Política de Seguridad de la Información

La presente Política establece los principios y compromisos de SISTEL CONTROL, S.L. (en adelante, SISTEL) en relación con la protección y gestión segura de la información, en cumplimiento de la norma ISO 27001.

ALCANCE

La Política de Seguridad de la Información es de aplicación a todos los empleados, colaboradores, equipos, aplicaciones y procesos en los que se realice tratamiento de información, así como a cualquier parte interesada interna o externa que interactúe con los activos de información gestionados por SISTEL.

COMPROMISOS

SISTEL asume la seguridad de la información asociada a sus servicios como uno de los factores clave en la realización de sus actividades con objeto de garantizar la confidencialidad, integridad y disponibilidad de la información, protegiendo los datos y los sistemas de información contra accesos indebidos y modificaciones no autorizadas.

Forma parte de la Política Estratégica de SISTEL la implantación y el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma ISO 27001, mediante el análisis, la prevención y la mejora continua. La Dirección proporciona los recursos necesarios y apoya activamente el cumplimiento de los objetivos y acciones del SGSI, fomentando una cultura organizacional orientada a la seguridad.

La Política de Seguridad de la Información, se basa en los siguientes pilares.

1. Fomentar una cultura preventiva: gestión proactiva de riesgos y oportunidades, priorizando la prevención de errores en lugar de su corrección reactiva.
2. La participación de todos es clave para conseguir los objetivos establecidos por SISTEL lo que redundará en el bien de nuestros clientes.
3. La formación continua, sensibilización y capacitación del personal y colaboradores es un pilar básico.
4. Asegurar que la empresa cumple con los requisitos de los clientes además de con los requisitos legales y reglamentarios aplicables, haciendo especial foco en aquellos establecidos por la legislación en materia de seguridad de la información.
5. Establecer acciones sistemáticas de identificación, análisis, evaluación, tratamiento y seguimiento de los riesgos e incidentes de seguridad.
6. Garantizar la confidencialidad, integridad y disponibilidad de la información en todo su ciclo de vida, protegiendo los datos y los sistemas de información contra accesos indebidos y modificaciones no autorizadas.
7. Garantizar la continuidad del negocio, en cuanto a seguridad de la información se refiere, protegiendo los procesos críticos contra fallos o desastres significativos.

La Dirección de SISTEL entiende que los procesos asociados a la seguridad de la información no pueden imponerse desde fuera, sino que deben nacer desde el interior del equipo humano que forma la empresa, y anima a todas las personas de la misma a hacer de la seguridad de la información su forma de trabajo. La Dirección se compromete a mejorar continuamente el Sistema de Gestión de Seguridad de la Información implantado, en las revisiones periódicas que mantiene anualmente y mediante el establecimiento de objetivos y acciones de mejora.

La política entrará en vigor desde la fecha de aprobación del documento por la Dirección.

Nombre, firma y fecha:

Firmado digitalmente por JAIME ISERN

Fecha: 2025.05.29 18:22:53 +02'00'

Mayo 2025