METODOLOGÍA DE GESTIÓN DE RIESGOS

El objetivo principal es implementar una metodología que permita a ARIADNA SAS dar cumplimiento de la normatividad local e internacional vigente, a través de la administración de los riesgos con acciones preventivas y/o correctivas para el control efectivo de los riesgos identificados.

La Metodología para la Gestión de Riesgos consta de las siguientes cinco etapas: Comprensión de la Compañía y su contexto, Valoración del riesgo, Actividades de control-Tratamiento del riesgo, Monitoreo y Supervisión, Comunicación y consulta; para cada una de ellas se cuenta con la participación de las personas que ejecutan los procesos para lograr que las acciones determinadas alcancen los niveles de efectividad esperados, presentado un grado aceptable de validez, confiabilidad y objetividad al ser aplicada.

1. COMPRENSIÓN DE LA COMPAÑÍA Y SU CONTEXTO

En esta primera etapa para gestión de riesgos, la compañía debe tener en cuenta las cuestiones internas y externas que se relacionan directamente con la misión y visión de la compañía y que podrían afectar negativamente los objetivos definidos.

Los factores para considerar en el análisis pueden ser:

a. Países, lugares y sectores económicos en los que opera la compañía o anticipa operar.
b. Entidades sobre las que la compañía tiene control y las que ejercen control sobre la compañía.
c. Canales de distribución
d. Naturaleza y alcance de las interacciones con los colaboradores públicos.
e. Deberes y obligaciones legales, reglamentarias, contractuales y profesionales aplicables.
f. Personas y procesos internos expuestos a soborno
g. Fuentes de información de organizaciones internacionales.

2. VALORACIÓN DEL RIESGO

2.1 Identificación de riesgos

La compañía debe realizar de forma regular identificación y/o actualización de los riesgos.

Al respecto, según la norma ISO 37001, para la identificación, se deben tener en cuenta los factores mencionados en el apartado anterior.

Los siguientes son los aspectos a identificar y documentar en la matriz de riesgo como primer paso:

a. Proceso: Identificación de los procesos con eventual afectación del riesgo.
b. Descripción del riesgo asociado al proceso evaluado.
c. Explicación clara y detallada del origen del riesgo (Cómo puede suceder).
d. Descripción de posibles causas y/o fallas del riesgo.
e. Descripción de consecuencias y/o efectos.

La identificación de causas o fallas, 6corresponde a las fuentes generadoras de riesgo, algunos están bajo el control de la compañía y otros están fuera de su control por obedecer a situaciones externas. Estos factores de riesgo se clasifican en internos o externos.

Son factores de riesgo de LA/FT/FPADM a considerar en el análisis del SAGRILAFT:

- Clientes: Es toda persona natural o jurídica con la cual la entidad establece y mantiene una relación contractual o legal para el suministro de cualquier producto propio de su actividad.
- Productos: Bienes y servicios que produce, comercializa, transforma u ofrece la Empresa o adquiere de un tercero.
- Canales de Distribución: Son los medios que se utilizan desde el proceso de comercialización de un producto desde el fabricante hasta el usuario o consumidor final
- Jurisdicciones: Países, territorios que presenten niveles significativos de corrupción u otras actividades criminales.
- Terceros: Es cualquier persona natural o jurídica con la que la Empresa tenga vínculos comerciales, de negocios, contractuales o jurídicos de cualquier orden.

Son factores de riesgo Soborno a considerar en el análisis del programa de transparencia y ética empresarial:

- Recurso humano: Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la entidad.
- Procesos: Es el conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad.
- Tecnología: Es el conjunto de herramientas empleadas para soportar los procesos de la entidad. Incluye: hardware, software y comunicaciones.
- Infraestructura: Es el conjunto de elementos de apoyo para el funcionamiento de una organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.
- Acontecimiento Externo: Son situaciones asociadas a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la entidad.

Como resultado de la etapa de Identificación de riesgos la Organización se obtienen: Inventario de riesgos clasificados de acuerdo con la tipología e impacto a objetivos; y causas asociadas a cada uno de los riesgos (factores internos y externos).

2.2 Análisis y priorización del riesgo

Una vez se han identificado los riesgos, se procede a hacer un análisis, de preferencia conjunto con las áreas críticas de la compañía, con el fin de priorizar los riesgos de acuerdo con su probabilidad e impacto.

La medición del perfil de riesgo se realiza a través de la estimación de la probabilidad de ocurrencia del evento, así como de sus impactos en caso de materializarse:

- **Probabilidad**

Hace relación a la cantidad de veces que ocurre el hecho en el periodo evaluado, los criterios para su definición están dados por la siguiente tabla:

Calificación	Valor	Descripción
Recurrente	5	Se espera que el evento o eventos puedan presentarse con cierta periodicidad – Frecuencia por lo menos una (1) vez cada mes.
Frecuente	4	Se espera que el evento o eventos puedan presentarse por lo menos una vez cada semestre.
Ocasional	3	Se espera que el evento o eventos puedan presentarse una (1) vez cada año.
Remoto	2	Se espera que el evento o eventos puedan presentarse una (1) vez cada cinco (5) años.
Improbable	1	El evento o los eventos no se han presentado en un período menor a cinco (5) años.

- **Impacto**

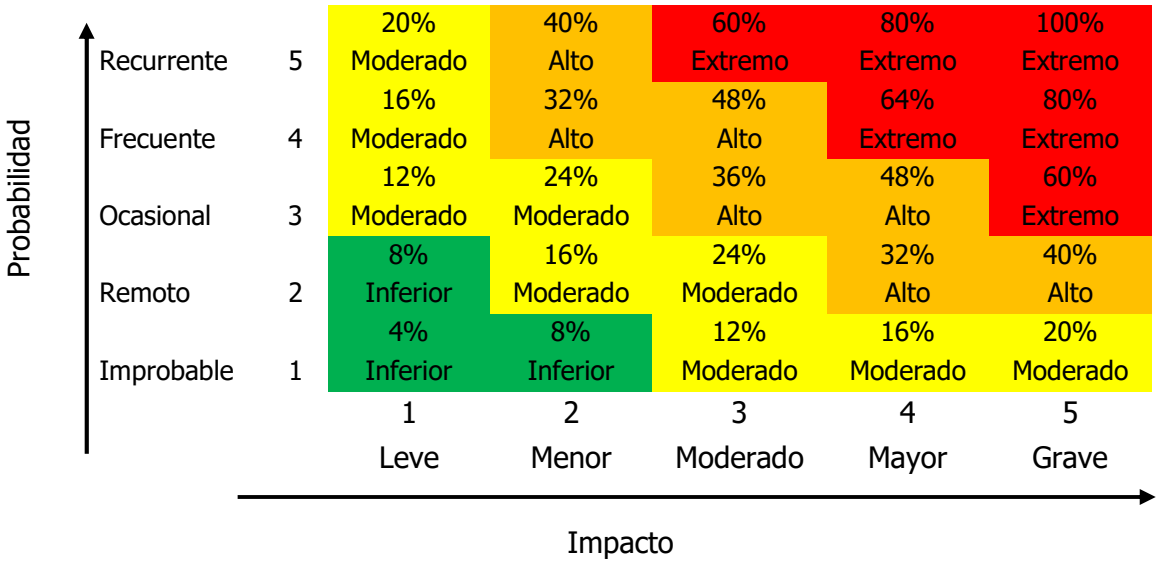
Las siguientes son las preguntas que permiten medir el impacto del riesgo a través de la metodología del panel de expertos:

- ¿Afecta al grupo de empleados del proceso relacionado?
- ¿Afecta el cumplimiento de metas y objetivos del área?
- ¿Afecta el cumplimiento de misión de la compañía?
- ¿Afecta el cumplimiento de la misión del sector al que pertenece la compañía?
- ¿Genera pérdida de confianza de la compañía, afectando su reputación?
- ¿Genera pérdida de recursos económicos?
- ¿Genera intervención de los organismos de control, de la Fiscalía, u otro ente?
- ¿Afecta la imagen de la compañía ante los clientes?
- ¿Puede dar lugar a procesos disciplinarios, sancionatorios, fiscales, penales?

De acuerdo con el número de respuestas afirmativas se mide el nivel de impacto del riesgo, teniendo en cuenta los siguientes criterios:

Medición del Impacto	Descripción
Grave	Si se responde entre ocho (8) y diez (10) preguntas afirmativas
Mayor	Si se responde entre cinco (5) y siete (7) preguntas afirmativas
Moderado	Si se responde entre tres (3) y cuatro (4) preguntas afirmativas
Menor	Si se responde al menos dos (2) preguntas afirmativas
Leve	Si se responde solo una (1) pregunta afirmativa

Así las cosas, una vez se asigna el valor aplicable para cada riesgo en probabilidad e impacto, el resultado se enmarca en un mapa de calor cuya dimensión corresponde a niveles de 5 filas por 5 columnas que le dan una mayor flexibilidad a la determinación de los riesgos intermedios.



Como se observa, la combinación de la probabilidad de ocurrencia y la magnitud del impacto, permiten determinar el nivel o perfil de riesgo inherente así:

	Riesgo Extremo	>50%	El Oficial de cumplimiento debe intervenir directamente e informar al Representante legal
	Riesgo Alto	> 24% y <= 50%	Se requiere diseñar/perfeccionar las medidas de control necesaria
	Riesgo Moderado	> 8% y <= 24%	Se requieren controles específicos para su tratamiento
	Riesgo Inferior	<8%	Se debe realizar un monitoreo periódico del cumplimiento del proceso.

2.3 Evaluación de riesgo

- **Apetito al riesgo**

La compañía tiene como objetivo llevar los riesgos inherentes hasta un nivel máximo de exposición moderado en los riesgos identificados. Lo anterior, sin limitar a que las diferentes áreas desarrollen un plan de acción para la implementación de controles en riesgos inferiores y moderados.

Nivel de Exposición Riesgo Inherente	**Nivel de Riesgo Residual Objetivo**
Extremo	Moderado
Alto	Moderado
Moderado	Inferior
Inferior	Inferior

Las opciones como respuesta a la evaluación de los riesgos son las siguientes:

Recurrente	5	Reducir	Reducir	Evitar/Reducir	Evitar/Reducir	Evitar/Reducir
Frecuente	4	Reducir	Reducir	Reducir	Evitar/Reducir	Evitar/Reducir
Ocasional	3	Reducir	Reducir	Reducir	Evitar/ Reducir	Evitar/Reducir
Remoto	2	Aceptar	Reducir	Reducir	Reducir	Evitar/ Reducir
Improbable	1	Aceptar	Aceptar	Reducir	Reducir	Reducir
		1 Leve	2 Menor	3 Moderado	4 Mayor	5 Grave

- **Evitar el riesgo:** Se evita el riesgo si se decide no proceder con la actividad que probablemente generaría el riesgo, utilizando un activo, servicio o producto distinto o modificando el proceso, de manera que las amenazas originales ya no lo afecten

- **Reducir o mitigar el riesgo:** Actividades y medidas tendientes a reducir la probabilidad y/o minimizar la severidad de su impacto. Se consigue mediante la

optimización de los procedimientos y la implementación de controles (prevención, planificación).

3. ACTIVIDADES DE CONTROL – TRATAMIENTO DEL RIESGO

Una vez identificado y evaluado el riesgo inherente, se deben diseñar y describir las actividades de control y herramientas necesarias para gestionar la probabilidad de ocurrencia e impacto de materialización de los riesgos identificados.

Conceptualmente un control se define como una actividad/acción/herramienta que permite reducir el riesgo.

Con el fin de identificar los controles existentes, actualizarlos, mejorarlos o diseñarlos, se recomienda realizar mesas de trabajo con los líderes de los procesos y expertos, quienes, con el apoyo de sus equipos de trabajo, serán los encargados de posteriormente implementar y monitorear su ejecución.

Estructura para la descripción del control:

Se deben detallar como mínimo los siguientes elementos:

- Qué se hace
- Cómo se hace
- Resultado/registro
- Responsable de la ejecución y seguimiento
- Frecuencia o periodicidad (en caso de que aplique)
- Describir o referenciar qué se hace en caso de que como resultado de la aplicación del control se identifique algún error (si aplica).

Posteriormente, se evalúa la idoneidad y eficacia de los controles que la compañía posee con el fin de mitigar y dar respuesta los riesgos evaluados. A partir de esta evaluación, se realiza medición del riesgo residual, el cual considera, por consiguiente, la consistencia de los controles.

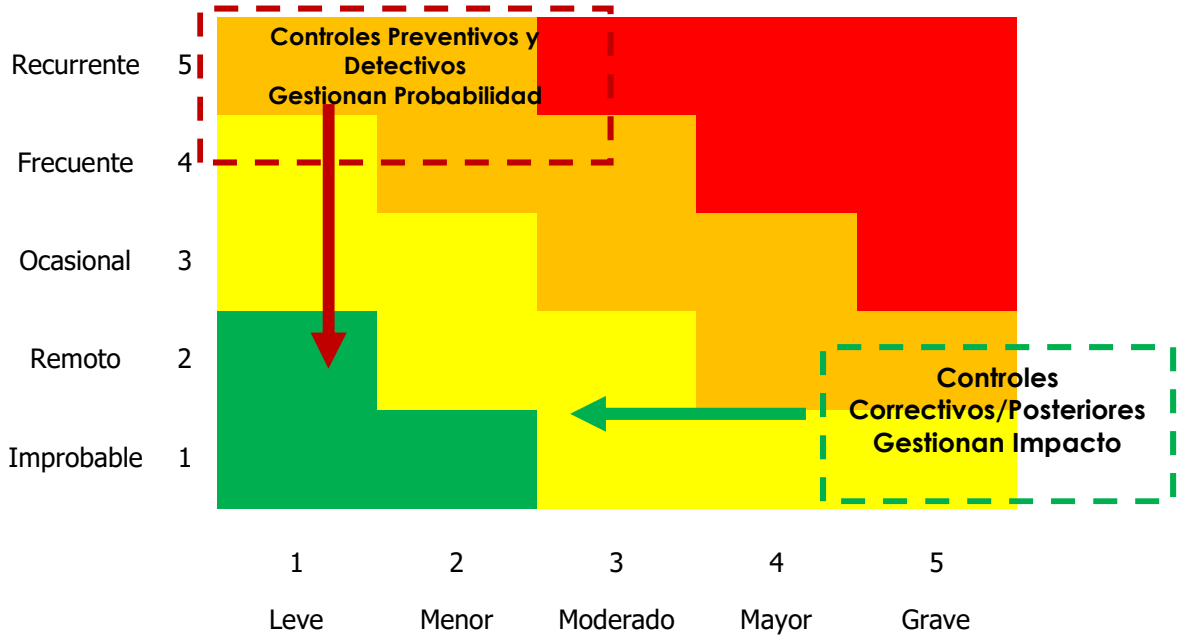
La evaluación de los controles se realiza teniendo en cuenta los siguientes criterios:

Descripción	Opción	Valor
Asignación responsable del control	Asignado	15
	No Asignado	0
Documentación del control	Documentado	15
	No Documentado	0
Frecuencia	Continua	15
	Aleatoria	0
Propósito	Prevenir	15
	Detectar	10
	Corregir	5
Clase de control	Automático	15
	Dependiente IT	10
	Manual	5
Evidencia	Con registro	10
	Sin registro	0
Qué pasa con las observaciones y desviaciones	Se tienen instrucciones específicas sobre cómo tratarlas oportunamente	15
	No se tienen instrucciones sobre cómo investigar o resolver oportunamente	0

De acuerdo con la estructura del control la cual se evalúa mediante los puntajes mencionados en la tabla, los controles pueden clasificarse de la siguiente manera:

Solidez Diseño		
Fuerte	80 a 100	80% de gestión en probabilidad o impacto
Moderado	40 a 79	50% de gestión en probabilidad o impacto
Débil	0 a 39	20% de gestión en probabilidad o impacto

De acuerdo con el tipo y propósito del control, la gestión de los riesgos se puede dar como se ilustra a continuación:



3.1 Tolerancia al riesgo

Una vez se encuentran definidos los niveles de riesgo residual, de no alcanzarse el perfil de riesgo residual esperado, se deben detectar las posibles debilidades existentes definiendo un tratamiento o plan de acción al riesgo residual orientado a:

Moderado	Riesgos evaluados continuamente por el coordinador o líder del proceso. Realizar reporte inmediato al oficial de cumplimiento. Si en la evaluación se determina un incremento en el nivel del riesgo, se harán los ajustes necesarios	Seguimiento semestral

Alto	El oficial de cumplimiento deberá establecer planes de acción que busquen reducir la exposición de la Compañía: 1. Implementar nuevos controles. 2. Modificar los controles existentes. 3. Realizar reporte inmediato al representante legal. 4. Evaluar acciones disciplinarias.	Seguimiento trimestral
Extremo	El oficial de cumplimiento deberá establecer planes de acción que busquen reducir la exposición de la compañía: 1. Implementar nuevos controles. 2. Modificar los controles existentes 3. Realizar reporte inmediato a los Altos Directivos de la Compañía o máximo órgano social 4. Evaluar acciones disciplinarias.	Seguimiento continuo

4. MONITOREO Y SUPERVISIÓN

La evaluación de los riesgos debe ser revisada de forma regular (mínimo una vez al año) de modo tal que se mantengan actualizados y que su nivel de criticidad sea acorde a la realidad. Adicionalmente, deben ser revisados en los casos extraordinarios, en los que existan cambios significativos en la estructura o procesos de la compañía.

Asimismo, dados los procedimientos recomendados, la compañía tiene la responsabilidad de identificar y evaluar los riesgos a través de procedimientos periódicos de Debida Diligencia y Auditoría, los cuales deben ser adelantados con recursos económicos y humanos que sean suficientes para cumplir con el objetivo de realizar una correcta evaluación

La eficacia es medida con base en el aporte de las actividades de control a la minimización del riesgo inherente, su eventual materialización y el comportamiento de los riesgos residuales. Como resultado de la revisión de la alta dirección se determina la eficacia de las

acciones establecidas y el cierre o ampliación del seguimiento sobre las oportunidades reportadas.

5. COMUNICACIÓN Y CONSULTA

La comunicación y consulta es transversal a todas las etapas del proceso para la gestión del riesgo, es por esto por lo que la compañía cuenta con planes de comunicación y consulta que involucra tanto las partes internas como externas responsables, interesadas, de control y que en general hacen parte de la gestión del riesgo, con el objetivo de abordar aspectos relacionados con los riesgos de la compañía, sus causas, sus consecuencias y las medidas que se establecen para su tratamiento.

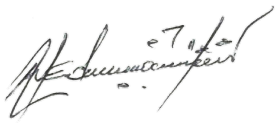
Lo anterior se realiza con el objetivo de garantizar que los responsables del proceso de gestión del riesgo y las partes involucradas entiendan las bases sobre las cuales se toman las decisiones, y las razones por las cuales se requieren acciones específicas.
Existen distintos mecanismos de comunicación y consulta a saber:

Capacitación

- Inducción a nuevos empleados: Como parte del proceso de inducción a la compañía, los nuevos colaboradores serán capacitados sobre la gestión de riesgos y sus obligaciones frente al mismo.
- Sensibilización: Fortalecimiento de la cultura de gestión del riesgo a través de campañas dirigidas a todo el personal con una periodicidad al menos anual.

Informes y Reportes Asociados a la Gestión de Riesgos

Los informes permiten a la compañía contar con un lenguaje común para administrar los resultados de la implementación y seguimiento de la gestión de riesgos y con ello entregar información que soporte la toma de decisiones en forma oportuna y efectiva.

Elaboró:	Aprobó:
	
Magda Sotelo	**Milton Cortés**
Oficial de Cumplimiento	**CFO**
Fecha: 30/11/2023	**Fecha: 30/11/2023**

CONTROL DE VERSIONES			
Versión	**Fecha**	**Autor**	**Descripción**
1.0	30/11/2023	Magda Sotelo	Creación del documento