POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PROPIEDADES DEL DOCUMENTO

Titulo documento:	Política Seguridad de la Información		
Propietario:	IT y Compliance Officer		
Aprobado por:	Dirección	Fecha aprobación:	01/09/2025

HISTORIAL DE REVISIONES

VERSIÓN	FECHA	DETALLES
1.0	01/09/2025	Versión inicial

ÍNDICE

1. FINALIDAD

PROYECTOS Y MANTENIMIENTOS MECÁNICOS, ELÉCTRICOS Y DE INSTRUMENTACIÓN, S.A. (en adelante "**MEISA**" o "la Compañía") mediante la presente Política, establece los principios y directrices con los que **MEISA** protegerá su información, de conformidad con la normativa aplicable y sus valores éticos.

La información es un activo crítico, esencial y de un gran valor. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su tratamiento.

En este sentido, se entiende por Seguridad de la Información, la salvaguarda y protección de la Información titularidad de **MEISA**; y la información titularidad de terceros, que se encuentre en los sistemas de **MEISA**.

La seguridad de la información es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos, en el que es fundamental la máxima colaboración e implicación de todos.

Los órganos de administración y de dirección, conscientes del valor de la información, están profundamente comprometidos con la política descrita en este documento.

2. ALCANCE

La presente Política se aplicará a **MEISA**, y vinculará a todo su personal (independientemente de la posición o función que desempeñen), sistemas y medios que accedan, traten, almacenen, trasmitan o utilicen información.

La aplicación de esta Política es complementaria a otras normas internas de obligado cumplimiento, como las establecidas para el Cumplimiento en Materia de Protección de Datos Personales y Privacidad, y todas aquellas relacionadas con la privacidad de la información.

3. OBJETIVOS

La presente Política constituye el marco sobre el que **MEISA** define las pautas de una protección eficaz de la información y tienes los siguientes objetivos:

- **Garantizar** el grado de confidencialidad necesario a cada clase de Información.
- **Mantener** la Integridad de la información, de modo que no sufra alteraciones con respecto al momento en que haya sido generada por los propietarios o responsables de la misma.
- **Asegurar** la disponibilidad de la Información, en todos los soportes y siempre que sea necesaria, asegurando la continuidad del negocio y el cumplimiento de cuantas obligaciones sean exigibles a Acuerdo.

4. PRINCIPIO GENERALES

MEISA entiende la Seguridad de la Información como un elemento fundamental para proteger los activos de negocio, considerándola como un proceso integral basado en la gestión y el control de riesgos con el fin de lograr sus objetivos y cumplir con su misión.

En este sentido, **MEISA** se compromete a dotar a las diferentes áreas de la compañía de los recursos técnicos, humanos, materiales y organizativos necesarios para garantizar una adecuada gestión de la Seguridad de la Información.

Para ello, el **MEISA** guiará su actuación de acuerdo con los siguientes principios:

I. Definir, desarrollar y mantener un marco integrado de controles: MEISA impulsará el desarrollo de un marco integrado de controles técnicos, legales y de gestión de la Seguridad de la Información acordes con sus objetivos y estrategias, y que permitan garantizar en todo momento el cumplimiento de los requisitos legales, reglamentarios y contractuales que le sean de aplicación.

II. Promocionar una cultura de Ciberseguridad: MEISA se compromete a promocionar de forma activa una "cultura de Seguridad de la Información" entre todos sus Profesionales y demás sujetos obligados por esta Política, y por tanto internamente y entre sus clientes y proveedores. En especial, promoverá la integración de dicha cultura en todos los ámbitos de la compañía como base de sus actividades y en relación con los productos y servicios que **MEISA** ofrece a sus clientes.

III. Gestionar permanentemente la seguridad: MEISA asume el compromiso de proteger la seguridad de las redes y sistemas de información, diseñando medidas de seguridad robustas, alineadas con las necesidades de las diferentes partes interesadas, así como con la normativa vigente aplicable en la materia, para lo cual **MEISA**, en sus procedimientos específicos se atendrá a los principios básicos de seguridad establecidos en la presente Política. Todo ello con el objetivo de identificar los riesgos y corregir todas las vulnerabilidades detectadas a fin de evitar la materialización de incidentes que comprometan la continuidad de negocio de **MEISA**.

IV. Proteger proactivamente los activos de información y asegurar la resiliencia: MEISA asumirá activamente el compromiso de lograr la salvaguarda de los niveles establecidos de confidencialidad, disponibilidad, autenticidad, trazabilidad e integridad de los activos de información de la compañía, así como para asegurar la Resiliencia Operativa Digital de **MEISA**.

V. Mejorar de forma continua la gestión de riesgos: MEISA persigue el progreso constante de todos los procesos vinculados a la gestión de riesgos en materia de Seguridad de la Información, así como de los controles para la seguridad de las redes y de los sistemas de información, analizando las vulnerabilidades, ciberamenazas e Incidentes de ciberseguridad para identificar sus causas y las mejoras necesarias en las operaciones y la continuidad de negocio **MEISA**.

5. RESPONSABILIDADES

La responsabilidad de la protección de la Información y de los Sistemas que la tratan, almacenan o transmiten alcanza a todos los niveles organizativos y funcionales de **MEISA**, en función de la medida que le corresponda, como se relacionan a continuación:

5.1 Responsabilidades de los empleados

Todos los empleados de **MEISA** deberán conocer, asumir y cumplir la Política, así como la normativa interna de seguridad y uso de los Sistemas vigentes, estando obligados a mantener el secreto profesional y la confidencialidad de la Información manejada en su entorno laboral y debiendo comunicar, con carácter de urgencia y según los procedimientos establecidos, las posibles incidencias o problemas de seguridad que se detecten.

Los empleados que contraten servicios de terceros que impliquen el uso o acceso de estos últimos a la Información deberán entender los riesgos derivados del proceso de externalización y asegurar una gestión eficaz de los mismos.

El uso de los Sistemas o servicios digitales por parte de los empleados, incluyendo expresamente el correo electrónico y los servicios de mensajería instantánea, estará limitado a fines lícitos y exclusivamente profesionales, para la realización de tareas relacionadas con el puesto de trabajo. En consecuencia, estos medios y sistemas no están destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.

5.2 Responsabilidades en relación con proveedores y otros terceros

La seguridad de la información y de los activos que la respaldan es responsabilidad de cada colaborador y de los Terceros que colaboran con **MEISA**, quienes participarán activamente en esta responsabilidad actuando éticamente en relación con la protección de la información, cumpliendo con las obligaciones contractuales en materia de seguridad de la información y garantizando que solo utilizarán la información y los sistemas de información para la finalidad establecida por **MEISA**.

5.3 Departamento de Seguridad de la Información

El Departamento de Seguridad de la Información ejercitará su función de control de manera independiente y es su responsabilidad implementar esta Política y monitorizar su cumplimiento, así como el de todos los requerimientos derivados de las leyes, normas y buenas prácticas en materia de seguridad de la Información que sean de aplicación. Por ello, es responsable de:

- Implementar una estrategia de seguridad de la Información que vele por el cumplimiento de los principios básicos de esta Política, y en particular que dé cobertura a los siguientes aspectos:
  1. Adecuado acceso a la Información, basado en el principio de mínimo privilegio y la aprobación del dueño del activo de Información.
  2. Segregación adecuada de roles y funciones en los Sistemas de Información.

3. Correcta configuración, administración y operación de la infraestructura, servicios y/o del software utilizado en todos los procesos de negocio tanto dentro como fuera de las instalaciones de **MEISA**.
4. Correcta implementación de los requisitos de seguridad durante el ciclo de vida de los Sistemas de Información que dan soporte a los procesos de **MEISA**.
5. Protección de los Sistemas y la Información que soportan frente a amenazas físicas o ambientales, en atención a su criticidad, que permita identificar, evaluar, prevenir y responder a cualquier riesgo que pueda comprometer su seguridad.

- Establecer y revisar los controles correspondientes para asegurar el cumplimiento de esta Política, incluyendo los mecanismos organizativos y tecnológicos necesarios para facilitar la monitorización continua de las actividades del acceso y uso de los Sistemas, servicios o Información gestionados por **MEISA**.
- Prevenir, detectar y responder ante cualquier incidente en materia de Seguridad de la Información.
- Establecer un enfoque de mejora continua.
- Velar por el cumplimiento con la legislación vigente en el ámbito de las competencias que le atribuye la presente Política.

5.4 Comité de Seguridad de la Información

MEISA creará un Comité de Seguridad de la Información integrado por miembros de la Dirección o quien en ellos deleguen, que, en cumplimiento de esta Política, tiene por objetivo asegurar que las buenas prácticas sobre la gestión de la seguridad se apliquen de manera efectiva y consistente en toda la organización

Entre otras funciones, asume la responsabilidad de supervisar la estrategia de Seguridad de la Información, incluyendo en su caso los planes de gasto, inversión y recursos en seguridad.

6. IMPLEMENTACIÓN

MEISA se compromete a asignar recursos específicos para asegurar la implementación efectiva de la Política.

7. CONTROL DEL SISTEMA

Las medidas de seguridad se reevalúan y actualizan periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. Asimismo, se someterá a revisiones y controles periódicos.

El Responsable de Seguridad de la Información revisa esta política anualmente o cuando hay cambios significativos que así lo aconsejen.

Las revisiones tienen en cuenta los cambios en el contexto de la organización, la evolución de la tecnología y la efectividad de la política.

8. COMUNICACIÓN DE LA POLÍTICA

La presente Política estará disponible en https://www.meisa-e.com/ para todos los empleados y para todos los grupos de interés de la organización en la web corporativa. Asimismo, la Política será objeto de las adecuadas acciones de comunicación, divulgación y sensibilización para su oportuna comprensión y puesta en práctica.

9. ACTUALIZACIÓN Y REVISIÓN DE LA POLÍTICA

La Política queda aprobada por la Dirección y será revisada y actualizada cuando proceda, con el fin de adaptarla a los cambios que puedan surgir en el modelo de negocio o en el contexto donde opere **MEISA**, garantizando en todo momento su efectiva implantación.

10. ENTRADA EN VIGOR Y DIFUSIÓN

La presente Política ha sido aprobada por la Dirección el día 1 de septiembre de 2025, entrando en vigor desde su publicación y está disponible para todos los empleados.

El Director General

Argamasilla de Calatrava, 1 de septiembre de 2025