1. OBJETIVO

El objetivo de la Política del Sistema de Autocontrol y Gestion Integral del Riesgo de CONSORCIO METALURGICO NACIONAL - COLMENA S.A.S., es asegurar la sostenibilidad de la Compañía, la continuidad de sus operaciones, la minimización del riesgo, y la generación de valor mediante el uso de herramientas efectivas que permitan gestionar los riesgos a los cuales está expuesta la compañía, manteniendo un adecuado ambiente de control al interior de la Compañía.

2. ALCANCE

La política del Sistema de Autocontrol y Gestion Integral del Riesgo, aplica a accionistas, miembros de la Asamblea de Accionistas, colaboradores, clientes, proveedores, contratistas y compañías donde se posea participación accionaria o se ejerza algún tipo de control y/o relación contractual.

3. CONTENIDO DE LA POLÍTICA

Este documento hace parte del Sistema Integral de Administración de Riesgos que se desarrolla y complementa con las políticas específicas de riesgos a través de los sistemas de gestión SARO, SAGRILAFT, PTEE, Protección de Datos Personales y Continuidad del Negocio (PCN), aseguramiento de controles en la cadena de suministro que prevea actividades ilíc itas y/o delicitivas, entre otras lavado de activos, contrabando, tráfico de estupefacientes, tráfico de sustancias para el procesamiento de narcóticos, terrorismo, financiación del terrorismo, tráfico de armas, y Proliferación de armas de destrucción masiva, que puedan establecerse en cada uno de los procesos, procedimientos y actividades de la compañía.

4. MARCO NORMATIVO

La presente política se basa en los siguientes principios normativos de los sistemas de gestión así:

NOMBRE CIRCULAR	AÑO	CONTENIDO
Committee of Sponsoring Organizations of the Treadway Comission (COSO).	**2017**	Marco integrado de administración de riesgos corporativos
Circular Externa 100-000016 de 2020, Superintendencia de Sociedades.	**2020**	Régimen de autocontrol y gestión del riesgo integral LA/FT/FPADM y reporte de Operaciones sospechosas a la UIAF
Ley 1778 de 2016de Superintendenciade Sociedades (buenas prácticas)	**2016**	Ley Antisoborno.
Decreto 1377 de 2.013		Por lo cual se reglamente parcialmente la ley de protección de datos
Documento CONPES 3793 del 18 de diciembre de 2013.	**2013**	Política Nacional Anti Lavado de Activos y contra la Financiación del Terrorismo.
La Ley Estatutaria 1581 de 2012		Se dictan disposiciones generales para la protección de Datos Personales (LEPD)
ISO 22301 – ICONTEC (Buenas prácticas)	**2012**	Sistema de Gestión de Continuidad del Negocio.
Prácticas en Administración y Supervisión del Riesgo Operacional Publicados por el Comité de Basilea en Supervisión Bancaria I, II y III.	**2010**	Marco regulador internacional para los bancos
ISO 31000- ICONTEC	**2009**	Gestión de Riesgos
Ley 1186 de 2009.- Congreso de la republica	**2009**	Memorando de Entendimiento entre los Gobiernos de los Estados del Grupo de Acción Financiera de Sudamérica contra el Lavado de Activos (Gafisud).

NOMBRE CIRCULAR	AÑO	CONTENIDO
Circular Externa 041 de la Superintendencia Financiera (Buenas prácticas)	**2007**	Reglas Relativas a la Administración del Riesgo Operativo - SARO
Artículo 20 de la Ley1121 de 2006. - Congreso de la republica	**2006**	Procedimiento para la publicación y cumplimiento de las obligaciones relacionadas con listas internacionales vinculantes para Colombia de conformidad con el derecho internacional.
Estándar de Australia y Nueva Zelanda 4360	**2004**	AS/NZ: Sobre administración de riesgos.
NTC 5254	**2004**	Norma Técnica Colombiana de Gestión de Riesgo.
Artículos 15 de la Constitución Política	**1991**	Derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.
Artículos 20 de la Constitución Política	**1991**	Libertad de expresar y difundir su Pensamiento y opiniones.
Ley 1778 de 2016. Circular Externa No.100-000003 del 26 de julio de 2016 Circular Externa No. 100-000011 del 9 de agosto de 2021 Circular Externa 100-000012 Superintendencia de Sociedades.	**2016** **2021**	Política de Supervisión de los Programas Transparencia y Ética Empresarial – PTEE

5. Política general

CONSORCIO METALURGICO NACIONAL - COLMENA S.A.S. se compromete a gestionar y administrar los Riesgos Estratégicos, Operativos, SAGRILAFT, Protección de Datos, Fraude, Corrupción, Soborno, actividades ilícitas y/o delictivas, contrabando, tráfico de estupefacientes, tráfico de sustancias para el procesamiento de narcóticos, terrorismo, tráfico de armas y Proliferación de armas de destrucción masiva. Continuidad de Negocio en todos sus niveles (dirección, misional, apoyo y control) utilizando las mejores prácticas del mercado en gestión de riesgos, generando planes de acción y formando parte de su direccionamiento estratégico y corporativo.

6. Políticas especificas

6.1. Adoptar un modelo de administración de riesgos que permita:

- Identificar los riesgos relevantes (estratégicos, operativos, fraude, corrupción, Protección de Datos, Continuidad de Negocio y SAGRILAFT,) que puedan vulnerar los objetivos estratégicos, operativos y de gobierno corporativo.
- Identificar actividades ilícitas y/o delictivas, contrabando, tráfico de estupefacientes, tráfico de sustancias para el procesamiento de narcóticos, terrorismo, tráfico de armas y Proliferación de Armas de Destrucción Masiva, especialmente en aquellos procesos relacionados con la cadena de suministro.
- Analizar su contexto contemplando factores internos y externos de la compañía.
- Estimar el nivel de riesgo inherente mediante la determinación de la probabilidad de ocurrencia y la magnitud del impacto.

- Estimar el nivel de riesgo residual mediante la aplicación de controles efectivos y eficientes que permitan disminuir y controlar el nivel de riesgo de la Compañía y su nivel de exposición.

- Identificar y proponer controles efectivos que permitan evitar la materialización de algún posible evento estimando el riesgo residual.

- Adoptar sistemas de información que permitan realizar una evaluación y comunicación periódica de los resultados del seguimiento (monitoreo) a la gestión de riesgos y sus controles.

6.2. La administración integral de riesgos es responsabilidad del Gerente General y del Director de Riesgos de la compañía quienes velaran porque el sistema se adopte y aplique por todos los empleados y contrapartes.

6.3. Las iniciativas y/o proyectos que presente la gerencia deberán contener un resumen de los riesgos que dicho plan o proyecto conlleva, a su vez una identificación de los posibles controles a aplicar a fin de mitigar y/o disminuir el nivel de riesgo que aporta el nuevo proyecto a la compañía.

6.4. Es responsabilidad de todos los colaboradores y en especial de los dueños de proceso identificar los riesgos, medirlos, y establecer controles de forma conjunta con la Dirección de Riesgos y Auditoría Interna, monitorearlos, documentarlos, y reportar eventos de riesgo, para lo cual contará con el asesoramiento metodológico del área de Riesgos y a su vez asegurar un adecuado ambiente de control en sus procesos y por ende en la Compañía.

6.5. Todos los sistemas del SAGIR deben contener planes de contingencia necesarios para mitigar el impacto de la materialización de los riesgos, definiendo de forma clara, tiempos de recuperación (RTORecovery Time Objective) y RPO (Recovery Point Objective) o Punto de recuperación objetivo).

6.6. En todos los eventos materializados, se deben establecer planes de tratamiento y/o acción, con el fin de mitigar el impacto de los eventos de riesgo reportados que se traduzcan en pérdidas económicas para la compañía.

6.7. Definir los imites de apetito y tolerancia al riesgo monitoreando las exposiciones frente a dichos niveles de acuerdo a la aversión al riesgo.

6.8. Cualquier persona en la Compañía, puede reportar eventos de riesgos en el siguiente orden de prelación: Líder de Procesos, Área de Riesgos, Auditoría Interna, Contraloría, Gerente General, y Asamblea de Accionistas.

6.9. La administración de los riesgos debe ser oportuna, integra, sistemática y debe estar alineada con los objetivos estratégicos de la Compañía y de cada área.

6.10. Al menos una (1) vez al año se deberá realizar una evaluación del Sistema de Administración de Riesgos de la compañía, partiendo de los objetivos de la Compañía de la efectividad de sus controles de los cambios en el mercado y de actualizaciones a nivel normativo tanto local como en el exterior.

6.11. Como mínimo una vez al año, la Dirección de Riesgos debe coordinar y gestionar a través del área de Talento Humano las capacitaciones de inducción para el personal nuevo que ingrese y reinducción dirigida a todos los colaboradores de la Compañía.

6.12. Todos los colaboradores, proveedores, clientes y demás contrapartes interesadas, deben conocer el Sistema de Autocontrol y Gestion Integral de Riesgos de la Compañía.

6.13. Si se presenta la materialización de un evento de riesgo, es responsabilidad del líder de proceso diligenciar, estimar, y definir la perdida presentada(cuantitativo o cualitativo) y enviar el formato de registro de eventos de Riesgos a la Dirección de Riesgo. Cuando no existan, debe certificarlo mensualmente por el mismo medio.

6.14. Se realizará el análisis e identificación de los riesgos en todos sus niveles, una vez se cuente con la caracterización de procesos o subprocesos divulgados en el Sistema de Gestión Integral- Isolucion.

6.15. La responsabilidad del Sistema de Autocontrol y Gestion Integral del Riesgo – SAGIR, es parte del desarrollo de las actividades que desempeña cada uno de los miembros de la Compañía, a través de la gestión efectiva de los procesos y la aplicación de los controles, evaluando la efectividad, y la ejecución de los mismos.

6.16. Los riesgos identificados y las estrategias de mitigación son información confidencial de la Compañía, y cualquier solicitud o entrega de la misma a terceros debe ser aprobada por la Dirección de Riesgos.

6.17. El Modelo Plan de Continuidad de negocio de COLMENA S.A.S. S.A., tiene definido claramente las funciones y responsabilidades de los líderes de los procesos críticos en caso de un evento o siniestro que impida el desarrollo normal de la operación e la Compañía.

6.18. El área de TIC cuenta con un sistema de copias de respaldo alternas, así como con procedimientos de restauración para los sistemas de información que se consideran críticos para la operación.

6.19. Todos los proveedores estratégicos y críticos (según definición de impacto dentro de la cadena de suministro), en los cuales se ve afectada la continuidad del negocio y/o procesos Core, deberán tener un plan de Continuidad de Negocio, que asegure la no interrupción de sus aspectos contractuales, así como también, participar activamente cuando la Compañía lo requiera para realizar las pruebas sobre el Plan de Continuidad.

6.20. Toda la información recibida por parte de colaboradores, clientes, proveedores deberá contar con la correspondiente autorización para la administración y tratamiento de datos personales.

6.21. Los derechos de acceso, actualización y supresión de datos serán atendidos a través de los canales de comunicación definidos por el Oficial de Protección de Datos de la Compañía.

6.22. Impulsar una cultura en de gestión y control del riesgo.

6.23. Establecer lineamientos para la prevención y solución de conflictos de interés, como son:

Conflicto de interés en la administración de Listas Restrictivas de SAGRILAFT:

Los empleados de la Compañía, que tengan a su cargo la administración de listas de control LA/FT/FPADM, deberán mantener confidencialidad sobre el uso de las listas, la(s) persona(s) consultadas, antecedentes, hallazgos, y obrar sin interés personal y sin buscar el favorecimiento de otra(s) persona(s).

Conflicto de interés en la atención de consultas de información por parte de las autoridades:

La persona encargada de atender consultas relacionadas con requerimientos de información solicitada por autoridades competentes deberá obrar sin interés personal y/o sin buscar el favorecimiento de otra (s) persona (s).

6.24. La Compañía no establecerá relaciones contractuales ni otorgará beneficios a personas naturales y/o jurídicas y/o terceros que se encuentren registrados en las listas restrictivas relacionadas con actividades o delitos fuentes de LA/FT/FPADM.

6.25. La Compañía incluye en todos sus contratos con terceros que el origen de los recursos que se utilizan en las operaciones descritas en el contrato proviene de actividades lícitas. Su no inclusión, en los contratos vigentes impedirá su renovación o celebrar nuevos contratos.

6.26. Cumplir con las demás políticas y procedimientos del Sistema de Autocontrol y Gestion Integral del Riesgo, Continuidad del Negocio, Programa de Ética empresarial, Protección de Datos Personales, Procedimientos internos, Código de Ética y Buen Gobierno, acuerdos de confidencialidad y Manual SAGRILAFT (Sistema de Autocontrol y Gestión Integral del Riesgo de Lavado de Activos, Financiación del Terrorismo y Financiamiento de Proliferación de Armas de Destrucción Masiva).

7. ESTRUCTURA DEL SISTEMA INTEGRAL DE ADMINISTRACIÓNDE RIESGOS

A. Asamblea de accionistas

- Asegurarse que la administración ha contemplado los riesgos que impactan en el plan estratégico.
- Tener claridad del impacto que pueden llegar a tener diferentes acontecimientos de riesgo sobre los objetivos estratégicos de la compañía. Aprobar las Políticas del Sistema de Autocontrol y Gestion Integral del Riesgo.
- Aprobar los planes de contingencia necesarios para mitigar el impacto de la materialización de los riesgos y la continuidad del negocio. Aprobar políticas, prácticas y otros mecanismos de control del Sistema de Administración Integral de Riesgos
- Conocer toda la información relevante, solicitar aclaraciones, correctivos, hacer seguimientos.
- Aprobar los niveles de apetito y tolerancia al riesgo dispuestos a asumir por la compañía.
- Aprobar los recursos y estructura necesarios para gestionar los riesgos de la Compañía.
- Aprobar los criterios de calificación los riesgos (probabilidad e impacto).
- Aprobar el SAGRILAFT y sus actualizaciones, presentadas por el representante legal y el Oficial de Cumplimiento.
- Aprobar el manual de procedimientos SAGRILAFT y sus actualizaciones.
- Seleccionar y designar al Oficial de Cumplimiento y su respectivo suplente, cuando sea procedente.
- Analizar oportunamente los informes sobre el funcionamiento del SAGRILAFT, sobre las propuestas de correctivos y actualizaciones que presente el Oficial de Cumplimiento, y tomar decisiones respecto de la totalidad de los temas allí tratados.
- Analizar oportunamente los reportes y solicitudes presentados por el Oficial de Cumplimiento.
- Pronunciarse sobre los informes presentados por la revisoría fiscal o las auditorías interna y externa, que tengan relación con la implementación y el funcionamiento del SAGRILAFT, y hacer el seguimiento a las observaciones o recomendaciones incluidas. Ese seguimiento y sus avances periódicos deberán estar señalados en las actas correspondientes.
- Ordenar y garantizar los recursos técnicos, logísticos y humanos necesarios para implementar y mantener en funcionamiento el SAGRILAFT, según los requerimientos que para el efecto realice el Oficial de Cumplimiento.
- Establecer los criterios para aprobar la vinculación de Contraparte cuando sea una PEP.
- Establecer pautas y determinar los responsables de realizar auditorías sobre el cumplimiento y efectividad del SAGRILAFT en caso de que así lo determine.
- Verificar que el Oficial de Cumplimiento cuente con la disponibilidad y capacidad necesaria para desarrollar sus funciones.
- Constatar que la Empresa Obligada, el Oficial de Cumplimiento y el representante legal desarrollan las actividades designadas por la Superintendencia de Sociedades y en el SAGRILAFT

B. Oficial de Cumplimiento

El Oficial de Cumplimiento debe participar activamente en los procedimientos de diseño, dirección, implementación, auditoría, verificación del cumplimiento y monitoreo del SAGRILAFT, y estar en capacidad de tomar decisiones frente a la gestión del Riesgo LA/FT/FPADM. Por su parte, la administración de la Compañia le brinda un apoyo efectivo y los recursos humanos, físicos, financieros y técnicos necesarios para llevar a cabo la implementación, auditoría y cumplimiento del SAGRILAFT.

- Velar por el cumplimiento efectivo, eficiente y oportuno del SAGRILAFT.
- Presentar, por lo menos una vez al año, informes a la asamblea de accionistas o, en su defecto, al máximo órgano

social. Como mínimo, los reportes deberán contener una evaluación y análisis sobre la eficiencia y efectividad del SAGRILAFT y, de ser el caso, proponer las mejoras respectivas. Así mismo, demostrar los resultados de la gestión del Oficial de Cumplimiento, y de la administración de la Empresa, en general, en el cumplimiento del SAGRILAFT.

- Proponer los límites del apetito de riesgo y nivel de tolerancia al riesgo.
- Promover la adopción de correctivos y actualizaciones al SAGRILAFT, cuando las circunstancias lo requieran y por lo menos una vez cada dos (2) años. Para ello deberá presentar a la asamblea de accionistas o al máximo órgano social, según el caso, las propuestas y justificaciones de los correctivos y actualizaciones sugeridas al SAGRILAFT.
- Coordinar el desarrollo de programas internos de capacitación.
- Evaluar los informes presentados por la auditoría interna o quien ejecute funciones similares o haga sus veces, y los informes que presente el revisor fiscal o la auditoría externa, si es el caso, y adoptar las Medidas Razonables frente a las deficiencias informadas. Si las medidas que deben ser adoptadas requieren de una autorización de otros órganos, deberá promover que estos asuntos sean puestos en conocimiento de los órganos competentes.
- Certificar ante la Superintendencia de Sociedades el cumplimiento de lo previsto en el SAGRILAFT, según lo requiera la Superintendencia de Sociedades.
- Verificar el cumplimiento de los procedimientos de Debida Diligencia y Debida Diligencia Intensificada, aplicables a la Empresa.
- Velar por el adecuado archivo de los soportes documentales y demás información relativa a la gestión y prevención del Riesgo LA/FT/FPADM.
- Diseñar las metodologías de clasificación, identificación, medición y control del Riesgo LA/FT/FPADM que formarán parte del SAGRILAFT.
- Realizar la evaluación del Riesgo LA/FT/FPADM a los que se encuentra expuesta la Empresa.
- Realizar el Reporte de las Operaciones Sospechosas a la UIAF y cualquier otro reporte o informe exigido por las disposiciones vigentes, conforme lo establezca la Superintendencia de sociedades o la UIAF.
- Gozar de la capacidad de tomar decisiones para gestionar el Riesgo LA/FT/FPADM y tener comunicación directa con, y depender directamente de, la asamblea de accionistas o el máximo órgano social.

C.Oficial de Protección de Datos Personales

- Es responsabilidad del Oficial de Protección de Datos establecer los lineamientos y controles frente al cumplimiento en la protección de datos, así como la frecuencia de los controles.
- Es responsabilidad del Oficial de Protección de Datos atender los requerimientos e inquietudes tanto del personal de la Compañía, como de personal externo, frente al tratamiento de los datos, en los tiempos definidos en la Ley 1581 de 2012.
- Presentar, en conjunto con el Representante Legal las políticas y procedimientos del sistema de Protección de Datos a la Asamblea de Accionistas. Coordinar con el proceso de Talento Humano el desarrollo de programas internos de capacitación en relación a Protección de Datos Personales.

D. Control y Auditoría

- Monitorear las exposiciones frente a los límites de tolerancia y apetito al riesgo.

- Evaluar e informar a la Asamblea de Accionistas el incumplimiento de la Gerencia y/o sus colaboradores de sus responsabilidades frente al del Sistema de Autocontrol y Gestión Integral del Riesgo.
- Asegurarse que los aspectos informados por las autoridades de vigilancia y control hayan sido resueltos satisfactoriamente.
- Proponer mecanismos, estrategias, políticas, responsabilidades, y/o protocolos para el cumplimiento del Sistema de Autocontrol y Gestion Integral del Riesgo.
- Evaluar la efectividad de las medidas de control utilizadas para mitigar los riesgos residuales.
- Evaluar y aprobar los planes y estrategias de continuidad de negocio.
- Informar sobre el cumplimiento del plan anual de auditoría.
- Informar sobre el Sistema de Control Interno de las Compañías.
- Cuando se requiera, se podrá solicitar el asesoramiento de auditorías externas especiales.
- Elaborar el plan de auditoria basado en riesgos. Asegurarse que los riesgos son correctamente evaluados.
- Evaluar los procesos de gestión de riesgo y control en las operaciones de la Compañía que resulten relevantes y concluir sobre lo adecuado y eficaces de los mismos.
- Informar a la gerencia y/o contraloria, sobre los resultados de las evaluaciones y las mejoras al Sistema de Autocontrol y Gestion Integral del Riesgo.
- Realizar revisiones periódicas sobre los registros de eventos de Riesgo Operativo, informando al Contralor sobre el cumplimiento de las condiciones.
- Verificar que los riesgos sean incorporados en los procesos de la compañía.
- Evaluar el diseño y verificar la efectividad de los controles existentes para reducir los riesgos.
- Asegurarse que existen planes de acción para responder a los riesgos en caso de materialización.
- Asegurarse de la construcción del mapa de riesgos.

E. Representante Legal y/o Gerente General

- Presentar el plan estratégico junto con los riesgos más relevantes que puedan afectar su cumplimiento.
- Desarrollar y velar la implementación de las estratégicas aprobadas con el fin de establecer el cambio cultural que implica del Sistema de Administración Integral de Riesgos en la compañía.
- Implementar los lineamientos aprobados por la Asamblea de Accionistas para el cumplimiento del Sistema de Autocontrol y Gestion Integral del Riesgo.
- Gestionar junto con sus colaboradores las medidas de control de los riesgos diarios de la operación y velar por el

cumplimiento de los mecanismosdel Sistema de Autocontrol y Gestion Integral del Riesgo, en cuanto al cumplimiento de las políticas, responsabilidades, medidas y/o protocolos establecidos.

- Informar a la Asamblea de Accionistas y al Comité de Riesgos y Auditoría sobre la gestión efectuada sobre riesgos. Velar por el cumplimiento efectivo de las políticas establecidas por la Asamblea de Accionistas.

- Desarrollar y velar porque se implementen las estrategias con el fin de establecer el cambio cultural que la administración de este riesgo implica para la entidad.
- Velar por la correcta aplicación de los controles del riesgo inherente, identificado y medido.

- Aprobar los planes de contingencia y de continuidad del negocio y disponer de los recursos necesarios para su oportuna ejecución.

- Presentar un informe periódico, como mínimo semestral, a la Asamblea de Accionistas sobre la evolución y aspectos relevantes del Sistema de Autocontrol y Gestion Integral del Riesgo, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.

- Estudiar los resultados de la evaluación del Riesgo LA/FT/FPADM efectuada por el Oficial de Cumplimiento y establecer los planes de acción que correspondan.

- Asignar de manera eficiente los recursos técnicos y humanos, determinados por la asamblea de accionistas o el máximo órgano social, necesarios para implementar el SAGRILAFT.

- Prestar efectivo, eficiente y oportuno apoyo al Oficial de Cumplimiento en el diseño, dirección, supervisión y monitoreo del SAGRILAFT.

- Presentar a la asamblea de accionistas o al máximo órgano social, los reportes, solicitudes y alertas que considere que deban ser tratados por dichos órganos y que estén relacionados con el SAGRILAFT.

- Asegurarse de que las actividades que resulten del desarrollo del SAGRILAFT se encuentran debidamente documentadas, de modo que se permita que la información responda a unos criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad.

- Certificar ante la Superintendencia de Sociedades el cumplimiento del SAGRILAFT.

- Verificar que los procedimientos del SAGRILAFT desarrollen la Política LA/FT/FPADM adoptada por la asamblea de accionistas o máximo órgano social.

F. Contralorías

- Proponer políticas, procedimientos normas y sistemas para minimizar, mitigar y/o limitar los riesgos a los que está expuesta la compañía.

- Establecer procesos prácticos de control que requieran y orienten a los jefes, directores y empleados a realizar sus obligaciones y responsabilidades de manera que se cumplan los objetivos de control.

- Velar porque los empleados cumplan con las políticas, normas, planes y procedimientos y con todas las leyes y reglamentaciones pertinentes respecto a los riesgos.

- Solicitar los recursos requeridos y proponer la estructura de control de riesgos de la compañía.

- Monitorear la eficacia del Sistema de Autocontrol y Gestion Integral del Riesgo y propender por la mejora continua del mismo solicitando los recursos parael aseguramiento del sistema.
- Identificar y monitorear los riesgos estratégicos.
- Proponer y aprobar el modelo de continuidad del negocio, la priorización de funciones críticas del negocio, análisis de impacto del negocio (análisis BIA) y del monitoreo de las estrategias de recuperación.

G. Dirección de Riesgos y Cumplimiento

- Definir la metodología, instrumentos y procedimientos para identificar, medir, controlar y monitorear los riesgos a los que se encuentra expuesta la compañía.
- Asesorar metodológicamente a los líderes de procesos y/o de riesgos en las etapas de identificación, medición, control y monitoreo de los riesgos, así como supervisar dicha gestión.
- Coordinar la entrega de los informes correspondientes a la gestión de riesgos.
- Liderar con el área Gestión de Talento Humano las capacitaciones en Gestión de Riesgos a todos los colaboradores y contrapartes interesadas.
- Proponer a Contraloría estrategias de gestión de riesgos para aprobación de la Asamblea de Accionistas.
- Proponer a la Contraloría estrategias de gestión de riesgos para ser presentados a las áreas de Control y Auditoría y posterior aprobación de la Asamblea de Accionistas.
- Evaluar la efectividad de las acciones de respuesta a los riesgos residuales propendiendo que se mantengan dentro de los límites de apetito y tolerancia aprobados.
- Elaborar los formatos requeridos para registrar eventos de riesgo operativo.
- Desarrollar e implementar el sistema de reportes internos y externos de riesgo operativo en la compañía.
- Revisar y actualizar al menos cada año el Plan de Continuidad de Negocio.
- Establecer los protocolos de comunicaciones tanto para los colaboradores, clientes, proveedores y medios de comunicación, así como se debe asignar un líder de dichas comunicaciones para efectos del Plan de Continuidad de Negocio.
- Incluir en el Sistema de Autocontrol y Gestion Integral del Riesgo de la compañía aspectos importantes de la cadena de suministro internacional, que prevea actividades ilícitas y/o delicitivas, entre otras, lavado de activos, contrabando, tráfico de estupefacientes, tráfico de sustancias para el procesamiento de narcóticos, terrorismo, financiación del terrorismo, tráfico de armas y proliferación de armas de destrucción masiva.

I. Líderes de proceso y funcionarios

- El líder de proceso debe identificar, medir, controlar y monitorear los riesgos junto con el asesoramiento metodológico de la Dirección de Riesgos.Servir de canal de comunicación entre la Dirección de Riesgos y Cumplimiento Normativo y el área correspondiente.

- El líder del proceso debe presentar a la Dirección de Riesgos y Cumplimiento Normativo, propuestas de mejora del Sistema de Autocontrol y Gestion Integral del Riesgo
- El líder de proceso debe mantener actualizado el perfil de riesgo de sus procesos y la matriz legal.
- El líder de proceso debe definir e implementar las acciones correctivas para los eventos de riesgo materializados.
- El líder de Proceso debe implementar Planes de Tratamiento para los riesgos que superen los niveles de tolerancia permitidos.
- El líder de proceso debe diligenciar y entregar el reporte de eventos de riesgo operativo de los procesos a su cargo a la Dirección de Riesgos. Cuando no existan. certificarlo mensualmente.
- El líder de proceso debe administrar las matrices de riesgos (conocimiento y actualización) de su proceso.
- El líder de proceso debe retroalimentar a la Dirección de Riesgos acerca del desarrollo del Sistema de Autocontrol y Gestion Integral del Riesgo– SAGIR, en el área, al igual que a la Auditoría Interna.
- El líder de proceso debe mantener actualizado el perfil de riesgo de sus procesos y la matriz legal.
- Todos los funcionarios deben cumplir con las políticas, principios, normas y procedimientos establecidos por la Compañía para mantener bajo controles riesgos de los procesos y actividades.
- El líder de proceso y todos los funcionarios deben mantener la eficacia de los procesos de control establecidos y promover la mejora continua de los mismos.
- Todos los funcionarios deben mantener archivado y bajo esquemas de seguridad de la información, todo tipo de documentación física de clientes, empleados o proveedores.

FECHA:23/09/2025
INTEGRAL DE RIESGOS - SAGIR

- Es responsabilidad de cada colaborador el no suministro a personal no autorizado (Familiares, amigos, compañeros de trabajo etc.) información o datos del titular.
- Ningún colaborador puede ingresar y/o usar bases de datos no autorizadas ni suministradas por la compañía.
- Cada área responsable del manejo de las bases de datos debe garantizar la confidencialidad, integridad y disponibilidad de la información, de acuerdo a los protocolos de seguridad establecidos.
- Los procesos involucrados en la gestión de Riesgos de LA/FT/FPADM, previo a la vinculación de un cliente, empleado, o proveedor se debe realizar la verificación en las listas restrictivas administradas por la Compañía relacionadas con actividades o delitos fuentes de LA/FT/FPADM, y documentar toda su información mediante los diferentes formatos de conocimiento (Crediexpress, Formulario de Conocimiento de Clientes, Formulario de Proveedores , Formato de vinculación de Empleados, formato de transacciones en efectivo, formato de creación de terceros) que tienen implementados los procesos transversales al SAGRILAFT / PTEE, en caso de identificar algún acto y/o evento sospechoso o señal de alerta debe informar de manera inmediata al Oficial de Cumplimiento quien realizara un análisis de riesgo más detallado a fin de determinar, evaluar y analizar las señales de alerta identificadas.
- Todos aquellos colaboradores, que detecten alguna operación inusual de acuerdo las señales de alerta descritas en el manual SAGRILAFT, deben notificarlas al Oficial de Cumplimiento mediante el Formato de Operaciones Inusuales,

cuando no existan, certificarlo mensualmente.

- Todo colaborador de la compañía, debe dar estricto cumplimiento al programa de Ética Empresarial de Anticorrupción y Prevención del Soborno Transnacional y las politicas contenidas en el.

La presente política es elaborada por el Director de Riesgos y Cumplimiento Normativo de COLMENA S.A.S., revisada por la Contraloría y aprobada por la Gerencia General y/o Asamblea de Accionistas.

Entra en vigencia la presente política a partir del 23 de septiembre de 2025.