Revisión	Fecha de aprobación	Descripción de la modificación	Realizado por:	Revisado Por:	Aprobado por:
Versión 1.0	08/02/2021	Creación del documento	Yessica Paola Ospina	John Mauricio Carreño	Laura Oyuela

Tipo	Realizado por:	Revisado por:	Aprobado por:
Nombre	Yessica Ospina	Mauricio Carreño	Laura Oyuela
Cargo	Financial Audit Controller	Director de Auditoría Interna	VP Financiero y Estrategia

TABLA DE CONTENIDO

POLÍTICA DE GESTIÓN DE RIESGOS

La política de gestión de riesgos es el documento elaborado por la Dirección de Auditoría Interna como parte del Sistema de Gestión de Riesgos y Anticorrupción para la implementación de mecanismos de prevención y mitigación de los riesgos,la cual busca generar una cultura de autocontrol al considerar el control como parte inherente de las funciones y responsabilidades de todos los funcionarios de la compañía.

La Gerencia General, Vicepresidencias, Direcciones, Dirección de Auditoría Interna, y todos los empleados de Merqueo S.A.S ("**Merqueo**" o la "**Compañía**") en los diferentes niveles que la integran, se comprometen a implementar, administrar y ejercer un control efectivo para gestionar y reducir todos los posibles riesgos de corrupción que puedan impedir el cumplimiento de los objetivos estratégicos de la compañía y el normal desarrollo de la operación de la misma.

1. OBJETIVO

Establecer los elementos y el marco general de actuación para la gestión de los riesgos de toda naturaleza a los que se pueda ver expuesta la Compañía en el desarrollo de sus actividades para el cumplimiento de sus objetivos estratégicos.

2. ALCANCE

Esta política aplica a todas las áreas y actividades de Merqueo. y todas las empresas vinculadas, controlantes y controladas, donde se evidencien riesgos que puedan llegar a impactar el cumplimiento de los objetivos de la Compañía, los cuáles serán identificados, valorados, tratados, monitoreados, comunicados y divulgados.

3. REFERENCIAS

La presente política se construyó considerando el marco de referencia COSO para la implementación, gestión y control de un adecuado Sistema de Control Interno y la norma ISO 31000 relacionada con una adecuada gestión del riesgo.

Por su parte, el modelo COBIT será aplicado para auditar la gestión y control de los sistemas de información y tecnología en observación de la norma ISO 27005 relacionada con la Gestión de riesgos de Seguridad de la Información.

Los documentos relacionados con esta política son:

- Política de Gobierno Corporativo
- Código de conducta y ética empresarial
- Reglamento interno de trabajo
- Política de Seguridad y Ciberseguridad
- Política de Protección de Activos de Información
- Política de Privacidad y Tratamiento de Datos
- Manual Interno de Protección de Datos
- Procedimiento de Análisis de Riesgos - CF-AI-PRC-.02

- Programa de Transparencia y Ética Empresarial
- Manual SAGRILAFT

4. DEFINICIONES

Control: Son las acciones o actividades implementadas por la Compañía para reducir la probabilidad de ocurrencia de un riesgo o para disminuir su impacto.

Evento: Sucesos internos o externos posibles que pueden llegar a impactar positiva o negativamente el cumplimiento de logros y objetivos de la compañía, y sobre los cuales se tiene incertidumbre de cuándo pueda ocurrir o cuanto pueda impactar de manera precisa.

Frecuencia: Número de veces que un evento ocurre en determinado tiempo.

Gestión de Riesgo: Es el proceso de identificación, valoración y control de los riesgos que amenazan el logro de los objetivos estratégicos de la Compañía.

Identificación de riesgos: Es el proceso de encontrar, reconocer y definir los escenarios de riesgo, sus causas y sus potenciales consecuencias.

Impacto: Es el resultado o consecuencia de la materialización de un evento o escenario de riesgo.

Nivel de Riesgo: Es la ponderación que se otorga al riesgo.

Probabilidad: Se refiere a la posibilidad de ocurrencia de un riesgo potencial.

Riesgo: Evento, acción u omisión que pueda impactar o impedir el cumplimiento de los objetivos estratégicos de la compañía.

Riesgo Inherente: Es el riesgo que se genera por el desarrollo de la actividad de la Compañía sin la aplicación de controles.

Riesgo Residual: Es el resultado del nivel de exposición al riesgo que tiene la Compañía una vez se han aplicado controles.

Riesgo LA/FT/FPADM: es la posibilidad de pérdida o daño de ser utilizada la Compañía directa o indirectamente a través de sus operaciones como instrumento para el Lavado de Activos, Financiación del Terrorismo, Financiamiento de la Proliferación de Armas de Destrucción Masiva.

Soborno Transnacional: El acto en virtud del cual, una persona jurídica, por medio de sus empleados, administradores, asociados o contratistas, da, ofrece o promete a un servidor público extranjero, de manera directa o indirecta: (i) sumas de dinero, objetos de valor pecuniario o (iii) cualquier beneficio o utilidad a cambio de que ese servidor público realice, omita o retarde cualquier acto relacionado con sus funciones y en relación con un negocio o transacción internacional. Enmarcado en el artículo 433 del Código Penal.

Tolerancia al riesgo: Es el nivel de riesgo aceptado y al que la Compañía está dispuesta a aceptar para que no afecte el desarrollo de los objetivos estratégicos.

Tratamiento del riesgo: Selección y aplicación de medidas, con el fin de poder modificar la magnitud del riesgo, para evitar de este modo los daños intrínsecos de materializarse

5. DISPOSICIONES GENERALES

Las Direcciones de área enfocarán sus esfuerzos en gestionar los riesgos de la Compañía, en concordancia con las buenas prácticas de la industria y de gobierno corporativo, las regulaciones vigentes y el riesgo aceptable determinado.

Cada compañía del grupo empresarial gestiona sus propios riesgos, con el objetivo de preservar y crear valor para la misma, mejorando los estándares de gobernabilidad.

Todos los empleados deben aplicar la gestión de riesgos en sus procesos de acuerdo con las políticas y metodologías definidas, además deben alertar sobre los posibles riesgos que puedan afectar el normal desarrollo del trabajo y reportar los eventos de riesgos que se hayan materializado.

La Dirección de Auditoría Interna mantiene en funcionamiento la línea ética como un mecanismo para recibir denuncias anónimas e identificar situaciones de fraude, abuso, riesgo, y eventos potenciales de riesgo, entre otras las cuales son gestionadas a través del correo electrónico lineadeetica@merqueo.com

6. ADMINISTRACIÓN DEL RIESGO

La Compañía define como nivel de tolerancia al riesgo todos aquellos que, de acuerdo con la valoración que realice la Dirección de Auditoría Interna, avalado por el Comité de Auditoría, no queden clasificados como Riesgos Críticos y Altos.

Los riesgos catalogados como Moderados y Bajos son considerados de menor impacto para la Compañía.

La valoración de los riesgos resulta de la aplicación de la matriz de análisis de riesgo descrita en el procedimiento CF-AI-PRC-.02, donde se considera el impacto, la probabilidad y la protección existente de dichos riesgos.

Para que el funcionamiento y administración del Sistema de Gestión de Riesgos sea adecuado debe:

- Establecer la Gestión de Riesgos como uno de los principales aspectos para la toma de decisiones y desarrollo de todas las actividades empresariales.

- Identificar los riesgos relevantes para la Compañía, teniendo en cuenta su posible incidencia sobre los objetivos estratégicos, el gobierno corporativo, la sostenibilidad y continuidad del negocio.

- Garantizar la independencia de la Dirección de Auditoría Interna como área encargada de administrar el Sistema de Gestión de Riesgos, de las áreas de negocio que generan y gestionan los riesgos.

- Asignar funciones y responsabilidades a los altos directivos y a los líderes, orientadas a gestionar los riesgos identificados.

- Efectuar revisiones periódicas para evaluar el grado de madurez del sistema, a través de:

  (i) cumplimiento de los requerimientos normativos y regulatorios
  (ii) la interiorización de la gestión integral de riesgos
  (iii) la capacidad de identificación de oportunidades de mejoramiento.

7. RESPONSABILIDADES

De control y aprobación

Es responsabilidad del Comité de Auditoría de cada compañía, realizar un seguimiento al cumplimiento de la Política de Gestión de Riesgo, así mismo, garantizar su aprobación, la cual está a cargo de la Junta Directiva de cada compañía.

También es responsabilidad de la Junta Directiva aprobar el nivel de tolerancia al riesgo dispuesto a asumir, así como la Matriz de Riesgos de la Compañía, además del seguimiento de acciones correctivas de acuerdo con los informes presentados por la Dirección de Auditoría Interna.

De la definición del nivel de Tolerancia de riesgo

El equipo de Auditoría Interna presentará una propuesta sobre el nivel de tolerancia al riesgo, esta será aprobada por el Comité de Auditoría, así como evaluar los escenarios de riesgos propuestos anualmente, además de aprobar los criterios relativos a la calificación de los riesgos (probabilidad de ocurrencia e impacto).

De la administración del riesgo

Los directores de área son responsables del riesgo, alertando sobre posibles riesgos o incidentes que puedan afectar el normal desarrollo del trabajo o afectar la continuidad del negocio, por lo que deben establecer y ejecutar planes de mitigación o actividades de control definidos para la gestión de riesgos.

De la seguridad de la información

El área de Data a través del Oficial de Protección de datos será el área encargada de facilitar y promover el desarrollo de iniciativas sobre seguridad de la información que garanticen la gestión adecuada para el tratamiento de datos personales al interior de la Compañía, además de apoyar los objetivos y estrategias de la auditoría de sistemas.

De monitoreo del Sistema

Es responsabilidad de la Dirección de Auditoría Interna efectuar seguimiento de la implementación de planes de mitigación diseñados por la dirección o vicepresidencia de cada proceso para administrar los riesgos, evaluar el diseño y la eficacia operativa de los controles establecidos, así como revisar la eficacia de las autoevaluaciones de gestión de riesgos.

De la estrategia

La función de la Gerencia General es alinear la estrategia de la Compañía con la gestión de riesgos al tener un rol activo en la administración que le permitirá incentivar la cultura de control, que permita asegurar que los ejecutivos de la compañía estén conscientes que la información emana de un ambiente de control.

8. VIGENCIA Y ACTUALIZACIÓN

Considerando la importancia de la presente política, una vez aprobada por el Comité de Auditoría, será publicada en el Web Site de Auditoría Interna o cualquier otro medio de comunicación que se determine.

Esta política rige a partir de su publicación y será revisada periódicamente o al menos una vez al año, cualquier cambio o modificación que se haga tendrá el mismo nivel de divulgación y será comunicado a todos los colaboradores, así como a los grupos de interés a través de los recursos publicados.

9. FORMATOS Y REGISTROS

Ninguno

10. ANEXOS

Ninguno