

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

<p>Autor: Arleth Torres Molina Responsable de Seguridad</p> <p>Organización: INGENIERÍA INFORMÁTICA EMPRESARIAL, S.L.</p>	<p>Validado por: Emilio Bravo García Dirección Técnica</p> <p>Organización: INGENIERÍA INFORMÁTICA EMPRESARIAL, S.L.</p>	<p>Aprobado por: José Luis Ramírez Dirección General</p> <p>Organización: INGENIERÍA INFORMÁTICA EMPRESARIAL, S.L.</p> <p style="text-align: center;">Firma:</p>
Fecha: 20/01/2025	Fecha: 21/01/2025	Fecha: 22/01/2025
Descripción: Política de Seguridad de la Información		
Control de Versiones:		
Versión	Fecha	Descripción del cambio
1.0	31/05//2021	Primera versión.
1.1	03/03/2023	Caducidad de contraseñas
1.2	10/10/2023	Actualización de la normativa y formato del documento.
1.3	20/01/2025	Actualización de la normativa Se incluye el uso responsable de la IA

Proyecto: SGSI	Versión:2.0	Fecha: 20/01/2025	
Nombre: Política de seguridad de la información		Clasificación: PÚBLICO	

DECLARACIÓN

INGENIERÍA INFORMÁTICA EMPRESARIAL, S.L. (en adelante, i2e) establece la seguridad de la información como factor para la competitividad del negocio y el cumplimiento normativo.

En consecuencia, i2e ha implantado los procesos de planificación e implantación de controles de seguridad, así como, de supervisión y mejora de la seguridad, para asegurar la confidencialidad, integridad y disponibilidad de los servicios que presta.

La Dirección de i2e es responsable de implantar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información, de conformidad con estándares internacionales, satisfaciendo las siguientes metas:

- Evaluar y tratar los riesgos de la seguridad de la información.
- Garantizar la continuidad del servicio.
- Gestionar las incidencias, potenciales o reales, de la seguridad de la información.
- Medir los indicadores de eficacia y eficiencia de la seguridad de la información.
- Optimizar los procesos de gestión y los controles en modo mejora continua.
- Concienciar y capacitar a los empleados y colaboradores.
- Cumplir la legislación de protección de datos personales y otra normativa aplicable.

La Dirección de i2e delega en la persona Responsable de Seguridad de la Información su mantenimiento, soporte y acreditación, contando con la participación y el respaldo de todo el personal y colaboradores.

INGENIERÍA INFORMÁTICA EMPRESARIAL, S.L.

JOSÉ LUIS RAMIREZ TERRY

Director General

20/01/2025

Proyecto: SGSI	Versión:2.0	Fecha: 20/01/2025	
Nombre: Política de seguridad de la información		Clasificación: PÚBLICO	

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Para dar cumplimiento a la política de seguridad de la información, i2e ha establecido un Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con la norma ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información Requisitos. Que cubre de forma adecuada todos los requisitos necesarios para asegurar la confidencialidad e integridad de la información y la disponibilidad de los servicios.

El anterior compromiso se concreta en los principios siguientes:

1. Nombrar una persona responsable de la Seguridad de la Información, encargada de la gestión, actualización, mantenimiento y mejora del SGSI.
2. Constituir el Comité de Seguridad de la Información.
3. Analizar los riesgos de seguridad de la información derivados de la prestación de servicios e implantar los controles, medidas o salvaguardas necesarias.
4. Asignar los recursos para satisfacer los requisitos de seguridad de la información, manteniendo el equilibrio entre coste y beneficio.
5. Impartir la formación y concienciación del personal y colaboradores, en materia de riesgos y amenazas a la seguridad de la información y a cumplir las medidas para su prevención y mitigación definidas y a participar de manera activa en la notificación de incidencias.
6. Implantar las medidas para garantizar los niveles de seguridad de la información y los servicios, respondiendo a las incidencias.

Proyecto: SGSI	Versión:2.0	Fecha: 20/01/2025	
Nombre: Política de seguridad de la información		Clasificación: PÚBLICO	

7. Medir y analizar los objetivos e indicadores de gestión de seguridad de la información, que permitan a i2e el seguimiento de los riesgos e incidencias de seguridad y de las actividades de control.
8. Implantar un proceso de revisión, auditoría y mejora continua del SGSI, que garantice la actualización, adecuación y el mantenimiento de los controles y medidas de seguridad establecidos.
9. Cumplir con los requisitos legales, normativos y reglamentarios aplicables.

Para abordar los referidos principios, la Dirección de I2e establece las pautas siguientes:

1. LA SEGURIDAD DE LA INFORMACIÓN ES RESPONSABILIDAD DE TODOS

- La Dirección de i2e supervisará las medidas de seguridad de la información y, en particular, su cumplimiento será responsabilidad de empleados y colaboradores.
- Para el despliegue efectivo de la presente política de seguridad, la Dirección de I2e aportará los medios necesarios, de acuerdo con un modelo de mejora continua, con especial énfasis en la formación de los recursos humanos y en el control y análisis de los resultados para verificar la eficiencia y eficacia de las medidas.

2. GESTIÓN DEL RIESGO

Con el fin de gestionar los riesgos derivados de las amenazas sobre los activos, se establecen las siguientes medidas:

- La Dirección de i2e proveerá de los recursos humanos, intangibles y materiales necesarios para el análisis de riesgos.

Proyecto: SGSI	Versión:2.0	Fecha: 20/01/2025	
Nombre: Política de seguridad de la información		Clasificación: PÚBLICO	

- Se realizará un registro de los análisis de riesgo realizados y se someterá a la aprobación del Comité de Seguridad de la Información.
- La Dirección de i2e establece, como valor objetivo de riesgo el 25% de la puntuación máxima posible.
- Con el fin de alcanzar el valor objetivo de riesgo, el Responsable de Seguridad de la Información de i2e actualizará anualmente el análisis de riesgos y propondrá la aprobación por el Comité de Seguridad de la información de los planes de tratamiento de riesgo para su mitigación.

3. EQUIPOS, COMUNICACIONES Y APLICACIONES

Para garantizar el buen uso de los equipos y los programas instalados, que se entregan a los usuarios debidamente configurados para su desempeño, se seguirán las siguientes medidas:

- Todos los equipos y sistemas son activos propiedad de i2e, asignados a los usuarios, debidamente inventariados y puestos a su disposición exclusivamente para la realización de sus funciones.
- La instalación y uso de cualquier programa software o contenido digital, ajeno a los instalados o autorizados expresamente, queda terminantemente restringida. Asimismo, no se admiten modificaciones a los elementos del hardware entregado.
- Todos los programas software instalados en los equipos contarán con las debidas licencias de uso y/o mantenimiento emitidas por sus fabricantes.

Proyecto: SGSI	Versión:2.0	Fecha: 20/01/2025	
Nombre: Política de seguridad de la información		Clasificación: PÚBLICO	

4. ACCESO FÍSICO

Para garantizar el debido acceso físico a las dependencias de i2e, donde se ubican los equipos y sistemas de información, se seguirán las siguientes medidas:

- El acceso físico a las dependencias de i2e de personas no pertenecientes a su organización o colaboradores estará controlado en la recepción y autorizado previamente por el responsable de la unidad a la que se vaya a visitar.
- El acceso de las visitas estará en todo momento monitorizado por i2e, registrándose la entrada y salida.
- Las visitas que accedan a las zonas donde se albergan los equipos y sistemas de información, debidamente delimitadas, deberán estar en todo momento acompañadas por personal de i2e.

5. MEDIOS DE PROTECCIÓN FÍSICA

Para garantizar la protección de los equipos, instalaciones generales y dependencias de i2e donde se ubican los equipos y sistemas de información, se seguirán las siguientes medidas:

- La disposición de medios de detección de incendios.
- La protección de las redes y canalizaciones de datos y voz.

6. IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS

Para garantizar el debido acceso a los equipos, aplicaciones e información, se seguirán las siguientes medidas:

Proyecto: SGSI	Versión:2.0	Fecha: 20/01/2025	
Nombre: Política de seguridad de la información		Clasificación: PÚBLICO	

- A todo usuario se asigna un nombre de usuario y una contraseña, que son estrictamente personales o grupales e intransferibles, en función de sus derechos y privilegios de acceso a la información y operaciones.
- Las contraseñas serán configuradas por los servicios informáticos de i2e.
- Las contraseñas de los usuarios deberán renovarse cada 120 días.
- Los nombres de usuarios y contraseñas serán cambiadas o eliminadas en el momento que se produzca algún cambio de funciones o baja en i2e, respectivamente.

7. USO DE INTERNET

Para garantizar el acceso a Internet y el uso correcto de sus recursos por parte de los usuarios, se seguirán las siguientes medidas:

- El acceso a Internet estará en todo momento monitorizado por i2e, registrándose la actividad realizada.
- La navegación por Internet se ajustará a las necesidades del desempeño de cada usuario, reconociendo el valor y utilidad de sus contenidos y servicios a efectos de eficacia y eficiencia interna y externa.
- Queda restringido el acceso de los usuarios a aquellas zonas de Internet consideradas inseguras o inapropiadas, de acuerdo con las prácticas de buen uso reconocidas y la legislación vigente.

8. USO DEL CORREO ELECTRÓNICO

Para garantizar el debido uso del correo electrónico por parte de los usuarios, se seguirán las siguientes reglas:

Proyecto: SGSI	Versión:2.0	Fecha: 20/01/2025	
Nombre: Política de seguridad de la información		Clasificación: PÚBLICO	

- Las cuentas de correo electrónico, asignadas a los usuarios exclusivamente para el desempeño laboral, son propiedad de i2e.
- Los contenidos de los correos electrónicos son confidenciales ajustándose al ordenamiento legal.
- A todo usuario de i2e se le asigna una dirección electrónica y una contraseña, que serán estrictamente personales e intransferibles.
- La contraseña será entregada por los servicios informáticos de i2e y configurada por los usuarios.

Como reglas generales se recomienda:

- No abrir nunca o reenviar mensajes de correo de remitentes desconocidos.
- No abrir nunca o reenviar mensajes de correo de remitentes conocidos, pero con asuntos en idiomas diferentes a su remitente.
- No abrir nunca los ficheros adjuntos de correos de procedencia dudosa.

9. COPIAS DE SEGURIDAD

Para garantizar la recuperación de los datos de los usuarios, en caso de pérdida o destrucción, se seguirán las siguientes medidas:

- Los datos almacenados serán objeto de la realización de copias de seguridad por parte de los servicios informáticos de i2e.
- Las copias de seguridad serán custodiadas y conservadas por los servicios informáticos de i2e

Proyecto: SGSI	Versión:2.0	Fecha: 20/01/2025	
Nombre: Política de seguridad de la información		Clasificación: PÚBLICO	

10. FILTRADO DE CONTENIDOS

Para garantizar la identificación, el bloqueo y eliminación de contenidos potencialmente maliciosos, i2e instala y mantiene un sistema antivirus en los equipos, siendo de obligado cumplimiento las siguientes medidas:

- No desactivar nunca los programas antivirus.
- Reiniciar siempre el ordenador para finalizar la instalación de todas las actualizaciones.

11. PROTECCIÓN DE SISTEMAS OPERATIVOS Y OTRAS UTILIDADES

Para reducir los riesgos y vulnerabilidades derivadas de los sistemas operativos y otras utilidades instaladas en los equipos de los usuarios, se seguirán las siguientes reglas:

- No desactivar nunca los programas de actualización.
- Reiniciar siempre el ordenador para finalizar la instalación de todas las actualizaciones recibidas.

12. INCIDENCIAS

Para mitigar y corregir cualquier incidencia relativa a los sistemas de información y comunicaciones y evitar su repetición, se seguirán las medidas siguientes:

- La comunicación inmediata a la persona Responsable de Seguridad de i2e de cualquier evento, tal como: anomalía informática o de comunicaciones, malfuncionamiento, pérdida de control de los programas, desconexión súbita del sistema, comunicación externa sospechosa, presencia física de desconocidos no identificados en las dependencias, etc., que se realizará preferentemente a través de la cuenta de correo seguridad@i2e.es creada para tal efecto.

Proyecto: SGSI	Versión:2.0	Fecha: 20/01/2025	
Nombre: Política de seguridad de la información		Clasificación: PÚBLICO	

- El registro y seguimiento hasta su solución y cierre de las anomalías denunciadas.
- El análisis periódico de las anomalías para la propuesta de medidas correctivas o preventivas y toma de decisión por el Comité de Seguridad de la Información.

13. CUMPLIMIENTO LEGAL

Para evitar las contingencias legales derivadas del manejo de los datos de carácter personal, se seguirán las siguientes medidas:

- La identificación y difusión a los usuarios de los tratamientos, automatizados o no, de datos de carácter personal y su nivel de protección.
- El seguimiento de todos los controles para el cumplimiento de la legislación vigente en materia de protección de datos personales, que serán debidamente difundidas entre los usuarios y monitorizadas por i2e
- La persona Responsable de Seguridad supervisará que el tratamiento de la información se realice correctamente con el fin de cumplir las políticas y normas de seguridad definidas por i2e.

14. PROTECCIÓN DE LA INFORMACIÓN

Para evitar la pérdida, robo o transferencia no autorizada de la información clasificada o propiedad intelectual de i2e, se seguirán las siguientes medidas:

- La identificación y clasificación de toda la información, en cualquier soporte, considerada de especial protección.
- El seguimiento y supervisión de los controles para el acceso, manejo, transmisión y reproducción de dicha información.

Proyecto: SGSI	Versión:2.0	Fecha: 20/01/2025	
Nombre: Política de seguridad de la información		Clasificación: PÚBLICO	

- El seguimiento por los usuarios de una práctica de puesto de trabajo despejado de expedientes y bloqueo de pantalla mediante contraseña cuando el equipo esté desatendido o no esté en uso.

15. CONTINUIDAD DE LAS OPERACIONES

Para reducir los riesgos derivados de la ocurrencia de un accidente, catástrofe, atentado o sabotaje de los equipos, aplicaciones e instalaciones y usuarios de i2e, se seguirán las siguientes medidas:

- La preparación, pruebas y actualización del plan de continuidad de negocio.
- La difusión y formación sobre las medidas de continuidad de negocio entre el personal y los colaboradores.

16. MEJORA CONTINUA

Para optimizar y mejorar de modo permanente la gestión de la seguridad de la información, se seguirán las siguientes medidas:

- La revisión anual de la Política o cuando se produzcan cambios, para asegurar su continua idoneidad, adecuación y eficacia.
- Mantener un registro de la revisión de la Política que el Comité de Seguridad de la información debe aprobar cada revisión.
- La propuesta de cualquier sugerencia, medida o idea, por medio de correo electrónico, por parte de los usuarios a la persona Responsable de Seguridad de la información.

Proyecto: SGSI	Versión:2.0	Fecha: 20/01/2025	
Nombre: Política de seguridad de la información		Clasificación: PÚBLICO	

- El registro y seguimiento hasta su propuesta y cierre de las mejoras propuestas.
- El análisis periódico de las mejoras propuestas y toma de decisión por el Comité de Seguridad de la Información.
- El reconocimiento público de los usuarios que propongan mejoras.

17. USO RESPONSABLE Y SEGURO DE LA INTELIGENCIA ARTIFICIAL

Para el uso responsable de las herramientas comerciales de Inteligencia Artificial (IA) y la incorporación de las tecnologías de IA en las soluciones que se desarrollan para los clientes, así como para mitigar los riesgos asociados, se establecen políticas, principios y prácticas responsables que promueven la seguridad, la ética y la transparencia. Entre estas se incluyen:

- **Transparencia:** todo uso de IA deberá ser comprensible y justificable, evitando aplicaciones que puedan resultar opacas o discriminatorias.
- **Privacidad y protección de datos:** el uso de herramientas de IA y los sistemas basados en IA deberán cumplir estrictamente con las normativas de protección de datos personales y confidenciales.
- **Prevención de riesgos:** se implementarán mecanismos de evaluación continua para identificar y mitigar riesgos relacionados con el uso de IA, incluyendo sesgos, vulnerabilidades de seguridad y posibles impactos negativos.
- **Capacitación y concienciación:** se fomentará el conocimiento y la comprensión de la IA entre los colaboradores, promoviendo un uso ético y responsable.
- **Cumplimiento normativo:** todas las aplicaciones de IA deberán adherirse a las leyes y regulaciones aplicables, así como a los valores y principios de i2e.

Proyecto: SGSI	Versión:2.0	Fecha: 20/01/2025	
Nombre: Política de seguridad de la información	Clasificación: PÚBLICO		

La presente política es conocida y suscrita por todo el personal y colaboradores de i2e.

La presente política será revisada con una periodicidad máxima anual, y sus cambios deberán ser aprobados por la Dirección de i2e