

## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Dirección de TAJAMAR en su compromiso para la implantación de un Sistema Integrado de Gestión de la Calidad, Medioambiente y Seguridad de la Información según las Normas UNE-EN ISO 9001, 14001 e ISO 27001 establece como fundamental, definir una Política Integrada que sea adecuada a sus intenciones, horizontes empresariales y estructuras, de acuerdo con el alcance especificado.

Para ello, **TAJAMAR** establece los siguientes compromisos:

### En **general**:

- Mejora continua del desempeño tanto de los sistemas de gestión como del resultado a obtener. Mejora de la eficacia de los sistemas.
- Actualización y cumplimiento del marco legal y de los requisitos propios y específicos que nos puedan poner tanto nuestros clientes como los proveedores y personas implicadas.
- Mantener un alto nivel de cualificación y talento para poder ser eficaces y eficientes en los procesos.
- Mantenimiento de los adecuados canales de comunicación con todas las partes interesadas, con objeto de asegurar su satisfacción con respecto al cumplimiento de sus necesidades, requisitos y expectativas.
- Se adoptarán las medidas necesarias para que todo el personal de TAJAMAR sea conocedor de esta política. Difundiéndose también ésta a los proveedores y colaboradores, estando además a disposición del público a través de la página web.

### En **seguridad de la información**:

- Política de Disminución del riesgo potencial grave. Se priorizarán las actuaciones sobre riesgos potenciales graves.
- Política de Tolerancia 0 con las incidencias. Se investigará y sancionará aquellas actuaciones dolosas o imprudentes.
- Política de impacto reputacional mínimo. La incidencia reputacional en materia de seguridad debe tender a 0.
- Controlar operativamente de forma eficaz las amenazas y riesgos sobre el activo y las instalaciones.
- Gestionar eficientemente las incidencias que afecten a la integridad, disponibilidad y confidencialidad de la información de la empresa.
- Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación vigente en materia de seguridad de la Información.
- Implantar planes de continuidad del negocio que garanticen la permanencia de las actividades de la sociedad en caso de incidencias graves o contingencias.

En Madrid, a 26 de mayo de 2026

Firmado: La Dirección