**REGLAMENTO INTERNO PARA LA GESTIÓN DEL RIESGO OPERATIVO**

**DOCUMENTO CONTROLADO**

**Autor de documento original: LOGC750219**

**Copia controlada No.: Original**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Nombre** | | **Puesto o Cargo** | | **Firma** | | **Fecha** |
| **Elaborado:** | Angeles Beatriz Guillen A. | | Subgerente Nacional de Gestión de Riesgos | |  | | 07/03/2023 |
| **Revisado:** | Comité de Gestión Integral de Riesgos | | N/A | | N/A | | 17/03/2023 |
| **Aprobado:** | Directorio | | N/A | | N/A | | 17/03/2023 |
| **Acta y Resolución de Directorio** | | Acta N° 09/2023  Resolución N° 35/2023 | | **Fecha inicio de vigencia** | | 27/03/2023 | |

**Control de Cambios**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Estado** | **Versión** | **Acta y Res. de Aprobación** | **Fecha de Aprobación** | **Fecha de Inicio de vigencia** | **Descripción del cambio realizado** |
| No vigente | 1.0.16 | Acta 17/2015 | 16/10/2015 |  | Primera versión |
| No vigente | 2.0.16 | Acta 20/2016 | 16/09/2016 |  | Lista de Distribución del documento / Cambio en metodología de definición de criticidad de procesos / Inclusión de análisis BIA en políticas de medición cualitativa del riesgo operacional / Desarrollo metodológico del análisis BIA / Inclusión de metodología para la evaluación y análisis del riesgo tecnológico / Medición Cualitativa de Riesgo Operacional / Criterios de codificación |
| No vigente | 2.1.16 | AEA-08/2016 | 24/06/2016 |  | Adecuación nueva estructura organizacional |
| No vigente | 3.0.17 | DIR/CIDRE/IFD 14/2017 | 17/04/2017 |  | Criterios para registro de pérdidas / Inclusión de identificación de “Eventos críticos” en metodología BIA / Elaboración Planes de Contingencia y Continuidad / Definición de Macroprocesos vigentes / Flujo evaluación cualitativa del riesgo operacional |
| No vigente | 3.1.17 | DIR/CIDRE/IFD 31/2017 | 13/10/2017 |  | Referencia a documento GR.PP.003.2 / Transferencia de metodologías de Anexos a documento GR.PP.003.1. |
| No vigente | 4.0.18 | DIR/CIDRE/IFD 06/2018 | 16/02/2018 | 16/02/2018 | Inclusión de definiciones |
| No vigente | V1.09.19 | Acta N° 27/2019  Resolución N° 78/2019 | 13/09/2019 | 01/11/2019 | Cambio de formato a partir de documento original  Manual de Políticas y Procedimientos de Gestión de Riesgo Operacional.  Ajustes y modificaciones generales a la reglamentación y a diferentes conceptos relacionados al Marco Interno para la Gestión Integral de Riesgos (MIGIR).  **Ratificación**: Directorio Acta N° 27/2020, Resolución N° 120/2020, Fecha 16/10/2020. |
| No vigente | V1.04.21 | Acta N° 13/2021  Resolución N° 45/2021 | 15/04/2021 | 24/06/2021 | Capítulo III, Artículo 5\*, Inciso 3). Modificación a la definición de evento crítico |
| No vigente | V1.02.22 | Acta N° 06/2022  Resolución N° 29/2022 | 18/02/2022 | 02/03/2022 | Inclusión de definición de “Error operativo” y “Hallazgo”; Consideración de la función del hallazgo para el registro de eventos |
| Vigente | V1.03.23 | Acta N° 09/2023  Resolución N° 35/2023 | 17/03/2023 | 27/03/2023 | Modificación en Capítulo III. |

**CLASIFICACION DE LA INFORMACIÓN:**

|  |  |
| --- | --- |
| **Confidencial** - Es el más alto nivel de clasificación de la información; el presente documento se encuentra estrictamente limitado para su acceso a un número restringido de personas, que se encuentran detalladas en la Lista de Distribución de este documento. | **[ ]** |
| **Reservada** - Información cuya divulgación debe ser restringida únicamente al personal que la requiere conocer (unidad organizacional y/o proceso). La divulgación externa es posible previa autorización de la instancia responsable de la seguridad de información de la entidad. | **[ x ]** |
| **Pública** - Información de uso general que por su contenido o contexto no requiere de protección especial y su distribución pública es permitida o por la aprobación de las instancias que corresponda o por política. | **[ ]** |

**LISTA DE DISTRIBUCIÓN:**

| **Área** | **Cargos y/o Funcionarios** |
| --- | --- |
| Directorio | Directores |
| Comité de Gestión Integral de Riesgos | Miembros del comité |
| Gerencia General | Gerente General |
| Gerencia Nacional de Servicios Financieros | Gerente Nacional de Servicios Financieros y personal dependiente |
| Gerencia Nacional de Finanzas y Administración | Gerente Nacional de Finanzas y Administración, y personal dependiente |
| Gerencia Nacional de Planificación e Innovaciones | Gerente Nacional de Planificación e Innovaciones y personal dependiente |
| Subgerencia Nacional de Auditoría Interna | Subgerente Nacional de Auditoría interna y personal dependiente |
| Subgerencia Nacional de Operaciones y Captaciones | Subgerente Nacional de Operaciones y Captaciones y personal dependiente |
| Subgerencia Nacional de RR.HH, Organización y Métodos | Subgerente Nacional de RR.HH., Organización y Métodos y personal dependiente |
| Subgerencia Nacional de Gestión de Riesgos | Subgerente Nacional de Gestión de Riesgos y personal dependiente |
| Subgerencia Nacional de Asesoría Legal | Subgerente Nacional de Asesoría Legal y personal dependiente |
| Unidad de Prevención y Cumplimiento | Jefe Nacional de Prevención y Cumplimiento |
| Unidad de Servicios Informáticos | Jefe Nacional de Servicios Informáticos |

## CONTENIDO

[CONTENIDO 4](#_Toc25252490)

[**1.** **Objetivo.** 6](#_Toc25252491)

[**2.** **Alcance y/o Aplicabilidad.** 6](#_Toc25252492)

[**3.** **Términos, definiciones y abreviaturas.** 6](#_Toc25252493)

[**4.** **Desarrollo.** 9](#_Toc25252494)

[PARTE I – DE LA GESTIÓN DEL RIESGO OPERATIVO 9](#_Toc25252495)

[CAPÍTULO I – MARCO INTERNO PARA LA GESTIÓN INTEGRAL DE RIESGOS 9](#_Toc25252496)

[ARTÍCULO 1° (Marco Interno para la Gestión Integral de Riesgos) 9](#_Toc25252497)

[CAPÍTULO II – ESTRATEGIA PARA LA GESTIÓN DE RIESGO OPERATIVO 9](#_Toc25252498)

[ARTÍCULO 1° (Objetivos de la gestión del riesgo operativo) 9](#_Toc25252499)

[ARTÍCULO 2° (Proceso de gestión de riesgo operativo) 9](#_Toc25252500)

[ARTÍCULO 3° (Organización de la gestión del riesgo operativo) 10](#_Toc25252501)

[CAPÍTULO III – PROTOCOLOS PARA LA GESTIÓN DE RIESGO OPERATIVO 10](#_Toc25252502)

[ARTÍCULO 1° (Políticas y procedimientos) 10](#_Toc25252503)

[PARTE II – DE LAS ETAPAS DE LA GESTIÓN DEL RIESGO OPERATIVO 11](#_Toc25252504)

[CAPÍTULO I – IDENTIFICACIÓN 11](#_Toc25252505)

[ARTÍCULO 1° (Identificación de riesgo operativo) 11](#_Toc25252506)

[CAPÍTULO II – MEDICIÓN (ANÁLISIS Y EVALUACIÓN DE RIESGOS) 11](#_Toc25252507)

[ARTÍCULO 1° (Medición del riesgo operativo) 11](#_Toc25252508)

[ARTÍCULO 2° (Base de datos de eventos de riesgo operativo) 11](#_Toc25252509)

[ARTÍCULO 3° (Riesgo por punto de atención financiera) 12](#_Toc25252510)

[ARTÍCULO 4° (Riesgo de continuidad del negocio) 12](#_Toc25252511)

[ARTÍCULO 5° (Riesgo tecnológico) 12](#_Toc25252512)

[ARTÍCULO 6° (Pruebas de estrés, escenarios o sensibilidad) 12](#_Toc25252513)

[CAPÍTULO III – MONITOREO 12](#_Toc25252514)

[ARTÍCULO 1° (Monitoreo del riesgo operativo) 12](#_Toc25252515)

[ARTÍCULO 2° (Gestión del apetito de riesgo operativo y límites internos) 13](#_Toc25252516)

[ARTÍCULO 3° (Visitas e inspecciones de riesgo operativo y seguridad física) 13](#_Toc25252517)

[ARTÍCULO 4° (Registro y seguimiento a eventos de riesgo operativo) 13](#_Toc25252518)

[ARTÍCULO 5° (Reporte de eventos críticos) 13](#_Toc25252519)

[CAPÍTULO IV – CONTROL Y MITIGACIÓN DE RIESGO OPERATIVO (TRATAMIENTO) 14](#_Toc25252520)

[ARTÍCULO 1° (Control del riesgo operativo) 14](#_Toc25252521)

[ARTÍCULO 2° (Control y mitigación de riesgo operativo) 14](#_Toc25252522)

[ARTÍCULO 3° (Gestión de la continuidad del negocio) 14](#_Toc25252523)

[CAPÍTULO V – DIVULGACIÓN (COMUNICACIÓN Y CONSULTA) 15](#_Toc25252524)

[ARTÍCULO 1° (Divulgación del riesgo operativo) 15](#_Toc25252525)

[ARTÍCULO 2° (Cultura de riesgo operativo) 15](#_Toc25252526)

[**5.** **Documentos Referenciales.** 15](#_Toc25252527)

[**6.** **Anexos.** 16](#_Toc25252528)

## **Objetivo.**

Contar con un proceso y una estrategia formal para la gestión del riesgo operativo que permita a la institución identificar, medir, monitorear, controlar, mitigar y divulgar las exposiciones de riesgo operativo que se están asumiendo.

## **Alcance y/o Aplicabilidad.**

Este documento es parte del “Manual de Gestión Integral de Riesgos”. Alcanza y aplica a todas las actividades, procesos y personas que forman parte de CIDRE IFD y que se relacionan a la gestión del riesgo operativo.

## **Términos, definiciones y abreviaturas.**

**Alta Gerencia:** Instancia conformada por Gerente General, Gerente Nacional de Finanzas y Administración, Gerente Nacional de Servicios Financieros y Gerente Nacional de Planificación e Innovaciones.

**Apetito de Riesgo:** Es la cantidad de riesgo que CIDRE IFD se dispone a asumir en su búsqueda de rentabilidad y solvencia.

**Central de Información de Riesgo Operativo (CIRO):** Sistema de información administrado por ASFI, que consolida los datos proporcionados por las entidades supervisadas, con relación a los eventos de riesgo operativo y pérdidas.

**Declaración de Apetito de Riesgo (DAR):** Documento a través del cual CIDRE IFD comunica el nivel máximo de riesgo que se dispone a asumir a fin de alcanzar sus objetivos estratégicos y sin poner en riesgo su solvencia.

**Errores operativos:** Son aquellos que se cometen de forma involuntaria al realizar las acciones necesarias para llevar adelante una determinada tarea, correspondiendo a aquellos errores cometidos por personas de manera involuntaria y sin que generen ningún daño de tipo económico.

**Etapa de Monitoreo:** Hace referencia al proceso continuo de monitoreo y revisión de las políticas, procedimientos y desempeño de la Gestión Integral de Riesgos, al desempeño de los planes de tratamiento de riesgo y su consecuente impacto sobre los Niveles de Severidad (Riesgo), y al desempeño de los indicadores o unidades de medición (IUM) respecto de los límites máximos y/o mínimos de exposición dispuestos de manera interna o externa, que hacen parte del perfil de riesgo.

**Etapa de Control de Riesgos:** La etapa de control de riesgos forma parte del proceso de Tratamiento de Riesgos. Esta etapa se define como aquella en la que se desarrollan estrategias, ejecutan actividades, y planifican controles con la finalidad de disminuir la probabilidad de ocurrencia de un evento capaz de originar pérdidas a la entidad. Asimismo, en esta etapa de la gestión de riesgos, como mecanismo de control, se determinan los límites de exposición al riesgo y el perfil de riesgo.

**Evento de riesgo operativo:** Es un incidente o conjunto de ellos, que provocan que los resultados difieran de los esperados, debido a procesos defectuosos, recursos humanos inadecuados, fallos en los sistemas o por causas externas.

**Evento crítico:** Es un incidente o conjunto de ellos, que provocan que los resultados difieran de los esperados, debido a procesos defectuosos, recursos humanos inadecuados, fallos en los sistemas o por causas externas, que superen el apetito al riesgo operativo de la entidad.

**Fuentes de Riesgo:** Se refiere a los activos clave, procesos u objetivos que dan nacimiento a la incertidumbre y a través de los cuales se identifican los riesgos a los que se expone CIDRE IFD.

**Gestión Integral de riesgos:** Es el proceso de identificar, medir, monitorear, controlar, mitigar y divulgar todos los riesgos a los cuales CIDRE IFD se encuentra expuesto, en el marco del conjunto de objetivos, políticas, procedimientos y acciones establecidas por la entidad para este propósito.

**Hallazgo:** Se refiere al caso en que un evento o error operativo es identificado a través de hallazgos formalizados a través de documentos oficiales emitidos por instancias internas o externas de control o regulación, como auditoría interna o externa, gestión de riesgos y la autoridad de supervisión, entre otros.

**Línea de negocio:** Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo definido en la planificación estratégica de la institución.

**Proceso:** Es un conjunto de actividades planificadas y estructuradas que implican la participación de un número de personas y de recursos materiales coordinados para conseguir un objetivo previamente identificado, que permite desarrollar con regularidad las operaciones propias de la institución.

**Proceso crítico:** Proceso o sistema de información que, al dejar de funcionar, afecta la continuidad operativa de la institución.

**Pérdida por riesgo operativo:** Es la cuantificación económica del impacto negativo registrado en las cuentas de resultados o en la situación patrimonial de la institución, que haya sido provocado a consecuencia de cualquier evento de riesgo operativo.

**Perfil de Riesgo:** Resultado consolidado de los riesgos a los que se expone CIDRE IFD.

**Riesgo:** Es la contingencia, probabilidad o posibilidad de que eventos, anticipados o no, puedan tener un impacto adverso contra ingresos y/o patrimonio de la entidad supervisada. Para fines prácticos de gestión, sin embargo, se entiende por riesgo al efecto que la incertidumbre o lo incierto puede tener sobre objetivos, procesos y/o activos clave (fuentes de riesgo).

**Riesgo de crédito:** Se entiende por riesgo de crédito a la probabilidad de que un deudor incumpla, en cualquier grado, con el repago de su(s) obligación(es), de modo que se genere una disminución en el valor presente del contrato.

**Riesgo Legal:** Es la posibilidad o probabilidad de que la institución incurra en pérdidas derivadas del incumplimiento de la legislación y normativa vigentes o de relaciones contractuales inadecuadamente instrumentadas, siendo este un componente del riesgo operativo.

**Riesgo Operativo:** Es la probabilidad de pérdida que se puede generar en la Entidad por fallas del sistema de control interno, fallas del sistema informático y desvíos en la aplicación de procedimientos, reglamentos, funciones y responsabilidades. Se entiende que tanto el riesgo tecnológico como el legal forman parte del riesgo operativo.

**Riesgo Reputacional:** Es la posibilidad de afectación del prestigio de la Entidad por cualquier evento externo, fallas internas hechas públicas o al estar involucrada la entidad en transacciones o relaciones con negocios ilícitos que puedan generar pérdidas y ocasionar un deterioro de la situación de esta.

**Riesgo Tecnológico:** Es la posibilidad o probabilidad de sufrir pérdidas por caídas o fallos en los sistemas informáticos o en la transmisión de datos, errores de programación u otros, siendo éste un componente del riesgo operativo.

**Riesgo Inherente:** Es el riesgo que por su naturaleza no se puede separar de la actividad financiera, al ser intrínseco a las distintas actividades y áreas de la institución, sin considerar los sistemas de gestión y control.

**Riesgo Residual:** Es el riesgo que persiste después de tomarse en cuenta las medidas de control existentes.Se lo conoce también como riesgo neto.

## **Desarrollo.**

PARTE I – DE LA GESTIÓN DEL RIESGO OPERATIVO

CAPÍTULO I – MARCO INTERNO PARA LA GESTIÓN INTEGRAL DE RIESGOS

ARTÍCULO 1° (Marco Interno para la Gestión Integral de Riesgos)

La gestión del riesgo operativo se lleva a cabo dentro del Marco Interno para la Gestión Integral de Riesgos (MIGIR), según lo contenido por el “Reglamento Interno para la gestión integral de riesgos”, tanto en términos de arquitectura, estrategia y protocolos. El contenido de este documento, sin embargo, aporta elementos adicionales y específicos que hacen a la gestión del riesgo operativo.

CAPÍTULO II – ESTRATEGIA PARA LA GESTIÓN DE RIESGO OPERATIVO

ARTÍCULO 1° (Objetivos de la gestión del riesgo operativo)

De manera adicional a los objetivos generales de la gestión integral de riesgos, manifiestos en el “Reglamento Interno para la gestión integral de riesgos”, los objetivos específicos de la gestión del riesgo operativo en CIDRE IFD son los siguientes:

1. Colaborar con la identificación y gestión de los principales riesgos operativos, siempre con relación a la planificación estratégica institucional y al modelo de negocio de CIDRE IFD.
2. Promover la adopción de los lineamientos básicos de gestión de riesgos dentro de la gestión de procesos y la gestión del riesgo operativo en general.
3. Asegurar la implementación de políticas y procedimientos suficientes para guiar y normar la gestión del riesgo por activos de información, procesos y productos.
4. Respaldar, con base en la provisión de información, la toma de decisiones asociadas a personas, activos de información, sistemas, eventos externos y diseño y ejecución de procesos.
5. Promover el desarrollo continuo del ambiente de control interno y de la gestión preventiva de continuidad del negocio.

ARTÍCULO 2° (Proceso de gestión de riesgo operativo)

El proceso aplicado para la gestión del riesgo operativo es el proceso de gestión integral de riesgos del “Reglamento Interno para la gestión integral de riesgos”.

ARTÍCULO 3° (Organización de la gestión del riesgo operativo)

1. CIDRE IFD gestiona el riesgo operativo a partir de los procesos inventariados, haciendo énfasis en aquellos que son críticos para la continuidad de sus operaciones y/o la consecución de sus objetivos estratégicos.
2. La gestión de la seguridad de la información es responsabilidad del Oficial de Seguridad de Información, quien ejecuta su gestión a partir de los activos de información y de acuerdo con lo dispuesto por el “Manual de la Seguridad de la Información”.
3. El riesgo operativo es inherente a todas las actividades ejecutadas por CIDRE IFD, razón por la cual, en consistencia con el modelo de las tres líneas de defensa, los responsables de las diferentes áreas o unidades de negocio u operativas están a cargo de la gestión del riesgo operativo.
4. Para lo anterior, la Subgerencia Nacional de Gestión de Riesgos es responsable de brindar asistencia a cada unidad de negocio u operativa en la implementación y ejecución de la gestión del riesgo operativo, siendo también responsable de implementar y mantener los aspectos del Marco Interno para la Gestión Integral de Riesgos (MIGIR) relacionados a la gestión del riesgo operativo.
5. El registro, seguimiento y solución de eventos de riesgo operativo es parte integral de la gestión del riesgo operativo.
6. Para la gestión del riesgo legal, cada unidad de negocio u operativa tiene la responsabilidad de asegurar el total cumplimiento normativo de sus operaciones.
7. La Subgerencia Nacional de Gestión de Riesgos evalúa periódicamente el nivel de riesgo operativo y seguridad física de los Puntos de Atención Financiera (PAF) de CIDRE IFD.

CAPÍTULO III – PROTOCOLOS PARA LA GESTIÓN DE RIESGO OPERATIVO

ARTÍCULO 1° (Políticas y procedimientos)

1. La gestión integral de riesgos, así como la de gestión del riesgo operativo, tienen como base normativa interna tanto el “Manual de gestión integral de riesgos” como el presente “Reglamento Interno para la gestión del riesgo operativo”.
2. La seguridad de la información, parte integral del riesgo tecnológico y, a su vez, del riesgo operativo, tiene como base normativa el “Manual de Seguridad de la Información”.
3. La continuidad del negocio se gestiona con base en el plan para la continuidad del negocio.
4. CIDRE IFD cuenta con un inventario de procesos.

PARTE II – DE LAS ETAPAS DE LA GESTIÓN DEL RIESGO OPERATIVO

CAPÍTULO I – IDENTIFICACIÓN

ARTÍCULO 1° (Identificación de riesgo operativo)

1. CIDRE IFD identifica y evalúa los principales factores que, al presentar comportamientos adversos o inesperados, pueden derivar en pérdidas y/o en el incremento de sus niveles de exposición, por conceptos relacionados a la ejecución de procesos, desempeño de personas y sistemas, y a la ocurrencia de eventos externos.
2. La identificación de riesgos operativos se lleva a cabo de acuerdo con los lineamientos definidos para este fin por el “Reglamento Interno para la gestión integral de riesgos”.

CAPÍTULO II – MEDICIÓN (ANÁLISIS Y EVALUACIÓN DE RIESGOS)

ARTÍCULO 1° (Medición del riesgo operativo)

1. Este capítulo hace referencia a los procedimientos y métodos empleados para la medición (análisis y evaluación) del riesgo operativo y tiene como base el contenido del “Reglamento Interno para la gestión integral de riesgos”.
2. La medición del riesgo operativo puede ser cualitativa y cuantitativa, y puede ejecutarse mediante la definición de indicadores o unidades de medida o mediante análisis y estudios diferentes.
3. Cuando corresponde, las metodologías son descritas en el documento “Metodologías para la gestión de riesgo operativo”.

ARTÍCULO 2° (Base de datos de eventos de riesgo operativo)

De acuerdo con la Recopilación de Normas para Servicios Financieros de ASFI, CIDRE IFD registra y clasifica los eventos de riesgo operativo en una base de datos histórica.

ARTÍCULO 3° (Riesgo por punto de atención financiera)

1. La Subgerencia Nacional de Gestión de Riesgos evalúa periódicamente el nivel de riesgo operativo y de seguridad física de los puntos de atención financiera (PAF) de CIDRE IFD.
2. Para ello, se utiliza información primaria y secundaria que permita aproximar el nivel de riesgo de un PAF, incluyendo datos, informes, reportes u otros elaborados por otras instancias de CIDRE IFD.
3. El riesgo por PAF puede estimarse desde diferentes perspectivas y para diferentes fines, sea para la determinación del nivel de riesgo por seguridad física, para el monitoreo al cumplimiento de políticas de seguridad física y riesgo operativo, incluyendo seguridad de la información, y/o para la identificación de riesgos.

ARTÍCULO 4° (Riesgo de continuidad del negocio)

1. CIDRE IFD, a través de la Subgerencia Nacional de Gestión de Riesgos, identifica y evalúa anualmente los principales riesgos de continuidad del negocio.
2. La evaluación de estos riesgos opera como la base para la recomendación de elaboración, determinación e implementación de estrategias de mitigación y/o planes de contingencia.

ARTÍCULO 5° (Riesgo tecnológico)

La medición del riesgo tecnológico es responsabilidad del Oficial de Seguridad de la Información y se lleva a cabo según los criterios y métodos definidos en el “Manual de Seguridad de la Información”.

ARTÍCULO 6° (Pruebas de estrés, escenarios o sensibilidad)

CIDRE IFD realiza pruebas periódicas de estrés, sensibilidad o simulaciones de posibles escenarios o situaciones extremas sobre la ocurrencia de eventos de riesgo operativo.

CAPÍTULO III – MONITOREO

ARTÍCULO 1° (Monitoreo del riesgo operativo)

El proceso de monitoreo del riesgo operativo se lleva a cabo según lo dispuesto por el “Reglamento Interno de gestión integral de riesgos”, en todo lo que respecta al i) monitoreo periódico de la evolución del perfil de riesgo operativo y de los riesgos operativos a los que CIDRE IFD se expone, y ii) al monitoreo y evaluación del desempeño y efectividad del Marco Interno para la Gestión Integral de Riesgos (MIGIR) en lo que corresponde a la gestión del riesgo operativo.

ARTÍCULO 2° (Gestión del apetito de riesgo operativo y límites internos)

1. La Declaración de Apetito de Riesgo (DAR) es el documento aprobado por Directorio mediante el cual CIDRE IFD comunica los niveles de riesgo operativo que se dispone a asumir a fin de alcanzar sus objetivos estratégicos.
2. El cumplimiento al apetito de riesgo operativo manifiesto a través de la DAR es de responsabilidad de todas las unidades de negocio y de todo el personal de CIDRE IFD.
3. La Subgerencia Nacional de Gestión de Riesgos presenta periódicamente al Comité de Gestión Integral Riesgos informes relacionados al estado y desempeño de los indicadores respecto de los límites internos dispuestos por riesgo operativo contenidos en la DAR.

ARTÍCULO 3° (Visitas e inspecciones de riesgo operativo y seguridad física)

La Subgerencia Nacional de Gestión de Riesgos, según lo considere oportuno, puede realizar visitas e inspecciones de riesgo operativo y seguridad física a puntos de atención financiera (PAF), con la finalidad de monitorear el estado al cumplimiento de políticas y procedimientos, así como con la intención de recolectar información para la identificación y medición de riesgos.

ARTÍCULO 4° (Registro y seguimiento a eventos de riesgo operativo)

1. Los eventos de riesgo operativo son registrados a través de un sistema de información implementado para este fin, construyéndose a partir de los registros realizados la base de datos interna de eventos de riesgo operativo. Esta base cumple con los requerimientos dispuestos por la Recopilación de Normas para Servicios Financieros de ASFI.
2. A través del sistema de información implementado, la Subgerencia Nacional de Gestión de Riesgos realiza seguimiento periódico a la implementación de acciones correctivas ante los eventos de riesgo operativo reportados a la CIRO de ASFI.
3. En el caso de eventos y errores operativos, puede definirse, a través del procedimiento correspondiente, el registro por hallazgo, con base en informes o documentos formales.

ARTÍCULO 5° (Reporte de eventos críticos)

1. Los eventos de riesgo operativo pueden ser críticos, siendo necesario en ese caso su reporte oportuno al ente regulador, de acuerdo con la Recopilación de Normas para Servicios Financieros.
2. CIDRE IFD define como evento crítico a todo evento cuya ocurrencia genere la imposibilidad total de abrir uno o más puntos de atención financiera (PAF) por un periodo igual o superior a las seis (6) horas.
3. En el caso concreto de eventos de seguridad de la información, se considera también como eventos críticos la materialización de eventos de tipo ataques de Ramsomware, contagio de Virus/Malware que afecten los equipos de cómputo de los centros de procesamiento de datos, acceso no autorizado a equipos de cómputo por medio de escritorio remoto, robo o suplantación de identidad (phishing), cortes por más de 6 horas en enlaces de comunicación y modificación no autorizada de información en sitios web, redes sociales, banca digital, servidores, y base de datos, que afecten la integridad de la información
4. Todo evento clasificado como crítico debe ser reportado al ente regulador el mismo día de su descubrimiento, dando lugar a un informe que detalle tanto lo ocurrido como las medidas correctivas asumidas, y que debe ser enviado hasta el siguiente día hábil administrativo a la comunicación del evento.
5. El reporte oportuno de un evento crítico es responsabilidad de la Subgerencia Nacional de Operaciones y Captaciones, de acuerdo con el “Procedimiento para la identificación, reporte y registro de Eventos Críticos”.

CAPÍTULO IV – CONTROL Y MITIGACIÓN DE RIESGO OPERATIVO (TRATAMIENTO)

ARTÍCULO 1° (Control del riesgo operativo)

Los procesos de control y mitigación (tratamiento) del riesgo operativo se llevan a cabo según los lineamientos expuestos en el “Reglamento Interno de gestión integral de riesgos”. Este documento expone las estrategias complementarias de control y mitigación asociados al riesgo operativo.

ARTÍCULO 2° (Control y mitigación de riesgo operativo)

1. Cada unidad de negocio u operativa es responsable de diseñar, implementar, mantener y evaluar los controles asociados a sus procedimientos y funciones.
2. La Subgerencia Nacional de Gestión de Riesgos puede evaluar el desempeño de controles implementados y sugerir modificaciones a los mismos o la implementación de controles adicionales.
3. Auditoría Interna cumple funciones de verificación y control al cumplimiento de lo contenido en este documento.

ARTÍCULO 3° (Gestión de la continuidad del negocio)

1. La gestión de la continuidad del negocio responde a una estrategia preventiva para la mitigación del riesgo operativo. Con mayor precisión, la gestión de la continuidad del negocio tiene por objetivo principal minimizar el impacto asociado a la ocurrencia de uno o más eventos de riesgo, buscando asegurar, adicionalmente, la recuperación oportuna de los recursos involucrados.
2. El proceso de gestión de la continuidad del negocio en CIDRE IFD se lleva a cabo según el plan de continuidad de negocio.

CAPÍTULO V – DIVULGACIÓN (COMUNICACIÓN Y CONSULTA)

ARTÍCULO 1° (Divulgación del riesgo operativo)

1. El proceso de divulgación del riesgo operativo en CIDRE IFD se lleva a cabo según los lineamientos expuestos en el documento “Reglamento Interno de gestión integral de riesgos”.
2. A su vez, los informes y reportes generados por la Subgerencia Nacional de Gestión de Riesgos, así como otra instancia, sobre el riesgo operativo, son compartidos al menos con la Gerencia General, a fin de dar a conocer cualquier evento y/o factor de riesgo que pudiese influir sobre el grado de exposición al riesgo operativo y/o dar paso al incumplimiento del apetito de riesgo operativo.

ARTÍCULO 2° (Cultura de riesgo operativo)

La cultura de riesgo se construye sobre la base de los parámetros establecidos por el “Reglamento Interno para la gestión integral de riesgos”.

## **Documentos Referenciales.**

* MANUAL DE GESTIÓN INTEGRAL DE RIESGOS – (MN-GR-001)
* MANUAL DE SEGURIDAD DE LA INFORMACIÓN – (MN-GR-GSI-001)
* OTROS INTERNOS - METODOLOGÍAS PARA LA GESTIÓN INTEGRAL DE RIESGOS (OTI-GR-001)
* OTROS INTERNOS - METODOLOGÍAS PARA LA GESTIÓN DE RIESGO OPERATIVO - (OTI-GR-003)
* PROCEDIMIENTO PARA EL REPORTE Y REGISTRO DE EVENTOS DE RIESGO OPERACIONAL E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN – (PR-GR-012)
* PROCEDIMIENTO PARA LA EVALUACIÓN E INSPECCIÓN DE RIESGOS OPERACIONALES POR AGENCIA - (PR-GR-013)
* PROCEDIMIENTO PARA EL REPORTE, REGISTRO Y ENVÍO DE EVENTOS CRÍTICOS – (PR-GR-019)
* REGLAMENTO INTERNO PARA LA GESTIÓN INTEGRAL DE RIESGOS – (RI-GR-001)
* RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS – (NT-001)

NOTA: La Recopilación de Normas para Servicios Financieros (RNSF), se pone a disposición de la colectividad financiera y contiene la compilación temática de toda la normativa vigente emitida desde 1987, año de la restitución de la ex Superintendencia de Bancos y Entidades Financieras actual ASFI, como organismo autónomo de regulación y control del sector financiero. Contempla, además, las actualizaciones que han sido incorporadas en algunos textos, para su correcta aplicación, dentro del marco de lo dispuesto por la Ley N° 393 de Servicios Financieros y del ámbito moderno y globalizador del Comité de Basilea.

La Recopilación de Normas para Servicios Financieros, será actualizada permanentemente por ASFI, y disponible a través de su página web (<https://www.asfi.gob.bo/index.php/norm-serv-fina-norm/recopilacion-de-normas.html>).

## **Anexos.**

Ninguno.