PROCEDIMIENTO INTERNO
SISTEMA DE GESTIÓN DE RIESGOS
COORDINADOR ELÉCTRICO NACIONAL
PI-001-2022

CONTROL DEL DOCUMENTO

APROBACIÓN

Versión	Aprobado por
1	Consejo Directivo
2	Consejo Directivo

REGISTRO DE CAMBIOS

Fecha	Autor	Versión	Descripción del Cambio
14-05-2020	Unidad de Auditoría y Cumplimiento Normativo	1	Confección del Procedimiento interno
18-05-2022	Unidad de Auditoría y Cumplimiento Normativo	2	Actualización del Procedimiento interno

REVISORES

Nombre	Cargo
Heinrich Meyerholz	Jefe Unidad de Calidad de Servicios e Innovación
Paula Millar	Jefe Unidad de Auditoría y Cumplimiento Normativo

AUTORES

Nombre	Cargo
Diego Farías	Supervisor de Auditoría y Cumplimiento
Valeska Bascuñán	Auditor Senior de Auditoría y Cumplimiento

1. Introducción

El Coordinador Eléctrico Nacional -como organismo autónomo de derecho público, técnico e independiente- debe velar por una operación segura y económica del conjunto de instalaciones del sistema eléctrico que operen interconectadas entre sí, permitiendo de esta forma abastecer de energía al país y sus habitantes.

Para el Coordinador la gestión y el control de riesgos es una actividad crítica para su funcionamiento y debe estar presente en todas sus actividades y decisiones.

2. Objetivo

El objetivo del presente Procedimiento es definir en forma clara y simple cómo será implementado el sistema de gestión de riesgos en el Coordinador, conforme a los lineamientos y principios establecidos en la Política de Gestión y Control de Riesgos, que define la gobernanza de los riesgos, los factores de riesgos, el proceso de gestión de riesgos y la tolerancia al riesgo.

3. Alcance

Este procedimiento es aplicable a todas las unidades u órganos internos que constituyen el Coordinador Eléctrico Nacional.

4. Definiciones

a) Coordinador Eléctrico Nacional o Coordinador: Coordinador Independiente del Sistema Eléctrico Nacional, definido en el artículo 212-1 de la Ley General de Servicios Eléctricos, modificada por la Ley Nº 20.936.

b) Consejo Directivo: Consejo Directivo del Coordinador, a que se refiere la Ley General de Servicios Eléctricos.

c) DE: Director Ejecutivo del Coordinador Eléctrico Nacional.

d) Unidad u Órgano interno: Corresponde a las Gerencias, Subgerencias, Departamentos o Unidades del Coordinador.

e) Riesgo: Es la probabilidad de que un evento, acción u omisión impacte negativamente en el cumplimiento de las funciones y objetivos del Coordinador o su reputación como organismo.

f) Tolerancia al riesgo: Corresponde a la exposición que la organización decide asumir y que le permite el cumplimiento de los objetivos que ha establecido.

5. Sistema de Gestión de Riesgos

El Sistema de Gestión de Riesgos tiene como propósito implementar y desarrollar una gestión integral de los riesgos a que se ve expuesto el Coordinador en sus actividades, estandarizando procesos y definiciones que faciliten su conocimiento y evaluación, para apoyar la toma de decisiones.
El Sistema de Gestión de Riegos se basa en los siguientes elementos:

- Gobernanza: Define la instancia responsable de administrar el riesgo, quiénes efectúan su evaluación y quiénes realizan el seguimiento.

- Metodología: Establece una metodología común, que estandariza conceptos, procesos y facilita el entendimiento, comparación y seguimiento de los riesgos.

- Cultura: Para asegurar una implementación exitosa del Sistema de Gestión de Riesgos, es clave avanzar en construir y compartir una cultura de riesgos en todos los procesos y decisiones del Coordinador, la cual está basada en definir conceptos básicos, y establecer criterios de tolerancia al riesgo.

6. Tolerancia al riesgo.

Conforme lo establece la Política de Gestión y Control de Riesgos del Coordinador, la tolerancia al riesgo corresponde a la exposición que la organización decide asumir y que le permite el cumplimiento de los objetivos que ha establecido.

Debido a la función de interés público que el Coordinador tiene asignada, su tolerancia al riesgo es baja, por lo que no asume riesgos que afecten o puedan llegar a afectar el cumplimiento de sus objetivos por lo que, en caso de presentarse algún riesgo, deberán tomarse todas las medidas de control necesarias que permitan la mitigación del mismo hasta donde sea posible.

7. Modelo de Gobierno, Tres líneas de Defensa.

Considerando las buenas prácticas en esta materia y adoptando el Marco de Gestión de Riesgos propuesto por la ISO 31000, el Coordinador se ha organizado en Tres Líneas de Defensa en términos de asignación de roles y responsabilidades para realizar una adecuada gestión de sus riesgos, de acuerdo a lo siguiente:

Primera Línea de Defensa: Está conformada por las Gerencias, Subgerencias y Jefaturas, que realizan una gestión directa sobre los procesos que están a su cargo y, en consecuencia, son los responsables de los riesgos a que están expuestos tales procesos. Una debilidad o error en la ejecución de los controles que se han definido para su mitigación podría implicar la materialización de uno o más riesgos.

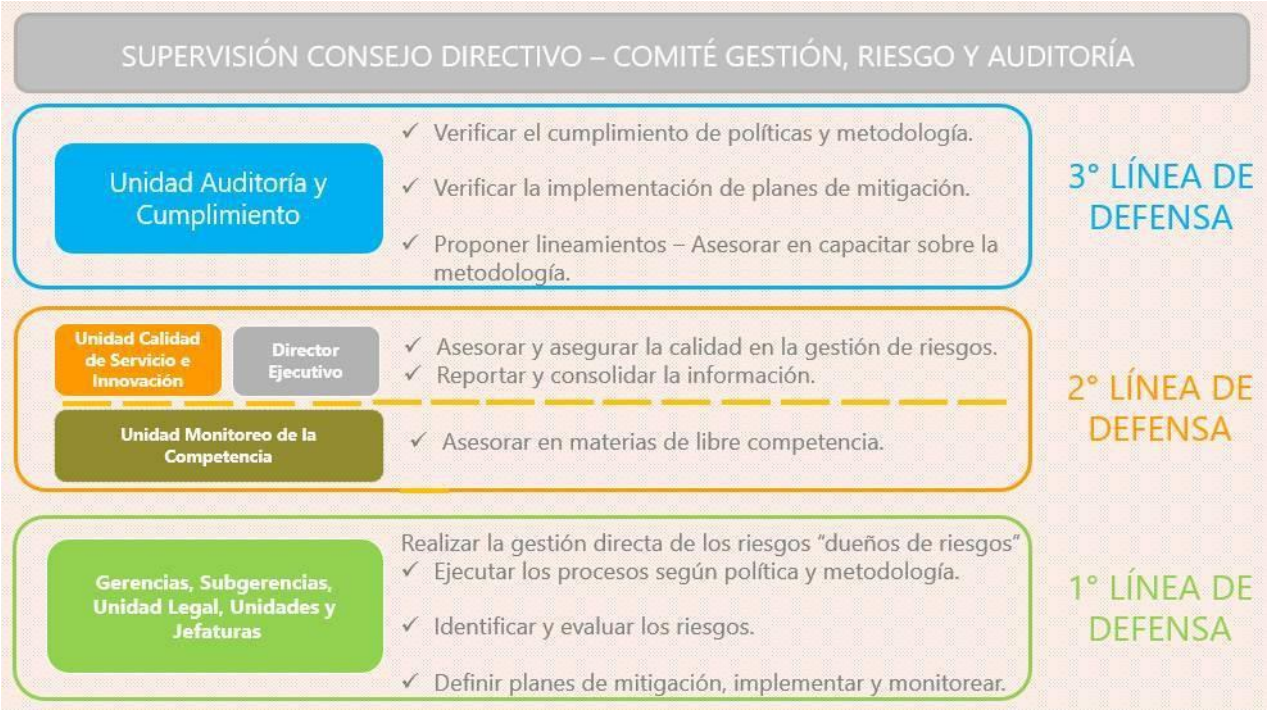
Es responsabilidad de esta Línea de Defensa, Identificar, Evaluar y Mitigar los riesgos de sus procesos.

Segunda Línea de Defensa: El Director Ejecutivo y la Unidad de Calidad de Servicio e Innovación tienen una visión amplia de los riesgos del Coordinador. Por lo tanto, a estas instancias les corresponde desafiar a la Primera Línea en los riesgos identificados, sus controles y evaluación, así como asesorar, asegurar la calidad y consolidar la información presentada por la Primera Línea de Defensa.

En la segunda línea de defensa, también se encuentra la Unidad de Monitoreo de la Competencia, quien asesora a la primera línea en materias de libre competencia.

Tercera Línea de Defensa: Corresponde a la Unidad de Auditoría y Cumplimiento que, como parte de su programa anual de auditoría, verifica el cumplimiento de las políticas y estándares de gestión de riesgos, así como la implementación en tiempo y forma de los planes de acción establecidos por los responsables de los procesos, para la mitigación de los riesgos.

No obstante lo señalado, y para apoyar en la etapa inicial de implementar una gestión integral de riesgos en el Coordinador, esta Unidad participará proponiendo lineamientos sobre esta materia y prestará asesoría a las distintas gerencias en la comprensión de la metodología de gestión de riesgos.



8. Factores de Riesgos

El modelo de gestión de riesgos del Coordinador está basado en las mejores prácticas internacionales en esta materia, y comprende primero una definición de los tipos de riesgos, su probabilidad de ocurrencia y áreas de impacto.

8.1 Catálogo de Riesgos:

El sistema de Gestión de Riesgos define los siguientes tipos de riesgos, según su naturaleza:

Riesgo Estratégico: Posibilidad de no cumplir con la misión del Coordinador, de consolidar su identidad corporativa y conservar su imagen ante sus stakeholders debido a decisiones y definiciones estratégicas inadecuadas, errores en el diseño de planes de alto nivel, de estructura organizacional y de control interno, fallas en la integración de modelos operativos con las estrategias corporativas, fallas en el estilo de dirección, asignaciones de recursos erróneas, e ineficiencias en la adaptación de cambios en los entornos internos y externos de la organización.

Riesgo Reputacional: Posibilidad de tener una imagen pública negativa debido a malas prácticas del Coordinador. Este tipo de riesgo puede afectar la apreciación del organismo frente a sus stakeholders, y/o implicar gastos por conceptos de juicios o demandas.

Riesgo Operacional: Potencial impacto negativo en el cumplimiento de las funciones del Coordinador ocasionado por procesos internos inadecuados, deficiencias en los sistemas de información, errores humanos como consecuencia de ciertos sucesos externos, incluyendo eventos de índole social, catástrofes naturales y ataques a instalaciones del Coordinador.

Riesgo Regulatorio: Aquellos provenientes de cambios en el marco normativo relativo a la estructura, financiamiento o funcionamiento del Coordinador, que afecten significativamente su rol y sus principios y eficacia de funcionamiento.

Riesgo de Cumplimiento: Aquellos que surgen debido a la posibilidad de incumplimiento o falta en relación a la normativa vigente o las políticas, códigos y/o reglamentos internos que ha establecido el Coordinador.

Riesgo Financiero: Posibilidad de incumplimiento de obligaciones económicas que produzcan una pérdida financiera. El incumplimiento puede ser por parte de trabajadores, coordinados, proveedores o contratistas.

El presente riesgo incluye posibles variaciones injustificadas en valores contables y/o económicos de activos y pasivos reflejados en la contabilidad.

Riesgo de Seguridad de la Información: Aquel relacionado con la preservación de la confidencialidad, integridad y disponibilidad de la información. También puede involucrar otras propiedades como autenticidad, responsabilidad, no – repudiación y confiabilidad.

Riesgo de Control Interno: Es la posibilidad que los procedimientos de control interno no puedan prevenir o detectar errores significativos de manera oportuna. Este riesgo si bien no afecta a la organización como un todo, incide de manera directa en sus dependencias.

Riesgo de Auditoría: Representa la posibilidad de que el auditor exprese una opinión errada en su informe debido a que la información suministrada a él esté afectada por una distorsión material o por una apreciación errónea del proceso o la información analizada.

8.2 Probabilidad de Ocurrencia de un Riesgo:

El Sistema de Gestión de Riesgos del Coordinador establece los siguientes 3 parámetros de probabilidad de ocurrencia de algún riesgo:

Improbable: Probabilidad de ocurrencia cercana a cero / no se ha materializado el riesgo en los últimos tres años.

Ocasional: Probabilidad de ocurrir alguna vez / El riesgo se ha materializado en el Coordinador al menos una vez en los últimos tres años.

Frecuente: Probabilidad de ocurrir repetidamente / El riesgo se ha materializado en el Coordinador frecuentemente, cinco o más veces en los últimos tres años.

8.3 Ámbitos de Impacto:

El Sistema de Gestión de Riesgos del Coordinador ha establecido 5 ámbitos de interés para evaluar los tipos de impactos cuando un riesgo se materializa. Estos son:

- Operacional
- Imagen y Reputación.
- Económico.
- Recursos Humanos
- Regulatorio / Legal.

La materialización de un riesgo puede afectar a uno, dos o todos los ámbitos, por eso es necesario que la evaluación del impacto se realice en cada uno de los ámbitos de posible afectación.

8.4 Nivel de Impacto de un Riesgo:

Para cada uno de los ámbitos, el Sistema de Gestión de Riesgos del Coordinador definió una escala con los tres niveles de impacto, según la siguiente tabla:

Escala de Impacto		Áreas de Impacto – Descripción				
	Nivel	Operacional	Imagen y Reputación	Económico	Recursos Humanos	Regulatorio / Legal
3	Catastrófico	• Evento energético G1 o G2. • Pérdida definitiva de información relacionada con la operación de procesos contenidos en la cadena de valor de la organización. • Indisponibilidad de las aplicaciones para la operación por más de 6 horas (SCADA, SIP, Neomante, Servidores programas optimización de la operación, Sistema de información técnica).	• Extensa y sostenida cobertura desfavorable en medios de comunicación nacional o internacional. Tiene potencial de disminuir la credibilidad de la compañía en el corto plazo	• Quiebra de una empresa generadora participante en mercado mayorista a consecuencia de que el Coordinador no cumple sus funciones de realizar los cálculos correctamente y dentro de los plazos y que casusa impacto relevante en la operación y seguridad del sistema. • Rompimiento de la cadena de pagos	• Pérdida de personal clave que impida la operación de los procesos contenidos en la cadena de valor de la organización	• Multas que involucren al Consejo Directivo y/o Director Ejecutivo. • Sanciones administrativas al Coordinador. • Dictamen desfavorable del panel de expertos con consecuencias mayores (que impida la continuidad de los procesos contenidos en la cadena de valor de la organización). • Formalización por parte de la FNE al Coordinador.
2	Moderado	• Evento energético G3. • Pérdida temporal de información relacionada con la operación de procesos contenidos en la cadena de valor de la organización. • Indisponibilidad de las aplicaciones para la operación por más de 24 horas (Sitio Web, Combustibles, SGER, RIO, Sistemas de Correspondencia). • Indisponibilidad de las aplicaciones para la operación entre 3 y 6 horas (SCADA, SIP, Neomante, Servidores y programas optimización de la operación. • Sistema de información técnica. • Atraso en el Desarrollo de la Transmisión que afecte procesos contenidos en la cadena de valor de la organización.	• Reacción adversa del público en general y organizacionales no gubernamentales o algún stakeholders. • Importante cobertura desfavorable en medios de comunicación nacional. Tiene potencial de disminuir la credibilidad de la compañía en el corto plazo.	• Perjuicio económico para una empresa participante, que causa efectos relevantes en el sistema eléctrico, a consecuencia de que el Coordinador no cumple sus funciones de realizar los cálculos correctamente y dentro de los plazos.	• Pérdida de personal clave con un impacto en la calidad de los productos de los procesos contenidos en la cadena de valor de la organización.	• Dictamen desfavorable del panel de expertos con consecuencias no mayores (que impida la continuidad de los procesos contenidos en la cadena de valor de la organización). • Investigación de la FNE a un proceso de responsabilidad del Coordinador. • CNE o SEC oficien al Coordinador por un incumplimiento. • Resultado desfavorable en Demanda Civil contra el Coordinador.
1	Menor	• Evento Energético con una perdida menor al 10% de la demanda. • Indisponibilidad de las aplicaciones para la operación menor a 3 (SCADA, SIP, Neomante, Servidores programas optimización de la operación, Sistema de información técnica). • Atraso en el Desarrollo de la Transmisión.	• Preocupación pública restringida a quejas locales. • Cobertura baja desfavorable en medios de comunicación regional / local.	• Atraso en el cumplimiento de la cadena de pagos a consecuencia de que el Coordinador no cumple sus funciones de realizar los cálculos dentro de los plazos y de monitorear adecuadamente la cadena de pagos.	• Pérdida de personal que afecte algún proceso sin comprometer la calidad y continuidad de los procesos contenidos en la cadena de valor de la organización.	• Discrepancia contra el Coordinador ante el Panel de Expertos • Consulta de CNE o SEC por posible incumplimiento. • Presentación de Demanda Civil contra el Coordinador.

Los eventos energéticos referidos precedentemente son los descritos en el "Manual de Comunicaciones para enfrentar situaciones de crisis" del Coordinador Eléctrico Nacional.

9. Metodología de Gestión de Riesgos

La metodología considera cinco etapas en el proceso de gestión de riesgos, cada una de las cuales establece roles y responsabilidades, conforme a las tres líneas de defensa definidas.

Etapa 1, Identificación de Riesgos: En esta etapa corresponde identificar, reconocer y describir los riesgos de los distintos procesos. El entregable es un registro preliminar de los riesgos, que incluye fuentes de los riesgos, eventos, causas y posibles consecuencias.

Etapa 2, Análisis de Riesgos: Los riesgos son analizados de acuerdo a su probabilidad de ocurrencia y nivel de impacto, considerando los controles existentes y su eficacia. Esta evaluación considera las cinco áreas de impacto del Coordinador (Operacional; Imagen y Reputación; Económico; Recursos Humanos; y Regulatorio/legal). El área de impacto con la consecuencia más alta definirá la posición del riesgo en el mapa de riesgos.

El riesgo debe ser evaluado a nivel de riesgo inherente o riesgo puro y a nivel de riesgo residual, según se explica a continuación:

a) Riesgo Inherente o Riesgo Puro. Corresponde a la multiplicación simple de las variables probabilidad e impacto, permite determinar el nivel de riesgo inherente de un determinado evento de riesgo.

Riesgo Inherente = Probabilidad de Ocurrencia * Impacto

El riesgo inherente será el valor del riesgo, sin considerar la eficacia de controles existentes (controles actuales). Para su determinación se deberá estimar la probabilidad de ocurrencia del evento y el impacto que pudiera provocar en caso de materializarse.

Para evaluar el impacto del riesgo inherente deberán considerarse las potenciales consecuencias que éste provocará en los siguientes ámbitos: Operacional; Imagen y Reputación; Económico; Recursos Humanos; Regulatorio y Legal.

Cada ámbito tendrá una escala de valorización propia, las cuales serán independientes entre sí y sus niveles de criticidad no serán equivalentes. La evaluación de impacto se llevará a cabo analizando cada ámbito y, para efectos de la valorización final del riesgo, se considerará la evaluación más alta. Ver ilustración 1 página N°8.

Determinación de la Probabilidad (Frecuencia) de Ocurrencia, corresponderá a la frecuencia con la que puede ocurrir un evento de riesgo, dada la experiencia y conocimiento de sucesos similares ocurridos en el Coordinador y/o en la industria eléctrica.

La probabilidad de ocurrencia de cada uno de los eventos de riesgos identificados se evaluará según la escala definida en el numeral 8) letra a) “Probabilidad de ocurrencia de un riesgo”.

b) Riesgo Residual. Corresponde a diferencia entre el riesgo inherente y la efectividad de los controles.

Evaluación de la efectividad de los controles, consiste en evaluar el diseño de los controles para determinar su nivel de efectividad. Los controles pueden ser preventivos o correctivos: los controles preventivos mitigarán la probabilidad inherente de ocurrencia de un riesgo, en tanto los controles correctivos mitigarán el impacto inherente de un riesgo.

Para evaluar el diseño de los controles se debe considerar lo siguiente:

Atributo	0	1	2	3
Documentación	No documentado	Parcialmente documentado	Documentado	
Automatización		Manual	Mixto	Automático
Cobertura del Control	Baja	Media	Alta	
Responsabilidad del Control	No asignado	Asignado		

El cálculo del diseño del control se obtendrá de la siguiente forma:

Cálculo del diseño = (Documentado + Automatizado) * Cobertura * Responsabilidad del Control

Numéricamente, el conjunto de combinaciones dará como valor mínimo 0 y un valor máximo de 10. A continuación con estos resultados se determinará la efectividad de los controles, en donde el diseño se clasificará en Inadecuado; Adecuado o Muy Adecuado, de acuerdo a la siguiente tabla:

Diseño	Valor	Efectividad
Muy Adecuado	9- 10	80%
Adecuado	4- 8	50%
Inadecuado	0-3	0%

Finalmente, se procederá a determinar el riesgo residual, donde:

- Impacto Residual.

Si el control es del Tipo Correctivo entonces:

*Impacto residual = Impacto Inherente * (1-Efetividad %)*

- Probabilidad Residual.

Si el control es del Tipo Preventivo entonces:

*Probabilidad residual = Probabilidad Inherente * (1-Efetividad %)*

En caso de existir más de un control mitigador por riesgo, entonces se tomará el promedio de la efectividad.

Etapa 3, Evaluación de Riesgos: En esta etapa se debe contrastar el nivel de riesgo identificado en el análisis con la tolerancia al riesgo definida por el Consejo Directivo, que es nivel “baja”, con el riesgo residual determinado.

Etapa 4, Tratamiento de los Riesgos: Para los riesgos evaluados a nivel residual (post controles) en una condición de "Altos" y "Medios" se debe definir planes de acción - mitigación que apunten a minimizar su impacto y su probabilidad de ocurrencia. Los planes de acción deben identificar claramente su objetivo, responsable y plazo de implementación.

Etapa 5, Monitoreo y Actualización de Riesgos: En esta etapa se realiza el monitoreo de la implementación de los planes de acción de mitigación definidos en la etapa anterior. Además, se efectúa una revisión permanente de posibles nuevos riesgos que puedan surgir en los distintos procesos.

10. Matriz de Riesgos Coordinador

El Coordinador ha definido una Matriz de Riesgos de valoración del riesgo de tres niveles, conforme a los siguiente:

		Impacto		
		Bajo (1)	**Medio (2)**	**Alto (3)**
Frecuencia	**Improbable (1)**	**1**	**2**	**3**
	Moderado (2)	**2**	**4**	**6**
	Probable (3)	**3**	**6**	**9**

De acuerdo a la valoración del riesgo, se establecen las siguientes clasificaciones y acciones a implementar:

Clasificación	Parámetros	Acciones a Implementar
Alto	**(6-9)**	El riesgo de no cumplir los objetivos es alto, por lo cual se deben implementar controles o medidas de mitigación adicionales inmediatamente.
		La tarea/actividad no puede ser realizada hasta que se baje el nivel de riesgo o en caso contrario la tarea/actividad debe ser validada por la Gerencia a cargo en el Coordinador
Moderado	**(3-4)**	El riesgo de no cumplir los objetivos es moderado, por lo cual se deben implementar controles o medidas adicionales de mitigación tan pronto como sea posible.
Bajo	**(1-2)**	El riesgo de no cumplir los objetivos es bajo, y no se requieren controles o medidas adicionales de mitigación a los ya implementados.

Celda de color Rojo: Incluye los riesgos calificados como "**Altos".** Son riesgos de importancia para el Coordinador y requieren un análisis completo conforme a la metodología, que permita identificar y ejecutar medidas de mitigación. El monitoreo de estos riesgos corresponde al DE, Comité de Gestión Riesgos y Auditoría y Consejo Directivo.

Celda de Color Amarillo: Representa riesgos de criticidad **Moderada**. Requieren una supervisión permanente de los controles identificados para evitar su materialización. El monitoreo de estos riesgos corresponde a los Gerentes "Responsables de los Procesos".

Celda de color verde: Son riesgos de criticidad baja, requieren una supervisión periódica de los controles. El monitoreo de estos riesgos corresponde a los "Responsables de los Procesos" (Jefes, Subgerentes).

11. Concordancia con normativa vigente

El presente procedimiento se encuentra en concordancia con la Política de Gestión y Control de Riesgos del Coordinador. Por lo mismo, este procedimiento no suprime, ni reemplaza otras obligaciones, inhabilidades, incompatibilidades o prohibiciones que pudieren constar en la ley o en la normativa interna de la empresa.

En caso de duda respecto de la aplicación e interpretación de este procedimiento, así como de eventuales conflictos con otras normas o reglamentos internos puede consultarse a la Unidad de Auditoría y Cumplimiento.

12. Vigencia y aprobación

La modificación de este Procedimiento ha sido aprobada en la Sesión Ordinaria del Consejo Directivo celebrada el 18 de mayo de 2022, y tiene vigencia a partir de esta fecha. Todas las modificaciones que sean efectuadas a este Procedimiento deberán constar por escrito y entrarán en vigencia una vez aprobadas por el Consejo Directivo.