

NOMBRE	POLÍTICA DE GESTIÓN Y CONTROL DE RIESGOS		
DIRECCIÓN	AUDITORÍA INTERNA		
PROCEDIMIENTO	DAI-02	FECHA	Febrero de 2016
VERSIÓN		Última revisión	Mayo de 2023

CONTROL DE VERSIONES

VERSIÓN	FECHA	CAMBIOS REALIZADOS
V.0	05/02/16	
V.1	18/05/2020	Adaptación al marco COSO ERM 2017
V.2	12/04/2023	Inclusión del alcance
	30/05/2023	Aprobación por Consejo de Administración

- 1. OBJETIVO**
- 2. MARCO NORMATIVO**
- 3. ALCANCE Y APLICACIÓN.**
- 4. GESTIÓN DE RIESGOS.**
- 5. OBJETIVOS DE LA GESTIÓN DE RIESGOS**
- 6. PRINCIPIOS DE LA GESTIÓN DE RIESGOS.**
- 7. CATEGORÍAS DE RIESGOS.**
- 8. APETITO DE RIESGO.**
- 9. MARCO DE GESTIÓN DE RIESGOS EN ENCE.**
 - 9.1.** Marco de Gestión de Riesgos
 - 9.2.** Proceso de Gestión de Riesgos
- 10. SISTEMAS DE INFORMACIÓN Y CONTROL INTERNO.**
- 11. ROLES Y RESPONSABILIDADES.**
- 12. ANEXO: FLUJOGRAMA DEL PROCESO DE GESTIÓN DE RIESGOS.**

1.- Objetivo

El presente documento tiene como objetivo formalizar la Política de gestión y control de riesgos aplicada en Ence Energía y Celulosa, S.A. y en todas las sociedades que forman parte de su Grupo (en adelante ENCE).

Mediante la aplicación de esta Política, ENCE se compromete a desarrollar todas sus capacidades para que los riesgos de toda índole a los que se enfrenta para cumplir sus objetivos se encuentren debidamente gestionados; es decir, identificados, evaluados, revisados, priorizados y tratados. Este compromiso es asumido por el Consejo de Administración y queda bajo su responsabilidad directa, tal y como se recoge en el Reglamento de dicho Consejo.

Esta Política define la contribución de la gestión de riesgos a la estructura de Gobierno Corporativo de ENCE e incluye la definición de competencias, funciones y responsabilidades de los distintos miembros de la organización que participan en la gestión de riesgos del Grupo.

El Sistema de Gestión de Riesgos definido en esta Política se complementa con el Procedimiento de Gestión y Control de Riesgos, con el Sistema de Control Interno sobre la Información Financiera (SCIIF) y con el Sistema de Control Interno sobre la Información no Financiera (SCIINF) implantado en ENCE, de acuerdo con los requisitos establecidos por la Comisión Nacional del Mercado de Valores (CNMV) en estas materias.

La metodología de esta Política de control y gestión de riesgos está basada en el marco definido por COSO (Committee of Sponsoring Organizations of the Tradeway Commission) en el modelo ERM (Enterprise Risk Management 2017) para la Gestión de Riesgos *“Integrando Estrategia y Desempeño”*.

2.-Marco Normativo

Las dos normas que regulan y establecen los puntos clave para la gestión de riesgos de las sociedades son la Ley de Sociedades de Capital y el Código de Buen Gobierno de la CNMV para las sociedades cotizadas. Ambas referencias se encuentran alineadas en sus disposiciones generales en materia de gestión de riesgos.

La Ley de Sociedades de Capital, en su artículo 529 ter establece las facultades indelegables del Consejo de Administración de una Sociedad, entre las que se encuentra “la determinación de la Política de gestión y control de riesgos, incluidos los fiscales, y la supervisión de los sistemas internos de información y control”.

Asimismo, en el artículo 529 quaterdecies establece las funciones que como mínimo debe tener asignadas la Comisión de Auditoría, entre las que se encuentra “supervisar la eficacia del control interno de la sociedad, la auditoría interna y los sistemas de gestión de riesgos, incluidos los fiscales, así como discutir con el auditor de cuentas las debilidades significativas del sistema de control interno detectadas en el desarrollo de la auditoría”.

Fecha: 30/05/2023	Política de gestión y control de riesgos	Página 2 de 13
-------------------	--	----------------

El Código de Buen Gobierno de las sociedades cotizadas (el Código de Buen Gobierno), aprobado por Acuerdo del Consejo de la CNMV de 18 de febrero de 2015, incluye recomendaciones al respecto de la gestión de riesgos en las compañías cotizadas:

- Que la Política de gestión y control de riesgos identifique al menos:
 - ✓ Los distintos tipos de riesgo, financieros y no financieros (entre otros los operativos, tecnológicos, legales, sociales, medio ambientales, políticos y reputacionales) a los que se enfrenta la sociedad, incluyendo entre los financieros o económicos, los pasivos contingentes y otros riesgos fuera de balance.
 - ✓ La fijación del nivel de riesgo que la sociedad considere aceptable.
 - ✓ Las medidas previstas para mitigar el impacto de los riesgos identificados, en caso de que llegaran a materializarse.
 - ✓ Los sistemas de información y control interno que se utilizarán para controlar y gestionar los citados riesgos, incluidos los pasivos contingentes o riesgos fuera de balance.

- Que bajo la supervisión directa de la Comisión de Auditoría o, en su caso, de una comisión especializada del Consejo de Administración, exista una función interna de control y gestión de riesgos ejercida por una unidad o departamento interno de la sociedad que tenga atribuidas expresamente las siguientes funciones:
 - ✓ Asegurar el buen funcionamiento de los sistemas de control y gestión de riesgos y, en particular, que se identifican, gestionan, y cuantifican adecuadamente todos los riesgos importantes que afecten a la sociedad.
 - ✓ Participar activamente en la elaboración de la estrategia de riesgos y en las decisiones importantes sobre su gestión.
 - ✓ Velar por que los sistemas de control y gestión de riesgos mitiguen los riesgos adecuadamente en el marco de la Política definida por el Consejo de Administración.

3.- Alcance y aplicación

La presente Política de control y gestión de riesgos es de aplicación en todas las sociedades y negocios que forman el Grupo ENCE, entendiéndose como tal todas y cada una de las sociedades en cuyo capital social la compañía Ence Energía y Celulosa, S.A. disponga, directa o indirectamente, de la mayoría de las acciones, participaciones o derechos de voto, o en cuyo órgano de gobierno o administración haya designado, o tenga facultad para designar, a la mayoría de sus miembros, de tal forma que controle la sociedad de una manera efectiva.

Fecha: 30/05/2023	Política de gestión y control de riesgos	Página 3 de 13
-------------------	--	----------------

La Política de gestión y control de riesgos es aplicable a todos los participantes, directos o indirectos, en el Proceso de Gestión de Riesgos de ENCE.

Este proceso cubre todas aquellas tipologías de riesgo que puedan amenazar el cumplimiento de los objetivos definidos por ENCE.

Todos los empleados, directivos, administradores y colaboradores de ENCE tienen la responsabilidad de contribuir al proceso de gestión de riesgos de una manera eficaz y eficiente.

4.- Gestión de riesgos

La gestión de riesgos es un proceso continuo efectuado por la organización aplicado en la definición y ejecución de la estrategia y diseñado para identificar, evaluar y tratar riesgos que, en caso de materializarse, podrían afectar negativamente a la consecución de los objetivos del Grupo, manteniéndolos dentro de un apetito de riesgo considerado aceptable.

Cada uno de los intervinientes en el proceso de gestión de riesgos, tienen definidas y asignadas responsabilidades y funciones concretas, siguiendo el modelo “ERM de COSO Gestión del Riesgo Empresarial —Integrando Estrategia y Desempeño”.

ENCE es consciente de la importancia de la gestión de los riesgos para el cumplimiento de las expectativas de sus “grupos de interés”, contemplando el binomio riesgo – rentabilidad, siendo por esta razón una organización no adversa al riesgo.

ENCE cree firmemente que los riesgos deben ser gestionados adecuadamente y no simplemente eliminados. Por tanto, la Política de gestión y control de riesgos de ENCE implica una gestión adecuada y eficaz de los riesgos que permitirá a la sociedad:

- Desde el punto de vista externo:
 - ✓ Crear y proteger el valor para los accionistas.
 - ✓ Generar confianza entre sus grupos de interés (accionistas e inversores, proveedores, clientes, reguladores, empleados, propietarios forestales, suministradores, administraciones públicas, vecinos, Administraciones Públicas, ONG’S etc.).
 - ✓ Asegurar el cumplimiento de las leyes y recomendaciones en materia de Gobierno Corporativo.
- Desde el punto de vista interno:
 - ✓ Alcanzar sus metas y objetivos.
 - ✓ Actuar de apoyo para el proceso de toma de decisiones.
 - ✓ Fortalecer el entorno de control interno.
 - ✓ Mejorar la supervisión.

Asimismo, ENCE considera que, para una adecuada gestión del riesgo, es imprescindible mantener el máximo nivel de transparencia en la información proporcionada, tanto hacia el interior como hacia el exterior de la

Fecha: 30/05/2023	Política de gestión y control de riesgos	Página 4 de 13
-------------------	--	----------------

organización. En este sentido, el personal de ENCE deberá tener en cuenta que la información proporcionada sobre la gestión de riesgos deberá cumplir los siguientes requisitos:

- ✓ Que sea completa, asegurando que se transmite toda la información relevante para una adecuada gestión de los riesgos.
- ✓ Que sea correcta y veraz, asegurando que la información transmitida no contiene errores ni sesgos.
- ✓ Que aporte valor, al fomentar el desarrollo de una cultura de control y gestión del riesgo.
- ✓ Que sea oportuna, es decir, debe ser transmitida a tiempo; en el momento que se conoce y es relevante para una adecuada gestión de riesgos

5.- Objetivos de la gestión de riesgos

El objetivo principal de una gestión de riesgos es integrar la información procedente de las diferentes empresas, funciones, áreas o departamentos para proporcionar una visión conjunta y, de esta manera, poder actuar con los riesgos de una forma eficiente, una vez fijada la estrategia y los objetivos de la Organización, conforme a la metodología definida en “ERM de COSO Gestión del Riesgo Empresarial —Integrando Estrategia y Desempeño”.

De manera concreta, las tareas asociadas a la gestión de riesgos pretenden alcanzar los siguientes objetivos:

- **Formar parte y apoyar a los procesos para la toma de decisiones.**

Las actividades que se llevan a cabo se centran en servir de apoyo a los gestores de la organización en el proceso de toma de decisiones de una manera cualificada y de acuerdo a una determinada metodología.

Asimismo, es objetivo complementario de la de gestión de riesgos, mejorar el grado de eficiencia de la información disponible para la toma de decisiones y su utilización en los procesos que se encuentran planificados dentro de la organización, teniendo en cuenta el contexto de las limitaciones determinadas por las posibles situaciones de riesgo que puedan presentarse.

- **Obtener una seguridad razonable para el cumplimiento de los objetivos.**

La gestión de riesgos en ENCE tiene por objetivo tratar los aspectos de la toma de decisiones que se sitúan en el ámbito de la incertidumbre, con el ánimo de:

- ✓ Incrementar la probabilidad de cumplir con los objetivos de la compañía.
- ✓ Mejorar las habilidades de transferencia de conocimiento de la gestión de riesgos orientada hacia la mejora de la gestión del resto de unidades de la organización.
- ✓ Evitar situaciones inesperadas, minimizando la ocurrencia de eventos inesperados.
- ✓ Proporcionar un sistema de alerta que permita anticiparse a potenciales problemas.

- **Delimitar el perfil de riesgo.**

Fecha: 30/05/2023	Política de gestión y control de riesgos	Página 5 de 13
-------------------	--	----------------

La gestión de riesgos en ENCE tiene por objetivo asegurar que las actividades de las diferentes áreas del negocio se encuentran alineadas con el nivel de riesgo que el Grupo considera adecuado, en concordancia con los objetivos y prioridades de la organización.

- **Facilitar un lenguaje y una metodología común sobre riesgos.**

La gestión de riesgos en ENCE tiene por objetivo proporcionar un entendimiento común y único del riesgo, documentado en un grupo de reglas, procedimientos y metodologías de medición sólidas y consistentes.

- Además, pretende establecer unas pautas de actuación que sean comunes para instaurar el proceso de gestión de riesgos dentro de las diferentes empresas de ENCE. **Permitir una asignación eficiente de los recursos.**

La gestión de riesgos en ENCE tiene por objetivo reflejar los riesgos que presentan un mayor impacto en los objetivos de la Compañía, de tal forma que se permita una priorización de la asignación de los recursos, enfocada en aquellas áreas donde el riesgo es más crítico.

- **Establecer pautas para el Buen Gobierno Corporativo.**

La gestión de riesgos tiene como meta proporcionar una base adecuada para integrar los procesos de gestión de riesgos y los de control interno, como parte esencial de unos principios efectivos de Buen Gobierno Corporativo.

- **Asignar responsabilidades a los participantes en el proceso.**

Por último, la gestión de riesgos en ENCE tiene por objetivo definir los roles y responsabilidades de los participantes, garantizando una adecuada segregación de funciones entre aquellos que tienen una responsabilidad directa en la gestión del riesgo (dueños de los riesgos) y aquéllos que tienen responsabilidad en el desarrollo, implantación y mantenimiento del Modelo de control y gestión de riesgos.

6.- Principios de la gestión de riesgos

Los principios sobre los que se asienta el Sistema de Gestión de Riesgos en ENCE son los siguientes:

La Gestión de Riesgos:
<ul style="list-style-type: none"> ✓ Crea valor a la organización. ✓ Es una parte integral de todos los procesos de ENCE. ✓ Forma parte de los procesos de toma de decisiones. ✓ Trata explícitamente la incertidumbre. ✓ Es sistemática, estructurada y adecuada. ✓ Es necesario que esté basada en la mejor información disponible. ✓ Se hace a medida de la organización. ✓ Contempla aspectos humanos y culturales.

- | |
|---|
| <ul style="list-style-type: none"> ✓ Es transparente, eficaz e incluyente. ✓ Es dinámica, repetible y responde al cambio. ✓ Facilita la mejora continua de ENCE. |
|---|

Tabla 1: Principios de la Gestión de Riesgos en ENCE.

7.- Categorías de riesgos

Se considera riesgo “cualquier evento potencial que pueda afectar negativamente al cumplimiento de los objetivos de negocio”. En este sentido, Ence tiene identificadas las siguientes tipologías de riesgo:

- **Riesgos de entorno:** situaciones que pueden implicar posibles pérdidas de valor o resultados derivados de la incertidumbre ligada a cambios en el escenario del negocio, la competencia y el mercado o cambios en el marco jurídico y político (entorno económico, comportamiento de clientes, competidores, cambios legislativos, relaciones con las administraciones, relaciones con el entorno vecinal, precio de venta).
- **Riesgos de integridad de la información:** situaciones que pueden implicar posibles errores derivados de un proceso incorrecto de formulación de la información que pudiera ser útil para la toma de decisiones (planificación estratégica, análisis de entorno, valoración, información financiera y contable, información fiscal e impositiva).
- **Riesgos legales:** situaciones derivadas del incumplimiento de normas internas o externas a la compañía, y de conflictos con terceras partes (formalización de contratos, cumplimiento normativo, arbitrajes y litigios, riesgo penal, cumplimiento SCIIF)
- **Riesgos financieros y fiscales:** Situaciones que pueden derivar en posibles pérdidas en los resultados y el patrimonio derivadas de variaciones en los tipos de interés, tipos de cambios, en la liquidez, la morosidad, la disponibilidad de capital, la financiación, el riesgo fiscal y el riesgo de contrapartida de operaciones comerciales.
- **Riesgos operacionales:** surgidos de las operaciones de ENCE (producción, clientes, proveedores, suministradores, tecnología y sistemas de información, fraude, capital humano, medioambiente y entorno).
- **Riesgos de organización:** situaciones que pueden derivar en posibles pérdidas como consecuencia de la gestión del Capital Humano, el fraude, la gestión de los Sistemas, la Continuidad de Negocio o el Gobierno Corporativo.
- **Riesgos derivados del cambio climático:** situaciones que pueden derivar en posibles pérdidas como consecuencia de la variación del clima global de la Tierra debido a causas naturales y a la acción del hombre y que se producen sobre todos los parámetros climáticos (temperatura, precipitaciones,

nubosidad, etc...). Se pueden agrupar en físicos (daños en instalaciones), de transición (políticos y legales, tecnológicos, de mercado y de reputación) y otros, como riesgos en la cadena de suministro y fenómenos sociales.

Para cada uno de los riesgos identificados, se lleva a cabo una clasificación adicional por medio de una categoría que identifica aquellos riesgos con afecciones relacionadas con factores ASG, que son aquellos riesgos relacionados con factores medioambientales, sociales y de gobierno que pueden causar un impacto en una entidad.

En este sentido, Ence aplica los principios y las prácticas del Modelo Enterprise Risk Management (ERM) a los riesgos relacionados con factores ASG a través de la aplicación del marco de “*ERM de COSO Gestión del Riesgo Empresarial —Integrando Estrategia y Desempeño*”.

8.- **Apetito de riesgo**

Se define el **Apetito de Riesgo** como el “nivel de riesgo” - que la compañía quiere aceptar para lograr sus objetivos.

Ence reconoce que su **apetito de riesgo** varía en función de las actividades realizadas y que su grado de aceptación del riesgo se encuentra supeditado a asegurar que los beneficios y los riesgos potenciales son entendidos completamente de manera previa a la toma de decisiones, estableciendo, siempre que sea el caso, medidas razonables para gestionar este tipo de situaciones.

Partiendo de la relación entre riesgo y rentabilidad, Ence analiza cada situación para evaluar cuán dispuesta está la organización a afrontar ese tipo de situaciones. A este respecto, en el análisis intervienen factores como la estrategia, las expectativas de los grupos de interés, la legalidad vigente, el entorno y las relaciones con terceros. En este sentido:

- Ence adopta un **apetito de riesgo nulo** para todas aquellas situaciones en las que la seguridad y la salud de los empleados y colaboradores pudieran verse comprometida, constituyendo una prioridad en sus modos de actuar.
- Ence adopta una **posición de riesgo nulo** para todas aquellas situaciones en las que la operación o realización de alguna actividad pueda suponer un daño para el entorno y el medio ambiente.
- Ence posee un **enfoque de reducir al mínimo su exposición** a aquellas situaciones que se encuentran relacionadas con el cumplimiento de la legislación y la regulación que afecta a la compañía.
- Ence cuenta con un equipo de asesores externos así como de personal interno especializado que han marcado las pautas internas de **cumplimiento fiscal y nula asunción de riesgo** en esta materia.
- Ence adopta un **apetito de riesgo moderado** para las situaciones relacionadas con la investigación, el desarrollo y la innovación de sus productos, orientado a proporcionar

soluciones que satisfagan íntegramente las necesidades de sus clientes y convertirse en un referente del mercado de la celulosa.

- Asimismo, consciente de las dificultades actuales en relación con el entorno económico donde Ence opera, Ence adquiere el compromiso de establecer una disciplina financiera que le permita mantener controlada la deuda total de la organización y le permita disponer de liquidez suficiente para hacer frente a sus pagos y sus inversiones prioritarias. En este sentido, **Ence adopta un apetito de riesgo bajo** de cara a realizar operaciones financieras.
- No obstante, un gran volumen de las operaciones de Ence están asociadas al tipo de cambio entre el dólar y el euro. Ence, consciente de la situación del entorno económico y de la evolución del tipo de cambio entre ambas divisas, adopta un **apetito de riesgo bajo** en este ámbito, por medio de una gestión rigurosa, de acuerdo con las directrices fijadas por la Comisión Ejecutiva del Consejo de Administración y en su caso, de la Dirección General de Finanzas.

9.- Marco de gestión de riesgos en ENCE

9.1 Marco de gestión de riesgos.

El Marco de gestión de riesgos de Ence se basa en el modelo COSO-ERM para la gestión de riesgos empresariales y se resume en que Ence, como organización que posee una visión, una misión, un propósito y unos valores determinados, procura alcanzar sus metas mediante la adopción e implementación de una estrategia global que concentra objetivos concretos desde cuatro perspectivas distintas; objetivos estratégicos, objetivos operacionales, objetivos de cumplimiento y objetivos de reporte e información financiera.

Para alcanzar dichos objetivos y cumplir, así, con su misión, las cosas deben suceder tal y como han sido ideadas y planificadas. No obstante, las características internas de la organización, es decir, sus personas, procesos y sistemas, junto con la naturaleza externa al negocio que presenta su entorno (mercado, normativa, regulación, medio ambiente, etc.) no proporcionan seguridad absoluta sobre si Ence logrará alcanzar sus objetivos y, en caso de hacerlo, de cómo será capaz de hacerlo.

Esta incertidumbre se plasma en situaciones de amenaza concretas sobre los objetivos de Ence (a todos sus niveles), y es por ello por lo que se crea un proceso de gestión de riesgos en el seno de la organización, con el objetivo de identificar, evaluar, priorizar y dar respuesta a esta incertidumbre, articulando metodologías, facilitando canales y flujos de información y reporte y asignando roles y responsabilidades concretas a los actores participantes en dicho proceso, todo ello con el fin último de tratar de ofrecer un nivel de seguridad razonable a la hora de que la organización pueda alcanzar sus metas.

El Marco de gestión de riesgos facilita una infraestructura de carácter sistemático y común para establecer, mantener y mejorar las principales pautas y directrices que constituyen el proceso para tratar los riesgos en todo el Grupo. Se instrumentaliza a través de un proceso orientado a la mejora continua, en el que se encuentran identificados los participantes y las principales responsabilidades que éstos tienen asociadas.

La Dirección de Auditoría Interna, de acuerdo con el marco de responsabilidades y funciones recomendado por el IAI y con el Estatuto de Auditoría Interna aprobado por el Consejo de Administración, lleva a cabo la función de gestión de riesgos en todo el Grupo Ence.

Fecha: 30/05/2023	Política de gestión y control de riesgos	Página 9 de 13
-------------------	--	----------------

Los componentes del Marco de gestión de riesgos se incorporan a toda la organización, ya que parten de un enfoque estratégico en el cual se encuentran alineadas todas las áreas, departamentos y funciones:

- 1) **El Gobierno** de la organización establece las responsabilidades y el ambiente de control para la gestión de riesgos. La **Cultura** de la organización marca los comportamientos deseados y la comprensión del riesgo.
- 2) **Desarrollo de la estrategia y establecimiento de objetivos:** la gestión de los riesgos va unida al establecimiento de la estrategia y la fijación de los objetivos. Se establece un apetito de riesgo y se alinea con la estrategia.
- 3) **Desempeño:** Se identifican y evalúan los riesgos que pueden afectar a la consecución de los objetivos estratégicos. Se priorizan y se establecen acciones mitigantes.
- 4) **Revisión y monitorización:** al examinar el desempeño de la organización, se puede determinar cómo funcionan los componentes de gestión del riesgo empresarial de forma dinámica y si existen aspectos susceptibles de modificación.
- 5) **Información, Comunicación y Reporte:** para ser efectiva, la gestión de riesgos empresariales requiere de un proceso continuo para obtener e intercambiar información necesaria tanto de fuentes internas como externas, con fluidez en todas las direcciones y en toda la organización.

Este marco se encuentra alineado con las mejores prácticas en Control Interno y Gestión de riesgos corporativos (COSO ERM¹ y normativas ISO 31000 en materia de Gestión de Riesgos²) y se muestra en el siguiente esquema, si bien se explica detalladamente en el Procedimiento de gestión de riesgos del ENCE.

9.2 Proceso de gestión de riesgos.

El proceso de gestión de riesgos, tiene su base en el Marco de gestión de riesgos definido en el punto anterior apoyado en el modelo COSO-ERM para la gestión de los riesgos empresariales, y consta de los siguientes elementos:

a) Gobierno y Cultura.

La organización establece las responsabilidades y el ambiente de control para la gestión de riesgos. La cultura de la organización marca los comportamientos deseados y la comprensión del riesgo.

b) Estrategia y establecimiento de objetivos.

ENCE define sus objetivos y el entorno donde opera, desde el punto de vista interno y externo, teniendo en cuenta los intereses de sus grupos de interés, que afecta a su forma de gestionar los riesgos, facilitando la priorización de los mismos.

¹ COSO: *Committee of Sponsoring Organizations of the Treadway Commission*, organización voluntaria del sector privado dedicada a la mejora de la calidad del reporte financiero a través de ética empresarial, controles internos efectivos y gobierno corporativo. El Informe COSO I que establece los 5 componentes básicos del Marco de Control Interno, fue publicado en 1992. En 2004, COSO publicó “*ERM-Integrated Framework*” (COSO II), expandiendo el Marco de Control Interno inicial. En 2017 publicó “*ERM-Integrating with Strategy and Performance*”, actualizando el Marco de Control Interno al entorno empresarial actual.

² ISO 31000:2009 – *Risk Management – Principles and guidelines on implementation*, ISO 31010:2009 – *Risk Management – Risk Assessment Techniques* e ISO Guide 73:2009 – *Risk Management – Vocabulary*.

c) Desempeño:

1) Valoración de Riesgos.

- Detección de riesgos: identificar eventos potenciales que puedan amenazar a los objetivos.
- Análisis de riesgos: determinar sus causas, las áreas de impacto y sus posibles consecuencias.
- Evaluación de riesgos: estimar las consecuencias y su probabilidad de ocurrencia, con el objeto de priorizar las situaciones más preocupantes, en función de la escala de clasificación de riesgos.

2) Tratamiento y respuesta al riesgo.

Consiste en seleccionar y aplicar la mejor respuesta al riesgo, de acuerdo a la situación de que se trate. Una vez implementada, proporciona un nuevo control o modifica uno existente. La respuesta a los riesgos puede ser asumir, transferir, mitigar o eliminar.

Los Responsables de los riesgos seleccionan e implementan las medidas de control de cada uno de los riesgos identificados en su área, siendo los encargados de velar por su correcta aplicación como mitigantes de los riesgos. Como dueños de los procesos de Ence, sus actividades crean o gestionan los riesgos que pueden contribuir o evitar que se alcancen los objetivos fijados por la Organización.

Periódicamente, conforme a la metodología definida en el “*Procedimiento de gestión y control de riesgos*”, se revisa la eficacia de las medidas de control definidas como mitigantes para los riesgos críticos y significativos.

d) Control y revisión del proceso.

Se efectúa un seguimiento y una revisión continua del proceso de gestión de riesgos para identificar, proponer y llevar a cabo las mejoras que sean necesarias.

e) Información, Comunicación y Reporte.

Debemos proporcionar **información** relevante en materia de riesgos desde y hacia todos los niveles implicados en la gestión de riesgos del ENCE, por medio de herramientas como el **registro de riesgos** y el **mapa de riesgos**.

Para la **comunicación**, disponemos de un entorno adecuado y una filosofía de gestión de los riesgos por medio de comunicaciones específicas de la Comisión de Auditoría, orientadas a las expectativas de comportamiento y responsabilidades del personal.

Asimismo, ENCE adopta un programa de comunicación interna destinado a apoyar la integración de su filosofía de gestión de riesgos basado, entre otros, en los siguientes puntos:

- La Dirección comenta los riesgos y las respuestas al riesgo asociadas en sesiones periódicas informativas con sus empleados a todos los niveles
- Las políticas, estándares y procedimientos de gestión de riesgos se facilitan a los empleados, junto con declaraciones firmes acerca de su cumplimiento
- Las sesiones de orientación a nuevos empleados incluyen información y documentación sobre la metodología de la y Política de gestión y control de riesgos.

Fecha: 30/05/2023	Política de gestión y control de riesgos	Página 11 de 13
-------------------	--	-----------------

- La metodología de gestión de riesgos se refuerza a través de programas continuos de comunicación interna y externa, con el fin de consolidar los principios de la cultura de la organización.

10.- Sistemas de información y control interno

Anualmente, Ence lleva a cabo la identificación y evaluación de nuevos riesgos, así como el seguimiento de la evolución de riesgos que hayan sido identificados en períodos anteriores y los riesgos que hayan terminado en el ejercicio. Asimismo, se actualiza la información referente a controles y planes de acción relacionados con los riesgos identificados.

Para ello, Ence cuenta con las siguientes herramientas de gestión:

a) Registro de Riesgos.

El Registro de Riesgos es el formato utilizado para el informe periódico de los principales riesgos identificados y evaluados en las diferentes unidades de negocio.

El Registro de Riesgos es una herramienta que proporciona información estratégica y operativa a las unidades de negocio involucradas en el proceso de gestión del riesgo.

b) Mapa de Riesgos.

El Mapa de Riesgos es el formato utilizado para representar de manera gráfica la probabilidad y el impacto asociados a cada riesgo, y poder identificar de manera inmediata si ha de ser tratado con el correspondiente nivel de prioridad.

De este modo, los Responsables de riesgos pueden centrar sus actuaciones en la gestión de los riesgos con carácter más urgente y, al mismo tiempo, realizar un seguimiento de los cambios de situación registrados en el resto de los riesgos.

11.- Roles y responsabilidades

Los roles y responsabilidades de cada uno de los miembros de la organización que intervienen en el proceso se han definido teniendo en cuenta la metodología COSO-ERM y al modelo de las tres líneas del Instituto de Auditores Internos (AI), asignándose como sigue:

a) Consejo de Administración.

Cuyos roles son los atribuidos en el Reglamento, en concreto:

- ✓ Establecer la Política de gestión y control de riesgos, incluidos los fiscales, y la supervisión de los sistemas internos de información y control.
- ✓ Aprobar las políticas corporativas, y por extensión la Política de gestión y control de riesgos.

b) Comisión de Auditoría.

Es el órgano supervisor de la Gestión de Riesgos. Sus principales funciones son, entre otras:

- ✓ Supervisar los servicios de Auditoría interna.
- ✓ Supervisar y evaluar la adecuación, integridad y eficacia de los sistemas de control interno y de gestión de riesgos financieros y no financieros, relativos a la Sociedad y, en su caso, al grupo,

Fecha: 30/05/2023	Política de gestión y control de riesgos	Página 12 de 13
-------------------	--	-----------------

incluyendo los operativos, tecnológicos, legales, sociales, medioambientales, climáticos, políticos y reputacionales, o relacionados con la corrupción y discutir con los auditores de cuentas o sociedades de auditoría las debilidades significativas del sistema de control interno detectadas en el desarrollo de la auditoría.

- ✓ Supervisar la correcta gestión de los aspectos medioambientales y auditorías de prevención de riesgos laborales.
- ✓ Supervisar el mapa de riesgos previamente a su aprobación por el Consejo de Administración.

c) Dirección de Auditoría Interna:

Es responsable de:

- ✓ Elaborar los procedimientos y criterios del Grupo para la gestión de riesgos y presentarlos al Consejo de Administración, a través de la Comisión de Auditoría, para su aprobación.
- ✓ Comunicar a la Comisión de Auditoría, para su aprobación, los riesgos identificados así como los planes y acciones propuestos por el responsable de riesgos.
- ✓ Elaborar y actualizar periódicamente el mapa de riesgos de Ence a partir de los aprobados previamente.
- ✓ Informar al Consejo de Administración, a través del Comisión de Auditoría, sobre los riesgos que se hubieran materializado, indicando las circunstancias que los han motivado y si han funcionado los sistemas de control establecidos.
- ✓ Asegurar el buen funcionamiento de los sistemas de gestión de riesgos y, en particular, que se identifiquen, gestionen, y cuantifiquen adecuadamente todos los riesgos importantes que afectan a Ence.
- ✓ Velar por que los sistemas de gestión de riesgos mitiguen los riesgos adecuadamente en el marco de la Política de gestión y control de riesgos, llevando a cabo una revisión de la eficacia de las medidas mitigadoras definidas por los responsables de los riesgos.
- ✓ Prestar soporte y asesoramiento a los responsables de los riesgos en todos los asuntos relacionados con la gestión de riesgos.
- ✓ Desarrollar e implementar los procesos de gestión de riesgo y control de la organización.
- ✓ Realizar un seguimiento periódico sobre el grado de ejecución de los planes de acción aprobados.

d) Responsables de riesgos.

Los directores y gerentes de los distintos departamentos de Ence son los responsables de riesgos dentro de sus áreas y desempeñan, entre otras, las siguientes funciones:

- ✓ Utilizar los procedimientos y criterios aprobados por ENCE para la gestión de los riesgos. En concreto:
 - Identificar las situaciones de riesgo que afecten a la consecución de los objetivos de ENCE, dentro de su ámbito de responsabilidad.
 - Evaluar los riesgos identificados, de acuerdo con la metodología disponible.
 - Informar de sus riesgos, mediante su participación en el proceso de reporte de riesgos establecido a tal efecto y mediante las herramientas puestas a su disposición.
- ✓ Seguir las directrices que se indiquen en cada momento en lo relativo a la gestión de riesgos
- ✓ Comunicar a la Dirección de Auditoría Interna los riesgos identificados, los planes y acciones propuestos para mitigar dichos riesgos, así como el grado de avance o implementación de los mismos.
- ✓ Tomar las decisiones sobre las respuestas a los riesgos y asegurar la implementación de las medidas de control.

Fecha: 30/05/2023	Política de gestión y control de riesgos	Página 13 de 13
-------------------	--	-----------------