# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

POSADAS, POSADAS & VECINO
POSADAS
DESDE 1926

## INTRODUCCIÓN

En Posadas, nos comprometemos a proteger la información de nuestra empresa, clientes y proveedores, garantizando la confidencialidad, integridad y disponibilidad de los datos con los que interactuamos. Como parte de nuestra certificación ISO 27001:2022 en el área de Tecnologías de la Información, hemos implementado un Sistema de Gestión de Seguridad de la Información (SGSI) que nos permite mantener altos estándares de seguridad en todas nuestras operaciones.

## ALCANCE

Esta política aplica a todos los empleados, colaboradores externos, clientes y proveedores que interactúen con nuestra infraestructura tecnológica y/o información, ya sea de manera directa o indirecta.

## COMPROMISO DE PROVEEDORES Y CLIENTES

Para fortalecer nuestra postura de seguridad, esperamos que nuestros clientes y proveedores:

- Respeten y apliquen principios de seguridad alineados con nuestra política.
- Protejan la información confidencial compartida, evitando su divulgación no autorizada.
- Cumplan con la normativa vigente en materia de seguridad de la información y protección de datos.
- Informen de inmediato cualquier incidente de seguridad.
- Apliquen controles de seguridad adecuados en la gestión de su infraestructura y operaciones, minimizando riesgos.

## DESARROLLO

Como base del desarrollo de la política de seguridad Posadas se basa en los siguientes objetivos:

- Establecer objetivos anuales con relación a la Seguridad de la Información.
- Desarrollar un proceso de evaluación y tratamiento de riesgos de seguridad, e implementar las acciones correctivas y preventivas adecuadas de acuerdo a su resultado.
- Contar con una política de gestión de incidentes de seguridad de la información.
- Garantizar la continuidad de las operaciones, desarrollando planes de continuidad de acuerdo con las mejores prácticas del mercado.
- Clasificar y proteger la información de acuerdo con la normativa vigente.
- Cumplir con los requisitos del servicio, legales o reglamentarios y las obligaciones contractuales de seguridad.
- Promover una cultura organizacional orientada a la seguridad de la información.
- Brindar concientización y formación en materia de seguridad de la información a todo el personal.
- La ciberseguridad como concepto amplio de protección, será implementada como un proceso continuo y permanente dentro de la organización. La misma abarca la protección de las operaciones de la organización en todas sus funciones.