POSGRADOS UPS

MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN

Módulo 3: AUDITORÍA DE SISTEMAS DE INFORMACIÓN

INFORME DE AUDITORÍA INTERNA

MSI-AI-2025-001

“Evaluación del plan de Continuidad de negocio y respaldos”

Carrión Sarmiento Carola Liseth

Moposita Suin Leonardo Javier

Moreno Vargas Gabriel Andrés

Nieves Guamán Edisson Ricardo

Sangacha Gaibor Bryan Joel

Sinchi Chaca Edgar Romero

Contenido

1. Fecha de Remisión

5 de septiembre de 2025

2. Departamento

Departamento de seguridad de la información y departamento de TI.

3. Justificación

La presente auditoría interna fue realizada con la finalidad de dar cumplimiento con el plan de auditoría interna de la Cooperativa XYZ específicamente al proceso de Continuidad del Negocio y respaldos. Dicha auditoría es necesaria para garantizar que la organización cuente con mecanismo efectivos para proteger la información crítica y asegurar la disponibilidad de los servicios en caso de incidentes, desastres o fallas técnicas.

4. Objetivo de la auditoría

Verificar que los procesos, procedimientos y controles relacionados con la continuidad del negocio y la gestión de respaldos implementados por el área de TI de la Cooperativa XYZ, cumplen con la política de la organización V2024 y con los requisitos de las normas ISO 22301, ISO 27001, asegurando su eficacia, pertinencia y capacidad para garantizar la disponibilidad, integridad y recuperación de la información crítica ante incidentes o desastres.

5. Alcance de la auditoría

La auditoría comprenderá la evaluación integral de los procesos específicamente la política de Seguridad y continuidad de negocio V2024, procedimientos y controles relacionados con la continuidad del negocio y la gestión de respaldos implementados por el área de TI en el año 2024, con el objetivo de verificar su eficacia, cumplimiento normativo y alineación con las políticas institucionales alineado con la norma ISO 22301, ISO 27001.

6. Descripción de las actividades de auditoría

Para el desarrollo de la presente auditoría se procedió con la realización de las siguientes actividades:

6.1 Revisión documental

- Análisis de política de Seguridad y continuidad de negocio V2024, procedimientos y registros relacionados con la continuidad del negocio y la gestión de respaldos (planes de respaldo, pruebas de restauración, logs de ejecución, manuales de contingencia, etc.).
- Verificación del cumplimiento de la Norma ISO 27001, ISO 22301 y SEPS 2022-002.

6.2 Entrevistas y levantamiento de información

- Reuniones con el personal responsable del área de TI y Riesgos para identificar prácticas, responsabilidades y acciones ejecutadas en 2024.
- Identificación de brechas en la gestión de continuidad y respaldo de información.

6.3 Evidencia y verificación in situ:

- Revisión de configuraciones, respaldos almacenados y mecanismos de recuperación.
- Verificación de la ejecución de pruebas de restauración y tiempos de recuperación (RTO/RPO), capacitación del personal.
- Contraste de la evidencia con las políticas internas de seguridad y continuidad.
-

6.4 Evaluación de resultados

- Análisis de hallazgos, desviaciones y buenas prácticas encontradas.
- Identificación de riesgos relacionados con la disponibilidad y recuperación de información crítica.

6.5 Informe de auditoría

- Elaboración del informe con los hallazgos, conclusiones y recomendaciones.

7. Descripción de resultados

La presente auditoría se enmarca en la revisión de los procesos y controles relacionados con la continuidad del negocio y la gestión de respaldos, de acuerdo con lo establecido en la Norma ISO 22301, ISO 27001 y política de seguridad y continuidad y respaldos V2024.

Con base a lo descrito y de acuerdo con los procedimientos de auditoría efectuados, a continuación, se presentan los resultados obtenidos respecto de la aplicación de los controles de seguridad y las observaciones de control interno.

Política interna	Control/Cláusula ISO 22301 Y 27001	Actividad	Objetivo	Obligatorio	Cumple	Comentario
1. Revisión de la Política de Continuidad del Negocio y Respaldos (ISO 22301, Políticas internas de continuidad de negocio y respaldo V2024)						
1.1	ISO 22301 Cláusula 5.2	La política de Continuidad del Negocio y Respaldos está documentada y disponible.	Confirmar que existe un documento formal aprobado.	Sí	Si	Existe la Política de "Políticas internas de continuidad de negocio y respaldo V2024"
1.2	ISO 22301 Cláusula 5.1	La política está aprobada por la Alta Dirección.	Verificar la firma, resolución o acta de aprobación.	Sí	Si	Se verifica que en la política V2024 si está la firma de la alta dirección.
1.3	ISO 22301 Cláusula 7.5	La política se encuentra actualizada (versión vigente 2024 o posterior).	Validar que el documento tiene versión, fecha y control de cambios.	Sí	Si	Se encuentra versionado: V2024
1.4	ISO 22301 Cláusula 4.2.2 y SEPS	La política está alineada a ISO 22301 y SEPS 2022-002.	Comprobar que el contenido cubre requisitos normativos aplicables.	Sí	Si	Fue creada en base a los criterios de la ISO 22301, ISO 27001 Y SEPS 2022
1.5	ISO 22301 Cláusula 5.3	La política incluye responsables y roles definidos.	Confirmar asignación de responsables de continuidad y respaldos.	Sí	Si	Se verifica los responsables dentro de la política
1.7	ISO 22301 Cláusula 7.4 (Comunicación)	La política contempla la comunicación y difusión al personal.	Verificar si se ha socializado en la organización.	Sí	Si	La política si contempla capacitación al personal; sin embargo, es necesario la evidencia formal.
2 Evaluación de Procedimientos de Respaldo (frecuencia, medios, almacenamiento externo)						
2.1	ISO 27001: Anexo A.8.13 ISO 22301: 8.4.4	Existe un procedimiento documentado de respaldos.	Confirmar que se encuentra aprobado, vigente y disponible para el área de TI.	Sí	Si	Se verificó que el procedimiento de respaldos se encuentra formalmente documentado, aprobado por la Dirección de TI y disponible en el repositorio institucional. La versión vigente corresponde a la V2024.

2.2	ISO 27001: A.8.13 ISO 22301: 8.4.5	Los respaldos se ejecutan con la frecuencia definida en la política.	Verificar registros o evidencias de ejecución periódica.	Sí	No	Durante la auditoría se identificó que, aunque las "*Políticas internas de continuidad de negocio y respaldo V2024*" establecen la obligación de ejecutar respaldos de información de manera mensual, los registros evidencian que durante el año 2024 los respaldos se realizaron de forma trimestral.
2.3	ISO 27001: A.8.13 ISO 22301: 8.3.3 y 8.4.4	El procedimiento contempla diferentes tipos de respaldo (completo, incremental, diferencial).	Asegurar que la estrategia cubra la continuidad de datos críticos.	Sí	Si	Se constató que el procedimiento institucional contempla la ejecución de respaldos completos, incrementales y diferenciales, de acuerdo con la criticidad de la información y la capacidad de almacenamiento.
2.4	ISO/IEC 27001: A.7.10	Se definen los medios de respaldo utilizados (discos externos, cintas, nube, almacenamiento SAN/NAS).	Confirmar que cumplen requisitos de seguridad y capacidad.	Sí	Si	Se validó que la organización dispone de medios de respaldo diversificados (discos externos cifrados, almacenamiento en cabina SAN/NAS y copia en nube). Los registros de inventario de almacenamiento evidencian que dichos medios cumplen con los requisitos de seguridad, capacidad y redundancia definidos en la política interna.
2.5	ISO/IEC 27001: A.7.10	Los respaldos cuentan con almacenamiento externo (offsite / nube).	Verificar la existencia de copias fuera del sitio principal.	Sí	Si	Se verificó la existencia de respaldos almacenados en una ubicación externa a las instalaciones principales, mediante servicios en la nube con cifrado y control de acceso.
2.6	ISO 27001: A.5.15 y A 8.24	Se aplican controles de seguridad en los respaldos (cifrado, acceso restringido, integridad de datos).	Asegurar que los respaldos están protegidos ante accesos no autorizados.	Sí	Si	Los respaldos revisados cuentan con cifrado AES-256, acceso restringido únicamente a personal autorizado y registros de verificación de integridad. Estos controles se encuentran implementados conforme a lo

						establecido en la Política Interna V2024.
2.7	ISO 27001: A.8.15 ISO 22301: 9.1	Existe un registro o log de cada respaldo ejecutado.	Validar evidencia de fecha, hora, usuario responsable y estado del respaldo.	Sí	Si	Se constató la existencia de logs detallados de cada respaldo, los cuales incluyen fecha, hora, usuario responsable y estado de la ejecución.
2.8	ISO 27001: Cláusula 5.3 ISO 22301: 5.3	El procedimiento define responsables claros de la ejecución y monitoreo de respaldos.	Confirmar roles asignados y evidencias de cumplimiento.	Sí	Si	El procedimiento vigente define de manera clara los roles y responsabilidades del personal encargado de la ejecución y monitoreo de respaldos.
2.9	ISO 27001: Cláusula 10.1 y 10.2	Se realizan revisiones periódicas del procedimiento de respaldo.	Verificar si se han hecho actualizaciones en función de cambios tecnológicos o incidentes.	Sí	Si	Se verificó que el procedimiento de respaldos fue revisado y actualizado en diciembre de 2024, incorporando mejoras derivadas de incidentes menores y de cambios tecnológicos.
3. Verificación de Pruebas de Restauración de Datos realizadas en 2024						
3.1	ISO 27001: A.5.1 ISO 22301: 8.5	Existe un procedimiento documentado para pruebas de restauración.	Confirmar que se han definido pasos, responsables y periodicidad de las pruebas.	Sí	Si	Si existe la política interna V2024
3.2	ISO 27001: A.8.13 ISO 22301: 8.4.5	Se han realizado pruebas de restauración durante el año 2024.	Verificar evidencias de ejecución (actas, reportes, logs).	Sí	No	Se hicieron 3 restauraciones no programadas en servidores no críticos. La política interna establece realizar respaldos de forma mensual.
3.3	ISO27001: A.8.13 ISO 22301: 8.2.2	Las pruebas cubren datos críticos y sistemas esenciales.	Asegurar que la restauración se realiza sobre la información más sensible.	Sí	No	No se cubrieron sistemas ni datos críticos, no se tiene definido sistemas críticos.
3.4	ISO 27001: Cláusula 7.5 ISO 22301 8.5 (e) y 7.5	Los resultados de las pruebas se encuentran documentados.	Confirmar existencia de reportes con tiempos de recuperación, incidencias y resultados.	Sí	No	No hay reportes ni documentación de resultados.
3.5	ISO 22301 8.2.2 , 8.3.3 y 8.4.5	Los tiempos de restauración	Verificar que los objetivos de tiempo de	Sí	No	No se verificaron los tiempos RTO/RPO

		cumplen con los RTO/RPO definidos.	recuperación son alcanzados.			definidos en ningún documento.
3.6	ISO 27001: Cláusula 9.1 y cláusula 10.1 ISO 22301: 10.1 y 10.2	Se han identificado fallos o incidencias en las pruebas.	Comprobar si los errores fueron registrados y evaluados.	Sí	Parcial	Restauraciones menores no mostraron fallos, pero sin evaluación formal.
3.7	ISO 27001: Cláusula 10.1 ISO 22301: 10.1 y 10.2	Se ejecutaron acciones correctivas o de mejora tras las pruebas.	Confirmar que los hallazgos fueron tratados y se mejoraron los procesos.	Sí	No	No se aplicaron acciones correctivas o de mejora documentadas.
3.8	ISO 27001: Cláusula 5.1 ISO 22301: 9.3 y 8.5	Las pruebas han sido aprobadas y validadas por la alta dirección.	Verificar que existe evidencia de revisión y aprobación de resultados.	Sí	No	No hubo validación ni aprobación de pruebas por Alta Dirección.
3.9	ISO 27001: Cláusula 9.3 cláusula 10.2 ISO 22301: 10.1 y 8.5	Existe un plan de pruebas para el presente año en base a los incidentes registrados en 2024.	Confirmar la planificación de nuevas pruebas de continuidad y restauración.	Sí	No	No existe un plan formal de pruebas para 2025, aunque la política establece realizar pruebas de forma trimestral.
4 Revisión de la Gestión de Incidentes relacionados con continuidad (últimos 12 meses)						
4.1	ISO/IEC 27001: A.5.30, cláusula 6.1.3 ISO 22301: 8.4	Existe un procedimiento documentado para la gestión de incidentes de continuidad.	Verificar que se cuenta con lineamientos para detección, reporte y resolución.	Sí	Si	El procedimiento existe, pero no hay evidencia de que haya sido socializado ni capacitado al personal responsable.
4.2	ISO/IEC 27001: A.5.10 ISO 22301: 9.1	Se dispone de un registro centralizado de incidentes.	Confirmar la existencia de bitácoras, tickets o informes de incidentes del año 2024.	Sí	Si	Existe un sistema de tickets donde se registran los incidentes
4.3	ISO/IEC 27001: A.5.30 ISO 22301: 8.2.2, 8.4.4, 8.3.3	Los incidentes fueron clasificados según criticidad e impacto.	Evaluar si existe categorización (alta, media, baja) y análisis de riesgos asociados.	Sí	Parcial	La clasificación está definida en el procedimiento, pero no hay evidencia de formación al personal para aplicarla adecuadamente.
4.4	ISO/IEC 27001: A.5.29 ISO 22301: 8.3.3, 8.4.3	Cada incidente cuenta con un tiempo de respuesta y resolución documentado.	Verificar si se cumplieron los SLA definidos o tiempos de recuperación.	Sí	Parcial	La respuesta a incidentes se encuentra documentada en los SLA; sin embargo, el personal clave no ha recibido capacitación en su cumplimiento.
4.5	ISO 22301: 10.1, 10.2	Se aplicaron acciones correctivas y preventivas frente a los incidentes.	Confirmar que los problemas no se repiten y se implementaron mejoras.	Sí	Parcial	Las acciones se aplicaron, pero no hay evidencia de que se capacite al personal para

						la gestión de acciones preventivas.
4.6	ISO/IEC 27001: Cláusula 5.1 ISO 22301: 8.4.3	La alta dirección o comité de TI recibió reportes de los incidentes más críticos.	Validar que existe evidencia de comunicación y escalamiento.	Sí	Parcial	Existe evidencia documental de reportes; sin embargo, no se evidencia capacitación al personal sobre protocolos de escalamiento.
4.7	ISO 22301: 8.4.4, 9.3 y 8.4.3	Los incidentes fueron relacionados con planes de continuidad y respaldos.	Confirmar que las acciones estuvieron alineadas con el plan de continuidad.	Sí	Parcial	La relación se encuentra documentada, sin embargo, no existe evidencia de capacitación al personal respecto a la aplicación práctica del plan.
4.8	ISO 22301: 10.2 y 8.4.3	Se documentaron lecciones aprendidas tras los incidentes y se comunicaron a las partes interesadas	Evaluar si se elaboraron informes de cierre con recomendaciones.	Sí	No	Existen Informes, pero no se evidencia capacitación al personal para integrar las lecciones aprendidas en futuras acciones.
4.9	ISO 22301: 10.2 y 8.5 (e y f), 8.4.3	Existe evidencia de mejora continua en la gestión de incidentes.	Verificar si el procedimiento ha sido actualizado tras lo ocurrido en el periodo evaluado.	Sí	Parcial	Los procedimientos se encuentran actualizados, pero no se evidencia capacitación al personal para la correcta adopción de las mejoras.
5. Auditoría a la Capacitación del personal en planes de continuidad y respaldo						
5.1	ISO 22301 Cláusula 7.2	Existe un plan anual de capacitación en continuidad y respaldos.	Verificar que la organización planificó capacitaciones formales en el periodo.	Sí	Si	Dentro de la política interna V2024 si indica capacitación de forma trimestral.
5.2	Políticas internas de continuidad de negocio y respaldo V2024	Se ha definido el alcance y objetivos de la capacitación.	Confirmar que incluyen continuidad operativa, gestión de respaldos y recuperación.	Sí	Si	Dentro de la política interna V2024 si indica capacitación al personal de TI.
5.3	ISO 27001 A 6.3 ISO 22301 Cláusula 7.2 Y 7.3	Se cuenta con registros de asistencia y participación del personal.	Validar listas de asistencia, firmas electrónicas o reportes de LMS.	Sí	No	No se tiene actas firmadas ni revisadas por la alta dirección, además no existe evidencia documentada de las capacitaciones.
5.4	ISO 27001 A 6.3 ISO 22301 Cláusula 7.2 Y 7.3	El contenido de la capacitación está alineado a los planes de continuidad y respaldo vigentes.	Verificar que la información transmitida corresponde a los procedimientos oficiales.	Sí	No	No se tiene documentación
5.5	ISO 27001 A 6.3 ISO 22301 Cláusula 7.2 Y 7.3	El personal con roles críticos (TI, riesgos,	Confirmar que los colaboradores clave fueron	Sí	No	No se tiene documentación

	Política interna V2024	operaciones) recibió formación específica.	incluidos en el programa.			
5.6	ISO 22301 Cláusula 8.5	Se realizaron simulacros o prácticas como parte de la capacitación.	Asegurar que el entrenamiento no fue solo teórico.	Sí	Si	Se realizaron simulacros, pero no se tiene documentado ni actas revisadas
5.7	ISO 22301 Cláusula 9.1 (a y b)	Se aplicaron evaluaciones o pruebas para medir el nivel de aprendizaje.	Verificar resultados y retroalimentación	Si	Si	Si se aplicaron, pero no existe evidencia suficiente a lo que indica
6. Revisión de la documentación del Plan de Recuperación ante Desastres (DRP)						
6.1	ISO 22301 Cláusula 8.4.4 (a y b) y 8.5.5	Existe un Plan de Recuperación ante Desastres (DRP) documentado.	Confirmar que el plan está formalmente escrito y disponible.	Sí	Si	El plan se encuentra disponible en la intranet de la organización "Plan de recuperación ante desastres V2023"
6.2	ISO 22301 Cláusula 5.2 ISO 27001 Cláusula 9.3	El DRP está aprobado por la alta dirección.	Verificar resolución, firma o evidencia de aprobación.	Sí	Si	Se encuentra con las firmas respectivas
6.3	ISO 22301 Cláusula 7.5.3 c y 8.5 g ISO 27001 Cláusula 7.5 y cláusula 9.3	El plan está actualizado al año 2024.	Comprobar que cuenta con versión, fecha y control de cambios.	Sí	No	Se evidenció que en el plan de recuperación consta un sistema que ya no forma parte de la empresa desde el 2023
6.4	ISO 22301 Cláusula 8.2.3	El DRP incluye un análisis de riesgos y escenarios de desastre.	Verificar que se consideren amenazas naturales, técnicas y humanas.	Sí	Si	En el documento que se encuentra publicado si se considera V2023 DRP
6.5	ISO 27001 A 5.9, cláusula 6.1.2 ISO 22301 Cláusula 8.2.2 , 8.2.3 y 8.3.2	Se definen los sistemas críticos, prioridades y dependencias.	Confirmar que la documentación clasifica servicios esenciales.	Sí	No	Los sistemas críticos están definidos pero la versión del DRP es del año 2023.
6.6	ISO 27001 Cláusula 6.1.2 ISO 22301 Cláusula 8.3.3	Están establecidos los RTO (Recovery Time Objective) y RPO (Recovery Point Objective).	Validar que existen objetivos medibles de recuperación.	Sí	Si	Si se define en la política V2023 estrategias de recuperación; sin embargo, sería importante revisar y actualizar
6.8	ISO 27001 Cláusula 5.3 ISO 22301 Cláusula 8.4.2	Se definen roles, responsabilidades y contactos de emergencia.	Verificar que exista un directorio actualizado de responsables.	Sí	Si	Los contactos se encuentran dentro de la política definido y presentado en la intranet
6.9	ISO 22301 Cláusula 8.4.2, 8.4.3 y 8.4.4	El DRP incluye procedimientos de comunicación interna y externa.	Confirmar canales de aviso a empleados, clientes, proveedores y entes reguladores.	Sí	Si	Dentro de la política V2023 si se incluye procedimientos de comunicación; sin embargo, es importante documentar y tener evidencia formal.

6.11	ISO 22301:2019 Cláusula 10.1 y 10.2	Se contemplan planes de mejora continua tras pruebas o incidentes.	Validar que el plan ha sido revisado y ajustado.	Sí	No	A pesar de que la política "Políticas internas de continuidad de negocio y respaldo V2024" establece actualizar los planos DRP, aún seguimos en la V2023
6.12	ISO 22301 Cláusula 8.3.2	El DRP está alineado a la política de continuidad y normas ISO/SEPS.	Confirmar cumplimiento con marcos regulatorios y normativos.	Sí	Si	En la Política DRP V2023 si se encuentra un mapa de trazabilidad normativa; sin embargo, es importante revisar y actualizar.

Tabla 1 Check list Auditoría Interna

OBSERVACIÓN DE LOS CONTROLES

Hallazgo 1

- ✓ **Del cumplimiento del control 2.2 dentro de la política "Política internas de continuidad de negocio y respaldo V2024" Frecuencia de Respaldos de Información.**

Durante la revisión de los registros de respaldos generados por el área de Tecnologías de la Información en el año 2024, se constató que la ejecución de copias de seguridad de los sistemas críticos no se realizó conforme a lo establecido en las "*Políticas internas de continuidad de negocio y respaldo V2024*", las cuales disponen que los respaldos deben ejecutarse de forma mensual. Del análisis de bitácoras y reportes del software de respaldo se identificó lo siguiente:

- Solo se registraron cuatro respaldos completos en el año (enero, abril, julio y octubre), lo que refleja una periodicidad trimestral en lugar de mensual.
- No se encontró documentación que justifique la omisión de respaldos mensuales, ni mecanismos de control que alerten sobre incumplimientos en la frecuencia definida.
- La situación fue corroborada con entrevistas al personal de TI.

Criterio

- De acuerdo con la norma ISO/IEC 27001:2022 – Control A.8.13 (Copias de seguridad de la información) se establece que, la organización debe realizar copias de seguridad de la información, software y sistemas con la periodicidad definida en su política, probando regularmente su efectividad.
- De acuerdo con la norma ISO 22301:2019 – Sección 8.4.5 (Procedimientos de respaldo de la información) se establece que, la organización debe implementar procedimientos que aseguren que la información esencial se respalde en intervalos apropiados y que dichos respaldos se protejan y estén disponibles para la recuperación en caso de incidentes.
- Adicionalmente, la normativa SEPS-IGT-2022-002 establece un control para los "*Procedimientos y mecanismos de resguardo de información física y digital, sensible o crítica*", donde indica que "*las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán: a) Respaldar la información sensible o crítica (física y digital) en lugares y ubicaciones adecuadas, considerando la triada de seguridad de la información; y, b) Disponer al menos de un documento evidenciable que compruebe el correcto funcionamiento de los respaldos*".
- De acuerdo con las "*Políticas internas de continuidad de negocio y respaldo V2024*", se establece que "*La frecuencia mínima de los respaldos será mensual, debiendo ejecutarse como máximo dentro de los primeros cinco (5) días hábiles de cada mes."*

Causa:

INFORMACIÓN CONFIDENCIAL

- No existe un proceso formal de seguimiento al cumplimiento de la frecuencia definida en la política de respaldos, lo que ha derivado en que el procedimiento real no se alinee a lo establecido.

Efecto:

- Al realizarse los respaldos únicamente cada tres meses, existe la posibilidad de que, en caso de un incidente (fallo de hardware, ataque de ransomware, error humano, etc.), se pierdan hasta 90 días de transacciones financieras y registros operativos, lo que impactaría directamente en la confiabilidad de los estados financieros y en la atención a los socios.
- Una pérdida masiva de información o una demora prolongada en la recuperación podría disminuir la confianza de los socios, acrecentar el riesgo reputacional y, en consecuencia, impactar en la estabilidad de la institución.

Recomendación 1:

Se recomienda a las áreas de Tecnología y Seguridad de la Información establecer un mecanismo de control y monitoreo (por ejemplo, checklist o dashboard de TI) que garantice la ejecución y evidencia de los respaldos en las fechas previstas.

Estrategia:

Implementar un plan de mejora para garantizar la ejecución de los respaldos en la frecuencia definida por las "*Políticas internas de continuidad de negocio y respaldo V2024*", ajustando los procedimientos operativos de TI y habilitando controles de seguimiento automatizados (alertas en el software de respaldo y reportes mensuales a Seguridad de la Información).

Entregable:

- Reportes automáticos de ejecución de respaldos (log del sistema de backup).

Responsable.

- Jefe de Infraestructura y Soporte Tecnológico, en coordinación con el Oficial de Seguridad de la Información.

Fecha de Cumplimiento:

- 30 de noviembre de 2025 (primer ciclo mensual evidenciado y documentado).

Hallazgo 2

✓ **Del cumplimiento del control 3.2 "Pruebas de restauración de respaldos realizadas en 2024" de la Política interna de Seguridad y Continuidad de la Organización v2024.**

Durante la revisión de la documentación y evidencias proporcionadas por el área de Tecnologías de la Información, se constató que en el periodo 2024 no se ejecutaron pruebas de restauración planificadas sobre los sistemas críticos de la Cooperativa. Únicamente se identificaron tres restauraciones no programadas en servidores no críticos: DLP, Antimalware y servidor de acceso remoto para proveedores. Esto limita la certeza de que los respaldos almacenados sean efectivos y recuperables en caso de incidentes que afecten la continuidad del negocio.

Criterio:

- De acuerdo con los controles definidos en la ISO/IEC 27001:2022 (A.8.13,Cláusula 9.1 y Cláusula 9.3, Cláusula 10.1 y Cláusula 10.2) y la ISO 22301:2019 (8.5.5, 8.2.2, 7.5, 8.2.3, 8.4.5, 9.3, 10.1 y 10.2), las organizaciones deben contar con un procedimiento documentado de pruebas de restauración, ejecutarlas periódicamente en sistemas críticos, documentar sus resultados, aplicar acciones correctivas y garantizar la aprobación de la

Alta Dirección. La normativa SEPS-IGT-2022-002 también exige disponer de mecanismos probados que aseguren la recuperación de la información crítica.

- De acuerdo con la política interna "*Políticas internas de continuidad de negocio y respaldo V2024*" apartado 3.2 establece realizar respaldos mensuales.

Causa:

- No existe un cronograma formal de pruebas de restauración.
- No se asignaron responsables específicos para la ejecución y documentación.
- Se limitó la práctica a restauraciones puntuales en sistemas secundarios.

Efecto:

- La falta de pruebas de restauración planificadas en sistemas críticos genera un riesgo de que, en caso de pérdida o corrupción de información financiera y operativa, la Cooperativa no pueda recuperarla oportunamente, afectando la continuidad de los servicios, el cumplimiento normativo y la confianza de los socios.

Recomendación 2:
Se recomienda establecer un plan anual de pruebas de restauración en sistemas críticos, complementado con restauraciones periódicas en sistemas de soporte, documentando los resultados, tiempos de recuperación, integridad de datos e incidencias. Estos informes deben ser revisados y aprobados por la Alta Dirección.

Estrategia:
Diseñar e implementar un cronograma anual de pruebas de restauración con responsables definidos y entregables claros. Documentar en informes técnicos cada prueba realizada, incluyendo bitácoras y evidencias gráficas.

Entregables:

- Plan de pruebas de restauración aprobado.
- Informe técnico de resultados de cada prueba.
- Bitácoras y capturas de ejecución.

Responsables:
Gerente de Tecnología de la Información y Gerente de Seguridad de la Información.

Fecha de Cumplimiento:
31 de diciembre de 2025.

Hallazgo 3

- ✓ **Del cumplimiento del control 8.4.3 de la Norma ISO 22301:2019 y 4.8 de la política interna, Falta de comunicación y reporte de incidentes de continuidad por parte del departamento de tecnología**

Descripción:

- Se identificó que durante el primer semestre de 2025 el Departamento de Tecnología no reportó al Área de Riesgos los incidentes que afectaron la continuidad de los servicios críticos. Esta falta de comunicación impidió que el Área de Riesgos tuviera conocimiento oportuno de los eventos para su análisis y gestión.

Criterio:

- De acuerdo con la Norma ISO 22301:2019 – Sistemas de gestión de la continuidad del negocio, en la cláusula 8.4.3 – Respuesta a incidentes, la organización debe:

a. La organización debe establecer, implementar y mantener procedimientos documentados para detectar, notificar, evaluar y responder a los incidentes que puedan afectar la continuidad del negocio.

b. Deben definirse roles, responsabilidades, autoridades y líneas de comunicación para la gestión de dichos incidentes.
c. Se debe garantizar el registro, seguimiento y aprendizaje de los incidentes para mejorar la capacidad de respuesta y la eficacia del sistema de gestión de continuidad del negocio. Asimismo, la Política de Continuidad de Negocio dispone que todos los incidentes que comprometan la disponibilidad de servicios críticos deben ser registrados, analizados y reportados al Área de Riesgos para su tratamiento y seguimiento.

- De acuerdo con el apartado 4.8 de la política interna "*Políticas internas de continuidad de negocio y respaldo V2024*", se debe documentar y comunicar las lecciones aprendidas a las partes interesadas.

Condición:

- En la revisión de la bitácora de incidentes del Área de Riesgos no se evidenció el registro de incidentes de Tecnología en el primer semestre de 2025. Sin embargo, en la mesa de servicio del Departamento de Tecnología constan los siguientes eventos:

a. El 06 de febrero de 2025: Falla en el proveedor de internet del DataCenter alterno, ocasionando la pérdida de comunicación con el DataCenter principal.
b. El 21 de mayo de 2025: Falla técnica en el servidor de virtualización, afectando la disponibilidad del servicio de llamadas telefónicas. De acuerdo con lo manifestado por el Jefe del Departamento de Riesgos, estos incidentes no fueron reportados por el Departamento de Tecnología, por lo cual el área desconocía su ocurrencia.

Causa:

- La omisión se debe a la ausencia de un procedimiento formal que regule la comunicación y reporte de incidentes de continuidad desde el Departamento de Tecnología hacia el Área de Riesgos.

Efecto:

- La falta de comunicación de los incidentes de tecnología limita la capacidad del Área de Riesgos para evaluar adecuadamente los incidentes que afectan la continuidad, impidiendo la actualización de los análisis de impacto, la definición de planes de respuesta y la implementación de medidas preventivas. Esto incrementa la exposición de la organización frente a interrupciones no gestionadas de manera oportuna.

Recomendación:

- Se recomienda a la Gerencia de Tecnología implementar un procedimiento formal que establezca los responsables, plazos y medios de comunicación para el reporte de incidentes de continuidad al Área de Riesgos, a fin de garantizar un adecuado control y seguimiento.

Estrategia:

- Elaborar y aprobar un procedimiento que formalice la comunicación y reporte de incidentes de continuidad al Área de Riesgos.

Responsable:

- Gerente de Tecnología en coordinación con gerente de Seguridad de la información.

Fecha Límite:

- 31 de octubre de 2025.

Evidencia:

a. Procedimiento aprobado por la Gerencia.
b. Registros de incidentes reportados al Área de Riesgos.
c. Bitácoras de seguimiento y análisis.

Hallazgo 4

- ✓ **Del cumplimiento del control 5.3 Capacitación del personal interno en planes de continuidad de negocio en la Política interna de Seguridad y Continuidad de la Organización v2024, se cuenta con registros de asistencia y capacitación personal.**

Descripción:

De acuerdo con la política interna de Seguridad y continuidad de la Organización v2024, el apartado 5.3 expresa capacitación del personal interno de forma trimestral con registro de actas y control de asistencia, el mismo que se realizará por áreas en el salón principal.

Sin embargo, en la auditoría se constató que no existe evidencia documentada que muestre que el personal de la organización haya recibido capacitación formal en planes de continuidad del negocio y respaldo. La ausencia de registros de capacitación limita la capacidad de la organización para asegurar que todo el personal pertinente esté preparado para responder de manera adecuada ante incidentes que afecten la continuidad operativa.

Criterio

Según la norma ISO 27001 (Anexo A, Concientización, educación y formación en seguridad de la información 6.3) e ISO 22301(Cláusula 7.3, 7.5), la organización debe garantizar que el personal clave reciba capacitación continua en seguridad de la Información y continuidad de negocio. Esto asegura que el personal de la organización esté preparado para ejecutar los procedimientos definidos en la política interna de Seguridad y continuidad de la Organización v2024 de forma correcta.
De acuerdo con la información obtenida en la auditoría, el personal de Talento Humano manifestó que las capacitaciones se realizaron; sin embargo, no existe un proceso de documentación para registrar la evidencia de los procesos realizados.

Causa:

La falta de documentación o evidencia en capacitación se debe a la falta de un plan formal y específico de Capacitación en Continuidad y Respaldo, únicamente nos referimos a la política interna regular de Seguridad y continuidad de la Organización v2024

Efecto

La falta de capacitación y documentación expone a la organización a riesgos elevados en caso de incidentes, ya que el personal podría no conocer o aplicar correctamente los procedimientos establecidos en la política interna. Esto podría ocasionar retrasos en la recuperación de servicios críticos, errores en la ejecución en el plan establecido e impacto negativo en la continuidad del negocio.

Recomendación 4:

Se recomienda al equipo de seguridad de la información y continuidad del negocio en coordinación con el área de talento humano desarrollar e implementar un plan formal de capacitación para el personal en continuidad de negocio y respaldo. Las capacitaciones incluirán procedimientos de recuperación, pruebas de restauración de respaldos y lineamientos de actuación ante incidentes.
Adicionalmente, se establecerá un proceso de documentación en el que se registrará toda la información relacionada con las capacitaciones, tales como: listas de asistencia, actas, evaluaciones de conocimientos, materiales entregados y reportes de cumplimiento. Esta información se deberá mantener organizada y disponible para futuras auditorías.

Estrategia:

Diseñar, documentar e implementar un Plan Formal de Capacitación en Continuidad del Negocio y Respaldo, alineado a la política interna v2024, a ISO 22301 y a ISO 27001, que asegure que el personal clave reciba formación periódica

Responsable.

- Área de Seguridad de la Información y Continuidad del Negocio: diseño y seguimiento del plan.
- Área de Talento Humano: organización logística, control de asistencia y evaluaciones.
- Dirección de TI: validación técnica de contenidos.

Fecha de Cumplimiento:

- Diseño y aprobación del plan: 30 diciembre 2025.
- Primera capacitación formal: en el siguiente trimestre (máximo 90 días).

- Ejecución continua: capacitaciones al menos trimestrales, con reportes semestrales a la Dirección.

Evidencia:

- Documento oficial del Plan de Capacitación en Continuidad y Respaldo aprobado por la Dirección.
- Registro de ejecución de capacitaciones (asistencia, evaluaciones, reportes).
- Informe de cumplimiento con evidencias organizadas (para futuras auditorías).

Hallazgo 5

✓ **Del cumplimiento del control 8.5 (g) ISO 22301:2019 y control 6.3 de la política interna, el plan de recuperación ante desastres se encuentra actualizado y cuenta con versión, fecha y control de cambios.**

Descripción:

Durante la revisión del DRP se evidenció que el plan está documentado y aprobado por la alta dirección; sin embargo, no se encuentra actualizado a la versión 2024 (6.3 V2024); además, no existe un control de cambios formal en el documento por lo que los sistemas críticos de la organización han variado y no se encuentran bien definidos.

Criterio:

- De acuerdo con la revisión del documento “Plan de recuperación ante desastres V2023", la cláusula 8.5 inciso g de la ISO 22301:2019 indica que los planes deben revisarse y actualizarse cuando haya cambios significativos en la organización o en el contexto en el que opera. Además, dentro de la política interna “Política interna y continuidad de negocio y respaldo V2024” inciso 6.3 expresa que las políticas deben revisarse de forma anual.
- Para ISO 27001:2022 Cláusula 6.1.2, A 5.9 y A 5.34 se deben identificar riesgos y priorizar activos de información al igual que en la ISO 22301:2019: 8.2.2, 8.2.3 y 8.3.2 señala que las estrategias de continuidad deben seleccionarse considerando los sistemas y procesos críticos.

Condición:

Durante la revisión del DRP se evidenció que:

- El plan está documentado y aprobado, pero no se encuentra actualizado al 2024 (6.3).
- Los sistemas críticos no están definidos en la organización (6.5).
- Falta control de cambios formal en el documento (6.3).

Causa

- No existe un proceso sistemático de revisión y actualización periódica del DRP.
- Se depende de la política general de continuidad, sin aterrizar en un plan operativo específico**.**

Efecto

- Riesgo de que, ante un desastre, la organización no logre recuperar los sistemas críticos dentro de tiempos aceptables, afectando la disponibilidad de información y servicios.
- Incumplimiento parcial con los requisitos de las normas ISO 22301 e ISO 27001, y con posibles exigencias regulatorias.
- Dificultad para coordinar acciones de recuperación de forma eficiente por falta de claridad en prioridades, dependencias y tiempos de recuperación.

Recomendación

- Actualizar el DRP, incorporando control documental (versión, fecha, cambios y aprobación).
- Definir y documentar los sistemas críticos, basados en un BIA actualizado.
- Fortalecer la alineación normativa con ISO 22301, ISO 27001 y regulaciones locales, generando trazabilidad entre políticas, análisis de riesgos y planes operativos.

Estrategia

- Implementar un proceso formal de revisión, actualización y control documental del DRP, que asegure:
- Depuración de sistemas y servicios incluidos en el plan, eliminando los obsoletos y manteniendo solo los vigentes y críticos.
- Control de cambios mediante registro de versión, fecha, responsable y motivo de la modificación.
- Validación periódica del DRP por las áreas responsables y aprobación de la alta dirección.
- Difusión del DRP actualizado en los canales internos oficiales

Responsable

Área de Continuidad de negocio, Área de TI y Alta dirección.

Fecha límite

28 Octubre 2025

Evidencia

- Acta de revisión y aprobación
- Registro de control de cambios
- DRP actualizado
- Comunicación interna

8. Conclusión y Riesgo

La auditoría interna conforme a los controles evaluados dentro de la política interna y seguridad de la información definidos en las normas ISO 27001 Y 22301, no alcanza un nivel de cumplimiento adecuado. Los hallazgos evidencian: controles críticos no cumplidos lo cual expone a la organización a un riesgo alto de pérdida de información y fallos en la recuperación en caso de incidente o desastre. Además, existe controles con cumplimiento parcial que los que existe mecanismos básicos implementados, pero sin la debida formalización. Esto se detalla en la siguiente tabla:

	Nivel de Riesgo		
Actividad / Subproceso	**Alto**	**Medio**	**Bajo**

Control 2.2 – Frecuencia de respaldos	X		
Control 3.2 – Pruebas de restauración en 2024	X		
Control 4.8– Comunicación y reporte de incidentes		X	
Control 5.3 – Capacitación en planes de continuidad		X	
Control 6.3 – Actualización del DRP	X		

Tabla 2 Hallazgo y Riesgo

En consecuencia, el nivel de madurez del plan de continuidad y respaldos es medio-bajo, ya que, si bien la organización dispone de procedimientos y políticas, la falta de actualización, pruebas, comunicación y evidencia documentada limita su capacidad de respuesta ante incidentes.

9. Resumen de estrategias y aceptación

Responsable	Nro. de Estrategia	Fecha de cumplimiento	Firma del responsable	Estado
Gerente de Seguridad de la Información	1	30-nov-25		Pendiente
	2	31-dic-25		Pendiente
	3	31-oct-25		Pendiente
	4	30-dic-25		Pendiente
	5	28-oct-25		Pendiente

Tabla 3 Resumen estrategia y aceptación

Atentamente;

AUDITOR INTERNO