Resumen público de la Política de Seguridad de la Información

Compromisos de iGEO para proteger la información y mantener la confianza en sus servicios

Documento	Versión	Fecha	Clasificación
Resumen público	1.0	26/06/2026	PÚBLICA

Documento derivado de SGSI-POL-001, versión 1.0, aprobada el 26/06/2026.

Nuestro compromiso

Intime Desarrollos Informáticos, S.L. (iGEO) considera la seguridad de la información un requisito esencial para prestar servicios fiables, proteger los datos confiados por clientes y usuarios y mantener la continuidad de su actividad. Para ello mantiene un Sistema de Gestión de la Seguridad de la Información basado en riesgos y alineado con los requisitos legales, regulatorios y contractuales que le resultan aplicables.

Ámbito de aplicación

La política se aplica a la información, los activos, los procesos, las personas y las relaciones con terceros incluidos en el SGSI. El alcance del SGSI es: “El sistema de la información que da soporte a los servicios de gestión integral de empresas dedicadas al control de plagas, higiene ambiental y salud pública, mediante el desarrollo, soporte, mantenimiento y explotación de la aplicación iGeo ERP ofrecida en modalidad SaaS. De acuerdo con la declaración de aplicabilidad en vigor.”

Sus principios son obligatorios para las personas que trabajan bajo el control de iGEO y, cuando corresponda, para los proveedores y terceros que acceden a información o recursos incluidos en este ámbito.

Principios que orientan nuestra actuación

- **Confidencialidad.** La información solo estará disponible para personas autorizadas que la necesiten para sus funciones.
- **Integridad.** Los datos, sistemas y registros se protegerán frente a modificaciones, pérdidas o destrucciones no autorizadas.
- **Disponibilidad y resiliencia.** Los servicios contarán con medidas proporcionadas de continuidad, recuperación y restauración.
- **Gestión basada en riesgos.** Las prioridades de seguridad se decidirán considerando activos, amenazas, consecuencias y requisitos aplicables.
- **Seguridad y privacidad desde el diseño.** La protección se incorporará desde el inicio de los desarrollos, servicios y cambios.
- **Mínimo privilegio.** Los accesos se limitarán a lo estrictamente necesario y se revisarán cuando cambien las funciones o necesidades.
- **Responsabilidad y trazabilidad.** Las decisiones, actuaciones relevantes y excepciones deberán quedar justificadas y registradas.

Compromisos de seguridad

iGEO se compromete a:

- Identificar y proteger la información durante todo su ciclo de vida según su sensibilidad, criticidad y requisitos aplicables.
- Gestionar las identidades y los accesos mediante autorización, identificación individual, mínimo privilegio y revisiones periódicas.
- Integrar requisitos de seguridad en el desarrollo de software y evaluar, autorizar, probar y registrar los cambios relevantes.
- Gestionar los servicios en la nube y los proveedores conforme al riesgo, los contratos y el modelo de responsabilidad compartida.
- Mantener medidas de configuración segura, monitorización, gestión de vulnerabilidades, copias de seguridad, restauración y continuidad.
- Identificar, evaluar, contener, resolver y documentar los incidentes, conservando las evidencias y realizando las notificaciones que correspondan.
- Formar y concienciar al personal para proteger la información en el trabajo presencial y remoto y comunicar sin demora eventos o debilidades.
- Autorizar y controlar el uso de inteligencia artificial, protegiendo la confidencialidad, la privacidad, la propiedad intelectual y la revisión humana de resultados relevantes.
- Cumplir los requisitos legales y reglamentarios de seguridad de la información aplicables y adaptar el SGSI ante nuevos requisitos.
- Mejorar continuamente la idoneidad, adecuación y eficacia del SGSI.

Gobierno y responsabilidades

La Alta Dirección aprueba la política, establece objetivos coherentes con ella y proporciona los recursos necesarios para operar y mejorar el SGSI. Todas las personas incluidas en su ámbito son responsables de cumplir las normas que les resulten aplicables, proteger la información a la que acceden y comunicar cualquier evento o debilidad de seguridad por los canales autorizados.

Cumplimiento revisión y disponibilidad

La política se revisa al menos una vez al año y siempre que se produzcan cambios significativos en el contexto, el alcance, los riesgos, los requisitos aplicables, los servicios o la tecnología. Los incumplimientos y las excepciones se gestionan de forma documentada, proporcionada y conforme al marco legal y contractual aplicable.

Comunicación. Las partes interesadas pueden trasladar consultas relacionadas con la seguridad mediante los canales corporativos publicados por iGEO. Las comunicaciones sobre datos personales se tratarán también conforme a la información de privacidad aplicable.