PL.073

GESTIÓN INTEGRAL DE RIESGOS

VERSION 05

CEO
Compañía Energética de Occidente

1. OBJETIVO Y ALCANCE

La presente política tiene como objetivo describir el marco común de actuación para la Gestión Integral de Riesgos en la Compañía Energética de Occidente S.A.S E.S.P (En adelante CEO) estableciendo los componentes y capacidades requeridas para asegurar su correcta implementación, despliegue y sostenibilidad en el tiempo.

La Política aplica a todo el personal y directivos de CEO. Este podrá ser modificado y/o complementado previo consentimiento de la Gerencia Corporativa de Riesgos y Cumplimiento de Promigas.

2. DEFINICIONES

- **Agregación de riesgos**: Es la representación gráfica que permitirá a la Alta Dirección de la compañía visualizar el Mapa de Riesgos en los que incurre el negocio y el nivel en el que estos se encuentran (Extremo, Alto, Moderado y Bajo).

- **Apetito de Riesgo:** Es la es el nivel de exposición al riesgo que una empresa está dispuesta a asumir en el desarrollo de su actividad con el fin de alcanzar sus objetivos estratégicos y cumplir con su plan de negocios. El importe total de los riesgos asumidos será la base inicial para el desarrollo de todos los procesos de gestión de riesgos y de sus límites.

- **Capacidad de Riesgo:** Máxima pérdida que la compañía puede llegar a mantener y permitiendo la viabilidad del negocio, esto sin incumplir los límites de capital, liquidez y a nivel de conductas.

- **Comité de Riesgos Compañías Vinculadas:** Comité dirigido por la Gerencia Corporativa de Riesgos y Cumplimiento de CEO, integrado por los líderes de riesgos de las compañías vinculadas como mecanismo de seguimiento, coordinación, cooperación e intercambio de buenas prácticas entre las compañías.

- **Control:** Actividad establecida para gestionar los riesgos y potenciar el logro de los objetivos. Debe ser específico, periódico y adaptable.

- **Límites de Tolerancia:** Es el nivel aceptable de variación o desviación frente al apetito de riesgo que la empresa está dispuesta a aceptar en la búsqueda del logro de sus objetivos. Esta se mide en términos absolutos o porcentuales y sirve de límite para evitar llegar a su capacidad máxima de asunción de riesgos.

- **Modelo de las Tres Líneas**: Modelo que facilita la asignación de deberes y funciones esenciales de la administración de los riesgos y controles, para asegurar la gestión eficaz de los mismos y el cumplimiento de los objetivos de la Organización.

    - **Primera línea:** Conformada por las gerencias, líderes de procesos y gerentes de proyectos de la Compañía. Son los responsables de ejecutar sus procesos y de autogestionar sus riesgos, a través de la identificación, evaluación y tratamiento de estos. Definen y ejecutan los procedimientos de control sobre los riesgos e implementar las acciones correctivas necesarias.

    - **Segunda línea:** Conformada por la Dirección de Riesgos y Cumplimiento. Es responsable de definir los lineamientos y metodología de la gestión de riesgos, monitorear su implementación y acompañar, asesorar y recomendar a la primera línea de defensa en la definición de prácticas efectivas de gestión de riesgos y en el logro de los objetivos de la Compañía.

    - **Tercera línea:** Conformada por la Auditoría Interna, quienes dependen directamente del Comité de Auditoría y Riesgos y son los responsables de evaluar, de forma independiente y objetiva, la gestión

de riesgos, de procesos y de sistemas de información en la Organización, reportando los resultados al Comité. Su evaluación proporciona seguridad razonable sobre la eficacia del gobierno, la gestión de riesgos y del control interno, incluyendo la forma en que la primera y segunda línea de defensa logran los objetivos de gestión de riesgos y control.

- **Perfil de Riesgo:** Es la categoría de clasificación de los riesgos de acuerdo con su criticidad (combinación de impacto y probabilidad). Se cuenta con cuatro niveles de riesgos (bajo, moderado, alto y extremo) las cuales son organizadas en una matriz de 5x5 de acuerdo con el apetito de riesgo, nivel de tolerancia y capacidad del riesgo definido por la empresa.

- **Riesgo:** Son eventos futuros inciertos, tanto positivos como negativos, que tienen el potencial de afectar el logro de las metas y objetivos de una empresa.

- **Riesgo Inherente:** Nivel de riesgo propio o natural de la actividad. Este nivel no tiene en cuenta el efecto mitigante de los controles.

- **Riesgo Residual:** Nivel resultante del riesgo después de aplicar el efecto mitigante de los controles.

- **Tolerancia al Riesgo**: Límite superior al apetito de riesgo, pero menor a la capacidad de riesgo, que requiere cierto nivel de retención de fondos para cubrirlo en caso de que llegase a materializarse.

- **Umbrales de Apetito de Riesgo:** Medidas cuantitativas por tipo de riesgo desarrolladas con base en supuestos, utilizadas para la definición del apetito de riesgos de la compañía, e incorporadas en la declaración del apetito de riesgos. Los límites pueden ser calculados por tipo de riesgo, a nivel de las líneas de negocios, para toda la Compañía, por jurisdicción o, pueden incorporar categorías específicas de riesgos y/o de concentraciones.

3. CONDICIONES GENERALES

3.1 GESTIÓN INTEGRAL DEL RIESGO

Este documento define el marco común del modelo de Gobierno de las funciones de Gestión Integral de Riesgos en CEO, el cual se soporta en las siguientes premisas:

- En CEO la Gestión Integral de Riesgos no es un tema aislado ya que desde el Código de Buen Gobierno se establece que todas nuestras actividades deben ser realizadas con una óptima gestión del riesgo. En cada uno de los compromisos se enfatiza esta gestión teniendo en cuenta los diferentes grupos de interés.

- En CEO todos son responsables de la adecuada gestión de riesgos asociados a cada actividad, proceso, proyecto, entre otros y así mismo del reporte oportuno de los eventos de riesgos materializados a la Dirección de Riesgos y Cumplimiento, propendiendo por la resiliencia Corporativa.

- El modelo de gestión integral de riesgos de CEO cumple y toma como base los requisitos establecidos en el componente de "Evaluación de Riesgos" de COSO 2013, en la NTC ISO 31000 Gestión del Riesgo y más requisitos aplicables como, M-AR-01 Política para la Gestión Integral de Riesgos del conglomerado y M-AR-RO-01 Política Corporativa para la gestión de riesgo operativo.

- La Gestión Integral de Riesgos Corporativa se realiza en cuatro niveles: Riesgos operativos, Riesgos por procesos, Riesgos Inherentes de Mayor Impacto y Riesgos estratégicos y adicional se realiza un análisis de riesgos por proyectos. Este se realiza a los proyectos que tienen un presupuesto superior a cinco (5) millones de dólares o para aquellos que requieren Formato de Revisión de Transacciones-

FRT, la gestión de riesgos es obligatoria, para aquellos que no superen este monto se realiza sólo si el Gerente del Proyecto lo requiere.

- De acuerdo con la naturaleza y el tipo del riesgo, la metodología de gestión de riesgos estratégicos, procesos y riesgos inherentes de mayor impacto debe realizarse de acuerdo con los lineamientos establecidos en el MN.157-Manual de Gestión Integral de Riesgos.

- La Gestión de Riesgos en CEO hace parte del Sistema de Control Interno de la Compañía.

- El reporte sobre el estado de la Gestión Integral de Riesgos a la Junta directiva se realiza a través del mecanismo establecido como el Comité de Auditoría, Riesgo y Buen Gobierno donde deberá hacerse por lo menos una (1) vez al año, en la presentación de los Riesgos Estratégicos.

- Todos los procesos que impliquen contratación de cualquier materia, generación de proyectos, nuevas inversiones, adquisiciones, Joint Ventures, mejoras en procesos y metodologías deben tener presente la política y documentación correspondientes a la identificación de riesgos para las actividades a ejecutar, contando con la asesoría, apoyo y el visto bueno, según aplique, de la Dirección de Riesgos y Cumplimiento.

3.2 PRINCIPIOS

La Política de Gestión Integral de Riesgos de CEO se rige por los siguientes principios de general aceptación a nivel internacional, como buenas prácticas para un marco efectivo de aplicación y control de riesgos.

3.2.1. Principio 1. Autocontrol y Autogestión

La Gestión Integral de Riesgos debe propender por el autocontrol, lo que implica que las personas deben considerar el control como parte inherente de sus responsabilidades, campos de acción y toma de decisiones, asegurando que se tengan implementados y documentados los controles pertinentes para mitigar los riesgos a los que se encuentren expuestos sus procesos o la empresa.

La gestión de riesgos debe ser integrada como parte de las responsabilidades diarias de las personas que participan en los distintos procesos (incluida la Alta Dirección), estas serán responsables, según se defina en la matriz de roles y responsabilidades de CEO, de identificar, evaluar, medir, controlar, monitorear y reportar los posibles riesgos o eventos de riesgos materializados.

En el mismo sentido, el autocontrol puede incluir pruebas independientes, observaciones, consultas, revisiones, entre otros, y pueden ser realizados por personal independiente a la operación diaria, pero que se encuentre capacitado sobre la forma en que funcionan las actividades sujetas a evaluación.

3.2.2. Principio 2. La Cooperación, Coordinación e Intercambio de Información entre CEO y Empresas:

CEO deberá propender por una oportuna y permanente cooperación e intercambio de información para fortalecer la cultura, filosofía y la gestión integral de riesgos que permitan la generación de mecanismos efectivos de reporte de información hacia arriba (hacia la Junta Directiva y la Alta Dirección) que sea veraz, comprensible y completa, de forma que constituya un efectivo apoyo para la administración.

3.2.3. Principio 3. Evaluación Independiente:

Corresponde a la Auditoría Interna desarrollar y mantener una sólida comprensión de sus operaciones, requerir las acciones correctivas oportunas que estimen y/o garanticen el cumplimiento del marco prudencial, a través de la realización de las

actividades de auditoría que estimen pertinentes, de acuerdo con su criterio y con la independencia que las caracteriza, enfocadas a generar cohesión a nivel de la Organización para la existencia de una Arquitectura de Control con alcance consolidado.

3.2.4. Principio 4. Realizar un Seguimiento Continuo:

El seguimiento continuo constituye un aspecto esencial de una sólida y eficaz gestión del riesgo. Cada compañía debe gestionar eficazmente sus riesgos gracias al conocimiento de las actividades operativas/financieras del negocio, así como del funcionamiento de los servicios en los que operamos.

3.2.5. Principio 5. Agregación de Riesgos:

CEO como parte de los objetivos de la presente Política de Gestión Integral de Riesgos, dará seguimiento a los riesgos materiales que se presenten en la Compañía.

3.2.6. Principio 6. Cultura con Enfoque en Gestión de Riesgos:

CEO debe contar con los procesos y procedimientos para generar una cultura de gestión de riesgos. La cultura se refiere a valores éticos, comportamientos deseados y comprensión del riesgo en la entidad, y se refleja en la toma de decisiones.

4. CONTENIDO

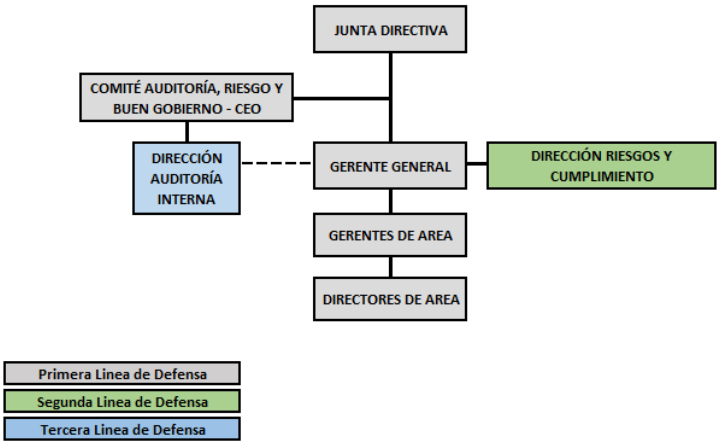
4.1. ESTRUCTURA Y GOBIERNO PARA LA GESTIÓN INTEGRAL DE RIESGOS

CEO dará seguimiento consolidado a la gestión integral de riesgos de la organización, propendiendo porque la misma cuente con una estructura funcional y de gestión transparente, que sea consistente con su estrategia y perfil de riesgo, necesaria para la ejecución apropiada del proceso, que permita generar información para la toma de decisiones.

CEO tiene estructurada las funciones y responsabilidades frente a sus riesgos, siguiendo el esquema de las tres líneas de defensa:

El siguiente esquema establece el marco de responsabilidad frente a la Gestión Integral de Riesgos de CEO:

FIGURA 1. Estructura y Gobierno para la Gestión de Riesgos



CEO ha definido las funciones y responsabilidades generales para la operación de La Gestión Integral de Riesgos, siguiendo el esquema de las tres líneas de defensa, esto es, considerando (i) la gestión por la línea de negocio, (ii) una función de gestión del riesgo independiente, y (iii) una revisión independiente.

4.1.1. PRIMERA LINEA

La primera línea de defensa la constituyen cada una de las áreas o colaboradores al interior de las compañías que gestionan el negocio, son los dueños de procesos, llamados gestores de riesgos. Esto significa que quienes conforman esta línea de defensa tienen las siguientes funciones:

- Responsables en primera medida de identificar, evaluar, gestionar, monitorear y reportar los riesgos asociados a sus procesos.
- Evaluar la suficiencia de los controles implementados para contener los riesgos de su proceso.
- Identificar, remediar y reportar brechas en los límites de riesgos.
- Reportar a la 2da línea los cambios presentados en los riesgos y controles asociados a sus procesos.
- Trabajar con el apoyo de la 2da línea para remediar las brechas identificadas.
- Mantener las matrices de riesgo vigentes de acuerdo con los cambios presentados en sus procesos.
- Reportar los eventos de riesgo presentados de manera oportuna, clara y concisa.

4.1.2. SEGUNDA LÍNEA

Esta línea de defensa está conformada por la Dirección de Riesgos y Cumplimiento, las cuales deben hacer un seguimiento continuo al cumplimiento de todas las obligaciones en materia de Riesgo:

- Establecer un marco de gestión del riesgo acorde con el tamaño, el perfil y la complejidad de las operaciones de la organización.
- Apoyar metodológicamente a la primera línea en la identificación y gestión de sus riesgos.
- Monitorear que los niveles de riesgo sean consistentes con el apetito, la política y los requisitos reglamentarios.
- Establecer el gobierno adecuado requerido para asegurarse que la primera línea sea la dueña de los riesgos.
- Presentar el perfil de riesgo de la organización y la gestión de riesgo efectuada a la Alta Gerencia.

4.1.3. TERCERA LÍNEA

La tercera línea de defensa juega un papel importante al evaluar de forma independiente la gestión y los controles de los riesgos de la Compañía, así como los procesos y sistemas que conforman, rindiendo cuentas al Comité de Auditoría y Riesgos. Las personas encargadas de auditorías internas que deben realizar estas revisiones deben ser competentes y estar debidamente capacitadas y no participar en el desarrollo, implementación y operación de la estructura de riesgo/control. Esta revisión puede ser realizada por el personal de auditoría o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados. Las funciones de esta línea son:

- Elaborar el plan anual de auditoría y darle estricto cumplimiento.
- Realizar una evaluación detallada de la efectividad y adecuación del SCI, en los procesos de la organización que resulten relevantes.
- Revisar los procedimientos adoptados por la administración para garantizar el cumplimiento con los requerimientos legales y regulatorios, códigos internos y la implementación de políticas y procedimientos.
- Hacer seguimiento a la implementación de los planes de acción, establecidos por la organización.

4.1.4. GOBIERNO DEL MODELO DE GESTIÓN INTEGRAL DE RIESGOS

CEO ha establecido las siguientes responsabilidades y funciones de la estructura del modelo de gobierno de la Gestión Integral de Riesgos:

Junta Directiva

- Asegurar el establecimiento de la Gestión Integral de riesgos para la Compañía y validar los avances en el aseguramiento y nivel de madurez de este.
- Asegurar una estructura organizacional adecuada que soporte La Gestión Integral de Riesgos.
- Aprobar anualmente los Riesgos Estratégicos.
- Conocer y Aprobar la Política de Gestión Integral de Riesgos.

Comité de Auditoría y Riesgo

La Junta Directiva a través de su Comité de Auditoría y Riesgo debe:

- Establecer directrices para la gestión de riesgos y cumplimiento de acuerdo con las mejores prácticas GRC y los objetivos de la Compañía.
- Promover la integración de la gestión de riesgos en todos los procesos de la organización.
- Impulsar la adecuación de la gestión del riesgo de la Compañía a un modelo avanzado que permita la configuración de un perfil de riesgos acorde con los objetivos estratégicos.
- Recomendar para aprobación de la Junta Directiva la Política de Gestión integral de riesgos de negocios, el Apetito de Riesgo, Perfil de riesgo, los Riesgos Estratégicos, entre otros aspectos de alto nivel relacionados con el tema.
- Conocer los principales riesgos de la Sociedad y el resultado de los monitoreos realizados a los mismos y realizar seguimiento a los planes de acción establecidos en Junta Directiva para la gestión de riesgos.
- Informar a la Asamblea General de Accionistas sobre la gestión de riesgos de la sociedad, mediante un apartado especial consignado en el informe de gestión de la Junta Directiva.

- Revisar y evaluar la integridad y la adecuación de la función de gestión de riesgos de la sociedad. (Analizar y evaluar los sistemas y herramientas de control de riesgos de la sociedad).
- Realizar seguimiento del grado de adecuación de los riesgos asumidos acorde con el perfil de riesgos definido.

Comité de Gerencia

Las responsabilidades de este Comité en materia de Gestión de Riesgos son las siguientes:

- Promover la apropiación de los temas de Riesgos
- Hacer seguimiento al desarrollo y resultados de los temas de Riesgos.
- Revisar y monitorear riesgos estratégicos, riesgos inherentes de mayor impacto, de reporte financiero y corrupción.
- Proponer mejoras a los lineamientos de la Gestión Integral de Riesgos para aprobación de la Junta Directiva.
- Identificar alertas o temas clave de gestión de riesgos que deban ser informadas a la Junta Directiva.
- Aprobar estrategias para la construcción de una cultura organizacional de gestión de riesgos.

Gerencia General y Gerencias de Área

La Alta Dirección es la dueña y la responsable final de los procesos y de los riesgos estratégicos, riesgos inherentes de mayor impacto, de procesos, de corrupción, LAFT, SOX, seguridad de la información, proyectos a su cargo y debe implementar la Gestión Integral de riesgos dentro de su dependencia o negocio, y asegurar la aplicación oportuna de las etapas del ciclo de gestión de riesgos.

Las principales responsabilidades en materia de Gestión Integral de Riesgos son:

- Velar por la aplicación de la Gestión Integral de Riesgos (planeación, identificación, evaluación, tratamiento, monitoreo y comunicación), de manera oportuna y de acuerdo con los lineamientos establecidos en materia de gestión de riesgos en la estructura de la Compañía.
- Proveer los recursos necesarios para la aplicación de la Gestión Integral de Riesgos. Asignar a cada uno de los riesgos un responsable de riesgo idóneo
- Revisar y asegurar la efectividad, eficacia y eficiencia de los controles definidos en los planes de tratamiento de riesgos.
- Asegurar y promover la cultura en gestión de riesgos en los procesos o programas y proyectos bajo su responsabilidad.

Dirección de Riesgos y Cumplimiento

- Proponer la estrategia y lineamientos para implementar la Gestión Integral de riesgos en CEO.
- Determinar los lineamientos mínimos para la Gestión de Riesgos en compañías vinculadas.
- Asegurar que la implementación del ciclo de Gestión Integral de Riesgos sea un proceso continuo y en constante desarrollo, basado en la planeación estratégica de la empresa.
- Asegurar la consolidación de una cultura con enfoque basada en riesgos.
- Reportar a la alta dirección el estado consolidado de la gestión integral de los riesgos de CEO (avance de planes de tratamiento, incidentes relacionados con la posible materialización de los riesgos).
- Reportar al Comité de Auditoría y Riesgo los riesgos estratégicos y política de gestión integral de riesgos.
- Presentar a la alta dirección propuestas de mejora a la de Gestión Integral de Riesgos.
- Proveer a la organización de los elementos de Gestión de Riesgos necesarios para el adecuado análisis de riesgos de casos de negocio a través del acompañamiento.

- Asegurar que la implementación del ciclo de Gestión Integral de Riesgos en cada compañía sea un proceso continuo y en constante desarrollo, basado en los lineamientos definidos en esta política y manual de gestión integral de riesgos.
- Reportar a la Gerencia de Riesgos y Cumplimiento de Promigas el seguimiento de la gestión integral de riesgos, al igual que cuando se presente un evento de riesgo en la Compañía o un incidente presentado con posible materialización de los riesgos.
- Proveer a la Compañía los elementos de Gestión de Riesgos necesarios para el adecuado análisis de riesgos de casos de negocio a través del acompañamiento.
- Participar activamente en los comités y encuentros de riesgos de las Compañías.

Gerente, Líder de proceso o Gerente de Proyecto

Cada Gerente, Líder de proceso o Gerente de Proyecto es responsable de elaborar con el apoyo del equipo de expertos de su proceso y la Dirección de Riesgos y Cumplimiento, el plan de tratamiento de cada uno de los riesgos a su cargo, para lo cual debe:

- Validar el análisis de causas de los riesgos a su cargo.
- Priorizar las causas identificadas para cada riesgo, con el objetivo de obtener el Pareto de las mismas y de concentrar los esfuerzos y recursos en aquellas causas de mayor incidencia en la ocurrencia o materialización del riesgo.
- Actualizar sus matrices de riesgos cuando consideren pertinente.
- Para las causas principales, seleccionar las opciones de tratamiento requeridas y establecer las acciones, que se consideren efectivas, eficaces, y eficientes, de tal manera que se disminuyan los impactos negativos o se incrementen las consecuencias y probabilidad de su ocurrencia.
- En caso de que un control deba ser ejecutada por un proceso ajeno al propio, el responsable del riesgo debe coordinar, que se involucre y se consulte, con el fin de concertar conjuntamente el ejecutor del control, los recursos y las fechas de inicio y finalización de esta.
- Designar el responsable del control, quien debe contar con el empoderamiento adecuado para llevar a cabo el cumplimiento de esta.
- Responsable porque se ejecuten los controles y de la realización de la evaluación de la eficacia de estos.
- Consolidar el plan de tratamiento del proceso o proyecto.
- Comunicar los resultados y responsabilidades establecidas en el plan de tratamiento a todos los interesados.
- Asegurar el reporte de los incidentes o eventos de riesgos materializados durante el periodo y las causas asociadas a los mismos a la Dirección de Riesgos y Cumplimiento en el momento que se presenten.

Colaboradores de CEO

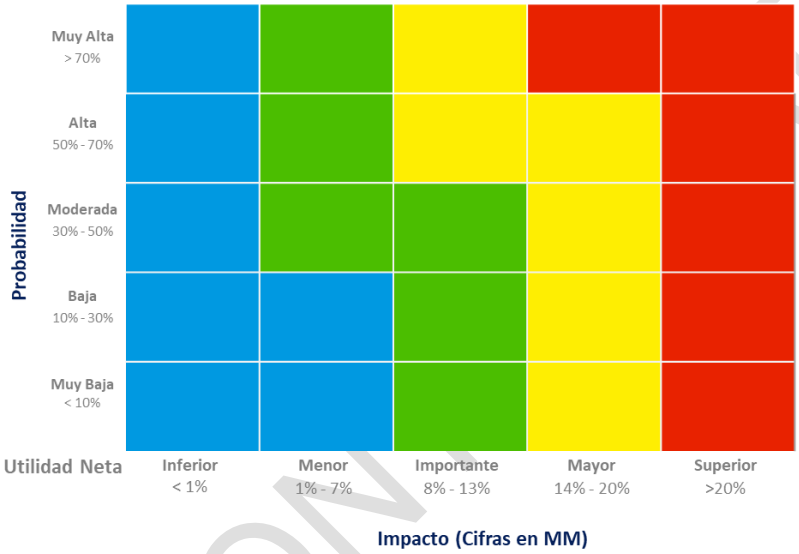
Todos los colaboradores son responsables por administrar los riesgos generados por los procesos o proyectos a su cargo, mediante la implementación del Ciclo de Gestión de Riesgos. Así mismo, deben participar en la implementación del ciclo, estableciendo medidas preventivas y reportando nuevos riesgos, incidentes o eventos de riesgos materializados, diligenciando el FR-960. “Reporte de Riesgo(s)/evento(s) de riesgos materializados”.

4.2. APETITO DE RIESGOS

El apetito de riesgos se constituye como un punto de enlace entre la estrategia de negocio, el plan financiero y la gestión integral de riesgos.

Se relaciona con la cantidad de exposición al riesgo o la afectación potencial de un evento que la corporación está dispuesta a aceptar para el logro de sus objetivos y tiene en cuenta la relación existente entre los riesgos estratégicos y las capacidades internas y externas de la organización para gestionar dichos riesgos.

Los riesgos estratégicos corporativos se calculan con base en la Utilidad Neta presupuestada para el año, los niveles de apetito y tolerancia al riesgo, este se actualizará de acuerdo valor presupuestado para cada año y cada Compañía. Estos se calculan utilizando el mayor valor de cada rango de las escalas de impacto y probabilidad y haciendo el cruce de estos en cada una de las casillas de la matriz de riesgos.



Este mismo procedimiento se realiza en todas las casillas de la matriz. El mayor valor resultante en la zona azul será el valor de Muy bajo apetito de riesgo, en la zona verde será bajo tolerancia del riesgo, la zona amarilla será moderado máxima tolerancia al riesgo y en la zona roja será el Alto máximo nivel de tolerancia.

NIVEL DE RIESGOS:

Corresponde al resultado de la combinación de la probabilidad y el impacto, que permite determinar el nivel de riesgo (perfil de riesgo) en CEO el cual estará dado bajo una calificación de 4 niveles, siendo el primer nivel bajo y el 4 extremo.

Niveles de riesgos
Extremo - Capacidad
Alto - Tolerancia
Moderado – Límite de apetito
Bajo - Apetito

Esta colorimetría será usada en los mapas de calor y en el apetito del riesgo para CEO.

Extremo - Capacidad: Corresponden a riesgos ubicados en la colorimetría roja en el mapa de calor con alto impacto, se ha superado el límite máximo de desviación, frente al riesgo que se planteó para su

estrategia. En caso de que aplique se definen planes de acción e implementación de controles fuertes que permitan que el nivel de amenaza disminuya y se ubique en niveles aceptables.

Alto – Tolerancia: Corresponden a riesgos ubicados en la colorimetría amarilla en el mapa de calor con un mayor impacto. Esta exposición es una desviación admisible para el cumplimiento de la estrategia que no pone en un riesgo desmedido a la Compañía. No requieren acciones inmediatas, pero en caso de que aplique se puede definir un plan de acción que permita que los mismos retornen a niveles aceptables.

Moderado – Límite apetito: Corresponden a riesgos ubicados en la colorimetría verde en el mapa de calor con un impacto importante, el riesgo ha ido incrementándose o deteriorándose. Sobre estos riesgos se debe monitorear los controles para que mantengan su efectividad e impidan el desplazamiento a niveles altos o extremos.

Bajo - Apetito: Corresponden a riesgos ubicados en la colorimetría azul en el mapa de calor con bajo impacto. El riesgo se encuentra en un nivel normal. Son riesgos ampliamente aceptables y adecuadamente controlados; deben ser monitoreados para evitar su desplazamiento a zonas de mayor riesgo.

4.3. COMUNICACIÓN

La comunicación permite la socialización de los resultados y el adecuado flujo de información y diálogo entre los interesados o partes involucradas. Se define como un proceso interactivo de intercambio de información y opinión.

La comunicación debe asegurar:

- Generación de un lenguaje común y cultura en materia de gestión de riesgos.
- Divulgación de los roles y responsabilidades de los participantes e involucrados.
- Divulgación de la información relevante que pueda tener injerencia en la percepción del riesgo que tienen las partes interesadas.
- Divulgación de los resultados (salidas) de la aplicación de cada etapa del ciclo de gestión de riesgos a las partes interesadas.
- Construcción de un ambiente de confianza y seguridad en los involucrados o partes relevantes, mediante la divulgación de la información y la transparencia frente a la gestión de riesgos y sus resultados.
- Identificación de sinergias entre las diferentes áreas para robustecer la gestión de los riesgos.
- Incorporación de la gestión de riesgos como variable estratégica para la toma de decisiones.

4.4. MARCO GENERAL DE CONTROL INTERNO

La documentación de los controles y el proceso de evaluación de la gerencia requieren que se utilice un "marco de control interno generalmente aceptado". Este marco de referencia define los elementos que se espera estén presentes y funcionando en un sistema de control interno efectivo. En la evaluación de la efectividad, la gerencia evalúa si el control interno sobre reporte financiero incluye políticas, procedimientos y actividades para cubrir los elementos que el marco de referencia describe.

Para el efecto, CEO seleccionó COSO (Committee of Sponsoring Organizations of the Treadway Commission) como marco de control interno para su evaluación, por considerar que el mismo es una buena práctica, mundialmente reconocida y se ajusta a tales requerimientos.

En este contexto el control interno se define como un proceso efectuado por las compañías como un todo, con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables.

El marco de gestión COSO identifica cinco componentes de control interno que deben existir de manera integrada para asegurar cada uno de los objetivos. Los 5 componentes del Control Interno interactúan entre sí, y forman un sistema. Este sistema debe estar integrado a las actividades operativas de las entidades. Cuanto más integrado esté el Sistema de Control Interno con las actividades de la entidad, tanto mayores serán las posibilidades de éxito de este. Todos los miembros de la organización son responsables de la implementación y el correcto funcionamiento del Sistema de Control Interno.

4.5. GESTION DE LA INFORMACION

MANTENIMIENTO DE REGISTRO

Mantener actualizada la información para que la compañía vigile eficazmente las actividades anómalas, y permita que los controles preventivos tengan la efectividad que de ellos se espera.

CEO debe informar oportunamente a Promigas acerca de los eventos de riesgo que se materialicen (estratégicos, RIMI, operativos, de ABAC) y que tengan la categoría de alto impacto, quien a su vez reportará estos eventos a Grupo Aval. Se deberá preparar y remitir en lo sucesivo un reporte uniforme de tales tipos de eventos de acuerdo con sus metodologías de evaluación.

5. ANEXOS

N.A