

Política de Control y Gestión de Riesgos

Contenido

1. Objeto.....	2
2. Ámbito de aplicación.....	2
3. Responsabilidades.....	2
4. Descripción del proceso	4
4.1. Identificación de riesgos	4
4.2. Evaluación de riesgos.....	5
4.3. Tratamiento del riesgo.....	5
4.4. Supervisión de riesgos	5
4.5. Actualización	6
4.6. Incumplimiento.....	6

	POLÍTICA DE CONTROL Y GESTIÓN DE RIESGOS	Código:	CIE CO CP PO 03
		Revisión:	02
		Página:	2 de 6

1. Objeto

El objeto de este documento es la definición de la Política de Control y Gestión de Riesgos de CIE Automotive, S.A. (en adelante, "CIE"), para establecer el marco general de actuación así como los procedimientos y las responsabilidades para llevar a cabo el control y la gestión de los riesgos a los que debe enfrentarse CIE de manera eficiente y efectiva.

El sistema de gestión de riesgos (en adelante, "SGR") de CIE permite asegurar razonablemente que todos los riesgos significativos: estratégicos, operacionales, financieros (ver política sobre el Sistema de Control Interno de la Información Financiera (SCIIF)) y ESG (obedece al acrónimo inglés de ambientales, sociales y de gobierno corporativo), sean prevenidos, identificados, evaluados, sometidos a un seguimiento continuo y reducidos a los niveles de apetito y tolerancia al riesgo definidos, y sean finalmente aprobados por el Consejo de Administración.

Con un compromiso fuerte y sostenido por parte de la Alta Dirección y el Equipo de Dirección, así como una planificación estratégica rigurosa, se pretende lograr un entorno donde exista la capacidad de trabajar con riesgos de manera controlada, gestionándolos de una manera activa, permitiendo aprovechar nuevas oportunidades.

Los principios en los que se basa son fundamentalmente:

- Potenciar una visión constructiva del concepto de riesgo.
- Compromiso y competencia de las personas que participan en él.
- Utilizar un lenguaje común.
- Comunicación transparente en toda la organización.

El personal de CIE con responsabilidades en relación al SGR contará con los medios materiales y humanos necesarios para el desempeño de sus funciones.

2. Ámbito de aplicación

Esta política es aplicable al SGR de CIE en todos sus centros, sociedades participadas y ámbitos, cubriendo todos los riesgos sobre la información financiera y no financiera que afecten o puedan afectar a CIE, ya se originen en su entorno o en sus actividades.

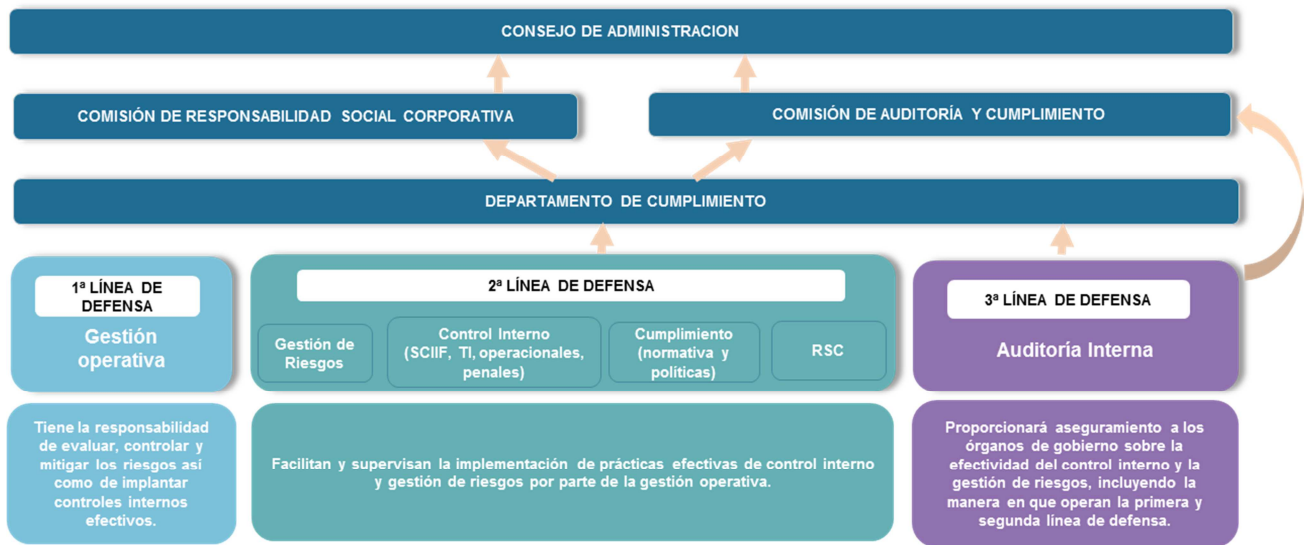
3. Responsabilidades

Los distintos roles que intervienen en el SGR pueden agruparse en tres líneas de defensa frente a los riesgos que amenazan el cumplimiento de los objetivos estratégicos, operativos, financieros y ESG. Mientras la que la primera línea de defensa depende directamente de la Alta Dirección y del Equipo de Dirección, tanto la segunda como la tercera línea de defensa se encuentran bajo la dirección del departamento de Cumplimiento.

Como se muestra en el gráfico adjunto, en el SGR las tres líneas de defensa se encuentran bajo la supervisión del Consejo de Administración:

Emitido y revisado: Dpto. Cumplimiento	Aprobado: Consejo de Administración	Fecha: Febrero 2018
---	--	----------------------------

	POLÍTICA DE CONTROL Y GESTIÓN DE RIESGOS	Código:	CIE CO CP PO 03
		Revisión:	02
		Página:	3 de 6



En este contexto, los roles y responsabilidades de cada uno de los miembros de la organización que intervienen en el SGR son los siguientes:

Órgano	Responsabilidades
Consejo de Administración	<ul style="list-style-type: none"> ✓ Responsable último ante los accionistas de la existencia y funcionamiento del SGR. ✓ Supervisión del SGR mediante las actividades realizadas por la Comisión de Auditoría y Cumplimiento.
Comisión de Auditoría y Cumplimiento	<ul style="list-style-type: none"> ✓ Evaluación y supervisión del SGR de CIE. ✓ Informar al Consejo de Administración sobre los resultados de las evaluaciones realizadas y del calendario asignado a las medidas propuestas para las debilidades detectadas.
Alta Dirección y Equipo de Dirección	<ul style="list-style-type: none"> ✓ Responsable de identificar y evaluar el riesgo. ✓ Implantar y transmitir una cultura enfocada a riesgos en la empresa. ✓ Definir, establecer y/o modificar el apetito de riesgo. ✓ Aprobar los planes y acciones propuestos por el departamento de Cumplimiento que puedan considerarse necesarios para afrontar los riesgos identificados.
Departamento de Cumplimiento	<ul style="list-style-type: none"> ✓ Responsable de diseñar e implantar el funcionamiento del SGR. ✓ Definir la metodología, procedimientos y criterios de CIE para la identificación, valoración, clasificación, aprobación y respuesta de riesgos. ✓ Responsable de la elaboración del Mapa de Riesgos. ✓ Informar periódicamente a la Comisión de Auditoría y Cumplimiento sobre la evolución de los riesgos así como el funcionamiento general del SGR.
Departamento de Auditoría Interna	<ul style="list-style-type: none"> ✓ Evaluar la eficacia del SGR e informar periódicamente de las debilidades detectadas y del calendario asignado a las medidas propuestas para su corrección.
Resto de empleados	<ul style="list-style-type: none"> ✓ Responsables de identificar riesgos que amenacen el cumplimiento de sus objetivos y de comunicarlos al responsable de área. ✓ Colaborar con los responsables de área en la valoración y clasificación del riesgo así como proponer planes de acción para afrontar los riesgos identificados y colaborar en la ejecución de los mismos.

	POLÍTICA DE CONTROL Y GESTIÓN DE RIESGOS	Código:	CIE CO CP PO 03
		Revisión:	02
		Página:	4 de 6

Matriz de segregación de funciones del SGR:

	Consejo de Administración	Comisión de Auditoría y Cumplimiento	Alta Dirección y Equipo de Dirección	Departamento de Cumplimiento	Departamento de Auditoría Interna	Resto de empleados
Identificación de riesgos		X	X	X		X
Evaluación de riesgos			X	X		
Tratamiento del riesgo				X		
Supervisión de riesgos	X	X		X	X	
Actualización			X	X		
Incumplimientos					X	X

4. Descripción del proceso

El SGR está basado en la metodología de la ISO 31000 y adaptado a las necesidades de CIE. Utiliza como soporte la herramienta de gestión de riesgos SAP GRC, y en él se definen los siguientes componentes principales:

4.1. Identificación de riesgos

El proceso de identificación de riesgos consiste en la búsqueda de eventos (asociados a factores internos o externos) que puedan afectar a los objetivos de CIE, tanto de los Planes Estratégico y de Responsabilidad Social Corporativa, así como del Presupuesto anual.

La comprensión de los **factores externos** es importante para asegurar que los objetivos e inquietudes de los grupos de interés se tienen en cuenta. El contexto externo puede incluir, pero no se limita a:

- a) El entorno social y cultural, político, legal, financiero, tecnológico, económico, natural y competitivo a nivel internacional, nacional, regional o local.
- b) Los factores y tendencias que tengan impacto sobre los objetivos de la organización.
- c) Relaciones con los grupos de interés.

Los **factores internos** son aquellos en los que la organización puede influir y en consecuencia gestionar el riesgo. El proceso de gestión de riesgo deberá ser coherente con la cultura, procesos, estructura y estrategia de la organización.

La categoría de riesgos definida es la siguiente:

- **Estratégicos:** aquéllos que afectan a los objetivos de alto nivel directamente relacionados con el Plan Estratégico.
- **Operacionales:** aquéllos que afectan a los objetivos vinculados al uso eficaz y eficiente de los recursos.
- **Financieros:** aquéllos que afectan a los objetivos financieros.
- **Riesgos ESG (Environmental, Social and Governance):** afectan a los aspectos ambientales, sociales, éticos y de gobierno corporativo y al cumplimiento de leyes y normas.

Emitido y revisado: Dpto. Cumplimiento	Aprobado: Consejo de Administración	Fecha: Febrero 2018
---	--	----------------------------

	POLÍTICA DE CONTROL Y GESTIÓN DE RIESGOS	Código:	CIE CO CP PO 03
		Revisión:	02
		Página:	5 de 6

4.2. Evaluación de riesgos

Con el objetivo de definir un criterio homogéneo para la valoración de los riesgos, se han definido unas escalas de valoración: **probabilidad de ocurrencia** e **impacto**, siendo el impacto medido en tres categorías: económico, organizacional y reputacional. Estas escalas sirven para ubicar cada riesgo en el **Mapa de Riesgos**, herramienta principal de evaluación de riesgos.

Además de definir escalas de valoración para cada riesgo se definirán los siguientes aspectos:

- a) Localización del origen del riesgo.
- b) Identificar las áreas de impacto del riesgo, es decir, definir en caso de ocurrencia de qué forma afectaría a la sociedad.
- c) Identificar los responsables de gestión de los riesgos.

El proceso de evaluación de riesgos recae sobre la Alta Dirección y el Equipo de Dirección, quienes tendrán que evaluar los riesgos identificados en los plazos establecidos.

Una vez obtenidas las valoraciones se procederá a la consolidación de las evaluaciones de cara a obtener el Mapa de Riesgos. La consolidación de los riesgos tendrá en cuenta el peso específico de las valoraciones de cada uno de los responsables y de cada área geográfica para cada tipología de riesgo, de manera que resulte en una visión global de CIE y así poder priorizar los mismos. Este proceso es realizado por el departamento de Cumplimiento.

4.3. Tratamiento del riesgo

Una vez se han identificado, evaluado y consolidado los riesgos, se deben determinar los planes de acción para llegar a alcanzar el nivel de riesgo aceptado por la organización.

La gestión de estos riesgos se puede clasificar en tres categorías según el binomio probabilidad e impacto:

- a) **Eliminar:** se llevan a cabo acciones encaminadas a eliminar los hechos que suponen un riesgo.
- b) **Mitigar:** reducir la probabilidad de ocurrencia, el impacto posible o los dos.
- c) **Aceptar:** aceptar el nivel de probabilidad y el impacto del riesgo identificado. Esta decisión debe estar comunicada y soportada.

El proceso de análisis y diseño de las respuestas a los riesgos recae sobre el departamento de Cumplimiento, quien posteriormente lo presentará a la Comisión de Auditoría y Cumplimiento.

4.4. Supervisión de riesgos

Con el objetivo de asegurarse de que las respuestas a los riesgos acordadas son viables y eficientes, cada año el departamento de Cumplimiento realizará un seguimiento que cubrirá los siguientes objetivos:

- ✓ Asegurar que los riesgos están siendo gestionados en la forma aprobada por la Alta Dirección y Equipo de Dirección.
- ✓ Evaluar si las respuestas acordadas son eficientes e iniciar los planes de acción en caso de que sea necesario.
- ✓ Determinar si el catálogo de riesgos anticipa y refleja cambios en las circunstancias de negocio y nuevas condiciones económicas.

Emitido y revisado: Dpto. Cumplimiento	Aprobado: Consejo de Administración	Fecha: Febrero 2018
---	--	----------------------------

	POLÍTICA DE CONTROL Y GESTIÓN DE RIESGOS	Código:	CIE CO CP PO 03
		Revisión:	02
		Página:	6 de 6

Adicionalmente, el departamento de Cumplimiento deberá identificar si se ha materializado algún riesgo y, en su caso, las medidas adoptadas para mitigarlo.

Para facilitar las labores de supervisión, se dispondrá de distintos niveles de reporting:

- a) **Reporting interno:** el [Mapa de Riesgos](#), donde se incluirá el catálogo de riesgos de CIE y una representación gráfica de los principales riesgos por área geográfica y por tipología de riesgo, incluyendo para los riesgos top las actividades de control de alto nivel implantadas, así como los planes de acción acordados para la mitigación de los mismos.
- b) **Reporting externo:** está compuesto por la información sobre la gestión de riesgos a incluir en el [Informe Anual de Gobierno Corporativo](#) y en el [Informe Anual](#), elaborado por el departamento de Cumplimiento, en el que se detallarán los principales riesgos a los que se enfrenta CIE y las acciones acordadas sobre los riesgos principales identificados.

La supervisión por parte del Consejo de Administración y de la Comisión de Auditoría y Cumplimiento de los riesgos ESG cumple con los Estándares GRI.

4.5. Actualización

Los riesgos del negocio se modifican con el tiempo y por lo tanto generan cambios en el SGR. En ese sentido, los riesgos que antes eran críticos pueden perder relevancia, mientras que otros ganan en criticidad.

Con el objetivo de mantener un SGR eficaz y actualizado el departamento de Cumplimiento realiza con carácter anual la actualización del Mapa de Riesgos, siguiendo el proceso descrito con anterioridad.

4.6. Incumplimiento

Todo empleado que tenga indicios o sospechas de comportamiento contrario y/o que pueda implicar la materialización de un riesgo debe ponerlo inmediatamente en conocimiento de CIE a través del canal ético a su disposición en la web corporativa.

Emitido y revisado: Dpto. Cumplimiento	Aprobado: Consejo de Administración	Fecha: Febrero 2018
---	--	----------------------------