

La Dirección del **GRUPO SEMI** desea **proteger a sus clientes y sus objetivos de negocio**, ofreciendo a las partes interesadas **un entorno de trabajo e información seguro**, mediante las medidas de control y procesos operativos adecuados.

Los **principios básicos** que se deben garantizar son:

**Confidencialidad:** La información debe ser **conocida exclusivamente por las personas autorizadas**.

**Integridad:** La información debe ser **completa, exacta, válida y no sujeta a manipulaciones**.

**Disponibilidad:** La información debe ser **accesible por los usuarios autorizados en todo momento y garantizar su persistencia** ante cualquier eventualidad.

La **Seguridad de la Información debe de ser flexible, eficaz y dar soporte al modelo de negocio de la compañía**, para ello:

- El **acceso** a la información **debe ser controlado** y estar basado en el rol de la persona en la organización.
- Los **servicios** proporcionados serán **seguros desde cualquier punto de acceso** cuando se conecta a la infraestructura de la compañía.
- Las medidas de seguridad deben **garantizar los requisitos de confidencialidad, integridad y disponibilidad de información y servicios**, manteniendo la **privacidad de datos personales** de acuerdo con la legislación vigente.
- Tiene que estar **alineada con la organización del negocio**, los requerimientos de seguridad de nuestros **clientes**, la **legislación aplicable** y las buenas prácticas del sector.
- **Sistema de Gestión de Seguridad de la Información** debe estar **integrado** en el **Sistema de Gestión de Calidad** que ha sido aprobado y es impulsado por la Dirección.
- La organización se apoya en la **mejora continua** tanto de los procesos productivos como de la eficacia del Sistema de Gestión en el que **prevenir los errores sea un aspecto fundamental**.

Nuestro **Sistema de Gestión de la Información**, basado en los estándares de la norma **ISO/IEC 27001:2013**, es el **marco de referencia** para el establecimiento de objetivos y actuaciones que nos **permitan una mejora continua** y que garantice la involucración **de toda la organización**, incrementando la **cultura en ciberseguridad** y logrando la **excelencia** en el **análisis, control y eliminación de riesgos** sobre los activos de información.

Los **principios de esta política** están alineados y se integran con el resto de las políticas y compromisos de gestión y ética corporativa del Grupo SEMI, siendo **aplicable a los trabajadores de todas las filiales, proveedores y empresas colaboradoras, incluyendo todos los activos de la información, tecnológicos o de infraestructuras**.

**D. Maikel García Sánchez**  
Director General

#### Políticas relacionadas:

A continuación, se detallan aquellas políticas que proporcionan principios y guía en aspectos específicos de la seguridad de la información:

- Política de protección del puesto de trabajo.
- Política de copias de seguridad.
- Política de uso de controles criptográficos.
- Política protección de datos y tratamiento información confidencial y sensible.
- Política de medidas disciplinarias por incumplimiento del SGSI.
- Política de contraseñas.
- Política de accesos.