

I.- PROPÓSITO

El propósito de esta política es asegurar el cumplimiento de la organización en la normativa que instruye la CMF sobre la implementación de la gestión del riesgo operacional. Además, del cumplimiento de los requerimientos del Principio 17 - Riesgo Operacional, establecido en los Principios para las Infraestructuras del Mercado Financiero del CPMI-IOSCO.

II.- ALCANCE

Esta Política General aplica a todos los empleados y define la estructura de trabajo (framework) para el Riesgo Operacional, que incluye: su identificación, evaluación, tratamiento, monitoreo y comunicación.

Esta Política cubre los riesgos operacionales a los servicios que son parte de los negocios de la organización y que se definen en la Política General de Nivel de Servicios para Participantes, o en su defecto en los contratos con los Participantes.

III.- DEFINICIONES

Riesgo Operacional:

La organización hace suya la definición de Riesgo Operacional de CPMI-IOSCO, que lo define como: "el riesgo de que las deficiencias en los sistemas de información o los procesos internos, errores humanos, fallos de gestión o alteraciones provocadas por acontecimientos externos deriven en la reducción, el deterioro o la interrupción de los servicios prestados por una FMI".

De la misma forma, también toma en consideración la definición de Riesgo Operacional de la CMF, que lo define como: "riesgo que las deficiencias que puedan producirse en los sistemas de información, los procesos internos o el personal, o las perturbaciones ocasionadas por acontecimientos externos provoquen la reducción, el deterioro o la interrupción de los servicios que presta la entidad y, eventualmente, le originen pérdidas financieras. Incluye el riesgo de pérdidas ante cambios regulatorios que afecten las operaciones de la entidad, como también pérdidas derivadas de incumplimiento o falta de apego a la regulación vigente".

Las fallas operacionales pueden dañar la reputación o confiabilidad percibida, traer consecuencias legales y resultar en pérdidas financieras incurridas por la IMFs, los participantes y otras partes.

De acuerdo a las definiciones anteriores y tomando en consideración la categorización de la "ERM (Enterprise Risk Management) Wheel" del Global Association of Risk Professionals (GARP), los tipos de riesgos que se incluyen en la categoría riesgo operacional son:

- Riesgo de Continuidad de Negocios
- Riesgo de Seguridad de la Información
- Riesgo de Calidad
- Riesgo de Fraude
- Ciber Riesgos
- Riesgos Ciber Seguridad

Continuidad de Negocio (ISO 22301:2019):

Capacidad de la organización de continuar la entrega de sus servicios a niveles aceptables predefinidos, luego de ocurrido un incidente disruptivo (Interrupción brusca).

Seguridad de la Información:

Es entendida como la preservación y protección de la confidencialidad, integridad y disponibilidad de la información, de una amplia gama de amenazas. Su propósito es minimizar el daño, garantizar la integridad, confidencialidad y disponibilidad de la información y los servicios, resguardando la imagen y reputación de la organización.

Calidad:

"Grado en el que un conjunto de características inherentes, cumplen con una necesidad o expectativa establecida, generalmente implícita u obligatoria" (Definición ISO 9000 Sistemas de Gestión de la Calidad – Fundamentos y Vocabulario).

Fraude:

COSO "Fraude es cualquier acto u omisión intencional diseñado para engañar a los demás, resultando en una pérdida para la víctima y/o una ganancia para el perpetrador. En general se consideran las siguientes categorías de fraude:

- Reporte fraudulento de información financiera
- Reporte fraudulento de información no financiera
- Malversación de activos
- Otros actos ilegales y de corrupción"

Apetito por Riesgo (CMF):

Es el nivel agregado y tipos de riesgo que una entidad está dispuesta a asumir, previamente decidido y dentro de su capacidad de riesgo, a fin de lograr sus objetivos estratégicos y plan de negocio.

Tolerancia al Riesgo (FAIR):

Es el grado de varianza del apetito al riesgo de la organización que la organización está dispuesta a tolerar.

IV.- REGLAS

1. La organización cualitativamente tiene un bajo apetito al riesgo operacional, por ende, no tiene tolerancia a las interrupciones y deterioro del servicio, y a las pérdidas ocasionadas por ellas. Por lo anterior, como estrategia, no asumirá riesgos que afecten la entrega de sus servicios y los evitará cuando sea posible, o en su defecto tomará las acciones de control apropiadas para reducirlos (mitigarlos) o compartirlos. La organización establecerá el nivel cuantitativo de riesgo aceptado y de tolerancia de acuerdo con lo aprobado por el Comité de Riesgo Operacional (ver sección V. Criterios de Evaluación y Tratamiento de Riesgo – Evaluación de Riesgos).
2. Para llevar a cabo una adecuada gestión de los Riesgos Operacionales, La organización adoptará el estándar ISO31000:2009 Risk Management - Principles and Guidelines como framework, que le permitirá la gestión de sus distintos tipos de riesgos, y cumplir con lo estipulado en la normativa de la CMF que instruye sobre la implementación de la gestión de riesgo operacional. Además, se realizará una gestión de riesgos por niveles basados en el estándar NIST 800-30, con la finalidad de integrar la gestión de riesgos en la organización.
3. Para la cuantificación del impacto de las perdidas asociadas al riesgo operacional, y con el fin de definir e implementar las mitigaciones necesarias, se adoptará preferentemente la metodología Factor Análisis for Information Risk (FAIR).
4. Las actividades de gestión de riesgo operacional, que forman parte del Proceso de Gestión de Riesgo son: Establecer el Contexto, Valorización del Riesgo, Tratamiento de Riesgos, Aceptación del Riesgo y Monitoreo/Revisión del Riesgos. El objetivo del proceso es cumplir con la estrategia de mitigación o reducción de los riesgos operacionales de la organización. Este proceso de gestión será realizado al menos anualmente y auditado periódicamente por un ente independiente a Operaciones y TI.
5. Los cambios o la incorporación de nuevos servicios serán evaluados conforme al marco de gestión de riesgos definido por la organización, considerando su naturaleza, alcance e impacto, con el fin de identificar y

gestionar oportunamente los riesgos asociados antes de su implementación.

6. Los planes de tratamiento de los riesgos de Seguridad de la Información, Ciber Riesgo, Calidad, Fraude y Continuidad de Negocios deberán ser revisados y aprobados al menos una vez al año por el Comité de Riesgo Operacional, o en su defecto por el Directorio. Mientras que los planes de contingencia TIC y de continuidad de negocios deberán ser probados periódicamente y aprobados por el Directorio.
7. Las Actividades de Control (políticas, procedimientos y controles) deben estar orientados a reducir o mitigar los riesgos identificados y a prevenir, detectar y corregir las fallas o problemas que puedan surgir.
8. De esta Política General de Riesgo Operacional, se desprende un conjunto de políticas específicas/propias en los ámbitos de la gestión del riesgo operacional, la seguridad de la información, continuidad del negocio, calidad de los procesos, fraude, ciber riesgo y externalización y contratos a terceros.
9. El diseño organizacional (funciones y procesos) debe asegurar la segregación de funciones. Por lo tanto, no se asignarán a una misma persona funciones con intereses contrapuestos y ningún proceso de la organización podrá ser ejecutado sólo por una persona, debiendo intervenir como mínimo dos.
10. La organización declara su decisión de cumplir con la normativa y legislación vigente de los Organismos Reguladores y Fiscalizadores, relacionadas con el riesgo operacional, outsourcing, continuidad del negocio y seguridad de la información.
11. Los riesgos relacionados a fallas en componentes tecnológicos como hardware, configuración base, aplicaciones y redes se monitorearán en forma automática. Los riesgos relacionados a los ámbitos de procesos se monitorean mediante indicadores de riesgo y los riesgos de recursos humanos a través de controles independientes que aseguren la segregación de funciones y la adherencia a las actividades de control implementadas.
12. La organización promoverá una cultura de riesgos en materia de riesgos operacionales, lo que incluye a los riesgos de seguridad de la información / ciberseguridad, continuidad de negocios, ciber riesgos, calidad y fraude, dando especial atención a los procesos de gestión de toma de conciencia de los respectivos sistemas de gestión.

13. El incumplimiento de esta política constituye una falta y será sancionado como tal.

V.- CRITERIOS DE EVALUACIÓN Y TRATAMIENTO DE RIESGO

Análisis de Riesgos

La organización utilizará una metodología de análisis-semi cuantitativa en la cual se le asignan valores a la probabilidad de ocurrencia y al impacto del riesgo de acuerdo a las siguientes tablas de Criterios de Probabilidad de Ocurrencia y Criterios de Impacto.

Nivel	Probabilidad de Ocurrencia
1	Raro
2	Improbable
3	Posible
4	Probable
5	Casi cierto

Criterios de Impacto

Niveles / Criterios	Cumplimiento	Pérdida Disponibilidad	Pérdida Económica	Pérdida de Confidencialidad	Pérdida de Integridad	Pérdida Reputacional
Gravísimo (5)	* Presidio o reclusión *Multas por incumplimiento regulatorio (ver pérdida económica).	*Pérdida de disponibilidad que afecta a servicios de negocio críticos con impacto en la continuidad, seguridad y/o otros ámbitos. * Pérdida de disponibilidad que afecta los servicios críticos y no críticos (con impacto organizacional) por ciberataques masivos prolongados por parte de un hacker, agente externo o interno. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	Pérdidas por fraude interno, externo o ataques: Cualquier pérdida por Multas: Sobre 300 UF por incidentes operacionales: Sobre 60 UF Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva).	*Pérdida de confidencialidad de información clasificada como confidencial fuera de la organización mediante ciberataques dirigidos, Ransomware o de otra índole. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	*Pérdida de integridad que afecta a servicios de negocio críticos de producto de ciberataques a los sistemas de información de infraestructura crítica, por parte de terceros (Malware, Ransomware, APT, otros) y/o por personal interno. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	Evento que genera interés público e interés de los medios *Publicación de un extracto de la sentencia condenatoria en el diario oficial y en otro de circulación nacional. *Impacto gravísimo para la imagen de la empresa, existe cobertura amplia en los medios de comunicación, redes sociales y/o pérdida de participantes. *Mayor involucramiento de algún organismo regulador, del Estado y reclamos de participantes, por brechas masivas de distintos ámbitos o por litigios públicos.

POLITICA GENERAL CORPORATIVA DE RIESGO OPERACIONAL

Control de Documentación

Referencia: SGIR.5.2_POLI03

Página 6 de 14

Niveles / Criterios	Cumplimiento	Pérdida Disponibilidad	Pérdida Económica	Pérdida de Confidencialidad	Pérdida de Integridad	Pérdida Reputacional
Grave (4)	* Sin presidio ni reclusión. * Multas acotadas por incumplimiento regulatorio (ver pérdida económica) * Incumplimiento normativo interno	* Pérdida de disponibilidad que afecta servicios de negocio no críticos con posible impacto en la continuidad, seguridad y/o otros ámbitos, debido a errores internos o ataques dirigidos. * Degradación que afecta servicios de negocios críticos. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	Pérdidas por Multas: Hasta: 300UF Pérdidas por incidentes operacionales: Hasta: 60UF Ver pérdidas económicas (productividad, multas, respuesta, reemplazo o ventaja competitiva).	* Pérdida de confidencialidad de información clasificada como confidencial dentro de la organización, producto de ataques a los sistemas de información, errores o accesos no autorizados por parte de personal interno. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	Pérdida de integridad que afecta servicios de negocio no críticos con posible impacto en los servicios críticos, producto de ataques a los sistemas de información o errores humanos, por parte de terceros y/o personal interno. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	Evento de conocimiento público que NO genera interés público e interés de los medios. * Impacto grave para la imagen de la empresa, No existe cobertura amplia en los medios de comunicación, redes sociales y/o pérdida de participantes. * Involucramiento de algún organismo regulador, del Estado y reclamos de participantes.
Moderado (3)	* Sin presidio ni reclusión. * Observaciones del regulador por falta de forma o fondo al cumplimiento normativo.	* Pérdida de disponibilidad que afecta servicios de soporte a la organización. * Degradación que afecta servicios de negocios no críticos. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva).	Pérdidas por incidentes operacionales: Hasta: 30 UF Ver pérdidas económicas (productividad, multas, respuesta, reemplazo o ventaja competitiva).	* Pérdida de confidencialidad de información de uso interno debido a un error no intencional por parte de personal interno. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	* Pérdida de integridad que afecta a servicios de soporte a la organización por error no intencional. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	* Evento que no es de conocimiento público, el alcance se limita a la industria y participantes. Impacto de mediana importancia en la imagen de la empresa ya que existe sin tener exposición en medios de comunicación (Email, Whatsapp, otros)
Leve (2)		* Degradación de servicios de soporte a la organización. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	Sin Pérdidas	* Pérdida de confidencialidad que no afecta lo establecido en la Política de Clasificación de Información. * Divulgación no intencionada de información crítica. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva).	* Pérdida de integridad de la información sin impacto en los servicios de negocio, debido a errores en la información. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	* Impacto poco significativo, no tiene cobertura en los medios de comunicación ni dentro de la industria. La imagen de la compañía no se ve afectado por la interrupción parcial del servicio. Reclamos aislados sin mayor repercusión.

POLITICA GENERAL CORPORATIVA DE RIESGO OPERACIONAL

Control de Documentación
Referencia: SGIR.5.2_POLI03
Página 7 de 14

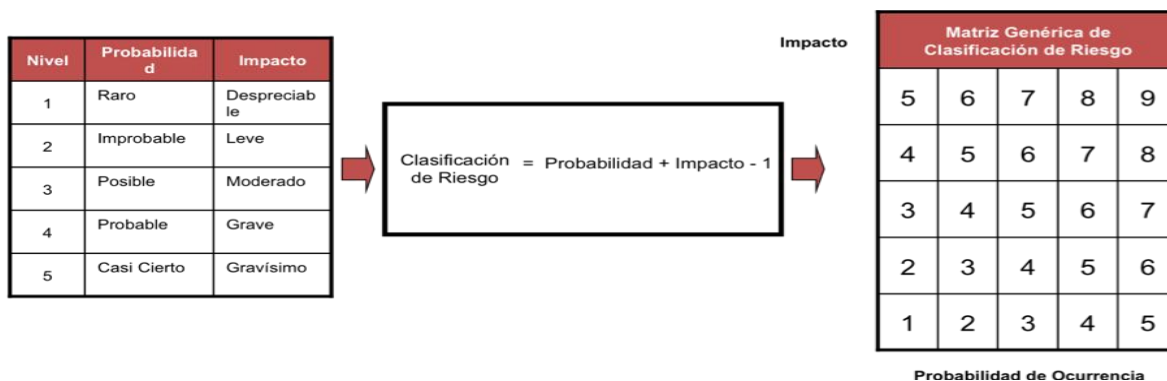
Niveles / Criterios	Cumplimiento	Pérdida Disponibilidad	Pérdida Económica	Pérdida de Confidencialidad	Pérdida de Integridad	Pérdida Reputacional
Despreciable (1)		*Sin pérdida de disponibilidad o degradación en los servicios. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	Sin Pérdidas	* Sin pérdida en la confidencialidad de la información. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	* Sin pérdida en la integridad de la información. Ver pérdidas económicas (productividad, respuesta, reemplazo o ventaja competitiva)	* Sin pérdida reputacional.
			Productividad: Pérdida que resulta de una incapacidad operativa para entregar productos o servicios, o de salarios perdidos debido a trabajadores inactivos. Respuesta: Pérdida asociada con los costos de gestión de un evento. Reemplazo: Pérdida que resulta de que una organización tenga que reemplazar activos de capital. Ventaja Competitiva: Pérdidas resultantes de la propiedad intelectual u otros diferenciadores clave de competitividad que han sido comprometidos o dañados. Multas y Sentencias: Costos impuestos a la organización a través de acciones civiles, penales o contractuales.			Reputación: Pérdida resultante de la percepción de un grupo de interés externo de que el valor de la organización ha disminuido y/o que su responsabilidad ha aumentado

Los criterios anteriores de probabilidad e impacto son válidos para las categorías de riesgos de Operador e Infraestructura, entre los que se encuentran los tipos de riesgo operacional (riesgo de continuidad de negocios, riesgo de seguridad de la información, riesgo de calidad y riesgo de fraude y ciber riesgo).

En la valoración de los riesgos, se utiliza como base una matriz general de 5 + 5 y la fórmula Clasificación de Riesgo= nivel de probabilidad + nivel de impacto -1.

El resultado obtenido se clasifica dentro de un nivel de la matriz, de acuerdo con el nivel de impacto y probabilidad del riesgo.

La siguiente figura grafica la matriz de Clasificación de Riesgos Impacto-Probabilidad de Ocurrencia.



Los criterios antes mencionados serán acompañados de juicio experto por parte del responsable del análisis.

Evaluación de Riesgo

Se evalúa el riesgo estimado y clasificado comparándolo con el siguiente criterio de aceptación del riesgo:

1. La aceptación de riesgos en cada categoría se lleva a cabo de acuerdo a las estrategias de mitigación para cada una de ellas.
2. En general, en la organización se aceptan riesgos de nivel 3 e inferior de la Matriz de General de Clasificación de Riesgo Impacto-Probabilidad.
3. La evaluación semi-cuantitativa de riesgos, definida arriba al inicio de esta sección, será complementada por una evaluación cuantitativa utilizando la metodología FAIR (ver documento Manual Metodológico de FAIR).
4. La organización definió un apetito por riesgo bajo, es decir, no superior a un tercio de la capacidad restante después del monto de conservación. Esto resultó en un riesgo aceptado de USD 1,6 millones.

Tratamiento de Riesgos

En caso de que el nivel del riesgo estimado sea mayor al nivel de aceptación del mismo, se debe tomar la primera decisión de riesgos, que consiste en elegir una opción de tratamiento de riesgos.

Las opciones de tratamiento de riesgos son:

1. Reducción o mitigación del riesgo
2. Retención del riesgo
3. Evitar el riesgo
4. Transferir el riesgo

Todos los riesgos con clasificación de alto impacto y alta probabilidad de ocurrencia deben contar con respuestas al riesgo y, en caso de asumir el riesgo, se debe contar con acciones mitigadoras explícitas que reduzcan el riesgo residual lo más posible. Esta misma definición aplica para los riesgos con alto impacto y baja probabilidad de ocurrencia, los que deben además contar con el respectivo Plan de Contingencia en caso de ocurrir.

Si se escoge como opción reducir o mitigar el riesgo, se debe confeccionar un Plan de Tratamiento de Riesgos (PTR) para cada categoría de riesgos. Un PTR corresponde a un listado de controles que permite mitigar el riesgo identificado.

El PTR del Riesgo Operacional es el agregado de controles de los riesgos relacionados a los sistemas (tecnología), procesos, persona y eventos externos que pueden producir una falla o interrupción de los servicios de la organización, riesgos que son tratados en las categorías de Seguridad de la Información, Continuidad y Calidad.

El PTR se debe confeccionar:

1. Seleccionando los controles específicos ejecutados en los procesos, que mitiguen los riesgos identificados.
2. Estimando en cuánto se disminuye la probabilidad y el impacto del riesgo con la acción de los controles seleccionados, de manera de reducir el riesgo a los niveles de aceptación.
3. Si los controles ya establecidos no son suficientes, se deben crear controles adicionales que aseguren el nivel de aceptación.
4. Finalmente, se monitorea la ejecución de los controles en la frecuencia definida para prevenir los riesgos.

Una vez confeccionados los PTR, éstos deberán ser sometidos al proceso de validación y aprobación definido en el Marco de Gestión de Riesgos de la organización. En caso de requerirse, la evaluación de los planes de tratamiento de riesgo puede ser complementada con un análisis cuantitativo.

Posteriormente, una vez elegida la opción de tratamiento de riesgos, se debe tomar la segunda decisión de riesgos, que es aceptar o no el riesgo residual resultante del tratamiento aplicado.

La opción de retención se tomará cada vez que el nivel de riesgo inherente sea igual o inferior al nivel de riesgo aceptado. Para esta opción no es necesario incluir un Plan de Tratamiento de Riesgos.

En caso de que se opte por la opción de evitar o compartir el riesgo, se debe plantear la opción al Comité de Riesgo Operacional, para que este determine si la opción puede ser realizada, o en su defecto determinar qué acciones deben ser realizadas.

VI.- ROLES Y RESPONSABILIDADES

Los roles y responsabilidades se encuentran definidos de acuerdo con la siguiente relación de rol y documento:

Rol	Documento
Directorio	Manual de Gobierno
Comités de Gobierno	Estatutos de Comité
Organización	Estructura Organizacional

VII.- CONTROL DE VERSIONES

El Directorio es el dueño de este documento. El Gerente General es el encargado de asegurar que la Política sea revisada al menos anualmente por el Directorio. El Gerente de Riesgo Operacional es el responsable de asegurar que la versión vigente de esta política se encuentre disponible y también es responsable de realizar el proceso de revisión con partes involucradas que identifiquen la necesidad de cambios en la Política. Esta Política es de Nivel 1, por lo tanto, debe ser aprobada por el Directorio.

La versión de esta política fue aprobada por el Directorio de Comder según consta en Acta de sesión n°154, con fecha 16/06/2026. Esta política es emitida en base a versiones controladas bajo la autorización del Gerente General

La versión vigente de este documento está disponible para el personal en el Portal de Gestión del Conocimiento.

VIII.- HISTORIAL DE CAMBIO

N° Versión	Fecha	Descripción
1.0	17/03/2015	Emisión Inicial
1.1	19/04/2016	Adecuación del Propósito de la Política. Inclusión de la definición de Apetito de Riesgo. Actualización de los servicios de negocios entregados por ComDer (se alinearon a los definidos en la APO09.3_POLI01Política de SLA para Participantes). Inclusión del Riesgo de Fraude en la definición del Riesgo Operacional y en la Matriz de impacto. Cambios de Forma como: Nombre del Comité de Riesgos no financiero por Comité de Gestión Operacional del SCC y Reemplazo del diagrama de Roles y Responsabilidades.

POLITICA GENERAL CORPORATIVA DE RIESGO OPERACIONAL

Control de Documentación

Referencia: SGIR.5.2_POLI03

Página 12 de 14

Nº Versión	Fecha	Descripción
1.2	18/05/2016	Cambio en código de encabezado
1.3	20/05/2016	Corrección signo "x" a signo "+", en sección de Análisis de riesgo, párrafo de Valoración de riesgo Inclusión de link a Mapa de Riesgo
1.4	18/04/2017	Se reemplaza la definición de Fraude con la definición de COSO 2013. Se agregan las definiciones de los otros riesgos operacionales En la matriz de impactos, se eliminan los riesgos no operacionales, los que trasladaron a la Política General de Riesgos. También, se agregaron los niveles de impacto para el riesgo de Fraude.
1.5	17/04/2018	Revisión sin modificaciones
1.6	22/05/2019	Se modifica SVS por CMF. Se incorpora definición de apetito por riesgo y tolerancia al riesgo de acuerdo con FAIR. Se incorpora regla con metodología FAIR (nº3) y regla relacionada a la promoción de la cultura de riesgos (nº12). Se incorporan acciones rol de Colaboradores Se modifica rol de auditoría interna Se incorpora FAIR como parte de la evaluación de riesgos. Se elimina rol del Gerente de Riesgo de la política Se incorpora descripción de opciones de tratamiento de riesgo
1.7	19/05/2020	Se incorporan criterios de impacto para Ciber Riesgos Se modifica el nivel de impacto en pérdidas de confidencialidad. Se modifica nivel de impacto para la confidencialidad de la información. Se incorpora al Subgerente de Riesgo Operacional y OSCC como responsable de actualización de la política
1.8	18/05/2021	Se incorpora párrafo indicando que el Comité de Riesgo Operacional aprueba el nivel de riesgo aceptado y tolerancia en términos cuantitativos. Se indica que se realizará una gestión de riesgos por niveles Se incorpora en roles y responsabilidades al Comité de Riesgo Operacional Se incorpora responsabilidad de informar a Comité de Auditoría por parte de Auditoría Se modifican responsables de la revisión y de mantener la política.
1.9	22/02/2022	Se incorporan modificaciones en el capítulo de roles y responsabilidades tanto para el Comité de Gestión Operacional como para el de Riesgo Operacional y Riesgos Operador.

POLITICA GENERAL CORPORATIVA DE RIESGO OPERACIONAL

Control de Documentación
Referencia: SGIR.5.2_POLI03
Página 13 de 14

Nº Versión	Fecha	Descripción
		En el punto Tratamiento de Riesgos, a raíz de una observación realizada por la CMF, se incorpora qué es un PTR. Estas modificaciones fueron aprobadas por el Directorio en el Acta N°102, con fecha 01 de marzo de 2022.
2.0	22/06/2022	Se define la política a un nivel organizacional Se elimina detalle de servicios y se hace referencia a política de SLA. Se reemplaza Circular 1939 por normativa. Se incorpora utilización de juicio experto en el proceso de análisis. Se actualiza referencia a norma ISO 22301 Se modifica aprobación por validación del Comité de Gestión Operacional, en relación a los PTR definidos. Se modifica regla 6, indicando al Comité de Riesgo Operacional como aprobador de los PTR y al Comité de Gestión como aprobador de los Planes de Continuidad.
2.1	20/06/2023	Se corrige la definición de Riesgo Operacional de CPMI-IOSCO. Se modifica la Regla n°8, indicando que de esta Política se desprende un conjunto de políticas específicas/propias en los ámbitos de la gestión del riesgo operacional.
2.2	19/07/2024	Se prescinde de IMERC para efectos de esta política. En la sección III: Definiciones, se actualiza definición de Riesgo Operacional y de Apetito de Riesgo, de acuerdo a la NCG N°510. En la sección IV. Reglas: - Regla 1., se incorpora referencia a la sección V. Criterios de Evaluación y Tratamiento de Riesgo. - Regla 8., se incorpora el ámbito de externalización y contratos a terceros. En la sección V. Criterios de Evaluación y Tratamiento de Riesgo – Evaluación de Riesgos, se detalla el criterio de riesgo aceptado cuantitativo.
2.3	17-12-2024	Se modifica riesgo aceptado de la organización Esta modificación fue aprobada por el Directorio en el Acta N°136, con fecha 17 de Diciembre de 2024.
2.4	18-03-2025	Se modificó la matriz de severidad e impacto. Esta modificación fue aprobada por el Directorio en el Acta N°139, con fecha 18 de Marzo de 2025.
2.5	17-06-2025	Revisión sin cambios aprobada por el Directorio en el acta N°142, con fecha 17 de junio de 2025.
2.6	16-06-2026	Se modifica redacción de reglas 3 y 5. En la regla 6, se actualiza que el Directorio es el encargado de aprobar los planes. En la sección V.- Criterios de Evaluación y Tratamiento de Riesgo, se modifica redacción y se elimina sección de estrategias de tratamiento por tipo de riesgo.

