Transformamos el presente.
Fortalecemos el mañana.

Política de Privacidad

Aprobado por el Consejo de Administración de CELSA STEEL el 30/10/2025

Índice

1. Objeto y alcance

Objeto:

Esta política tiene como finalidad establecer los principios y obligaciones fundamentales en materia de privacidad dentro de CELSA. Busca garantizar el respeto al derecho fundamental a la privacidad de todos los miembros de la organización, socios de negocio y terceros. Además, define las pautas para asegurar la privacidad y documentar el cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), incluyendo todos los requisitos necesarios para demostrar dicho cumplimiento.

Alcance:

Esta Política se aplica a CELSA y a todas las sociedades que integran su Grupo, atendiendo a sus características propias, así como los tratamientos de datos personales realizados por CELSA, incluyendo los sistemas de información, soportes y equipos empleados para dicho tratamiento de datos de carácter personal, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Las actividades afectadas por la presente Política son todas las que realiza CELSA , o pueda acometer en el futuro, en el desarrollo de su actividad empresarial, que implique, esté relacionada o pueda suponer un Tratamiento de Datos personales, entre otros, de miembros de la organización, socios de negocio y terceros.

Los principios y directrices establecidos en este documento se aplicarán respetando las particularidades normativas y regulatorias en materia de privacidad de cada jurisdicción donde opere CELSA. En aquellos casos donde las legislaciones locales establezcan requisitos específicos, adicionales o divergentes respecto a los principios generales aquí recogidos, se podrán desarrollar anexos específicos a la presente política que garanticen el pleno cumplimiento de la normativa aplicable en cada territorio, manteniendo en todo caso los estándares mínimos de protección establecidos en el presente documento.

Esta política ha sido aprobada por el Consejo de Administración de CELSA STEEL, S.A. el 30/10/2025.

2. Definiciones

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

Datos personales: toda información que permita identificar directa o indirectamente a una persona física. A título ilustrativo, se considerarán Datos personales, por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre *Datos personales* o conjuntos de *Datos personales*, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

AEPD (Agencia Española de Protección de datos): Autoridad independiente encargada de garantizar el cumplimiento de la normativa sobre protección de datos personales en España y de proteger los derechos de los ciudadanos en este ámbito. Es la Lead Supervisory Authority (Autoridad de Control Principal) del grupo CELSA, con exclusión de otras autoridades.

PIA (Privacy Impact Assessment): un análisis de los riesgos que un determinado sistema de información, producto o servicio puede implicar para los datos de carácter personal que se tratan dentro de una organización.

Manual de Privacidad: conjunto de documentos que incluye esta Política de Privacidad y todos los procedimientos mencionados en la misma, que conforman el marco normativo interno de CELSA en materia de privacidad.

Incidencias de seguridad: Entre otras, cualquier incumplimiento de la normativa desarrollada en el Reglamento General de Protección de Datos (RGPD) y/o normativa que la substituya o actualice, así como cualquier anomalía o evento que afecte o pueda afectar a la seguridad de los datos de carácter personal en sus tres vertientes de confidencialidad, integridad y disponibilidad.

Violación de seguridad: Cualquier incidente que cause destrucción, pérdida, alteración o acceso no autorizado a datos personales.

3. Desarrollo de la Política de Privacidad

Este documento resume las directrices generales de actuación para cumplir con la Política de Privacidad de CELSA, las cuales están desarrolladas en el conjunto de

documentos que componen el Manual de Privacidad de CELSA. Incluye los pasos clave para la gestión adecuada del tratamiento de datos personales, la prevención de riesgos y la respuesta ante incidentes.

3.1 Principios Generales

CELSA establece los siguientes principios para el tratamiento de datos personales:

- **Licitud, lealtad y transparencia** – Para tratar los datos personales legalmente, habrá una base legítima y se informará a la persona afectada
- **Limitación de la finalidad** – Los datos personales sólo se usarán para fines concretos y legítimos, y no pueden emplearse para otros fines distintos sin justificación
- **Minimización** – Solo se tratarán los datos necesarios y adecuados para el fin previsto
- **Exactitud** – Los datos deberán ser correctos y estar actualizados.
- **Limitación del plazo de conservación** – Los datos personales se conservarán solo el tiempo necesario y se eliminarán cuando ya no se usen, salvo que exista una obligación legal o se mantengan con fines específicos.
- **Transparencia e información** – Se informará de forma clara y accesible a las personas sobre cómo se tratarán sus datos personales.
- **Integridad y confidencialidad** – Los datos personales se protegerán con medidas de seguridad adecuadas y se tratarán siempre con confidencialidad
- **Responsabilidad activa** – El responsable del tratamiento cumplirá con los principios de protección de datos y guardará evidencia de ellos.
- **Obtención legítima** – Está prohibido obtener datos personales de fuentes ilegales o que no garanticen su origen legítimo.
- **Transferencias internacionales** – Las transferencias de datos fuera del Espacio Económico Europeo cumplirán estrictamente con la normativa europea aplicable.
- **Derechos de los interesados** – CELSA garantizará que las personas puedan ejercer sus derechos sobre sus datos mediante procedimientos adecuados.

3.2 Análisis de riesgos y medidas de seguridad

CELSA aplica medidas técnicas y organizativas para garantizar la seguridad de los datos personales, como cifrado, control de accesos, recuperación ante incidentes y revisiones periódicas. Estas medidas se basan en un análisis de riesgos anual que identifica amenazas, vulnerabilidades y daños potenciales.

3.2.1 Privacy Impact Assessment (PIA)

CELSA realizará un PIA, o *evaluación de impacto de protección de datos*, antes de cualquier tratamiento de datos que pueda implicar un alto riesgo para los derechos

de las personas, especialmente si se usan nuevas tecnologías. Se requiere en casos como:

- Elaboración de perfiles automatizados con efectos jurídicos.
- Tratamiento masivo de datos sensibles o especialmente protegidos.
- Vigilancia sistemática en espacios públicos.

La lista oficial de tratamientos que requieren PIA está disponible en el sitio web de la AEPD, y puede consultarse en https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-el-listado-de-tratamientos-en-los-que-no-es.

Cuando se identifique un nuevo tratamiento de datos personales o se planifique una modificación sustancial de un tratamiento existente, la persona responsable del mismo deberá notificar al Equipo de Privacidad a través de la dirección gdpr@gcelsa.com con la antelación suficiente para evaluar la necesidad de realizar un PIA. Esta notificación deberá incluir una descripción detallada del tratamiento propuesto, las categorías de datos personales involucrados, los fines del tratamiento, el plazo de conservación de los datos personales, las categorías de interesados afectados y cualquier tecnología o metodología específica que se pretenda utilizar. El Equipo de Privacidad evaluará si el tratamiento propuesto presenta un alto riesgo para los derechos y libertades de las personas físicas y, en su caso, determinará la necesidad de realizar un PIA conforme a los criterios establecidos en el artículo 35 del RGPD y las directrices de las autoridades de protección de datos competentes.

3.3 Notificación, gestión y respuesta ante incidencias

3.3.1 Registro de incidencias

El DPO deberá mantener un registro de incidencias para aplicar medidas correctoras, prevenir futuros ataques y responsabilizar a quienes comprometan la seguridad del tratamiento de datos.

Todo usuario que detecte una incidencia debe comunicarlo según se determina en la *PR-00144 Gestión y notificación de brechas de seguridad.*

3.3.2 Notificación de las violaciones de seguridad

CELSA debe notificar a la AEPD en un máximo de 72 horas si ocurre una violación de seguridad que afecte datos personales.

También debe informar a los afectados si hay alto riesgo para sus derechos, salvo que los datos estén protegidos, el riesgo haya desaparecido o la comunicación sea desproporcionada.
Toda violación debe documentarse con detalles, consecuencias y medidas correctoras.

3.4 Derechos de los interesados

Los interesados pueden ejercer los siguientes derechos ante CELSA: acceso, rectificación, supresión (derecho al olvido), limitación del tratamiento, portabilidad, oposición, así como no ser objeto de decisiones automatizadas.

Ante una solicitud de ejercer derechos, CELSA debe responder en un plazo máximo de un mes (prorrogable dos meses en casos complejos) de acuerdo con el procedimiento de atención a ejercicios de derechos.

La solicitud es gratuita, salvo que sea manifiestamente infundada o excesiva, en cuyo caso se podrá cobrar un canon o rechazarla justificadamente. Dichas solicitudes se podrán ejercer a través del envío de un correo electrónico a la dirección gdpr@gcelsa.com.

3.5 Sistema de Gobierno de la Privacidad

CELSA ha designado a su Comité de Ciberseguridad y Privacidad como Delegado de Protección de Datos (DPO), encargado de asesorar, informar y actuar como enlace con las autoridades de control.

El DPO puede ser contactado por correo (GDPR@gcelsa.com) o por correo postal en Castellbisbal:

A/a Delegado Protección de Datos. C/Ferralla n. 12, 08755 Castellbisbal, Barcelona, España.

Se realizarán auditorías internas o externas periódicas para verificar el cumplimiento de las medidas de seguridad y la normativa de privacidad. También se harán auditorías extraordinarias si hay cambios significativos en los sistemas de información.

4. Roles y responsabilidades

El cumplimiento de la normativa aplicable sobre Privacidad es responsabilidad de todos los miembros del Grupo CELSA, quienes deben actuar conforme a los principios establecidos en esta Política.

Adicionalmente, se definen las siguientes responsabilidades:

Consejo de Administración:

- Revisar y aprobar la presente política y procedimientos asociados.
- Aprobar la gobernanza desde una perspectiva de privacidad del Comité de ciberseguridad y privacidad.

Comité de Dirección:

- Supervisar que la política y sus procedimientos se desplieguen correctamente en toda la organización.

- Impulsar una cultura de cumplimiento y responsabilidad en materia de privacidad en todos los niveles de la organización.

Delegado de Protección de Datos (DPO), representado colectivamente por el Comité de Ciberseguridad y Privacidad:

- Asesorar e informar a los trabajadores de CELSA sobre el tratamiento de datos personales.
- Coordinar con todas las unidades de negocio del grupo.
- Actuar como punto de contacto con las autoridades de control.

Equipo de privacidad, miembros del equipo legal y compliance designados para dar soporte como punto de contacto para todas las cuestiones relacionadas con el tratamiento de datos personales. Sus funciones principales son:

- Proporcionar asesoramiento técnico y normativo.
- Supervisar el cumplimiento de la política y el resto de normativa interna en materia de Privacidad.
- Identificar, analizar y mitigar los riesgos relacionados con el tratamiento de datos personales.
- Coordinar las diferentes áreas de negocio para asegurar la correcta implementación de la política de privacidad y su alineamiento con RGPD.
- Formar y concienciar a todos los miembros de la organización, en colaboración con la red de Data Privacy Advisors.

***Data Privacy Advisors*:**, son las personas designadas dentro de las distintas unidades de negocio para actuar como enlace operativo con el Equipo de Privacidad. Sus funciones principales son:

- Asesorar a sus equipos sobre la correcta aplicación de la normativa de protección de datos en las actividades diarias.
- Promover el cumplimiento de la política y resto de normativa interna en materia de privacidad y seguridad de la información.
- Identificar y comunicar posibles riesgos o incumplimientos relacionados con el tratamiento de datos personales.
- Colaborar en la gestión de incidentes de seguridad que afecten a datos personales.
- Canalizar dudas, consultas o necesidades hacia el Equipo de Privacidad.
- Participar en iniciativas de formación y concienciación en materia de privacidad dentro de su ámbito

Todos los Miembros de Celsa:

- Conocer y aplicar las normas de protección de datos.

- Notificar cualquier incidencia de seguridad mediante los cauces establecidos por la organización en el documento *PR-00144 Gestión y notificación de brechas de seguridad*.
- Guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Socios de Negocio y Terceros (incluyendo proveedores, subcontratistas, encargados del tratamiento, socios comerciales, clientes, consultores externos y cualquier otra entidad que tenga acceso a datos personales en el marco de la relación contractual con CELSA):

- Cumplir con las medidas de seguridad y confidencialidad definidas en este documento.

5. Aprobación, comunicación y actualización

El DPO revisará esta política una vez al año, y la actualizará según sea necesario para mantener su relevancia y eficacia. Las actualizaciones de esta política deben ser aprobadas tanto por el Comité de Ciberseguridad y Privacidad como por el Consejo de Administración, previa validación del Comité de Dirección.

Para garantizar su adecuada implementación y cumplimiento, esta Política está publicada en la página web corporativa de CELSA (Políticas de Celsa), así como a través de los canales internos 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 Documentos Relacionados

Esta política se complementa con una serie de procedimientos y anexos que conforman el Manual de Privacidad, el cual desarrolla con mayor detalle y profundidad los aspectos operativos y específicos de su aplicación.

En concreto se incluyen los siguientes procedimientos y anexos:

- Procedimiento de gestión de ejercicio de derechos
- Procedimiento de mantenimiento, supresión y bloqueo de datos personales
- Procedimiento de gestión y notificación de brechas de seguridad
- Procedimiento de uso y tratamiento de datos personales en formato papel.
- Procedimiento para realización de una Evaluación de Impacto de Privacidad
- Anexo I. Funciones y obligaciones del personal
- Anexo II. Registro de actividades de tratamiento
- Anexo III. Análisis de riesgos
- Anexo IV. Medidas de seguridad implantadas

Asimismo, esta política se alinea con la normativa vigente en materia de privacidad, en particular:

- **Reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).
- **Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Cualquier otra normativa nacional o sectorial aplicable en función del contexto y la jurisdicción de los tratamientos realizados.