



Versión 1.0

POLÍTICA PÚBLICA DE SEGURIDAD DE LA INFORMACIÓN DEL GRUPO SAMPOL

1 de Septiembre de 2026.

Compromiso de la Dirección

La Dirección de SAMPOL manifiesta su compromiso con la protección de la información, los sistemas tecnológicos y los servicios gestionados por la organización, considerándolos elementos esenciales para el desarrollo de sus actividades y para la confianza de clientes, empleados, proveedores, socios y organismos públicos.

La seguridad de la información constituye un elemento estratégico en la prestación de nuestros servicios energéticos y tecnológicos, garantizando que la información se gestione de forma segura durante todo su ciclo de vida.

Objeto

La presente Política establece los principios generales que rigen la gestión de la seguridad de la información en SAMPOL.

Su finalidad es garantizar la protección adecuada de la información y de los sistemas que la soportan, preservando:

- La confidencialidad.
- La integridad.
- La disponibilidad.
- La autenticidad.
- La trazabilidad.

Alcance

Esta Política resulta de aplicación a las actividades, procesos, sistemas de información, servicios tecnológicos y recursos gestionados por SAMPOL, así como a todas las personas y entidades que participen en su operación, mantenimiento o utilización.

Principios de Seguridad

SAMPOL basa su modelo de gestión de seguridad en los siguientes principios:

- **Gestión del riesgo**

Las decisiones relativas a seguridad se fundamentan en el análisis y tratamiento continuo de riesgos, permitiendo identificar amenazas, vulnerabilidades e impactos potenciales sobre los servicios y la información.

- **Seguridad integrada**

La seguridad se incorpora desde el diseño y durante todo el ciclo de vida de los sistemas, procesos y servicios.

- **Prevención, detección, respuesta y recuperación**

La organización mantiene capacidades destinadas a prevenir incidentes, detectar eventos de seguridad, responder de forma eficaz y recuperar los servicios afectados dentro de tiempos aceptables.

- **Cumplimiento normativo**

SAMPOL desarrolla sus actividades de acuerdo con la legislación aplicable y con los requisitos contractuales asumidos con clientes y organismos públicos.

- **Mejora continua**

La eficacia de los controles de seguridad se revisa periódicamente mediante auditorías, revisiones de gestión, análisis de riesgos y seguimiento de indicadores.

Marco de Referencia

La gestión de la seguridad de la información en SAMPOL se desarrolla conforme a estándares y marcos reconocidos, entre los que destacan:

- Esquema Nacional de Seguridad (ENS).
- ISO/IEC 27001.
- Reglamento General de Protección de Datos (RGPD).
- Ley Orgánica 3/2018.
- Normativa nacional y europea aplicable en materia de ciberseguridad y protección de la información.

Gestión de Incidentes y Continuidad

SAMPOL dispone de mecanismos organizativos y técnicos destinados a la gestión de incidentes de seguridad y a la continuidad de los servicios esenciales para el negocio.

La organización mantiene procedimientos específicos para la detección, análisis, comunicación, escalado y resolución de incidentes, así como planes de continuidad y recuperación ante situaciones que puedan afectar a la disponibilidad de los servicios.

Seguridad de Terceros

Los proveedores, colaboradores y socios que accedan a información o sistemas gestionados por SAMPOL deben cumplir los requisitos de seguridad establecidos por la organización y por la normativa aplicable.

Cuando resulte necesario, dichos requisitos serán incorporados a los acuerdos contractuales correspondientes.

Formación y Concienciación

SAMPOL promueve una cultura de seguridad mediante actividades de formación y concienciación dirigidas a sus profesionales, con el objetivo de fortalecer la protección de la información y reducir los riesgos asociados a errores humanos o amenazas emergentes.

Revisión de la Política

La presente Política será revisada periódicamente o cuando se produzcan cambios relevantes en el contexto normativo, tecnológico, organizativo o de riesgos, con el fin de garantizar su adecuación y vigencia.

Información de Contacto

Para cuestiones relacionadas con la seguridad de la información o la notificación de incidentes, puede contactarse con:

ciberseguridad@sampol.com

o a través de los canales corporativos publicados por SAMPOL.

Terceras partes

SAMPOL exige que los proveedores, colaboradores y terceros que accedan a información o sistemas gestionados por la organización cumplan los requisitos de seguridad aplicables, así como las obligaciones legales, regulatorias y contractuales que resulten de aplicación.

La organización establece mecanismos de coordinación y comunicación con terceros para garantizar la protección de la información compartida, la gestión adecuada de los riesgos y la respuesta eficaz ante incidentes de seguridad.

Asimismo, SAMPOL promueve que el personal de terceros que participe en la prestación de servicios disponga del nivel de concienciación y capacitación en seguridad adecuado a las funciones desarrolladas.

Cualquier excepción a los requisitos de seguridad establecidos será evaluada y gestionada mediante los procedimientos internos de gestión de riesgos de la organización.



Camí del Reis, 308. 1ª Planta. Edificio Mapfre
07011 Palma de Mallorca. Islas Baleares
+34 971 76 44 76
www.sampol.com