilla y declarar el nivel 2	Coordinador de Sistemas	T0 + 30 min
4	Activar la operación degradada OD-01 y emitir el mensaje inicial a los socios	Jefe de Negocios	T0 + 45 min
5	Abrir el reclamo con el operador y escalar a su nivel gerencial si el tiempo estimado supera 2 h; en ese caso, proponer el nivel 3	Coordinador de Sistemas	T0 + 2 h
6	Al restablecerse el enlace (objetivo: 2 h con el enlace secundario; 4 h como máximo): verificar los servicios en el orden de la sección 5.3 y retirar la operación degradada	Ingeniero de Sistemas	≤ T0 + 4 h
7	Digitar y conciliar las operaciones manuales con doble control	Tesorería y Cajas	Mismo día

5.8.2. PR-02: indisponibilidad del core financiero o de su base de datos (SD-01; RTO 4 h; RPO 1 h)

Paso	Acción	Responsable	Tiempo objetivo
1	Confirmar la falla y abrir el ticket de prioridad crítica con el proveedor del core, con llamada al contacto de emergencia	Ingeniero de Sistemas	T0 + 15 min
2	Determinar con el proveedor si la falla es recuperable en sitio (reinicio, reversión de un cambio) y el tiempo estimado	Coordinador de Sistemas	T0 + 30 min
3	Declarar el nivel 2, activar la operación degradada OD-01 y comunicar a los socios	Coordinador de Sistemas; Jefe de Negocios	T0 + 45 min
4	Si la falla no es recuperable en sitio en menos de 30 min: declarar el nivel 3 y ordenar la ejecución del DRP del proveedor (conmutación a la réplica, E-02 B, o restauración RMAN del último respaldo físico íntegro con aplicación de los archivos de registro, E-02 A)	Gerente General	T0 + 30 min

Paso	Acción	Responsable	Tiempo objetivo
5	Validar la integridad de los datos restaurados: totales de control, saldos de cuentas de muestra y número de la última transacción	Coordinador de Sistemas; Contabilidad	T0 + 4 h con restauración RMAN (3,5 h); T0 + 1 h 30 min con la réplica E-02 B
6	Habilitar la ventanilla y luego los canales en el orden de la sección 5.3	Ingeniero de Sistemas	≤ T0 + 4 h 30 min hasta que opere la réplica; ≤ T0 + 2 h con la réplica
7	Conciliar con COONECTA y verificar las transferencias SPI pendientes antes de reenviarlas	Tesorería	Mismo día

5.8.3. PR-03: pérdida o corrupción de datos, incluido ransomware (SD-01 a SD-06)

Paso	Acción	Responsable	Tiempo objetivo
1	Aislar los equipos y segmentos afectados y preservar la evidencia, con apoyo del SOC	Oficial de Seguridad de la Información	T0 + 30 min
2	Declarar el nivel 3 y convocar al Comité de crisis; no negociar ni pagar rescates	Gerente General	T0 + 1 h
3	Identificar el último respaldo íntegro, verificando su integridad antes de usarlo, a partir de la copia fuera del sitio (E-01)	Coordinador de Sistemas	T0 + 2 h
4	Restaurar con RMAN en un entorno limpio y aplicar los archivos de registro hasta el punto más reciente sin compromiso	Proveedor del core; Coordinador de Sistemas	T0 + 4 h
5	Cambiar las credenciales privilegiadas y revisar los accesos antes de reconectar los servicios	Oficial de Seguridad de la Información	Antes de reconectar
6	Notificar a la SEPS y, si hubo datos personales comprometidos, a la autoridad de protección de datos y a los titulares	Gerente General; Oficial de Seguridad de la Información	Según la sección 5.7

5.8.4. PR-04: indisponibilidad de la red de tarjetas (SD-05; RTO 4 h)

Paso	Acción	Responsable	Tiempo objetivo
1	Confirmar la indisponibilidad con el centro de operaciones de COONECTA y obtener el tiempo estimado	Oficial de Seguridad de la Información	T0 + 30 min
2	Declarar el nivel 2 y emitir el mensaje a los socios con la alternativa de retiro en ventanilla	Coordinador de Sistemas; Jefe de Negocios	T0 + 45 min
3	Habilitar el retiro en ventanilla con cédula (OD-02) y mantener el bloqueo de tarjetas por vía telefónica	Jefe de Negocios	T0 + 1 h

Paso	Acción	Responsable	Tiempo objetivo
4	Si la interrupción supera 2 h en día de pago o fin de mes: extender el horario de atención de las agencias	Gerente General	T0 + 2 h
5	Al restablecerse: conciliar las transacciones con COONECTA y registrar los débitos no reconocidos	Tesorería	Siguiente día hábil

5.8.5. PR-05: falla de un cajero automático (SD-04; RTO 8 h)

Paso	Acción	Responsable	Tiempo objetivo
1	Retirar el cajero de servicio, colocar el aviso con la ubicación del otro cajero y de la ventanilla	Tesorería y Cajas	T0 + 30 min
2	Reportar la falla al proveedor de mantenimiento con la prioridad del SLA (E-06)	Coordinador de Sistemas	T0 + 30 min
3	Verificar el efectivo y cuadrar el cajero; registrar los débitos sin entrega de efectivo	Tesorería y Cajas	T0 + 2 h
4	Si ambos cajeros están fuera de servicio: declarar el nivel 2 y aplicar OD-03	Coordinador de Sistemas	T0 + 2 h
5	Verificar el funcionamiento tras la reparación y reponer el servicio	Tesorería y Cajas	≤ T0 + 8 h

5.8.6. PR-06: siniestro en el centro de datos o corte prolongado de energía

Paso	Acción	Responsable	Tiempo objetivo
1	Evacuar y proteger a las personas; activar a los organismos de emergencia si corresponde	Oficial de Seguridad Física y Electrónica	Inmediato
2	En corte de energía: verificar el arranque del generador y la autonomía disponible; solicitar combustible si el corte supera 6 h	Oficial de Seguridad Física y Electrónica	T0 + 15 min
3	En agencias sin generador: cerrar las sesiones del core de forma ordenada antes de agotar las UPS y aplicar OD-01	Jefe de Negocios	T0 + 20 min
4	Si el centro de datos queda inutilizable: declarar el nivel 3 y trasladar la administración al sitio alterno de trabajo (E-11)	Gerente General; Coordinador de Sistemas	T0 + 2 h
5	Restablecer la conectividad de las agencias con OCI desde el sitio alterno y recuperar los respaldos de la copia fuera del sitio (E-01)	Coordinador de Sistemas	T0 + 4 h
6	Evaluar los daños, gestionar el seguro y planificar la reconstrucción	Gerente General	Siguiente día hábil

5.9. Operación degradada

La operación degradada mantiene el nivel mínimo de cada servicio mientras dura la recuperación, con registro prenumerado, límites, doble control y conciliación. El monto máximo de

retiro lo fija la Gerencia General al aprobar el plan, y el reporte de saldos del cierre anterior se genera y resguarda cada día, con acceso restringido al personal de cajas.

Cód.	Servicio afectado	Nivel mínimo (MBCO)	Procedimiento manual	Controles
OD-01	Core financiero o conectividad (SD-01, SD-07)	Consultas, depósitos y retiros de montos pequeños en ventanilla	Consulta con el reporte de saldos del cierre anterior; depósitos y retiros en formularios prenumerados; digitación al restablecerse	Monto máximo de retiro fijado por la Gerencia; verificación de identidad y firma; doble control en la digitación; cuadre de caja
OD-02	Tarjetas de débito (SD-05)	Bloqueo de tarjetas y retiro en ventanilla	Bloqueo por vía telefónica; retiro con cédula en ventanilla; registro de reclamos	Registro de cada bloqueo; conciliación con COONECTA
OD-03	Cajeros automáticos (SD-04)	Un cajero operativo o retiro en ventanilla	Aviso en el cajero; redirección al otro cajero o a la ventanilla	Registro de débitos sin entrega; cuadre del cajero
OD-04	Web y aplicación móvil (SD-02, SD-03)	Consultas de saldo por la ventanilla	Mensaje a los socios; atención en ventanilla; extensión de horario si la interrupción coincide con días pico	Registro de los reclamos recibidos
OD-05	Transferencias y recaudaciones (SD-06)	Recepción de depósitos con registro diferido	Comprobante manual prenumerado; transferencias SPI diferidas al siguiente ciclo	Verificar que la transferencia no se haya ejecutado antes de reenviarla
OD-06	Monitoreo y carpetas (SD-08)	Atención de alertas críticas por el área de TI	Revisión diaria de alertas del firewall y del antivirus; uso de la ubicación alterna de archivos (NAS o SharePoint)	Registro de alertas revisadas

5.10. Retorno a la normalidad y cierre

El retorno a la normalidad lo declara quien declaró el nivel, cuando se cumplen las siguientes condiciones (Anexo 8.6):

- Los servicios afectados operan con normalidad durante al menos 30 minutos y se verificó la integridad de los datos.
- Las operaciones registradas manualmente fueron digitadas y conciliadas con doble control, y las diferencias están resueltas o documentadas.
- Los accesos excepcionales y las configuraciones temporales fueron revocados.
- Se emitió el mensaje de restablecimiento a los socios y al personal.

Dentro de los cinco días hábiles siguientes, el Oficial de Continuidad elabora el informe posterior (Anexo 8.5) con la cronología de la bitácora, los tiempos alcanzados frente al RTO y al RPO, las causas, las lecciones aprendidas y las acciones correctivas, y lo presenta al Comité en su siguiente sesión.

5.11. Ejercicios y pruebas

El programa del primer año combina pruebas técnicas mensuales de bajo costo con ejercicios de mesa y simulacros de toda la estructura de respuesta; los meses se cuentan desde la aprobación del plan. Los ejercicios se programan fuera de horas pico y de días de pago, y las pruebas técnicas se ejecutan en el ambiente de pruebas o con plan de reversión. El Auditor Informático observa los ejercicios EJ-06 a EJ-10 y registra los resultados en el informe de ejercicio (Anexo 8.7).

Cód.	Ejercicio	Tipo	Procedimiento	Participantes	Frecuencia o mes
EJ-01	Restauración del respaldo del core en el ambiente de pruebas, midiendo el tiempo y el RPO	Prueba técnica	PR-02, PR-03	Coordinador de Sistemas; proveedor	Mensual
EJ-02	Verificación de la integridad de la copia fuera del sitio	Prueba técnica	PR-03	Coordinador de Sistemas	Mensual
EJ-03	Prueba del árbol de llamadas y de los contactos de proveedores	Prueba de comunicación	Todos	Oficial de Continuidad	Trimestral
EJ-04	Revisión de escritorio del plan con titulares y suplentes	Revisión	Todos	Comité y equipos	Meses 2 y 8
EJ-05	Conmutación al enlace secundario en horario de baja demanda	Prueba técnica	PR-01	Equipo técnico; operador	Meses 4 y 10
EJ-06	Simulación de mesa: caída del core en día de pago	Ejercicio de mesa	PR-02	Comité y tres equipos	Mes 5
EJ-07	Simulacro de operación degradada en una agencia	Simulacro	OD-01	Negocios, Cajas, Tesorería	Mes 6
EJ-08	Ejecución del DRP del proveedor del core con presencia de la cooperativa	Prueba técnica	PR-02	Proveedor; Coordinador de Sistemas; Auditor	Mes 7
EJ-09	Simulación de mesa: ransomware en la base de datos	Ejercicio de mesa	PR-03	Comité; SOC; equipo técnico	Mes 9
EJ-10	Simulacro integral: pérdida del enlace con operación degradada y comunicación	Simulacro	PR-01, OD-01, comunicación	Toda la estructura de respuesta	Mes 11

5.12. Capacitación y concienciación

Audiencia	Contenido	Duración	Frecuencia	Responsable
Titulares y suplentes de los roles	El plan, los niveles de activación, sus procedimientos y la bitácora	4 h	Inicial y actualización anual	Oficial de Continuidad
Personal de agencias	Operación degradada, formularios y mensajes a los socios	2 h	Anual, antes del simulacro EJ-07	Jefe de Negocios
Área de TI	Procedimientos de recuperación y capacitación cruzada	4 h	Semestral	Coordinador de Sistemas

Audiencia	Contenido	Duración	Frecuencia	Responsable
Todo el personal	Concienciación en continuidad, integrada a la capacitación anual de seguridad de la información	1 h	Anual	Talento Humano y Oficial de Seguridad de la Información

5.13. Evaluación del desempeño

El Oficial de Continuidad reporta los siguientes indicadores al Comité cada trimestre; la auditoría interna incluye el plan en su programa anual y verifica los ejercicios y el cierre de las acciones correctivas.

Indicador	Fórmula o medición	Meta	Frecuencia	Fuente
Tiempo de activación	Minutos entre T0 y la declaratoria del nivel	≤ 30 min	Por evento	Bitácora
Cumplimiento del RTO	Servicios recuperados dentro de su RTO / servicios interrumpidos	100 %	Por evento y ejercicio	Bitácora e informes
RPO alcanzado	Horas de transacciones perdidas en la restauración	≤ 1 h	Mensual	EJ-01
Pruebas de restauración exitosas	Pruebas exitosas / pruebas programadas	100 %	Mensual	EJ-01 y EJ-02
Disponibilidad de los canales digitales	Tiempo disponible / tiempo total, sin contar el mantenimiento programado	Meta regulatoria: ≥ 99,99 % anual para los servicios críticos (SD-01, SD-05, SD-07), conforme a la Resolución SEPS 0116. Meta transitoria del primer año: ≥ 99,5 % mensual para todos los canales, hasta que operen el enlace secundario (E-03) y la réplica (E-02 B)	Mensual	Monitoreo de disponibilidad
Ejercicios ejecutados	Ejercicios ejecutados / ejercicios programados	≥ 90 %	Trimestral	Programa de ejercicios
Acciones correctivas cerradas a tiempo	Acciones cerradas en plazo / acciones abiertas	≥ 90 %	Trimestral	Registro de acciones
Personal capacitado	Titulares y suplentes capacitados / total de roles	100 %	Semestral	Talento Humano

La meta regulatoria del 99,99 % anual equivale a unos 53 minutos de indisponibilidad al año y no se cumple con la arquitectura actual: las caídas breves registradas suman entre 2 y 12 horas al año y la interrupción de 6 horas de marzo de 2025 la superó por sí sola. Por eso el primer año se mide contra la meta transitoria del 99,5 % mensual, se reporta la brecha al Comité y a la SEPS, y la meta regulatoria se exige desde el segundo año, cuando operen el enlace secundario (E-03), la réplica en espera (E-02 B) y la protección frente a denegación de servicio (E-08).

5.14. Mantenimiento, revisión y mejora

El Comité revisa el plan al menos una vez al año, en la sesión que precede a la aprobación del presupuesto, y además cuando ocurre alguno de estos eventos:

- Una activación real del nivel 2 o 3, o un ejercicio con resultados por debajo de las metas.
- La incorporación o el retiro de un servicio digital, o un cambio de proveedor crítico o de sus contratos.
- Un cambio de infraestructura, como la entrada en operación del segundo enlace o de la réplica, o del personal con roles en el plan.
- Una nueva disposición de la SEPS o de la normativa de protección de datos, o una observación de auditoría.

Antes de la primera aprobación, el Comité ratifica en acta los parámetros del análisis de impacto (MTPD, RTO, RPO y MBCO) con los propietarios de los servicios. Cada versión aprobada se registra en el historial de modificaciones, se distribuye a los titulares y suplentes y reemplaza las copias anteriores, incluidas las impresas de las oficinas y la copia que se mantiene fuera de la red institucional. El directorio de contactos se actualiza cada trimestre sin necesidad de una nueva versión del plan.

6. Documentos de referencia

- ISO 22301:2019. Seguridad y resiliencia Sistemas de gestión de la continuidad del negocio Requisitos.
- ISO 22313:2020. Seguridad y resiliencia Sistemas de gestión de la continuidad del negocio Orientación sobre el uso de ISO 22301.
- ISO/TS 22317:2021. Seguridad y resiliencia Directrices para el análisis de impacto al negocio.
- ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad Sistemas de gestión de la seguridad de la información Requisitos.
- MAGERIT v3. Metodología de análisis y gestión de riesgos de los sistemas de información (Ministerio de Hacienda y Administraciones Públicas de España, 2012).
- NIST SP 800-34 Rev. 1. Guía de planificación de contingencias para sistemas de información.

- Resolución SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116 (2024). Norma de control para la administración del riesgo operativo en las entidades del sector financiero popular y solidario, que sustituye a la Resolución SEPS-IGT-IR-IGJ-2018-0279.
- Resolución SEPS-IGS-IGT-IGJ-INGINT-INTIC-INSESF-INR-DNSI-2022-002. Norma de control respecto a la seguridad de la información en las entidades del sector financiero popular y solidario.
- Ley Orgánica de Protección de Datos Personales (Registro Oficial, Quinto Suplemento 459, 26 de mayo de 2021).
- Reglamento General a la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo 904, Registro Oficial Tercer Suplemento 435, 13 de noviembre de 2023) y Norma técnica de notificación de vulneraciones de la seguridad de los datos personales (Resolución SPDP-SPD-2026-0040-R).

7. Normativa interna

- Manual de seguridad de la información (2024).
- Manual de procesos de TI (2026): proceso de ejecución de planes operativos de contingencia, gestión de incidentes y problemas, gestión de cambios y procedimiento de respaldos.
- Informe de riesgos de seguridad de la información (2026).
- Inventario de activos MAGERIT y matrices de riesgo de TI.
- Manuales descriptivos de funciones del personal de TI.

8. Anexos

Los formatos se imprimen y se guardan junto a cada copia del plan, porque se usan cuando los sistemas no están disponibles.

8.1. Directorio de contactos de emergencia

Rol o proveedor	Titular	Teléfono	Correo	Suplente	Teléfono del suplente
Gerente General (líder de crisis)					
Oficial de Continuidad del Negocio					
Coordinador de Sistemas					
Ingeniero de Sistemas					
Oficial de Seguridad Física y Electrónica					
Jefe de Negocios					
Responsable de Tesorería					
Presidente del Consejo de Administración					

Rol o proveedor	Titular	Teléfono	Correo	Suplente	Teléfono del suplente
Proveedor del core (soporte de emergencia)					
Contratista de OCI					
Operador de telecomunicaciones					
COONECTA (centro de operaciones)					
Proveedor del SOC					
Mantenimiento de cajeros					
Proveedor de combustible del generador					

8.2. Bitácora del incidente

Servicio afectado: _____ Nivel declarado: _____ T0 (fecha y hora de detección): _____

Hora	Evento, decisión o acción	Responsable	Observaciones

8.3. Declaratoria de activación

Campo	Registro
Fecha y hora de la declaratoria	
Nivel declarado (2 Contingencia / 3 Crisis)	
Servicios afectados	
Criterio de activación cumplido (sección 5.6.1)	
Procedimientos activados (PR y OD)	
Equipos convocados	
Declarado por (nombre y firma)	

8.4. Formulario de registro manual de operaciones (OD-01)

N.º de formulario (prenumerado): _____ Oficina: _____ Cajero: _____
Fecha: _____

Hora	N.º de cuenta	Nombre del socio	Cédula	Depósito o retiro	Monto	Firma del socio	Digitado por y fecha	Verificado por

8.5. Informe posterior al incidente

- Resumen del evento: servicios afectados, T0 y hora de restablecimiento.
- Cronología tomada de la bitácora.
- Tiempos alcanzados frente al RTO y al RPO de cada servicio.
- Causa raíz.
- Impacto: socios y operaciones afectados, reclamos, costos y diferencias de conciliación.
- Comunicaciones emitidas, incluida la notificación a la SEPS.
- Lecciones aprendidas.
- Acciones correctivas con responsable y plazo.
- Cambios propuestos al plan.

8.6. Lista de verificación para el retorno a la normalidad

Verificación	Cumple (sí/no)	Responsable
Servicios operando con normalidad durante al menos 30 minutos		
Integridad de los datos verificada		
Operaciones manuales digitadas y conciliadas con doble control		
Transacciones con COONECTA y transferencias SPI conciliadas		
Accesos excepcionales y configuraciones temporales revocados		
Mensaje de restablecimiento emitido a socios y personal		
Bitácora cerrada y entregada al Oficial de Continuidad		

8.7. Informe de ejercicio

Campo	Registro
Código y nombre del ejercicio	
Fecha, duración y participantes	

Campo	Registro
Escenario y procedimientos probados	
Tiempos objetivo y tiempos alcanzados	
Resultado (cumple, cumple parcial-mente, no cumple)	
Problemas encontrados	
Acciones de mejora, responsable y plazo	
Observaciones del Auditor Informático	

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Steve Geovanny Defas Ludizaca, portador de la cédula de ciudadanía N.º 0302488846. En calidad de autor y titular de los derechos patrimoniales del trabajo de investigación "**Plan de Continuidad de negocio para los servicios digitales de COAC Yuyay Ltda basado en la norma ISO 22301:2019"**de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de investigación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, 29 de octubre de 2026

F: .....

Steve Geovanny Defas Ludizaca
C.I. 0302488846