POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Autor: Arleth Torres Molina Responsable de Seguridad **Organización:** INGENIERÍA INFORMÁTICA EMPRESARIAL, S.L.	**Validado por:** Emilio Bravo García Dirección Técnica **Organización:** INGENIERÍA INFORMÁTICA EMPRESARIAL, S.L.	**Aprobado por:** José Luis Ramírez Dirección General **Organización:** INGENIERÍA INFORMÁTICA EMPRESARIAL, S.L. Firma:
Fecha: 04/03/2026	**Fecha:** 05/03/2026	**Fecha**: 06/03/2026
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
1.4	04/03/2026	Se mejora la redacción en general. Se incorporan como novedades el uso obligatorio de conexiones seguras mediante VPN para el acceso remoto, el refuerzo de las medidas de prevención frente a la fuga de información y la integración de prácticas de inteligencia de amenazas para la identificación y mitigación de riesgos emergentes.

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 procesos de planificación, implementación, supervisión y mejora de los controles de seguridad, con el fin de garantizar 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, conforme a estándares internacionales, con el objetivo de alcanzar las siguientes metas:

- Evaluar y tratar los riesgos de 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 la gestión, mantenimiento y acreditación del sistema, contando con la participación activa y el respaldo de todo el personal y colaboradores de la organización.

INGENIERÍA INFORMÁTICA EMPRESARIAL, S.L.
JOSÉ LUIS RAMIREZ TERRY
Director General
04/03/2026

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. Este sistema cubre de manera integral todos los requisitos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información y los servicios que presta la organización.

El compromiso de i2e se concreta en los siguientes principios:

1. Nombrar una persona responsable de la Seguridad de la Información, encargada de la gestión, actualización, mantenimiento y mejora continua del SGSI.

2. Constituir un Comité de Seguridad de la Información, encargado de supervisar y validar las políticas, procesos y medidas de seguridad adoptadas.

3. Analizar los riesgos de seguridad de la información asociados a la prestación de servicios e implementar los controles, medidas y salvaguardas necesarias para su mitigación.

4. Asignar los recursos necesarios para satisfacer los requisitos de seguridad de la información, manteniendo un equilibrio adecuado entre coste y beneficio.

5. Impartir formación y concienciación al personal y colaboradores sobre los riesgos y amenazas a la seguridad de la información, promoviendo el cumplimiento de las medidas preventivas y de mitigación, así como la participación activa en la notificación de incidencias.

6. Implementar medidas de seguridad que garanticen los niveles requeridos de protección de la información y los servicios, asegurando la respuesta adecuada ante incidencias

7. Medir y analizar objetivos e indicadores de gestión de seguridad de la información, facilitando el seguimiento de riesgos, incidencias y eficacia de los controles implementados.

8. Implantar un proceso de revisión, auditoría y mejora continua del SGSI, que garantice la actualización, adecuación y mantenimiento de los controles y medidas de seguridad establecidos.

9. Cumplir con la legislación, normativa y reglamentación aplicable.

Para dar cumplimiento a estos principios, la Dirección de i2e establece las siguientes pautas:

1. LA SEGURIDAD DE LA INFORMACIÓN ES RESPONSABILIDAD DE TODOS

- La seguridad de la información constituye una responsabilidad compartida por toda la organización. La Dirección de i2e establecerá, supervisará y revisará las medidas de seguridad de la información, mientras que empleados y colaboradores serán responsables de su cumplimiento en el ejercicio de sus funciones.

- Para el despliegue efectivo de la presente Política de Seguridad, la Dirección de i2e proporcionará los recursos humanos, técnicos y organizativos necesarios, conforme a un modelo de mejora continua. Se prestará especial atención a la formación y concienciación del personal, así como al seguimiento, control y análisis de resultados, con el fin de verificar la eficacia y eficiencia de las medidas adoptadas.

2. GESTIÓN DEL RIESGO

Con el fin de gestionar los riesgos derivados de las amenazas que puedan afectar a los activos de información, se establecen las siguientes medidas:

- La Dirección de i2e proporcionará los recursos humanos, técnicos, organizativos y económicos necesarios para la adecuada realización del análisis y gestión de riesgos.

- Se realizará y mantendrá actualizado un registro de los análisis de riesgos efectuados, que será sometido a la revisión y 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 dicho objetivo, el Responsable de Seguridad de la Información actualizará, al menos con carácter anual o cuando se produzcan cambios significativos, el análisis de riesgos y propondrá al Comité de Seguridad de la Información la aprobación de los correspondientes planes de tratamiento de riesgos para su mitigación.

3. EQUIPOS, COMUNICACIONES Y APLICACIONES

Para garantizar el uso adecuado y seguro de los equipos y programas instalados, que se entregan a los usuarios debidamente configurados para el desempeño de sus funciones, se establecen 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 el ejercicio de sus funciones profesionales.

- La instalación o uso de cualquier programa software o contenido digital distinto de los previamente instalados o expresamente autorizados por la organización queda terminantemente prohibida. Asimismo, no se permiten modificaciones no autorizadas de los elementos de hardware entregados.

- Todos los programas software instalados en los equipos deberán contar con las correspondientes licencias de uso y/o mantenimiento emitidas por sus fabricantes.

- El acceso remoto a los sistemas corporativos se realizará exclusivamente mediante VPN corporativa autorizada, siendo obligatorio su uso cuando el acceso se efectúe desde redes externas o no seguras, con el fin de garantizar la seguridad de la información y los sistemas.

4. ACCESO FÍSICO

Con el fin de garantizar un control adecuado del acceso físico a las dependencias de i2e, donde se ubican los equipos y sistemas de información, se establecen las siguientes medidas:

- El acceso a las instalaciones por parte de personas ajenas a la organización deberá estar previamente autorizado por el responsable del área correspondiente y será controlado en el punto de recepción.

- El acceso de las visitas estará en todo momento monitorizado por i2e, registrándose la entrada y salida.

- Las personas visitantes que accedan a zonas donde se encuentren ubicados equipos y sistemas de información, previamente delimitadas como áreas restringidas, deberán permanecer en todo momento acompañadas por personal autorizado de i2e.

5. MEDIOS DE PROTECCIÓN FÍSICA

Con el objetivo de proteger los equipos, las instalaciones generales y las dependencias de i2e donde se ubican los sistemas de información, se adoptarán las siguientes medidas:

- Instalación y mantenimiento de medios de detección y prevención de incendios, así como sistemas de alarma asociados.

- Protección física y control de acceso a las redes, canalizaciones y equipos de datos y voz, garantizando la integridad y disponibilidad de la infraestructura de comunicaciones.

6. IDENTIFICACIÓN Y AUTENTIFICACIÓN DE USUARIOS

Con el fin de garantizar un acceso adecuado y seguro a los equipos, aplicaciones e información de i2e, se aplicarán las siguientes medidas:

- A cada usuario se le asignará un nombre de usuario y una contraseña, estrictamente personales o, en casos excepcionales, grupales, e intransferibles, de acuerdo con los derechos y privilegios de acceso asignados.

- La creación y configuración inicial de las contraseñas será gestionada por los servicios informáticos de i2e, siguiendo criterios de seguridad establecidos.

- Las contraseñas de los usuarios deberán renovarse cada 120 días.

- Los nombres de usuario y contraseñas deberán ser modificados o eliminados inmediatamente ante cualquier cambio de funciones, reasignación de responsabilidades o baja del usuario en la organización.

7. USO DE INTERNET

Para garantizar un acceso seguro y adecuado a Internet y un uso responsable de sus recursos, se establecen las siguientes medidas:

- El acceso a Internet será monitorizado y registrado por i2e, dejando constancia de la actividad realizada para fines de seguridad y control interno.

- La navegación por Internet deberá limitarse a actividades relacionadas con el desempeño de las funciones de cada usuario, reconociendo el valor y la utilidad de los contenidos y servicios utilizados para garantizar la eficacia y eficiencia de los procesos internos y externos.

- Queda expresamente restringido el acceso a sitios web considerados inseguros o inapropiados, conforme a las prácticas de buen uso reconocidas por la organización y la legislación vigente.

8. USO DEL CORREO ELECTRÓNICO

Con el fin de garantizar un uso seguro y adecuado del correo electrónico por parte de los usuarios, se aplicarán las siguientes disposiciones:

- Las cuentas de correo electrónico asignadas a los usuarios son exclusivamente para fines laborales y constituyen propiedad de i2e.

- Los contenidos de los correos electrónicos se consideran confidenciales y su tratamiento deberá ajustarse a la normativa legal vigente.

- A cada usuario se le asignará una dirección de correo electrónico y una contraseña, estrictamente personales e intransferibles.

- La contraseña será proporcionada por los servicios informáticos de i2e y deberá ser configurada y mantenida en secreto por el usuario.

Como reglas generales se recomienda:

  - No abrir ni reenviar mensajes provenientes de remitentes desconocidos
  - No abrir ni reenviar mensajes de remitentes conocidos si el contenido o el idioma del asunto resulta sospechoso o inesperado.
  - No abrir ni ejecutar archivos adjuntos de correos electrónicos de procedencia dudosa o no verificada.

9. COPIAS DE SEGURIDAD

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

- Los datos almacenados serán objeto de copias de seguridad periódicas, gestionadas por los servicios informáticos de i2e, según los procedimientos internos establecidos.

- Las copias de seguridad serán custodiadas, protegidas y conservadas por los servicios informáticos de i2e, asegurando su integridad, confidencialidad y disponibilidad.

10. FILTRADO DE CONTENIDOS

Con el objetivo de identificar, bloquear y eliminar contenidos potencialmente maliciosos, i2e instala y mantiene un sistema antivirus actualizado en todos los equipos. Se aplicarán las siguientes medidas obligatorias:

- No desactivar nunca los programas antivirus instalados en los equipos corporativos

- Reiniciar siempre el equipo tras la instalación de actualizaciones, para asegurar que todos los cambios y parches se apliquen correctamente.

11. PROTECCIÓN DE SISTEMAS OPERATIVOS Y OTRAS UTILIDADES

Con el objetivo de minimizar los riesgos y vulnerabilidades asociadas a los sistemas operativos y otras utilidades instaladas en los equipos de los usuarios, se aplicarán las siguientes medidas obligatorias:

- No desactivar nunca los programas de actualización de los sistemas operativos y aplicaciones.

- Reiniciar siempre el equipo tras la instalación de actualizaciones, para garantizar que todos los parches y mejoras de seguridad se apliquen correctamente.

- Mantener los sistemas operativos y aplicaciones actualizados siguiendo las políticas de seguridad establecidas en el sistema de gestión.

12. INCIDENCIAS

Para mitigar, corregir y prevenir la repetición de cualquier incidencia relacionada con los sistemas de información y comunicaciones, se aplicarán las siguientes medidas:

- Comunicación inmediata a la persona responsable de Seguridad de i2e de cualquier evento, tales como: anomalías informáticas o de comunicaciones, malfuncionamiento de sistemas, pérdida de control de programas, desconexión súbita de servicios, comunicaciones externas sospechosas, o presencia de

personas no autorizadas en las dependencias, etc. La notificación deberá realizarse preferentemente a través de la cuenta de correo seguridad@i2e.es, creada para tal efecto.

- Registro y seguimiento de todas las incidencias hasta su resolución y cierre, asegurando la trazabilidad de las acciones correctivas realizadas

- Análisis periódico de las incidencias registradas, con el fin de proponer medidas correctivas o preventivas, y sometiendo las decisiones relevantes al Comité de Seguridad de la Información para su aprobación y seguimiento.

13. CUMPLIMIENTO LEGAL

Para evitar contingencias legales derivadas del tratamiento de datos de carácter personal, se aplicarán las siguientes medidas:

- Identificación y difusión a los usuarios de todos los tratamientos de datos de carácter personal, automatizados o no, incluyendo su finalidad y nivel de protección requerido.

- Seguimiento y control de todas las medidas necesarias para garantizar el cumplimiento de la legislación vigente en materia de protección de datos personales. Estas medidas serán debidamente difundidas entre los usuarios y monitorizadas de forma continua 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 y la normativa aplicable.

14. PROTECCIÓN DE LA INFORMACIÓN

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

- Identificación y clasificación de toda la información, en cualquier soporte, que requiera especial protección.
- Establecimiento y supervisión de controles para el acceso, tratamiento, transmisión y reproducción de dicha información.
- Aplicación de la política de “puesto de trabajo despejado”, incluyendo el archivo de documentación sensible y el bloqueo de pantalla mediante contraseña cuando el equipo esté desatendido.
- Implementación de medidas técnicas, organizativas y físicas destinadas a prevenir la fuga, pérdida o acceso no autorizado a la información.
- Incorporación de prácticas de inteligencia de amenazas, mediante la monitorización de fuentes especializadas y el análisis continuo de riesgos emergentes, con el fin de anticipar, detectar y mitigar posibles amenazas que puedan afectar a la seguridad de la información.

15. CONTINUIDAD DE LAS OPERACIONES

Para minimizar 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:

- Preparación, pruebas y actualización del plan de continuidad de negocio.

- Difusión y formación sobre las medidas de continuidad de negocio entre el personal y los colaboradores.

16. MEJORA CONTINUA

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

- Revisión anual de la Política de Seguridad de la Información, así como cada vez que se produzcan cambios significativos, para asegurar su idoneidad, adecuación y eficacia continua.

- Registro de revisiones, que deberá ser aprobado por el Comité de Seguridad de la Información tras cada actualización de la política.

- Propuesta de mejoras, sugerencias o medidas por parte de los usuarios, que podrán enviarse a la persona responsable de Seguridad de la Información mediante correo electrónico.

- Registro y seguimiento de las propuestas hasta su evaluación, decisión y cierre, garantizando trazabilidad de las acciones realizadas.

- Análisis periódico de las propuestas por parte del Comité de Seguridad de la Información, con la finalidad de aprobar, priorizar e implementar las mejoras consideradas pertinentes.

- Reconocimiento a los usuarios que presenten propuestas de mejora, fomentando la participación y la cultura de seguridad en la organización.

17. USO RESPONSABLE Y SEGURO DE LA INTELIGENCIA ARTIFICIAL

Con el objetivo de garantizar un uso responsable, seguro y ético de las herramientas comerciales de Inteligencia Artificial (IA) y de las tecnologías de IA incorporadas en las soluciones desarrolladas para los clientes, se aplicarán las siguientes medidas:

- 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 la formación y el conocimiento de la IA entre los colaboradores, promoviendo un uso ético, responsable y alineado con los valores de i2e.

- Cumplimiento normativo: todas las aplicaciones de IA deberán adherirse a las leyes y regulaciones aplicables, así como a los valores y principios de i2e.

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

Esta política será revisada como máximo una vez al año, y cualquier modificación deberá ser aprobada por la Dirección de i2e.