Transformamos el presente.
Fortalecemos el mañana.

Política de Gestión de Riesgos y Control Interno

Aprobada por el Consejo de Administración de CELSA STEEL el 30/10/2025.

Índice

1. Objeto y alcance

Objeto: Establecer un marco de actuación eficiente y efectivo para la identificación, evaluación, control y mitigación de los riesgos a los que se enfrenta la organización, y que pueden impedir o dificultar el logro de los objetivos estratégicos del grupo CELSA (en adelante "CELSA" o "Grupo"). Este documento sienta las bases para una gestión homogénea, proactiva y sistemática de los riesgos, dentro de los umbrales de tolerancia y apetito al riesgo establecidos por el Consejo de Administración.

Por la naturaleza de sus operaciones, CELSA está sujeta a diversos riesgos inherentes en los países, sectores y mercados en los que opera, que pueden impedirle lograr sus objetivos estratégicos con éxito. Por ello, esta política define las bases del sistema de gestión de riesgos, basado en el marco metodológico establecido en COSO (Committee of Sponsoring Organizations of the Treadway Commission) III – Enterprise Risk Management Framework[1], como estándar de referencia, adaptado a las necesidades específicas de CELSA

Alcance: aplicable a todas las entidades, empleados y niveles organizativos del Grupo, abarcando todas sus actividades, ubicaciones y operaciones. En aquellas sociedades participadas en las que este documento pudiera no ser de aplicación, el área de *Internal Audit & Risk Control* promoverá unos principios coherentes con los establecidos en este documento, manteniendo siempre los mecanismos necesarios para garantizar su adecuado control.

2. Definiciones

Para una aplicación clara y uniforme de la política, se establecen las siguientes definiciones:

- **Riesgo:** Evento o conjunto de circunstancias que pueden impactar negativamente en la organización, afectando el cumplimiento de sus objetivos estratégicos. Los riesgos se pueden aceptar, evitar, transferir o mitigar. Cada riesgo tiene una o varias naturalezas distintas, y requiere de una

[1] https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf

gestión particular. En CELSA, los agrupamos, según su naturaleza, en cuatro grandes bloques:

- **Riesgos Estratégicos**: derivados de la posición estratégica de CELSA en el entorno en que desarrolla su actividad, las relaciones con terceros, la planificación y organización de las personas, así como los eventos que puedan afectar negativamente el cumplimiento de los objetivos definidos en el plan estratégico.
- **Riesgos Operacionales**: referidos a las pérdidas económicas, directas o indirectas, ocasionadas por procesos internos inadecuados, fallos tecnológicos, errores humanos o como consecuencia de sucesos externos, incluyendo desastres naturales, afectación a la cadena de suministro, y de las tecnologías de la información.
- **Riesgos Financieros**: asociados con alteraciones en los mercados financieros y/o de bienes y servicios que afectan a los costes e ingresos de la actividad, incluyendo la gestión de tipos de cambio, el riesgo de liquidez, el de tipo de interés, o el riesgo de crédito relacionado con la posibilidad de que una contraparte incumpla sus obligaciones de pago.
- **Riesgos de Cumplimiento**: asociados con el incumplimiento de disposiciones legales, contractuales, o de estándares y códigos de conducta aplicables a la actividad, y que pueden conllevar sanciones y/o deterioros de la reputación, provocando en consecuencia, un impacto adverso en los resultados del Grupo.

- **Apetito al Riego:** Nivel de riesgo que una organización está dispuesta a asumir para conseguir sus objetivos estratégicos.
- **Tolerancia al Riesgo:** Margen de variación aceptable respecto al nivel de riesgo que la organización está dispuesta a soportar en la consecución de sus objetivos. Representa el límite donde el riesgo puede fluctuar sin desencadenar una respuesta correctiva inmediata, y se define en función del apetito al riesgo.
- **Controles:** Medida, acción o mecanismo implementado para mitigar (de manera preventiva o detectiva) un evento de riesgo, reduciendo su probabilidad de ocurrencia o el impacto en la organización.
- **KPI (Key Performance Indicator / Indicador Clave de Desempeño):** Métrica cuantitativa utilizada para evaluar el desempeño de una actividad, proceso o área, en relación con un objetivo o el desempeño de un área.
- **KRI (Key Risk Indicator / Indicador Clave de Riesgo):** Métrica cuantitativa que permite anticipar la probabilidad de ocurrencia o el impacto potencial de un riesgo. Se utiliza como señal de alerta temprana para detectar desviaciones

que podrían indicar la potencial materialización de un riesgo, permitiendo anticipar la toma de decisiones.

3. Principios generales

1. **La gestión de riesgos es parte de la estrategia para conseguir los objetivos,** incluyendo el proceso de identificación, evaluación y mitigación, en base al apetito al riesgo definido por el Consejo de Administración. Cada área debe seguir las directrices establecidas en el modelo de riesgos de CELSA para garantizar la coherencia y la integridad de la gestión de riesgos del Grupo.
2. **Proteger la cadena de valor, las personas, los activos, el medioambiente y la reputación**, a través del desarrollo de mecanismos y procesos que permitan mitigar los riesgos de manera eficiente, dentro de los márgenes de tolerancia definidos. Esto incluye la evaluación y mitigación proactiva de los riesgos, así como la definición de planes de contingencia, resiliencia y gestión de crisis, que permitan a CELSA reducir el efecto de un riesgo materializado, tanto en la probabilidad como en el impacto.
3. **Preservar la continuidad y la fiabilidad e integridad de la información** hacia los accionistas, así como cualquier parte interesada. La implementación de controles internos que aseguren la fiabilidad, integridad y trazabilidad de la información (financiera y no financiera) es esencial para responder a las expectativas de reguladores y/o partes interesadas en el Grupo. Cada área liderará el despliegue de los controles de mitigación que estén bajo su responsabilidad, así como la coordinación con el resto de las áreas a las que les aplique.
4. **Establecer un modelo único de aseguramiento y un lenguaje común** en toda la organización para gestionar los riesgos, garantizando la integración y coexistencia del mapa de riesgos corporativo, junto con los mapas de riesgos específicos de detalle/áreas concretas. Cada área organizativa es responsable de gestionar sus riesgos y podrá apoyarse en el equipo de gestión de riesgos corporativo para garantizar la coherencia del reporte, tanto al equipo directivo como al Consejo de Administración.
5. **Fomentar la gestión proactiva e integrada en la toma de decisiones**, valorando tanto los riesgos como las oportunidades, tanto al definir los objetivos estratégicos como al tomar decisiones para su consecución, alineado con las directrices de los modelos de gestión de riesgos medioambientales, sociales y de gobernanza (ESG).
6. **Promover la formación, concienciación y seguimiento en materia de gestión de riesgos como parte de la mejora continua**, mejorando la eficacia y la eficiencia de los controles a través de la función de aseguramiento (auditoria), mitigando o transfiriendo los riesgos, y evaluando de forma proactiva y preventiva la capacidad de CELSA para responder ante impactos disruptivos en su cadena de valor. Esto incluye la definición de cuadros de

mandos con indicadores de actividad (KPI's) e indicadores de riesgos (KRI's) para monitorizar la evolución de los riesgos y tomar decisiones de acuerdo con el apetito al riesgo.

4. Roles y responsabilidades

Para garantizar su correcto funcionamiento, la gestión de riesgos de CELSA dispone de un marco de gobernanza integrada, basada en el modelo de las tres líneas, considerado como mejor práctica en los modelos comúnmente aceptados a nivel mundial, que otorga segregación entre las funciones de diseño, ejecución y supervisión de riesgos.

Todos los miembros de CELSA tienen la responsabilidad de conocer e implantar esta política en su ámbito de responsabilidad. Adicionalmente, se definen las siguientes responsabilidades en el modelo:

Consejo de Administración:

- Aprobar y supervisar la implementación de la Política de Gestión de Riesgos y Control, en la que se define la estrategia en materia de gestión de riesgos, así como aprobar y dar seguimiento a la evolución del apetito al riesgo.

Comisión de Auditoría y Control:

- Supervisar el adecuado funcionamiento del sistema de gestión de riesgos y control interno.
- Trasladar, de forma periódica, al Consejo de Administración, los aspectos más relevantes relacionados con la supervisión del modelo de gestión de riesgos de CELSA.

Comité de Dirección y CEO

- Liderar el diseño, la implementación y el seguimiento del sistema de gestión de riesgos, así como liderar la estrategia de gestión de riesgos, de acuerdo con el apetito al riesgo definido por el Consejo de Administración.
- Validar las políticas que desarrollen la gestión y el control de riesgos en cada una de sus áreas de responsabilidad.
- Facilitar los recursos suficientes para desplegar los planes de mitigación de los riesgos, en línea con el apetito al riesgo de CELSA.

Responsables de área y equipo directivo

- Comprender, evaluar y monitorizar los riesgos que formen parte de su área de responsabilidad, garantizando que los mapas de riesgos de CELSA se mantienen actualizados, de acuerdo con la metodología establecida por el área de riesgos y control.

- Asegurar que los controles que mitigan los riesgos están adecuadamente diseñados y, en caso contrario, liderar la implantación de los planes de remediación necesarios.

Equipo de riesgos y control

- Supervisar, integrar y coordinar todos los mapas de riesgos de CELSA, asegurando la consistencia y coherencia entre ellos, y garantizando una fuente de reporte unificada.
- Apoyar al Comité de Dirección en el análisis de los riesgos, controles y planes de acción, así como en su monitorización y reporte de la evolución del modelo para el Consejo de Administración y la Comisión de Auditoría y Control.
- Dar soporte a todos los equipos que gestionan riesgos en el Grupo, garantizando una evaluación y tratamiento homogéneos, a través de formación o de acompañamiento en el diseño de sus modelos.

Auditoría Interna

- Evaluar, de manera independiente y objetiva, la eficacia operativa del sistema de control y gestión de riesgos de CELSA, así como informar periódicamente a la Comisión de Auditoría y Control y al Comité de Dirección, sobre las debilidades detectadas y medidas correctoras propuestas.

5. Aprobación, comunicación y actualización

Esta política será revisada periódicamente para asegurar su relevancia y efectividad, como mínimo, cada 12 meses, o con mayor frecuencia si las circunstancias lo requieren.

Para garantizar su adecuada implementación y cumplimiento, esta política será difundida de manera interna y externa a través de la página web del Grupo. Adicionalmente, se adoptarán los medios adecuados para promover su conocimiento y asegurar su cumplimiento por parte de todas las áreas implicadas.

6. Referencias y anexos

La presente Política de Riesgos y Controles constituye el marco general de gestión del riesgo y control interno y articula los diferentes procedimientos específicos detallados a continuación:

- *Procedimiento de identificación, evaluación y análisis de riesgos*
- *Procedimiento de gestión del riesgo de contrapartes*
- *Procedimiento del Sistema de Control Interno de Información Financiera y No Financiera (SCIIF y SCIINF)*
- *Procedimiento de resiliencia y continuidad de negocio*
- *Procedimiento del plan general de gestión de crisis*