



Gestión de Riesgos Empresariales Política

NEXA
LISTED
NYSE

Summary

1. OBJETIVO.....	3
2. ALCANCE.....	3
3. REFERENCIAS.....	3
4. DEFINITIONS.....	3
5. RESPONSABILIDADES.....	4
5.2 Comités del Consejo.....	5
5.3 Comité de Gestión.....	5
5.4 Risk Comité de Riesgos.....	6
5.7 Puntos Focales.....	7
5.8 Área de Riesgos.....	7
6. ESTRUCTURA DE GOBERNANZA DE RIESGOS.....	7
7. PROCESO DE GESTIÓN DE RIESGO.....	8
7.2 Análisis de Riesgos.....	9
7.3 Evaluación de Riesgos.....	9
7.4 Apetito de Riesgo.....	9
7.5 Priorización de Riesgos.....	9
7.6 Tratamiento de Riesgos.....	10
7.7 Monitoreo de Riesgos.....	10
7.8 Informes.....	10



1. OBJETIVO

El objetivo de esta política es establecer directrices para el proceso de Gestión de Riesgos Empresariales (ERM) en Nexa Resources S.A. ("Nexa" o la "Empresa"). Define las responsabilidades de todos los participantes en el proceso de ERM, incluyendo la identificación, evaluación, tratamiento, monitoreo y reporte de Riesgos. Esta política tiene como fin integrar las consideraciones de Riesgos en la toma de decisiones estratégicas de la Empresa.

2. ALCANCE

Esta política se aplica a Nexa, sus contratistas supervisadas directamente y todas las subsidiarias y activos que son propiedad, controlados u operados por Nexa, ya sea directa o indirectamente, en todo el mundo.

3. REFERENCIAS

- Marco COSO ERM
- ISO 31000: 2018 Directrices de Gestión de Riesgos
- Estatuto del Comité de Riesgos
- Manual de ERM de Nexa
- Reglamento Interno del Directorio
- Estatutos del Comité de Auditoría, Comité de Finanzas, Comité de Compensaciones, Nominaciones, y Gobernanza, y Comité de Sostenibilidad y Proyectos de Capital
- Reglamento Interno del Management Committee (ManCo)
- Política de Riesgos Financieros de Nexa

4. DEFINITIONS

Apetito de Riesgo: Los tipos y el nivel de Riesgo que la Empresa está dispuesta a asumir en busca de valor.

Área de Riesgo: Área de Nexa responsable de coordinar el proceso de ERM de Nexa y de garantizar el correcto flujo de información y reportes de Riesgos dentro de la Empresa.

Categorías de Riesgo: Taxonomía de Riesgo utilizada para mejorar la gestión integrada de Riesgos, así como para ayudar a la Empresa a determinar su Apetito.

Controles: Actividades que forman parte de las operaciones regulares de la organización, realizadas para mitigar el Impacto o la Probabilidad de un Riesgo.

Directores Ejecutivos: Conjuntamente, el Director General, Vicepresidentes y Directores.

Factores de Riesgo: Factores que contribuyen a que el Riesgo eventualmente se materialice. El mismo Riesgo puede contener uno o más factores relacionados.

Gestión de Riesgos Empresariales ("ERM"): Proceso que tiene como objetivo identificar eventos potenciales que pueden afectar la capacidad de la Empresa para cumplir sus objetivos estratégicos y definir e implementar acciones para gestionarlos. ERM incluye la cultura, capacidades y prácticas, integradas con la definición de estrategias y su desempeño, en las que las organizaciones confían para gestionar Riesgos en la creación, preservación y realización de valor.

Impacto: El resultado o efecto de un Riesgo. Puede haber una variedad de Impactos posibles relacionados con un Riesgo. El Impacto del Riesgo puede ser positivo o negativo en relación con la estrategia de la entidad o sus objetivos empresariales.



Matriz de Riesgos: Diagrama elaborado con base en el análisis general de los Riesgos y en la evaluación propia de la gestión, considerando el Impacto y la Probabilidad de los Riesgos.

Modelo de Gobernanza de Riesgos: Procesos y actividades que Nexa sigue para gestionar los Riesgos.

Plan de Acción: Es una acción temporal y específica con un plazo definido para su implementación. Diseñado para abordar una deficiencia en la gestión de Riesgos o implementar nuevos Controles. Su propósito es cerrar brechas, mejorar o reforzar el control existente. El Plan de Acción debe tener una persona responsable y una fecha de conclusión.

Probabilidad: La posibilidad de que ocurra un Riesgo.

Registro de Riesgos: Registro de información de los Riesgos identificados.

Responsables de Riesgos: Individuos responsables de gestionar Riesgos específicos en sus unidades / áreas.

Riesgo: Cualquier evento potencial que pueda afectar la capacidad de la Empresa para alcanzar sus objetivos y sus planes estratégicos de negocio.

Riesgo Inherente: Nivel intrínseco de Riesgo para el negocio o actividad, sin considerar la implementación de Controles mitigantes o planes de acción.

Riesgo Residual: Nivel remanente de Riesgo después de considerar todos los Controles y planes de acción implementados para mitigar los Riesgos Inherentes.

Riesgos Aceptados: Riesgos que la Empresa opta por no abordar activamente con nuevas medidas porque los Controles existentes se consideran suficientes y, basado en la evaluación, no es posible ni razonable implementar acciones adicionales. Estos Riesgos se aceptarán en su nivel actual de exposición, con un monitoreo continuo para garantizar que no se conviertan en Riesgos que requieran una mitigación o intervención adicional.

Riesgos Emergentes: Riesgos que aún no se han manifestado completamente, pero podrían tener un Impacto significativo en la consecución de los objetivos estratégicos de la organización y potencialmente alterar su perfil de Riesgo en el futuro. Estos Riesgos pueden surgir de cambios tecnológicos, sociales, regulatorios y otros en el contexto empresarial.

Riesgos Priorizados: Riesgos relacionados con la estrategia que son relevantes para la Empresa, ya sea para alcanzar objetivos específicos, que están fuera del Apetito de Riesgo definido, clasificados como “Altos” o “Críticos”

5. RESPONSABILIDADES

5.1 Consejo de Administración

Las principales responsabilidades de supervisión en relación con el ERM de Nexa son:

- Aprobar la orientación general de los negocios de la Empresa, su misión, sus objetivos estratégicos y sus directrices, y asegurar que los Directores Ejecutivos cumplan con dicha misión, objetivos estratégicos y directrices, teniendo en cuenta los Riesgos y el Apetito de la Empresa y de acuerdo con la recomendación de los Comités del Consejo de Administración.
- Revisar y aprobar la declaración de Apetito de Riesgo de la Empresa y sus cambios, cuando sea aplicable.
- Aprobar el presupuesto y el plan estratégico que tienen en cuenta los Riesgos y el Apetito de la Empresa.
- Aprobar la política de ERM de Nexa y monitorear el cumplimiento de esta política.

- Supervisar los Riesgos Priorizados y la exposición al Riesgo de la Empresa.

5.2 Comités del Consejo

Las principales responsabilidades de supervisión de los Comités de Auditoría; Finanzas; Compensaciones Nominaciones y Gobernanza; y Sostenibilidad y Proyectos de Capital en relación con ERM de Nexa son:

- Apoyar al Consejo en su supervisión del ERM de Nexa en asuntos relacionados con las responsabilidades de cada Comité, de acuerdo con los estatutos de cada comité.
- Discutir los Riesgos que serán clasificados como Riesgos Aceptados y someterlos para aprobación del Consejo.
- Discutir los Riesgos Priorizados y cómo se tratan y se monitorean, manteniéndose al tanto de sus Planes de Acción.
- Monitorear los procesos o Controles de la Empresa, incluidas las Acciones de Mitigación que se están tomando.
- Reportar periódicamente al Consejo de Administración su supervisión del proceso de ERM.

Además de las responsabilidades enumeradas anteriormente, el **Comité de Auditoría también asume las siguientes atribuciones:**

- Monitorear los Controles y procesos de gestión de Riesgos de la Empresa, de acuerdo con la Política de ERM.
- Comprender el marco de evaluación de Riesgos de la Empresa, incluidas las directrices y políticas adecuadas para regular el proceso.
- Evaluar la estructura organizativa y las actividades del proceso de gestión de Riesgos de la Empresa.
- Evaluar la implementación y el mantenimiento de las estructuras y políticas de gestión de Riesgos por parte de la dirección.
-

5.3 Comité de Gestión

Las principales atribuciones en relación con el ERM de Nexa son:

- Adoptar un proceso de planificación estratégica y, anualmente, proponer al Consejo el presupuesto de la Empresa y el plan estratégico que considera los Riesgos del negocio.
- Promover y asegurar el cumplimiento de las políticas de la Empresa, así como la política de ERM de la Empresa.
- Proponer el Apetito de Riesgo y presentarlo al Consejo para su revisión y aprobación, conforme a la recomendación de los comités, cuando sea aplicable.
- Recomendar los Riesgos que serán clasificados como Riesgos Aceptados y someterlos para aprobación de los Comités del Consejo.
- Recomendar los Riesgos que serán clasificados como Riesgos Priorizados y someterlos para aprobación de los Comités del Consejo.
- Ejecutar y coordinar el proceso de gestión de Riesgos, asegurando la aplicación de la metodología definida, asistiendo en la supervisión de los Riesgos y el monitoreo del Plan de Acción y los Riesgos Priorizados.
- Individualmente, cada Director Ejecutivo debe realizar periódicamente reuniones con sus respectivos equipos para monitorear los Riesgos identificados y los planes de acción para responder a estos Riesgos y los Controles asociados.



5.4 Comité de Riesgos

El Comité de Riesgos ("RiskCo") es un comité permanente del Comité de Gestión con el propósito principal de ayudarlos a cumplir sus responsabilidades de implementación y ejecución con respecto a:

- Monitorear y gestionar los Riesgos de la Empresa que pueden afectar el logro de los objetivos de la Empresa.
- Proporcionar supervisión en todas las Categorías de Riesgos y mejorar la cultura de Riesgos
- Aprobar y supervisar los procesos utilizados para identificar, evaluar y gestionar Riesgos
- Emitir recomendaciones al Comité de Gestión relacionadas con a) el desempeño de los Controles de Riesgo, b) el cumplimiento de los planes de acción y c) las estrategias de respuesta a Riesgos, entre otros.

5.5 Área de Auditoría Interna, Controles Internos, Cumplimiento y Línea Ética

Las principales atribuciones en relación con el ERM de Nexa son:

- Auditoría Interna: El equipo de Auditoría Interna incorpora la Matriz de Riesgos ERM como insumo para su planificación anual de auditoría, para garantizar un enfoque basado en Riesgos. Identifican Riesgos durante los procesos de auditoría y comunican observaciones significativas a la área de ERM. Además, evalúan la efectividad de los procesos de gestión de Riesgos, garantizando el cumplimiento de las políticas establecidas, y proporcionan recomendaciones para mejorar la mitigación de Riesgos.
- Controles Internos: El equipo de Controles Internos mejora el entorno de control para garantizar que los Controles mitiguen efectivamente los Riesgos identificados y colabora con la área de ERM para compartir el estado de efectividad de los Controles implementados.
- Cumplimiento: El equipo de Cumplimiento integra la Matriz de Riesgos ERM en su planificación anual para abordar los Riesgos clave, asegurando la adhesión a todos los requisitos de cumplimiento relevantes. También investigan posibles violaciones de cumplimiento y comunican cualquier Riesgo identificado al área de ERM.
- Línea Ética: El equipo de Línea Ética proporciona un mecanismo confidencial y seguro para que los empleados informen preocupaciones éticas, mala conducta o Riesgos potenciales. Ellos monitorean e investigan los informes recibidos a través de la línea ética, comunican cualquier Riesgo identificado o cuestiones éticas al área de ERM para su inclusión en el proceso de evaluación de Riesgos, y promueven la conciencia sobre los estándares éticos y la importancia de informar dentro de la organización.

5.6 Responsables de Riesgos

Las principales atribuciones en relación con el ERM de Nexa son:

- Liderar los esfuerzos de gestión de Riesgos, asegurando monitoreo y actualizaciones continuas.
- Promover la participación efectiva y un enfoque multidisciplinario en las evaluaciones de Riesgos.
- Asegurar la definición e implementación de medidas de respuesta en coordinación con los Responsables de Controles y los Responsables de Planes de Acción.



- Monitorear la evolución del Riesgo y el estado de las medidas de respuesta, informando el progreso al Equipo de Riesgos y otros principales interesados.
- Asegurar que las acciones implementadas sean efectivas y estén alineadas con los objetivos estratégicos de Nexa.
- Comunicar los Riesgos Emergentes al Área de Riesgos para incluirlos en la Matriz de Riesgos.

5.7 Puntos Focales

Las principales atribuciones en relación con el ERM de Nexa son:

- Asistir al Área de ERM en el Proceso de Evaluación de Riesgos en su unidad o área corporativa.
- Ayudar al Área de ERM a contactar a los Responsables de Riesgos y expertos.
- Apoyar el monitoreo de Cumplimiento con los Controles y planes de acción.
- Participar en reuniones de seguimiento y monitoreo.
- Promover la comunicación con el equipo de ERM.
- Fomentar la participación en sesiones de capacitación de ERM

5.8 Área de Riesgos

Las principales atribuciones en relación con el ERM de Nexa son:

- Desarrollar la estrategia, aplicar la metodología y promover la cultura de ERM, de acuerdo con las regulaciones vigentes y las mejores prácticas de mercado.
- Monitorear los Riesgos reportados por las unidades y áreas corporativas.
- Monitorear la implementación de los Planes de Acción desarrollados para mitigar los Impactos de los Riesgos identificados.
- Reportar el nivel de exposición de Nexa a los Riesgos identificados a los Directores Ejecutivos, al Comité correspondiente, al Comité de Auditoría y al Consejo de Administración, cuando sea aplicable.
- Monitorear las tendencias del mercado y su conexión con el negocio y posibles Impactos para Nexa.
- Proporcionar entrenamientos para difundir la cultura y la metodología de ERM.
- Discutir la Matriz de Riesgos con las áreas de Auditoría Interna, Controles Internos, Cumplimiento y Línea Ética.

6. ESTRUCTURA DE GOBERNANZA DE RIESGOS

El Modelo Estructurado de Gobernanza de Riesgos de Nexa comprende tres niveles: (i) un **nivel ejecutivo**, que incluye una visión ejecutiva clara en la consolidación de información de Riesgo para el monitoreo por parte del Consejo de Administración; (ii) un **nivel táctico**, donde los líderes tienen foros formales de discusión; y (iii) un **nivel operacional**, donde hay una integración metodológica para que la información esté alineada. A través de este modelo, hay discusiones estructuradas sobre los Riesgos y su priorización, junto con informes periódicos disponibles por los Responsables de Riesgos con el apoyo del área de ERM. Estos tres niveles se detallan a continuación:

- **Nivel Ejecutivo**, El nivel ejecutivo aborda los Riesgos estratégicos y priorizados que podrían impactar significativamente los objetivos a largo plazo y la viabilidad de la empresa. Los principales objetivos en este nivel son proporcionar a la alta dirección una visión consolidada de los Riesgos más significativos y establecer alineación entre la gestión de Riesgos y los objetivos estratégicos de la organización. Este nivel abarca el Consejo de Administración, los Comités del Consejo y los Directores Ejecutivos, quienes son responsables de supervisar la política de Gestión de Riesgos



Empresariales (ERM), definir el Apetito de Riesgo y asegurar la efectividad de los procesos de gestión de Riesgos.

Este nivel comprende el Consejo de Administración, el Comité de Gestión, el Comité de Riesgos y los VPs Corporativos y Directores Ejecutivos (cuando sea aplicable), quienes son responsables de supervisar la política de Gestión de Riesgos Empresariales (ERM), definir el Apetito de Riesgo y asegurar la efectividad de los procesos de gestión de Riesgos.

- **Nivel Táctico**, El nivel táctico aborda los Riesgos identificados por las áreas de negocio y las unidades operativas, teniendo discusiones estructuradas sobre los Riesgos Priorizados y cuáles deben escalar al nivel Ejecutivo. Los principales objetivos en este nivel son traducir las políticas estratégicas en acciones concretas y asegurar que las estrategias definidas por la alta dirección se ejecuten correctamente.

Este nivel incluye VPs Corporativos, Gerentes Generales de Unidades Operativas y Gerentes Generales de Áreas Corporativas, quienes supervisan la implementación de estrategias de mitigación, monitorean los planes de acción y toman decisiones informadas sobre cuáles Riesgos escalar.

- **Nivel Operacional**, El nivel operacional aborda los Riesgos que surgen en los procesos operativos diarios, incluida la salud y seguridad del personal. El objetivo principal en este nivel es gestionar los Riesgos que surgen de las actividades diarias y procesos operativos, evitando que escalen a niveles superiores de la organización. Este nivel está enfocado en abordar eventos que pueden comprometer los procesos de producción, así como la salud y seguridad de los involucrados. Este nivel está compuesto por todos los empleados relacionados con la primera fase del proceso de ERM y es una actividad recurrente.

Este nivel involucra a los Gerentes Generales de Unidades Operativas, Gerentes de Área dentro de las Unidades y Líderes de Proceso que participan en la fase inicial del proceso de ERM, enfocándose en la identificación y el reporte de Riesgos operativos y de seguridad de manera recurrente.

7. PROCESO DE GESTIÓN DE RIESGO

Nuestro proceso general para evaluar y gestionar Riesgos es consistente con los marcos de COSO ERM e ISO 31000. Incluye prácticas sistemáticas y comunes dentro de Nexa y sus subsidiarias para establecer el contexto de Riesgo y comunicar, discutir, identificar, evaluar, tratar, monitorear, registrar e informar sobre los Riesgos.

El proceso de ERM en Nexa incluye Riesgos de diferente naturaleza: Estratégicos, Financieros, Operacionales y Cumplimiento.

El ERM también debe relacionarse con otros procesos de gestión. El ERM se vuelve más efectivo al integrar prácticas de ERM con actividades empresariales y comprender cómo el Riesgo afecta potencialmente a la entidad en su conjunto. De esta manera, como parte del proceso de ERM, junto con todas las áreas y unidades de negocio, se identifican más Riesgos operacionales y relacionados con proyectos para ayudar a la Empresa a mantener sus Riesgos dentro de su Apetito de Riesgo.

Todos los Riesgos identificados son, al menos, revisados y actualizados anualmente si es necesario. Además, las áreas de negocio y las unidades de Nexa tienen la facultad de incluir Riesgos Emergentes en cualquier momento, fuera de la fase anual de identificación del proceso de ERM, ya que pueden surgir nuevas situaciones o ocurrir cambios.

Las principales etapas del proceso de gestión de Riesgos son las siguientes:

7.1 Identificación de Riesgos



La etapa de identificación de Riesgos implica reconocer y documentar sistemáticamente los Riesgos que podrían afectar potencialmente el logro de los objetivos de la organización. Esto incluye identificar Riesgos, Factores de Riesgo y sus Impactos potenciales. Los Riesgos se clasifican de acuerdo con la taxonomía de Riesgos definida, lo cual ayuda a categorizarlos y organizarlos para un análisis posterior.

7.2 Análisis de Riesgos

Durante la fase de análisis de Riesgos, se mapean los Controles existentes y se designan los Responsables de Riesgos. Este paso es crucial para comprender el entorno de Riesgo actual e identificar dónde pueden ser necesarios Controles o intervenciones adicionales.

7.3 Evaluación de Riesgos

Evaluar los Riesgos en función de su Impacto y Probabilidad.

- *Impacto:* Se consideran las consecuencias de su materialización y se evalúan en siete (7) dimensiones: financiera, ambiental, salud y seguridad, social y derechos humanos, legal y Cumplimiento, reputacional y cibernética y seguridad de la información. El Impacto se clasifica en cinco (5) niveles: mínimo, menor, moderado, mayor y extremo.
- *Probabilidad:* La posibilidad de su ocurrencia se determina y se evalúa en cinco (5) niveles: remoto, improbable, ocasional, probable y muy probable.

Como resultado de la evaluación, los Riesgos se clasifican en cinco (5) niveles: Muy Bajo, Bajo, Medio, Alto o Crítico.

7.4 Apetito de Riesgo

El Apetito de Riesgo es el grado de Riesgo que la Empresa está dispuesta a asumir en busca de valor o para alcanzar un nivel deseado de retorno o crecimiento – resultado. Busca un equilibrio entre Riesgo y recompensa y puede variar a lo largo del tiempo y de área en área dentro del trabajo. El Apetito de Riesgo debe ser propuesto por el Comité de Gestión y aprobado por el Consejo de Administración, siendo comunicado en toda la organización.

El Apetito de Riesgo de Nexa es parte de su proceso general de Riesgo, y sus principales objetivos se describen a continuación:

- Crear transparencia y coherencia para el tipo y nivel de Riesgos que la Empresa está dispuesta a asumir para alcanzar objetivos estratégicos y operativos.
- Promover el comportamiento en relación con los Riesgos y establecer el tono para la cultura de Riesgos en la Empresa.
- Proporcionar un punto de referencia para la evaluación comparativa de la toma de Riesgos y las estrategias de respuesta requeridas.
- Eliminar la aversión excesiva al Riesgo, articulando la preferencia por la toma de Riesgos.
- Definir umbrales para la toma de Riesgos que optimicen Riesgo y recompensa.
- Ayudar a integrar la toma de Riesgos y la gestión del desempeño.
- Auxiliar en la definición de métricas de Riesgo que apoyen las operaciones comerciales diarias.

7.5 Priorización de Riesgos



Con base en la evaluación y el apetito, los Riesgos se priorizan para definir las opciones de tratamiento apropiadas.

7.6 Tratamiento de Riesgos

Los Riesgos clasificados como “Altos” o “Críticos” y los Riesgos “Fuera del Apetito” deben ser priorizados para mitigar su Impacto y/o Probabilidad. El desarrollo de planes de acción para reducir los niveles de Riesgo es obligatorio.

El propósito del tratamiento de Riesgos es seleccionar e implementar opciones para abordar los Riesgos, implicando la selección, formalización e implementación de planes de acción. Estas opciones pueden incluir eliminar la fuente del Riesgo, alterar su Probabilidad, aprovechar oportunidades, modificar sus consecuencias, compartir el Riesgo o retener el Riesgo. El tratamiento más adecuado implica equilibrar los beneficios potenciales contra los costos, esfuerzos o desventajas de la implementación.

Los Responsables de Riesgos juegan un papel clave en el desarrollo de planes de acción, especificando recursos necesarios, individuos responsables y cronogramas. El Área de Riesgos proporciona orientación y apoyo metodológico a los Responsables de Riesgos. Los Riesgos que no pueden ser mitigados para reducir la exposición de Nexa deben ser discutidos en el nivel apropiado para su aprobación como Riesgos Aceptados, considerando el Apetito de Riesgo de Nexa.

7.7 Monitoreo de Riesgos

El monitoreo de los planes de acción, la evaluación de cambios en el nivel de Impacto o la Probabilidad del Riesgo, debido a factores internos o externos, debe realizarse regularmente.

7.8 Informes

El Área de Riesgos es responsable de estructurar las acciones necesarias y los materiales relevantes a lo que debe ser presentado en cada nivel de gobernanza, considerando la jerarquía de la información. Estos materiales deben ser actualizados de acuerdo con la frecuencia de los foros aplicables.

