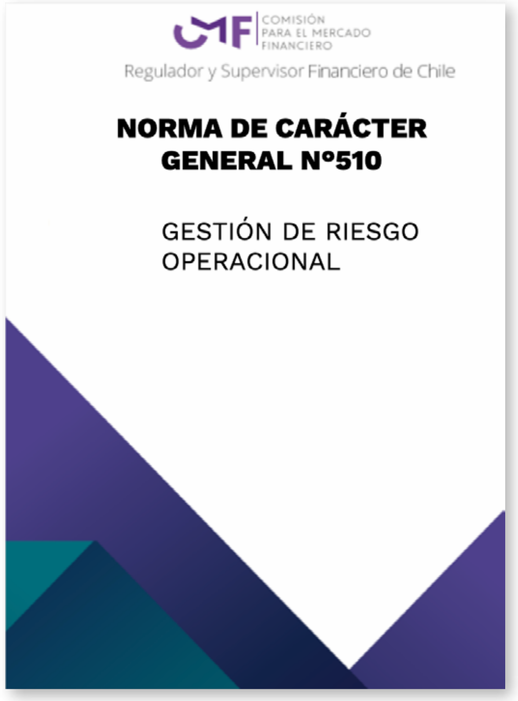
NCG 510:
Gestión de Riesgo Operacional

Diciembre 2025

ARMMA

Resumen Ejecutivo



Objetivo

Instrucciones respecto a la gestión del riesgo operacional en Instituciones no bancarias.

Pilares del Riesgo Operacional

- Gobierno y gestión general.
- Seguridad de la información y ciberseguridad.
- Continuidad del negocio.
- Externalización de servicios.
- Información de incidentes operacionales.

Entidades

- Administradoras Generales de Fondos (AGF).
- Bolsas de Valores.
- Bolsas de Productos.
- Sociedades adm. de Sistemas de Compensación y Liquidación de Instrumentos Financieros.
- Entidades de Déposito y Custodia de Valores.

Normativas Complementarias

NCG 510
Vigencia: Feb-2025

NCG 529
Modificaciones + Reportes de incidentes operacionales

NCG 531
Cambia NCG 529 para vigencia Jul-2025

NCG 510: Pilares del Riesgo Operacional

Gobierno y Gestión General

1. **Formalización de Políticas:** Las políticas y procedimientos de gestión de riesgo operacional deben estar formalmente establecidas, documentadas y formar parte de la gestión de riesgos integral.
2. **Aprobación del Directorio:** Las políticas deben ser aprobadas por el directorio u órgano equivalente.
3. **Apetito por Riesgo:** Se deben establecer los niveles de apetito por riesgo definidos por el directorio, lo cual determinará la necesidad de un plan de tratamiento (evitar, reducir, transferir o aceptar).
4. **Recursos y Personal:** El directorio debe dotar a las instancias pertinentes de los recursos y personal necesarios en función del volumen y complejidad de las operaciones.
5. **Medición y Monitoreo:** Se requiere contar con indicadores claves de medición del riesgo operacional, consistentes con la metodología de evaluación integral, para establecer niveles de alerta y evaluar la eficacia de los controles.

Seguridad de la Información y Ciberseguridad

ARMMA

1. **Política de Seguridad:** Contar con una política que considere la implementación y mantención de un sistema de gestión de seguridad de la información y ciberseguridad para resguardar la disponibilidad, confidencialidad e integridad de los activos.
2. **Gestión de Activos Críticos:** Definir los activos de información críticos, implementar un inventario continuo y clasificarlos según disponibilidad, confidencialidad e integridad.
3. **Controles de Acceso:** Implementar controles de acceso a sistemas e infraestructura (física y lógica), privilegiando el uso de mecanismos de autenticación multifactor para sistemas críticos.
4. **Detección y Protección Proactiva:** Implementar herramientas como firewalls (incluyendo WAF), sistemas de prevención de intrusos (IPS), sistemas de prevención de pérdida de datos (DLP), antivirus, etc., diseñadas según la complejidad de las operaciones.
5. **Respaldo y Recuperación:** Implementar procesos de administración de respaldos que aseguren la disponibilidad, confidencialidad e integridad, manteniéndolos en ambientes libres de códigos maliciosos y en instalaciones distintas a los sitios de producción.
6. **Pruebas de Seguridad:** Ejecutar pruebas periódicas (al menos anuales) para identificar amenazas y vulnerabilidades, tales como pentesting, red team o ethical hacking, y reportar sus resultados al directorio.
7. **Roles Especializados (Bolsas/Depósito/Compensación):** Contar con una persona encargada de la seguridad de la información independiente de las áreas operativas y de auditoría interna.

NCG 510: Pilares del Riesgo Operacional

Continuidad del Negocio

1. **Análisis de Impacto:** Realizar o actualizar anualmente un Análisis de Impacto de Negocio (BIA) para identificar procesos críticos, el impacto de su interrupción y los recursos necesarios.

2. **Definición de Métricas:** Basado en el BIA, se deben determinar los:
   - Tiempos Máximos Tolerables de Interrupción (MTPD).
   - Tiempos Objetivo de Recuperación (RTO).
   - Puntos Objetivo de Recuperación (RPO).

3. **Niveles Mínimos Aceptables de Operación (MBCO).**

4. **Planes y Sitio Secundario:** Contar con un Plan de Continuidad de Negocio y Recuperación de Desastres (PCN/DRP) aprobado anualmente. Se debe disponer de un sitio secundario (físico o en la nube) que permita reanudar la operación.

5. **Pruebas Anuales:** Probar anualmente el PCN/DRP en escenarios de riesgo que se asimilen a eventos reales, incluyendo ataques cibernéticos, desastres y otras contingencias.

6. **Requisitos Críticos (Compensación/Depósito/Bolsas):** El PCN/-DRP debe permitir la reposición de servicios con un RTO no mayor a 2 horas y un RPO cercano a 0.

Externalización de Servicios

1. **Gestión de Riesgos de Proveedores:** Considerar los servicios externalizados en los procesos de gestión de riesgo. Analizar riesgos como el de sustitución, intervención, subcontratación y concentración.

2. **Política de Externalización:** Contar con una política que defina la estructura de gobierno, los objetivos, los niveles de apetito por riesgo y los procedimientos para la determinación de servicios críticos.

3. **Contratación Mínima:** Los contratos deben incluir requisitos de seguridad de la información, ciberseguridad, continuidad de negocios, y la obligación de que el proveedor cumpla con procedimientos de gestión de incidentes y continuidad de negocios.

4. **Derecho de Auditoría:** La entidad debe poder pactar con el proveedor la realización de auditorías, siendo la entidad la responsable final por la calidad del servicio externalizado.

5. **Registro de Servicios:** Mantener un registro de servicios externalizados, incluyendo si se realiza subcontratación en cadena o si se utiliza la nube, el cual debe estar disponible para la Comisión.

6. **Cloud Computing:** Si se contratan servicios en la nube, se requiere un análisis reforzado de riesgos, considerando la jurisdicción de procesamiento, la existencia de normas de protección de datos personales, y el uso de técnicas de encriptación.

NCG 510: Pilares del Riesgo Operacional

Información y Reporte de Incidentes Operacionales

1. **Reporte a la CMF:** Se deben comunicar a la Comisión (CMF) los incidentes operacionales que afecten la continuidad del negocio, la información de la entidad o clientes, y la calidad de los servicios (ej. fallas de sistemas, ataques cibernéticos, pérdidas de información).

2. **Plazos Estrictos:** El plazo máximo de notificación es de 15 minutos para Bolsas y Sociedades Administradoras de Sistemas de Compensación/Depósito, y de 2 horas para Administradoras Generales de Fondos.

3. **Base de Datos:** Mantener una base de datos de incidentes y otra de pérdidas operacionales para el mejoramiento continuo.

4. **Pérdidas Financieras:** Reportar semestralmente a la CMF las pérdidas operacionales individuales mayores a 150 Unidades de Fomento (UF).

Ámbitos de Gestión de Riesgo Operacional

MARCO DE RIESGO OPERACIONAL

Gobierno y gobernanza – Políticas y procedimientos – Metodologías y modelos – Reportes regulatorios y de gestión – Formación y cultura – Tecnología y Soporte

Evaluación y Control

- Mapa de procesos, riesgos y controles.
- Matriz de autoevaluación y testeo de controles.
- Seguimiento de indicadores (KRI) y planes de acción.
- Captura, análisis de eventos y de escenarios extremos.
- Evaluación de proyectos, nuevos productos y servicios.

Riesgos Temáticos

- Gestión de Proveedores.
- Continuidad del Negocio.
- Riesgo Tecnológico y Ciberseguridad.
- Gestión del Fraude (interno/externo).
- Seguimiento eventos y pérdidas operacionales.
- Riesgos No Financieros (reputacional, ESG, otros).

Capital por RO y Apetito por Riesgo

- Cálculo de Capital por Riesgo Operacional (APRO).
- Pruebas de Tensión RO y Backtesting RO.
- Integración con la Medición Integral de Riesgos (MIR).
- Integración con el Marco de Apetito al Riesgo (MAR).
- Perfil de Riesgo e integración con el Informe de Autoevaluación.

Integración Metodológica

- Visión integral de riesgos y controles.
- Relación Riesgo – Evento – Impacto.
- Analítica de datos e inteligencia operacional.
- Consistencia con otras metodologías relacionadas.
- Registros contables de pérdidas ajustado a Norma.

HERRAMIENTAS TECNOLÓGICAS Y AUTOMATIZACIÓN

SUPERVISIÓN Y AUDITORÍA

SOPORTE REGULATORIO: NCG 510

Cómo te podemos ayudar en ARMMA?

Entendimiento y diagnóstico*

(4 semanas)

- Entendimiento de impacto y áreas involucradas.
- Evaluación AS IS / TO BE.
- Identificación de brechas y planes de remediación.
- Generación de plan director con responsables y áreas.

Apoyo según necesidad

- Gobernanza y documentación.
- Analisis de impacto y Riesgo.
- Planificación de Continuidad.
- Pruebas de Resiliencia.
- Gestión de Ciberseguridad.
- Externalización de Servicios.
- Seguridad de la Información.
- Validación Externa.
- Evaluación de Estructura.

Dikson Pradenas
Partner & Co-Founder

Karla Bittencourt
Sales Manager

Ma. Josefa González
Especialista Experta

ARMMA | Advisory Services | Technology and Analytics Solutions

Acerca de ARMMA
ARMMA es una consultora en gestión de riesgos y soluciones tecnológicas. Nuestros servicios ayudan a impulsar el éxito sostenible de nuestros clientes en diversas industrias. Nos comprometemos a trabajar en equipo para cumplir con nuestras promesas hacia todos los interesados. A través de nuestro trabajo, desempeñamos un papel en la mejora de la estabilidad financiera y la promoción de la innovación para nuestros clientes y nuestro equipo. ARMMA CONSULTING LIMITADA opera como una firma de consultoría independiente, proporcionando servicios de asesoría y tecnología adaptados a las necesidades únicas de nuestros clientes. Para más información sobre nuestra organización, visita armma.cl.

Los Militares 5953, Piso 5, Las Condes, Santiago, Chile.

armma.cl

ARMMA

CONTÁCTANOS

Dikson Pradenas
Partner & Co-Founder
ARMMA Consulting
dpradenas@armma.cl
+569 9748 7311

Karla Bittencourt
Sales Manager
ARMMA Consulting
kbittencourt@armma.cl
+569 8292 8634

Ma. Josefa González
Especialista Experta
ARMMA Consulting
jgonzalez@armma.cl
+569 9217 0058