Política de Seguridad de la Información CHEMIK - Web

CHEMIK HI TECH, S.L. — CHEMIK GROUP

Versión resumida

Este documento resume la Política de Seguridad de la Información de CHEMIK HI TECH, S.L. (POLI_PoliticaSeguridadInformacion_Privada_CHEMIK, aprobada y firmada por la Dirección el 3/11/2026). La política completa está a disposición de clientes, autoridades y demás partes interesadas que la soliciten en ciberseguridad@chemik.es.

1. NUESTRO COMPROMISO

CHEMIK HI TECH, del grupo CHEMIK, diseña proyectos llave en mano de salas eléctricas prefabricadas y gestiona su fabricación e integración. La seguridad de la información forma parte de ese compromiso de calidad.

La Dirección considera la información y los servicios que presta a sus clientes como activos esenciales y se compromete a protegerlos frente a cualquier amenaza, interna o externa, deliberada o accidental, que afecte a su **confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad**.

Para ello ha implantado un **Sistema de Gestión de Seguridad de la Información** conforme a la norma **ISO/IEC 27001:2022** y al **Esquema Nacional de Seguridad** (Real Decreto 311/2022).

La Dirección se compromete a **cumplir los requisitos aplicables** relacionados con la seguridad de la información (legales, contractuales y de sus clientes) y a la **mejora continua** del Sistema de Gestión.

2. ALCANCE

Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad de CHEMIK HI TECH, S.L. que da soporte al diseño de proyectos llave en mano de salas eléctricas prefabricadas y a la gestión del proceso de fabricación e integración de salas eléctricas prefabricadas, desde sus emplazamientos de Tarazona y Zaragoza.

3. NUESTROS OBJETIVOS

a) Ofrecer a nuestros clientes las garantías de seguridad que exigen, mediante las certificaciones ISO/IEC 27001 y del Esquema Nacional de Seguridad.
b) Proteger el conocimiento técnico que hace competitiva a la empresa: diseños, cálculos y métodos de fabricación.
c) Asegurar la continuidad de los servicios que prestamos a nuestros clientes.
d) Mantener el riesgo dentro del nivel que la Dirección acepta, decidiendo con datos dónde invertir.

4. PRINCIPIOS

a) **Gestión basada en los riesgos:** analizamos periódicamente los riesgos que afectan a la información y aplicamos medidas proporcionadas a ellos.
b) **Cumplimiento:** cumplimos la legislación aplicable —en particular la de protección de datos personales y ciberseguridad—, los requisitos contractuales de nuestros clientes y los compromisos que adquirimos. Mantenemos identificada la legislación que nos aplica y evaluamos su cumplimiento una vez al año.
c) **Seguridad integral:** la seguridad afecta a las personas, los procesos, la tecnología y las instalaciones, y es responsabilidad de todos.
d) **Mínimo privilegio y control de accesos:** cada persona accede solo a la información que necesita para su trabajo.
e) **Prevención, detección y respuesta:** protegemos nuestros sistemas, vigilamos su funcionamiento y respondemos con rapidez ante los incidentes.
f) **Continuidad:** preparamos los medios para mantener los servicios ante interrupciones graves.
g) **Proveedores y terceros:** exigimos a quienes nos prestan servicios un nivel de seguridad acorde con esta política.
h) **Formación y concienciación:** todo el personal conoce sus obligaciones de seguridad y recibe formación adecuada a su función.
i) **Mejora continua:** revisamos el sistema de gestión, fijamos objetivos medibles y los evaluamos para mejorar de forma continua.

5. ORGANIZACIÓN

La **Dirección** aprueba esta política, asigna las responsabilidades de seguridad y revisa el sistema de gestión al menos una vez al año. La seguridad de la información está gobernada por un **Comité de Seguridad** , que fija los objetivos, aprueba las normas y supervisa su cumplimiento, y por un **Responsable de la Seguridad** , que coordina su aplicación. Esta política

se desarrolla en un cuerpo normativo de obligado cumplimiento para todo el personal y para los terceros que trabajan con nosotros.

6. REVISIÓN

Esta política se revisa al menos una vez al año y siempre que haya cambios relevantes en la organización, en sus servicios o en el marco legal.

7. CONTACTO

Para comunicar un incidente o hacer una consulta sobre seguridad de la información: **ciberseguridad@chemik.es** .

Aprobada por la Dirección de CHEMIK HI TECH, S.L. el 3/11/2026.