


|   |  |               |                 |
|---|--|---------------|-----------------|
|  | Sistemas de gestión de seguridad de la información (SGSI) ISO/IEC 27001:2023 | Código        | PC01 ANEXO III. |
|   |  | Página        | 1 de 3          |
|   | POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN                                      | Versión N°    | 00              |
|   |  | Fecha edición | 01/06/2024      |
|   | Confidencialidad   | Público       |                 |

Para **GESNAER**, la información que maneja tiene un valor incalculable, así como los activos y metodologías de trabajo que utilizamos, para ello hemos implantado un Sistema de Gestión de Seguridad de la Información (SGSI), el cual nos permitirá de una forma fiable, tener todos nuestros recursos tanto humanos como materiales, perfectamente controlados y bajo una supervisión exhaustiva, garantizando a nuestros clientes y proveedores una total confidencialidad a la hora de la ejecución de los servicios.

La Dirección de **GESNAER**, es consciente y tiene asumido que uno de los objetivos más importantes de la compañía es la protección de los activos de información de cualquier amenaza, ya sea interna o externa, deliberada o accidental, que suponga un riesgo para la confidencialidad, integridad o disponibilidad de la información.


**GESNAER** considera que la planificación, la implantación de controles, la supervisión y la mejora continua de la seguridad de la información son procesos de gestión esenciales para asegurar la competitividad y la sostenibilidad del negocio

Es por ello que la Dirección asume la responsabilidad de implantar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información, conforme a los estándares nacionales e internacionales, que facilite los siguientes objetivos:

1. **Concienciación y formación** en seguridad de la información de los empleados.
2. Evaluación y tratamiento de riesgos de la seguridad de la información.
3. La **continuidad del negocio** ante sucesos que pudieran afectar a los activos críticos.
4. Medición de los indicadores de eficacia y eficiencia de la seguridad de la información.
5. Garantizar la **Confidencialidad** de la información.
6. Mantener la **integridad de la información**. Gestión de las incidencias, potenciales o reales, de la seguridad de la información
7. La **Disponibilidad** de la información para los procesos de las áreas de negocio.
8. **Cumplimiento de la legislación** de protección de datos de carácter personal, de propiedad intelectual y cualquier otra que sea de aplicación.
9. Apuesta por la **Innovación** y el desarrollo de las últimas tecnología y aplicaciones de mercado.

Las **directrices generales** que se establecen para la consecución de estos **objetivos** son las siguientes:

- ✓ **Promover una cultura en toda la organización** orientada a la protección de los activos de información.
- ✓ **Protección de la información** de la Organización en general, y de forma particular aquella relativa a datos de carácter personal y la intimidad de las personas.
- ✓ **Tratamiento de la información** de los clientes de acuerdo a sus especificaciones.
- ✓ Lograr plena **satisfacción de nuestros clientes**, proporcionándoles servicios y productos acordes con los requisitos, necesidades, expectativas y especificaciones establecidas, incluyendo las normas o legislación vigente.
- ✓ Cumplimiento de los **requisitos legales aplicables** y otros requisitos.
- ✓ Cumplir con los **controles y medidas de seguridad** establecidos con la implantación del Sistema de Gestión de Seguridad de la información.

|   |  |               |                 |
|---|--|---------------|-----------------|
|  | Sistemas de gestión de seguridad de la información (SGSI) ISO/IEC 27001:2023 | Código        | PC01 ANEXO III. |
|   |  | Página        | 2 de 3          |
|   | POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN                                      | Versión N°    | 00              |
|   |  | Fecha edición | 01/06/2024      |
|   | Confidencialidad   | Público       |                 |


Para la consecución de los objetivos derivados de las directrices que se indican en esta política y del análisis de la organización y de su contexto, la Dirección de **GESNAER** se compromete a facilitar los recursos humanos y materiales necesarios para llevarlos a cabo; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el **Sistema de Gestión de Seguridad de la Información (SGSI)**.

La gestión de nuestro sistema se encomienda al Responsable de Gestión y el sistema estará disponible en nuestro sistema de información en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos. Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de la presente Política Integrada de Sistemas de Gestión. Los roles o funciones de seguridad definidos son:

| Función  | Deberes y responsabilidades  |
|--|--|
| Responsable de la información<br>Dirección                       | - Tomar las decisiones relativas a la información tratada.   |
| Dirección<br>Responsable del Sistema<br>Responsable de Seguridad | - Determinar la idoneidad de las medidas técnicas.<br>- Proporcionar la mejor tecnología para el servicio. |
| Responsable del Sistema  | - Coordinar la implantación del Sistema.<br>- Mejorar el sistema de forma continua.                        |
| Dirección  | - Proporcionar los recursos necesarios para el Sistema.<br>- Liderar el Sistema.                           |

Esta definición se completa en los perfiles de puesto y en los documentos del sistema. El procedimiento para su designación y renovación será la ratificación en el comité de seguridad. El comité para la gestión y coordinación de la seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité. Los miembros del comité de seguridad de la información son:

- Responsable de la información.
- Responsable de la seguridad.
- Responsable del sistema.
- Dirección.

|   |  |               |                 |
|---|--|---------------|-----------------|
|  | Sistemas de gestión de seguridad de la información (SGSI) ISO/IEC 27001:2023 | Código        | PC01 ANEXO III. |
|   |  | Página        | 3 de 3          |
|   | POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN                                      | Versión N°    | 00              |
|   |  | Fecha edición | 01/06/2024      |
|   | Confidencialidad   | Público       |                 |

Todos los empleados son responsables de garantizar que cumplen con todas las políticas y procedimientos publicados por la empresa.

**GESNAER** pretende con esta Política incrementar su competitividad, ganar la confianza de sus clientes y lograr un sentimiento de satisfacción entre sus empleados por la calidad del trabajo realizado y la protección de la seguridad de la información.

La Dirección ha nombrado a un Responsable de Seguridad de la Información que tiene bajo su responsabilidad directa la de mantener esta Política y proporcionar consejo y guía sobre su implantación.

Esta Política es revisada periódicamente por la comité de seguridad de la información mediante reuniones establecidas a tal efecto, se encuentra difundida a todos los niveles de la empresa y a disposición del público así como de todas aquellas partes interesadas que la soliciten.

Esta política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión.

Dirección  
Fecha: 01 de Junio de 2024