CIF: A58147901 · VAT: ES-A58147901
c/Bailén 71 bis, 5º 2ª
08009 Barcelona · Spain
Tel. +34 93 424 92 72

POLITICA DE CIBERSEGURIDAD

SACOEL, S.A. (en adelante Sacoel) considera que la información, sistemas y hardware asociados son activos críticos que deben ser protegidos para asegurar el funcionamiento de la actividad empresarial y confidencialidad de los datos.

La Política de Ciberseguridad está orientada a gestionar de manera eficaz la seguridad de la información tratada por los sistemas informáticos de la empresa, así como los activos que participan en sus procesos.

Esta Política tiene por objeto garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información y cumplir en todo momento con las Leyes y reglamentos vigentes, manteniendo un equilibrio con proporcionalidad entre los niveles de riesgo y el uso eficiente de los recursos disponibles.

Los principios básicos descritos en esta Política de Ciberseguridad garantizan que los sistemas de información y telecomunicaciones disponibles disponen de un nivel suficiente de seguridad y resiliencia.

Se ha llevado a cabo una sensibilización de todos los empleados y colaboradores acerca de los riesgos de Ciberseguridad y se garantiza que disponen de los conocimientos y capacidades tecnológicas para el cumplimiento de los objetivos de Ciberseguridad de la empresa, potenciando a su vez la capacidad de prevención, detección, reacción, análisis recuperación, respuesta y coordinación frente a nuevas amenazas. Para ello disponen de herramientas que permiten adaptarse con agilidad a los cambios del entorno tecnológico.

El modelo adoptado por Sacoel se basa en:

- Disponer de un marco de gestión de Ciberseguridad alineado con la estrategia y objetivo del negocio, coherente con el contexto de la empresa.
- Crear mecanismos reales para establecer objetivos medibles referentes a la Ciberseguridad, de conformidad con los requisitos legislativos y contractuales.
- Disponer de mecanismos para reaccionar frente a los incidentes que se produzcan en la gestión del sistema y procedimientos operativos dependientes del mismo.
- La existencia de un conjunto de funciones y responsabilidades en materia de Ciberseguridad claramente definidos en el organigrama corporativo.
- Un proceso de revisión y actualización continua del modelo de gestión de la Ciberseguridad que permita adecuarlo en todo momento a las amenazas que surjan.