

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

PROMAN PERSONAS ETT, consciente de la importancia estratégica de la información, los sistemas tecnológicos y los servicios digitales en la prestación de sus servicios de trabajo temporal, establece esta Política de Seguridad de la Información y Ciberseguridad en conformidad con la norma ISO/IEC 27001.

La presente política tiene como finalidad proteger los activos de información de la organización frente a amenazas internas o externas, deliberadas o accidentales, así como prevenir, detectar, responder y recuperarse frente a amenazas cibernéticas que puedan afectar a la confidencialidad, integridad y disponibilidad de la información, los sistemas, redes, aplicaciones, dispositivos y servicios de **PROMAN PERSONAS ETT**.

La Dirección asume el compromiso de desarrollar, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información eficaz, basado en la gestión de riesgos, la mejora continua, la ciberseguridad, la protección de datos personales y el cumplimiento de los requisitos legales, reglamentarios, contractuales y de las partes interesadas aplicables.

Para ello, **PROMAN PERSONAS ETT** se compromete a:

- Proteger la información y los activos asociados frente a accesos no autorizados, pérdidas, modificaciones, divulgaciones, destrucciones, usos indebidos o interrupciones no planificadas.
- Preservar la confidencialidad, integridad y disponibilidad de la información en todos los procesos, sistemas, aplicaciones, redes, soportes, equipos y servicios utilizados por la organización.
- Cumplir la legislación vigente, en particular la normativa sobre protección de datos personales, LOPDGDD y RGPD, propiedad intelectual, seguridad informática, confidencialidad y cualquier otro requisito legal, reglamentario o contractual aplicable.
- Identificar, analizar, evaluar y tratar los riesgos de seguridad de la información y ciberseguridad, aplicando controles adecuados para reducirlos a niveles aceptables y revisándolos periódicamente.
- Proteger los sistemas, redes, aplicaciones, dispositivos y servicios digitales frente a amenazas como malware, ransomware, phishing, accesos no autorizados, explotación de vulnerabilidades, pérdida de información, interrupciones de servicio, errores humanos o uso indebido de los recursos tecnológicos.
- Mantener medidas de seguridad relacionadas con la actualización de software y hardware, protección antimalware, gestión de accesos, uso de contraseñas seguras, autenticación, copias de seguridad, continuidad tecnológica, gestión de vulnerabilidades, cifrado, uso seguro del correo electrónico e internet, dispositivos móviles, teletrabajo y desarrollo seguro de software.
- Garantizar la disponibilidad y continuidad de los servicios críticos, estableciendo planes de contingencia, copias de seguridad, medidas de recuperación y procedimientos de actuación ante incidentes de seguridad de la información o ciberseguridad.

- Establecer responsabilidades y autoridades claras en materia de seguridad de la información y ciberseguridad, incluyendo la Dirección, el Comité de Seguridad, el Responsable del SGSI, el Departamento de IT, el DPO o responsable de protección de datos, los responsables de proceso y todo el personal de la organización.
- Concienciar, formar y responsabilizar al personal sobre la importancia de la seguridad de la información, la ciberseguridad, la confidencialidad, la protección de datos personales, el uso adecuado de los sistemas tecnológicos y la comunicación de incidentes o sospechas de seguridad.
- Aplicar controles técnicos, organizativos y físicos adecuados para proteger la información durante su creación, almacenamiento, tratamiento, transmisión, conservación, eliminación o destrucción.
- Gestionar de forma segura las relaciones con proveedores, especialmente aquellos que puedan acceder a información, sistemas, servicios tecnológicos, servicios en la nube o datos personales de PROMAN PERSONAS ETT, estableciendo requisitos de seguridad, confidencialidad y protección de datos cuando corresponda.
- Promover la detección temprana, comunicación, análisis, tratamiento y aprendizaje de los incidentes de seguridad de la información y ciberseguridad, incluyendo la conservación de evidencias cuando sea necesario.
- Fomentar la mejora continua del SGSI y de la ciberseguridad mediante auditorías internas, revisiones por la dirección, seguimiento de indicadores, análisis de incidentes, evaluación de amenazas, revisión de riesgos y aplicación de acciones correctivas y oportunidades de mejora.
- Mantener una comunicación adecuada con clientes, proveedores, autoridades competentes y otras partes interesadas relevantes en relación con la seguridad de la información, la protección de datos y la ciberseguridad.

Esta política se aplica a todo el personal, sistemas, procesos, instalaciones, redes, aplicaciones, dispositivos, proveedores y activos de información incluidos en el alcance del Sistema de Gestión de Seguridad de la Información de PROMAN PERSONAS ETT.

La política será comunicada al personal y puesta a disposición de las partes interesadas pertinentes cuando sea necesario. Asimismo, será revisada periódicamente y siempre que se produzcan cambios significativos que puedan afectar a su adecuación, vigencia o eficacia.

CEO
PROMAN PERSONAS ETT
Enero 2026
Versión 2.