

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Introducción

La Dirección de **Torrecid** reconoce que la **información** es un activo estratégico fundamental para el desarrollo de su actividad, su ventaja competitiva y la confianza depositada por sus **clientes, proveedores, colaboradores y otras partes interesadas**. Por ello, se compromete a implantar, mantener y mejorar de forma continua un **Sistema de Gestión de Seguridad de la Información (SGSI)** conforme a las mejores prácticas internacionales (ISO 27001, Esquema Nacional de Seguridad, RGPD, LOPDGDD y normativa aplicable del sector industrial) y en particular con la **Directiva 2022/2555** del Parlamento Europeo y del Consejo, conocida por NIS2

La presente Política de Gestión de Seguridad de la Información establece un marco de trabajo que permite que la información se gestione de forma segura, real y eficaz y de acuerdo al propósito de la organización. Con este objeto se busca la implicación de todo el personal de esta en la aplicación de las medidas que se determinen.

Torrecid manifiesta expresamente su compromiso de potenciar la Seguridad y Ciberseguridad de la Información del servicio prestado, y se compromete a satisfacer las necesidades y expectativas de las partes interesadas, según el marco legal y regulatorio en el que se desarrollan las actividades. Además, es plenamente consciente de la relevancia que tiene la seguridad de la información que gestiona, así como de la necesidad de garantizar la **confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad** de sus sistemas de información. Estos principios constituyen un elemento esencial e inseparable del trabajo diario y una parte fundamental de la calidad, eficacia y fiabilidad del servicio que la empresa ofrece a sus clientes, dentro de los más altos estándares de excelencia tecnológica y productiva.

En este sentido:

- La **gestión de la seguridad de la información** deberá desarrollarse conforme a los requisitos establecidos por el **Sistema de Gestión de Seguridad de la Información (SGSI)** y, cuando aplique, por el **Esquema Nacional de Seguridad (ENS)**,) y en particular con la **Directiva 2022/2555 (NIS2)** del Parlamento Europeo y del Consejo, cumpliendo en todo momento con la normativa legal vigente y las buenas prácticas reconocidas a nivel nacional e internacional.
- La **información** es un **activo estratégico** para **Torrecid** y, por tanto, se debe garantizar su protección adecuada tanto en el desempeño de las actividades diarias como en las relaciones con **clientes, proveedores, colaboradores y otras partes interesadas**, asegurando el tratamiento seguro de todos los datos técnicos, comerciales y confidenciales que se manejen.
- La **seguridad y ciberseguridad de la información** son responsabilidades que competen a todo el personal de Torrecid, tanto de forma individual como mediante la cooperación entre los distintos departamentos, áreas y unidades de negocio. La empresa promueve una cultura organizativa basada en la **sensibilización, responsabilidad y compromiso** de todos los empleados en materia de seguridad de la información.
- La **normativa interna de seguridad** y los procedimientos derivados del SGSI y del ENS serán **difundidos, comprendidos y asumidos** por todo el personal de Torrecid, siendo de **obligado cumplimiento** en todos los niveles jerárquicos y funcionales.

- Se deberán **identificar, evaluar y gestionar los riesgos y oportunidades** relacionados con la seguridad de la información, con el fin de garantizar que el sistema alcance los resultados previstos, prevenir o mitigar los efectos no deseados y fomentar la **mejora continua**.
Se adoptarán medidas de protección proporcionales al **valor de los activos de información**, al **nivel de riesgo existente** y al **impacto potencial** de las amenazas, incluyendo aquellas derivadas del tratamiento de **datos personales**, de acuerdo con la LOPDGDD, el RGPD y la **normativa interna de Torrecid**.
- Torrecid se compromete a **preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad** de la información durante todo su ciclo de vida, independientemente del medio en que se encuentre o del lugar en que sea tratada, garantizando su protección tanto en formato físico como digital.
- La empresa mantiene un firme **compromiso de mejora continua** del proceso y del sistema de gestión de la seguridad de la información.

2. Ámbito de aplicación. Alcance

La presente política aplica a todas **las áreas, empleados, sistemas, procesos y ubicaciones** de Torrecid. Asimismo, se extiende a las relaciones con colaboradores, contratistas y demás partes interesadas con las que la empresa mantiene vínculos laborales o profesionales, siempre dentro del marco de la legislación vigente y los valores corporativos de la Compañía.

3. Objetivos generales

Torrecid establece una **estrategia de análisis y gestión de riesgos y oportunidades** orientada a la comprensión exhaustiva de las amenazas que pueden afectar a la seguridad de la información y a la definición de las **salvaguardas** necesarias para su correcta protección. Esta estrategia se integra en los procesos de gestión y en la toma de decisiones, contribuyendo a la mejora continua de la seguridad, la eficiencia operativa y la confianza de nuestros **clientes, proveedores, colaboradores y otras partes interesadas**.

En el marco de esta estrategia, la Dirección de **Torrecid** define los siguientes compromisos u **objetivos** generales:

- **Establecer las necesidades básicas de protección** de la información y desarrollar los **planes de seguridad** que permitan aplicar las salvaguardas adecuadas para mitigar los riesgos identificados y aprovechar las oportunidades de mejora detectadas en el entorno tecnológico y organizativo.
- **Organizar la seguridad de la información** en base a criterios claros de clasificación, propiedad y responsabilidad, asignando a cada propietario de la información la obligación de su protección. Se definirán y mantendrán actualizados los procedimientos y tareas de seguridad, los protocolos de actuación ante incidentes o violaciones de seguridad, así como las medidas disciplinarias aplicables en caso de incumplimiento de las normas internas. Asimismo, se llevarán a cabo verificaciones periódicas de conformidad en materia de seguridad y se aplicarán mecanismos de gestión de la configuración y control de cambios, asegurando la coherencia, trazabilidad y actualización continua del sistema.
- **Fomentar la mejora continua** de los servicios y del soporte técnico prestado, integrando la **seguridad y ciberseguridad** de la información como **elemento inherente y transversal** en todos los procesos de la organización. La seguridad no se concibe como un requisito adicional, sino como un **pilar esencial del servicio**, orientado a garantizar la calidad, eficacia y fiabilidad de las operaciones.
- **Reforzar el posicionamiento de Torrecid** como empresa de referencia en el sector cerámico, reconocida por su compromiso con la innovación, la protección de la información y la excelencia en sus

servicios, dentro de un marco de gestión seguro y conforme a los más altos estándares nacionales e internacionales.

- **Proporcionar soluciones seguras y eficientes** que permitan a nuestros **clientes** transformar los datos y la información en conocimiento útil, facilitando la toma de decisiones estratégicas y la optimización de sus procesos productivos.
- **Asegurar la disponibilidad de un equipo humano altamente cualificado y especializado**, capaz de ofrecer una atención técnica inmediata, eficaz y coordinada, garantizando la continuidad del servicio y la protección de la información en todas las circunstancias.
- **Mantener una prestación del servicio basada en la mejora continua** de los sistemas de gestión, integrando la **seguridad y ciberseguridad de la información** como componentes fundamentales y por defecto en todas las fases del ciclo operativo. La gestión de riesgos y oportunidades se revisará de forma periódica, promoviendo la adaptación constante a los cambios tecnológicos, normativos y del entorno empresarial.

4. Principios que rigen esta política

Torrecid adopta como principios fundamentales de la seguridad de la información los siguientes:

1. **Confidencialidad:** garantizar que la información solo sea accesible por personal y terceros autorizados.
2. **Integridad:** asegurar que la información y los sistemas se mantengan completos, exactos y sin alteraciones no autorizadas.
3. **Disponibilidad:** garantizar el acceso a la información y a los sistemas por parte de usuarios autorizados cuando sea necesario.
4. **Autenticidad y trazabilidad:** verificar la identidad y la responsabilidad de quienes acceden o modifican la información.
5. **Cumplimiento normativo:** cumplir con todas las leyes, reglamentos y obligaciones contractuales aplicables.
6. **Protección de terceros:** proteger con el mismo rigor la información de clientes, proveedores, colaboradores y partes interesadas.

5. Requisitos mínimos

Torrecid estructura e implanta su **proceso de seguridad de la información** mediante un conjunto coordinado de medidas organizativas, técnicas y humanas orientadas a garantizar la protección eficaz de los activos de información y la continuidad del negocio. Para la consecución de lo anterior y de la estrategia se establecen los siguientes requisitos mínimos:

- Control de accesos físicos y lógicos a las instalaciones y sistemas.
- Copias de seguridad y planes de continuidad y recuperación ante desastres.
- Clasificación y tratamiento seguro de la información.
- Cifrado y protección de la información sensible.
- Eliminación segura de documentos y soportes.
- Protección de redes y sistemas frente a amenazas cibernéticas.
- Evaluación y control periódico de proveedores críticos.
- Cumplimiento estricto del RGPD, LOPDGDD y demás normativa aplicable.

6. Protección de la información de terceros

Torrecid reconoce su responsabilidad en la protección de la información que le confían sus clientes, proveedores, colaboradores y otras partes interesadas, adoptando las siguientes medidas:

- Formalización de acuerdos de confidencialidad (NDA) antes de intercambiar información sensible.
- Limitación del acceso a datos de terceros al personal estrictamente necesario.
- Aplicación de protocolos de cifrado, control de acceso, almacenamiento seguro y eliminación controlada.
- Supervisión y evaluación de las medidas de seguridad implantadas por los proveedores.
- Notificación diligente de incidentes que afecten a la información de terceros, conforme a la normativa vigente.

7. Formación, concienciación y cultura de seguridad

Torrecid fomentará la **formación continua y la concienciación** del personal sobre la importancia de la seguridad y la protección de la información. Se impartirán programas específicos sobre protección de datos, buenas prácticas digitales, respuesta ante incidentes y confidencialidad, tanto para empleados como para terceros con acceso a información de la empresa.

8. Revisión, auditoría y mejora continua

La presente política será revisada **al menos una vez al año** o cuando se produzcan cambios significativos en el entorno tecnológico, normativo u organizativo. Las auditorías y revisiones de dirección permitirán verificar la eficacia del SGSI y establecer acciones de mejora.

La gestión de riesgos y oportunidades se actualizará también **anualmente**, asegurando la adaptación del sistema a los nuevos retos de seguridad y a la evolución del negocio.

9. Estructura de gestión del SGSI / Responsabilidades

Se establecen las siguientes estructuras de gestión de la seguridad de la información:

- **Comité de Seguridad de la Información (CSI):** con el objetivo de coordinar y supervisar todas las actividades relacionadas con la seguridad de la información. Dentro del Comité se establecen los siguientes roles, con un delegado en cada caso:
 - **Responsable del Servicio:** Establece los requisitos de seguridad aplicables a los servicios.
 - **Responsable de la Información:** establecer los requisitos de seguridad aplicables a la información.
 - **Responsable de Seguridad de la Información:** Dirige y coordina las reuniones del Comité de Seguridad y Supervisa la aplicación de la estrategia de seguridad.
 - **Responsable de Sistemas:** Garantiza la correcta aplicación de medidas de seguridad.
- **Comité de Crisis:** con el objetivo de coordinar y supervisar todas las actividades relacionadas con la gestión de crisis y la continuidad de negocio. Se encuentra constituido por los mismos miembros que el Comité de Seguridad de la Información.

Dentro del Sistema de Gestión de Seguridad de la Información se incluyen y definen los siguientes documentos y procedimiento internos:

- 01 Política de seguridad
- 02 Gestión de riesgos
- 03 Gestión de incidentes
- 04 Continuidad de negocio
- 05 Cadena de suministro
- 06 Seguridad en adquisición, desarrollo y mantenimiento
- 07 Seguimiento
- 08 Formación y competencia
- 09 Seguridad RRHH
- 10 Control de accesos
- 11 Gestión de activos
- 12 Criptografía

10. Aprobación, comunicación y entrada en vigor

Esta Política de Gestión de la Seguridad de la Información, la composición y creación de los Comités de Seguridad y Crisis, así como todos los procedimientos internos asociados al Sistema de Gestión de Seguridad de la Información de TORRECID, S.A. han sido aprobados por la Dirección General de Torrecid, S.A. en fecha 03 de diciembre de 2025, y son de obligado cumplimiento para todo el personal y terceros relacionados con la organización. Será comunicada y difundida internamente, así como puesta a disposición de clientes, proveedores, colaboradores y partes interesadas que lo requieran.