

Diciembre 2025

Política de Continuidad Operacional y Resiliencia Operativa

ÍNDICE

1.	INTRODUCCIÓN	3
2.	ALCANCE	4
3.	NORMATIVA APLICABLE Y BUENAS PRÁCTICAS	4
4.	OBJETIVOS.....	4
5.	RESPONSABILIDADES Y LÍNEAS DE DEFENSA	5
6.	HITOS DEL PROCESO DE CONTINUIDAD OPERACIONAL	7
6.1.	Identificación y Clasificación de Procesos y Servicios Críticos	7
6.2.	Análisis de Impacto de Negocio (BIA)	7
6.3.	Evaluación de Riesgos y Amenazas para la Continuidad Operacional	8
6.4.	Planes y Estrategias de Continuidad y de Recuperación	8
6.5.	Pruebas, Ejercicios y Actualización.....	8
7.	CONTROLES Y MONITOREO PERIÓDICO	9
8.	GESTIÓN INTEGRAL DE INCIDENTES Y CRISIS	10
9.	REPORTE A LA ALTA DIRECCIÓN	10
10.	CULTURA Y FORMACIÓN	11
11.	REVISIÓN, ACTUALIZACIÓN Y MEJORA CONTINUA	11
12.	CUADRO DE VERSIONES Y CAMBIOS.....	12
13.	GLOSARIO DE TÉRMINOS:	13

Política de Continuidad Operacional y Resiliencia Operativa del Administrador del Fondo Autónomo de Protección Previsional

1. INTRODUCCIÓN

El Administrador del Fondo Autónomo de Protección Previsional (en adelante, el “Administrador”) es un organismo público, de carácter técnico y autónomo, cuya función es financiar las prestaciones y beneficios del Seguro Social Previsional. Para ello, tiene el mandato de administrar la gestión e inversión de los recursos del Fondo Autónomo de Protección Previsional (en adelante, “el Fondo”), con el objetivo de maximizar su rentabilidad de largo plazo, velando en todo momento por su sustentabilidad financiera a través de generaciones.

Su misión es administrar de manera autónoma, eficiente y transparente los recursos destinados a financiar los beneficios del Seguro Social Previsional que complementarán las pensiones basadas en ahorro previsional, con el fin de aportar a una mayor protección previsional para los actuales y futuros pensionados. Por ello, resulta de la mayor relevancia para el Administrador del Fondo asegurar la protección de los recursos previsionales que le corresponde gestionar y contribuir a la continuidad del sistema en beneficio de los cotizantes y beneficiarios.

El Administrador asume que la continuidad operacional es un componente central de su deber fiduciario, siendo responsable de anticipar, resistir, adaptarse y recuperarse ante disrupciones que puedan afectar su capacidad de cumplir su mandato legal.

En efecto, la operación continua del Administrador es esencial para asegurar la protección de los recursos previsionales, garantizar la entrega oportuna y correcta de los beneficios del Seguro Social Previsional y sostener la confianza del sistema previsional.

En este contexto, la **Política de Continuidad Operacional y Resiliencia Operativa del Administrador** del Fondo constituye un marco esencial para definir las principales tareas y responsables que permitan gestionar los riesgos inherentes al cumplimiento de su mandato, y así garantizar la disponibilidad continua de los servicios críticos, en particular, ante eventos disruptivos que pudieran comprometer su funcionamiento.

En esta política se establecen las directrices principales para la posterior elaboración de los Planes de Continuidad Operacional, los que expondrán las estrategias para la recuperación

y mitigación de riesgos ante la presencia de eventos disruptivos que puedan afectar el normal desempeño de las actividades del Administrador y el Fondo.

En consecuencia, esta política busca definir los factores claves de organización y gobernanza que propendan a fortalecer la capacidad del Administrador para anticipar, resistir, adaptarse y recuperarse ante incidentes que afecten su operación, preservando la integridad de los recursos administrados por el fondo, la confianza pública y el cumplimiento de sus obligaciones legales y normativas, sujetas a la supervisión de la Superintendencia de Pensiones (SP) y Contraloría General de la República (CGR).

2. ALCANCE

Esta Política se aplica transversalmente a todos los procesos y actividades que sean definidos como críticos o prioritarios para mantener la continuidad operativa del Administrador y el Fondo, resguardando el cumplimiento de su mandato.

3. NORMATIVA APLICABLE Y BUENAS PRÁCTICAS

3.1. Normativa Nacional, el Administrador declara como vinculante:

- Ley N° 21.735 de 2025, crea el Fondo y su Administrador.
- Normas de Carácter General, emitidas por la SP para la regulación del Administrador.
- D.L. N° 3.500, de 1980, y sus modificaciones.
- Libro V del Compendio del Sistema de Pensiones, en lo relativo a la gestión de riesgos (normativa de referencia).

3.2. Normativas Internacionales y Buenas Prácticas

- Directiva DORA (Digital Operational Resilience Act) de la Unión Europea.
- ISO 22301 — Sistema de Gestión de Continuidad de Negocio.
- Principios de Basilea para la Resiliencia Operativa.
- COSO ERM (Enterprise Risk Management Framework).

4. OBJETIVOS

- Asegurar la continuidad ininterrumpida de los procesos y servicios críticos del Administrador y el fortalecimiento de la resiliencia organizacional y mitigación de riesgos de interrupción, con el propósito de que pueda cumplir su mandato legal.

- Proteger la integridad disponibilidad y confidencialidad de la información y activos operacionales del Fondo.
- Establecer mecanismos que permitan reducir el impacto ante interrupciones mediante tolerancias al impacto, RTO (*Recovery Time Objective*) y RPO (*Recovery Point Objective*) formalmente aprobados.
- Desarrollar resiliencia organizacional, asegurando la preparación del personal y la robustez de los sistemas.
- Establecer un marco de gobierno robusto que dirija y gestione la continuidad operacional y la resiliencia operativa, promoviendo la mejora continua.
- Cumplir con las exigencias regulatorias respecto a planes de contingencia y gestión de riesgos operacionales.
- Impulsar el conocimiento y el comportamiento de la organización a fin de tener una cultura de resiliencia ante eventos indeseados o disruptivos.
- Asegurar la continuidad de procesos críticos externos mediante gestión activa de proveedores.
- Establecer lineamientos claros para la gestión de crisis, preparando al Administrador para contener y responder ante emergencias o eventos disruptivos que conlleven un riesgo de las operaciones de las áreas o servicios críticos u otro tipo de situaciones de alto impacto institucional y/o sistémico que puedan afectar el cumplimiento de su mandato legal.

5. RESPONSABILIDADES Y LÍNEAS DE DEFENSA

Consejo Directivo: Aprueba esta Política, aprueba los escenarios de contingencia y las estrategias de continuidad y recuperación, define las tolerancias al impacto, asegura los recursos humanos, tecnológicos y financieros necesarios para mantener la continuidad de las actividades críticas en niveles aceptables, aprueba informes anuales de pruebas y auditorías. Recibe reportes semestrales de continuidad.

Director Ejecutivo: Responsable de implementar la Política, asignar recursos y liderar la gestión de continuidad.

Comité de Gestión de Crisis: Instancia de gobierno institucional que decide sobre declarar crisis; activar planes de continuidad; gestionar comunicación interna y externa; coordinar con autoridades (SP, CGR, Banco Central de Chile, Tesorería General de la República, Instituto de Previsión Social, ministerios, entre otros).

Comité Integral de Riesgos: Supervisa riesgos de continuidad y resiliencia operativa.

Primera Línea de Defensa (Unidades operativas del Administrador): Ejecuta procesos críticos. Define y actualiza el Análisis de Impacto de Negocio (BIA) de sus procesos. Diseña e implementa los controles de continuidad, mitigadores y medidas preventivas, para garantizar su ejecución de sus procesos ante contingencias. Identifica y evalúa el impacto en la continuidad operacional de los servicios que brindan apoyo en sus procesos críticos. Identifica e informa oportunamente cualquier incidente o evento anómalo que puedan generar interrupción en los procesos críticos (personas, servicios, recursos, información y/o tecnologías), contribuyendo así a la detección temprana y mitigación de riesgos.

Define y actualiza periódicamente los planes de continuidad operacional (BCP) de sus procesos críticos, estableciendo las estrategias de continuidad y recuperación.

Refuerza la cadena de suministros mediante la gestión de proveedores de su ámbito, estableciendo acuerdos de nivel de servicio sólidos para asegurar la continuidad de servicios críticos y minimizar impactos en caso de interrupciones significativas.

Segunda Línea de Defensa (Dirección de Riesgos): Supervisa la aplicación de la política, valida el resultado de los BIA de todos los procesos del Administrador, revisa los niveles de tolerancia al impacto y realizar seguimiento al cumplimiento de pruebas y reportes. Supervisa proveedores críticos. Coordina y valida las pruebas de continuidad institucionales. Acompaña y desafía a las unidades operativas del Administrador en la mejora continua de los planes de continuidad.

Diseña e implementa mecanismos de concientización para reforzar en toda la institución la importancia del ciclo de la continuidad operacional y resiliencia, capacita y entrena al personal crítico del Administrador para la comprensión de su rol y responsabilidad en los planes de continuidad operacional de sus procesos críticos.

Tercera Línea de Defensa (Auditoría Interna): Evalúa independencia, eficacia y suficiencia de la efectividad del sistema de continuidad operacional y resiliencia operativa, la adecuación de los planes de continuidad operacional del Administrador, la efectividad de las estrategias de continuidad y recuperación, y la calidad de los reportes emitidos.

6. HITOS DEL PROCESO DE CONTINUIDAD OPERACIONAL

6.1. Identificación y Clasificación de Procesos y Servicios Críticos

Se deben identificar todos los procesos y servicios involucrados en la gestión del Administrador, que resultan esenciales para la entidad y cuya interrupción afectaría el funcionamiento operativo del organismo y el Fondo, los que se pueden clasificar según el ámbito en el que generan un impacto (operacional, en beneficiarios, financiero, fiduciario, reputacional, regulatorio) y que incluyen procesos tales como: recepción de recaudación y validaciones, gestión y valorización de inversiones, custodia y liquidación, registro de cotización con rentabilidad protegida, validación del cálculo y pago de beneficios del seguro social, contabilidad del Fondo y su Administrador, emisión de estados financieros, entre otros.

6.2. Análisis de Impacto de Negocio (BIA)

El Administrador elaborará y actualizará anualmente un BIA, el cual debe recopilar todas las actividades que forman parte de las áreas operativas y de gestión del organismo y el Fondo. La propuesta de BIA se someterá a aprobación del Consejo Directivo.

Como consecuencia de lo anterior se debe aplicar un análisis de impacto en caso de interrupción y disrupción significativa sobre la gestión del Administrador y el Fondo respecto de cada área o actividad, identificando así aquellas que sean críticas para el desarrollo de las actividades esenciales del Administrador y el Fondo.

Se deberán establecer los requerimientos y recursos necesarios para su restauración en los tiempos requeridos, y a un nivel de servicio aceptable, estableciendo una priorización de la recuperación de estas en una situación de contingencia y en consecuencia de los servicios críticos asociados.

El BIA incluirá:

- RTO (*Recovery Time Objective*)
- RPO (*Recovery Point Objective*)
- MAO (*Maximum Allowable Outage*)
- Impacto cualitativo y cuantitativo
- Dependencias tecnológicas y de terceros

6.3. Evaluación de Riesgos y Amenazas para la Continuidad Operacional

En línea con lo anterior, se identificarán y valorarán los riesgos que podrían generar interrupciones o disrupciones, tales como:

- Fallas en la infraestructura tecnológicas (caída total o parcial de sistemas).
- Fallas en la infraestructura física (indisponibilidad de instalaciones).
- Interrupciones de telecomunicaciones y data centers.
- Ausencia masiva de personal o ausencia de personal crítico.
- Ciberataques y *ransomware*.
- Falla de proveedores estratégicos.

6.4. Planes y Estrategias de Continuidad y de Recuperación

Como resultado de lo anterior, el Administrador elaborará y aprobará sus estrategias de continuidad, las que, entre otras cosas, incluirán:

- Planes de recuperación tecnológica (DRP - plan de recuperación de desastres).
- Infraestructura y sistemas con redundancia.
- Capacidades de recuperación tecnológicas documentadas.
- Planes de respaldo de datos y comunicaciones.
- Sitio alternativo operativo o conexión remota.
- Planes de sustitución de personal crítico/trabajo remoto seguro bajo contingencia.
- Acuerdos con terceros que aseguren tiempos de recuperación compatibles con los RTO del Administrador.
- Implementación del Comité de Gestión de Crisis, en línea a los descrito en el Protocolo de Gestión de Crisis.
- Estrategias comunicacionales y mitigación de impacto reputacional.

6.5. Pruebas, Ejercicios y Actualización

El Administrador definirá un plan de pruebas anual, que incluya pruebas de escritorio, parciales, totales y ejercicios de crisis y participación de proveedores críticos, según corresponda, que será validado regularmente por las áreas de Riesgos y Tecnología y Datos, orientado hacia la consecución de los siguientes objetivos:

- Verificar la eficacia de las estrategias de continuidad y recuperación definidos en los planes de continuidad operacional.
- Verificar la recuperación de las actividades críticas y su alineación a los RTO y RPO definidos.

- Verificar que el resultado de las pruebas esté dentro de los niveles de tolerancia de impacto establecida para las áreas, funciones y servicios críticos.
- Propender a la mejora continua de los planes, identificando brechas y e iniciativas de mejora.

El resultado de las pruebas será presentado en el Comité Integral de Riesgos, instancia de gobierno que propondrá la actualización de los planes de continuidad operacional para su posterior aprobación por parte de Consejo Directivo.

7. CONTROLES Y MONITOREO PERIÓDICO

Parte de las actividades fundamentales relacionadas a la gestión de continuidad, es la ejecución de controles de seguimiento y el monitoreo continuo, que permitan asegurar la efectividad de las estrategias e identificar espacios de mejora continua, algunas de estas actividades son:

- Revisión semestral del catálogo de servicios críticos y aprobación de los planes.
- Actualización anual de los planes de continuidad operacional (BCP) y Plan de recuperación de desastres (DRP.)
- Definición de indicadores de desempeño (KPI de disponibilidad/KRI de resiliencia), en caso de ser necesario.
- Monitoreo continuo de sistemas y proveedores.
- Identificación de eventos disruptivos no contenidos en los planes.
- Identificación de nuevas áreas, procesos o servicios críticos.
- Identificación de nuevos proveedores críticos.
- Informes trimestrales a la Alta Dirección.
- Informes semestrales al Consejo Directivo.

Cuando sea considerado necesario por la institución, la detección de cambios relevantes en los componentes de alguna de las estrategias, escenarios u orgánica del Administrador, conllevará una nueva actualización inmediata de los planes de continuidad, la que se sujetará a la aprobación por el Consejo Directivo.

8. GESTIÓN INTEGRAL DE INCIDENTES Y CRISIS

El Administrador implementa un enfoque integral para prevenir, detectar, responder, recuperar y mejorar continuamente la gestión de incidentes que puedan afectar a personas, recursos, información, tecnologías y procesos relacionados con actividades críticas.

La administración de crisis busca resguardar el riesgo frente a incidentes cuyo impacto pudiera comprometer el cumplimiento del mandato, objetivos estratégicos, recursos previsionales que le corresponde gestionar y/o la reputación del Administrador, y que pudieran generar interés de la opinión pública y de los medios de comunicación.

Para la gestión de crisis ante incidentes internos y externos, se propenderá a una respuesta ágil y coordinada ante situaciones de crisis, con liderazgo activo de todas las unidades bajo la dirección del Comité de Crisis.

El Administrador fortalecerá su capacidad de respuesta ante incidentes que puedan generar riesgos a nivel de sistema de pensiones, en coordinación con actores relevantes del ecosistema previsional

9. REPORTE A LA ALTA DIRECCIÓN

- Periodicidad: Reporte semestral y extraordinario en caso de contingencia material.
- Destinatarios: Comité Integral de Riesgos y Consejo Directivo.
- Los informes estarán a disposición de la Superintendencia de Pensiones en caso de requerirlos.
- Contenido mínimo del informe:
 - Estado de planes de continuidad operacional y resiliencia.
 - Evaluación de pruebas y hallazgos de auditorías deberán remediarse en plazos definidos.
 - Brechas detectadas y planes de acción.
 - Lecciones aprendidas y mejoras implementadas.

10. CULTURA Y FORMACIÓN

El Administrador establecerá un programa anual de capacitación obligatoria en continuidad y resiliencia para todo el personal, efectuará una evaluación de competencias en roles críticos, simulacros anuales para equipos claves, programas de sensibilización en resiliencia operativa promoviendo la conciencia sobre la importancia de la disponibilidad operativa, el rol de cada actor y los protocolos de emergencia.

11. REVISIÓN, ACTUALIZACIÓN Y MEJORA CONTINUA

La Política será revisada anualmente por el Consejo.

12. CUADRO DE VERSIONES Y CAMBIOS

N° de versión	Principales cambios	Responsable	Instancia de aprobación	Fecha
1	Primera Versión	Dirección de Riesgos	Consejo Directivo	Diciembre 2025

13. GLOSARIO DE TÉRMINOS:

Resiliencia Operativa:

Capacidad de la entidad para seguir ejecutando sus servicios críticos ante eventos disruptivos. Esta capacidad permite al Administrador anticipar, identificar y protegerse de las amenazas y posibles fallos, responder, adaptarse, recuperarse y aprender de los eventos disruptivos con el fin de minimizar su impacto en la entrega de servicios críticos en estas situaciones de interrupción.

Continuidad del Negocio:

Capacidad estratégica y táctica del Administrador para garantizar que los procesos esenciales del negocio sigan funcionando dentro de niveles aceptables y que se recuperen en tiempos definidos (RTO - RPO).

Proceso o actividad crítica:

Corresponden a aquellos procesos, subprocesos y actividades que, por su naturaleza, al enfrentar una interrupción o interrupción podría generar impactos relevantes en el cumplimiento de los objetivos estratégicos del Administrador, los activos previsionales que debe gestionar o la reputación.

Servicios críticos:

Son los recursos provistos, internamente y por terceros, que ante una interrupción podría generar impactos relevantes en el cumplimiento de los objetivos de los procesos o actividades críticas.

Desastre:

Situación en que se han producido pérdidas humanas, materiales, económicas o ambientales, cuyas consecuencias exceden las capacidades de la organización afectada para responder y recuperarse utilizando sus propios recursos.

Interrupción:

Incidente que produce una alteración o daño a los recursos o estructura de una actividad y/o proceso, generando un efecto negativo y daño, no esperado, en la entrega de productos y/o servicios.

Interrupción:

Incidente que produce una alteración en una actividad o procesos, generando un efecto no esperado, en la entrega de productos y/o servicios, de acuerdo con los objetivos del Administrador.

Tiempo Objetivo de Recuperación (sigla en inglés RTO - Recovery Time Objective):

Corresponde al período de tiempo después del incidente en que la actividad, proceso, servicio debe reanudarse o los recursos deben ser recuperados.

Punto Objetivo de Recuperación (sigla en inglés RPO - Recovery Point Objective):

Es el punto en el cual la información utilizada por una actividad debe ser restaurada para que la actividad pueda operar. Puede referirse, también a la máxima pérdida de datos.

Máximo Tiempo de Interrupción Permitido) (sigla en inglés MAO (Maximum Allowable Outage)

Corresponde al período máximo de tiempo durante el cual un proceso, servicio o sistema crítico puede permanecer interrumpido, antes de que dicha interrupción genere impactos inaceptables para la entidad y/o para los afiliados, pensionados o beneficiarios, desde el punto de vista legal, operativo, financiero, reputacional y regulatorio.

Tolerancia al impacto:

El nivel máximo tolerable de interrupción de un servicio crítico que las unidades críticas del Administrador están dispuestas a aceptar dada una serie de escenarios severos pero plausibles. La Tolerancia al Impacto se puede medir como un período de tiempo o cualquier métrica de volumen/valor (por ejemplo, volumen de beneficiarios afectados).

Planes de Continuidad Operacional (BCP):

Se refiere a los procedimientos orientados a recuperar las operaciones ante la ocurrencia de fallas producto de la materialización de alguno de los escenarios de contingencia definidos por el Administrador. Son complementarios, en lo que corresponde, al Plan de recuperación ante desastres.

Planes de Recuperación ante Desastres:

Los planes de recuperación ante desastres (DRP) contemplan procedimientos y actividades para recuperar la normalidad de los recursos que soportan los procesos o actividades críticas y que están siendo afectados por algún evento disruptivo. Para el desarrollo de DRP

se deberá tener en consideración los parámetros e indicadores de continuidad determinados en la evaluación de los procesos o actividades críticas acordados por las unidades de negocio en estas instancias (RTO - RPO).

Pruebas de continuidad:

Instancias de simulación de los escenarios abordados en los planes de continuidad, cuyos resultados se contrastan con los parámetros de contingencia que requieran las actividades críticas y/o recursos relacionados.