analizA
Sociedad de Diagnóstico

Política de Seguridad de la Información

Aprobación y Vigencia

La presente Política de Seguridad de la Información se encuentra alineada con el Sistema de Gestión de Seguridad de la Información (SGSI) de Analiza Sociedad de Diagnóstico S.L. (en adelante, Analiza), conforme al Esquema Nacional de Seguridad (ENS) en nivel ALTO y a la norma ISO/IEC 27001:2022.

Será revisada y actualizada periódicamente para garantizar su adecuación al contexto organizativo, tecnológico y normativo.

Misión

En Analiza reconocemos la importancia crítica de las Tecnologías de la Información y las Comunicaciones (TIC) para el cumplimiento de nuestros objetivos estratégicos y operativos.

Nos comprometemos a proteger la información utilizada en nuestras actividades, garantizando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, así como la continuidad de los servicios prestados.

La seguridad de la información constituye un elemento esencial para garantizar la calidad asistencial y la confianza de nuestros pacientes, clientes y colaboradores.

Alcance

Esta política es de aplicación a todos los sistemas de información, servicios, procesos y activos gestionados por Analiza, así como a todo el personal, colaboradores y terceros que participen en el tratamiento de la información.

Objetivos

• Garantizar la protección de la información frente a amenazas internas y externas.
• Asegurar la continuidad de los servicios y la resiliencia operativa.
• Prevenir, detectar y responder a incidentes de seguridad.
• Cumplir con los requisitos legales, regulatorios y contractuales aplicables.
• Promover una cultura de seguridad de la información en toda la organización.

Marco Normativo

Analiza cumple con los requisitos legales aplicables y los compromisos adquiridos con clientes y partes interesadas, incluyendo, entre otros:

- Esquema Nacional de Seguridad (ENS)
- ISO/IEC 27001:2022
- Reglamento General de Protección de Datos (RGPD)
- Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)

Organización de la Seguridad

La responsabilidad de la seguridad de la información recae en la Dirección, que establece la estrategia, asigna recursos y supervisa su cumplimiento.

Se definen roles y responsabilidades específicas en materia de seguridad de la información, garantizando la adecuada segregación de funciones y la coordinación entre las distintas áreas.

Comité de Seguridad de la Información

El Comité de Seguridad de la Información actúa como órgano de supervisión y coordinación del SGSI, siendo responsable de la supervisión, coordinación y toma de decisiones estratégicas en materia de seguridad de la información.

Gestión de Riesgos

La organización realiza análisis de riesgos de forma periódica, identificando amenazas, evaluando impactos y definiendo medidas de tratamiento adecuadas para garantizar la protección de los activos de información.

Uso seguro de la Inteligencia Artificial

El uso de herramientas de Inteligencia Artificial deberá realizarse de forma segura, responsable y conforme a la normativa interna de la organización.

En todo caso, será necesaria la supervisión y validación humana de los contenidos generados, evitando el tratamiento de información sensible en entornos no autorizados y garantizando el cumplimiento de los requisitos de seguridad y protección de datos.

Mejora Continua

Analiza mantiene un compromiso de mejora continua en la gestión de la seguridad de la información, adaptándose a la evolución del entorno tecnológico y de las amenazas.

Aprobación

Aprobado por la Dirección

Fecha: 13/05/2026