

POLÍTICA DE CIBERSEGURIDAD



Principios generales

La Política de ciberseguridad del Grupo Talgo (en adelante Talgo) establece los principios básicos y los marcos generales de control relativos a la seguridad de la información, la gestión de riesgos y la resiliencia frente a ciberincidentes que puedan afectar a la organización o su relación con las diferentes partes interesadas de la misma.

La Política de ciberseguridad de Talgo vela por todos los procesos de negocio, productos y servicios suministrados, siendo de aplicación en todas las fases del ciclo de vida de la información y activos que la gestionan.

Objetivo y ámbito de aplicación

Esta política es de obligado cumplimiento para todas las personas que trabajan en Talgo, y colaboradores, con acceso a la información o activos que la gestionan.

La Dirección de Talgo se compromete a dar soporte a la gestión de la ciberseguridad mediante el establecimiento de directrices para cumplir con los principios básicos de:

- ▶ Definir un marco para la difusión y cumplimiento de los objetivos de ciberseguridad, implementando un proceso de mejora continua que permita la adaptación y optimización constante de los objetivos de ciberseguridad
- ▶ Implantar los controles pertinentes para supervisar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, así como su tratamiento en las operaciones, comunicaciones y ubicaciones físicas y lógicas de almacenamiento.
- ▶ Cumplir con los requerimientos legales, reglamentarios o contractuales relacionados con la ciberseguridad y que sean aplicables a Talgo de forma directa, indirecta o a través de compromisos contractuales como suministrador de productos o servicios.
- ▶ Promulgar la adecuada responsabilidad y diligencia en la valoración y gestión de los riesgos identificados en materia de ciberseguridad.
- ▶ Garantizar que los activos, la información y los sistemas de Talgo que la soportan, tengan los niveles de seguridad y resiliencia adecuados a su nivel de criticidad, basado en la valoración de las partes interesadas.
- ▶ Impulsar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a ciberincidentes y nuevas amenazas.
- ▶ Establecer requisitos de ciberseguridad adecuados sobre las relaciones contractuales con proveedores y colaboradores, que regulen los criterios y medidas para el intercambio y compartición de información.
- ▶ Sensibilizar y concienciar a la plantilla y colaboradores de Talgo sobre los riesgos relativos a la ciberseguridad y su impacto en los procesos y actividades operativas de la organización de una forma apropiada, entendible y accesible.
- ▶ Proporcionar los recursos materiales, económicos y humanos necesarios para cumplir con los objetivos y tareas relacionadas con la ciberseguridad, permitiendo reducir los niveles de riesgo globales y específicos del ámbito sectorial.
- ▶ Ampliar las capacidades de ciberseguridad al producto y servicios comercializados por Talgo, en línea con las obligaciones contractuales y legales aplicables en cada caso.

Carlos Palacio Oriol
Presidente