GROUP MINGOTHINGS

Política de la Seguridad de la Información

Política Compliance

compliance@mingothings.com

Versión	Fecha de creación	Contenido	Autor	Revisado por	Confidencialidad
V0.0	24/08/2026	Versión Inicial	Carles Lorente	Chloë Tadros	Pública

Mingothings ha decidido implantar un Sistema de Gestión de la Seguridad de la Información basado en la norma **ISO 27001:2022** con el objetivo de preservar la **confidencialidad, integridad y disponibilidad** de la información y protegerla de un amplio grupo de amenazas. Este sistema está destinado a asegurar la continuidad de las líneas de negocio, minimizar los daños, maximizar la rentabilidad de las inversiones y oportunidades de negocio y fomentar la mejora continua. La Dirección de Mingothings es consciente de que la información es un activo valioso para la organización y requiere, por tanto, una protección adecuada.

La Dirección establece como objetivos de base, punto de partida y soporte de los objetivos y principios de la seguridad de la información los siguientes:

- Protección de la propiedad intelectual y datos de clientes y proveedores, garantizando la seguridad en la gestión de diseños, firmware y otros activos críticos.
- Salvaguarda de los registros de la organización, asegurando su integridad y disponibilidad.
- Protección de los datos personales y la privacidad.
- Clasificación de la información y aplicación de medidas de cifrado para la protección de datos sensibles.
- Control y seguridad en la gestión de accesos, tanto para empleados como para terceros (proveedores, subcontratistas, etc.).
- Establecimiento de auditorías periódicas internas y externas para verificar el cumplimiento de la seguridad de la información.
- Capacitación y formación en seguridad de la información para concienciar a los empleados sobre las mejores prácticas y amenazas emergentes.
- Registro y gestión de incidencias de seguridad, con mecanismos de respuesta ante ciberataques, brechas de seguridad o fugas de información.
- Gestión de la continuidad del negocio, mediante planes de contingencia y simulaciones periódicas.
- Implementación de un proceso seguro de eliminación y retención de datos, asegurando que la información se almacena sólo el tiempo necesario y se elimina de manera segura.
- Evaluación de seguridad de proveedores y subcontratistas, asegurando que cumplen con los estándares de seguridad de la información de Mingothings.
- Monitorización continua y detección de ciber amenazas avanzadas, incluyendo ataques APT, ransomware y phishing dirigido.

- Gestión de los cambios organizativos con impacto en la seguridad de la información.

Y adquiere los siguientes compromisos:

- Cumplir con los requisitos legales y contractuales aplicables a la seguridad de la información.
- Prevenir y detectar virus y otro tipos de malware, estableciendo acuerdos con organizaciones especializadas.
- Aplicar un enfoque de mejora continua en la seguridad de la información.
- Desarrollar planes de formación en seguridad y concienciación para empleados y colaboradores.
- Realizar simulaciones periódicas de incidentes de seguridad para evaluar la preparación de la organización.
- Asegurar que cualquier violación de esta política conlleva consecuencias claras, reflejadas en los contratos con empleados, proveedores y subcontratistas.
- Actuar en todo momento bajo estrictos principios de ética profesional.
- Comprometerse con la sostenibilidad y mitigación del cambio climático, reduciendo el impacto ambiental de la empresa y fomentando buenas prácticas de sostenibilidad.

Esta política proporciona el marco de referencia para la mejora continua del sistema de gestión de seguridad de la información y para establecer y revisar sus objetivos. Se comunica a toda la Organización a través de la plataforma interna de gestión corporativa y web empresarial, y es revisada anualmente o cuando concurran cambios sustanciales en el Sistema de Gestión de Seguridad de la Información.

La Política está a disposición del público en general.

Dirección

Mingothings has decided to implement an Information Security Management System based on the **ISO 27001:2022** standard with the aim of preserving the **confidentiality, integrity and availability** of information and protecting it from a wide range of threats. This system is intended to ensure the continuity of business lines, minimise damage, maximise returns on investments and business opportunities, and promote continual improvement. Mingothings Management recognises that information is a valuable asset for the organisation and therefore requires appropriate protection.

Management establishes the following basic objectives as the starting point and foundation for the information security objectives and principles:

- Protection of intellectual property and customer and supplier data, ensuring security in the management of designs, firmware and other critical assets.
- Safeguarding the organisation's records, ensuring their integrity and availability.
- Protection of personal data and privacy.
- Classification of information and application of encryption measures to protect sensitive data.
- Control and security in access management for both employees and third parties (suppliers, subcontractors, etc.).
- Establishment of periodic internal and external audits to verify compliance with information security requirements.
- Information security training and education to raise employee awareness of best practices and emerging threats.
- Recording and management of security incidents, with mechanisms for responding to cyberattacks, security breaches or information leaks.
- Business continuity management through contingency plans and periodic simulations.
- Implementation of a secure data deletion and retention process, ensuring that information is stored only for as long as necessary and is securely deleted.
- Security assessment of suppliers and subcontractors, ensuring that they meet Mingothings' information security standards.
- Continuous monitoring and detection of advanced cyber threats, including APT attacks, ransomware and targeted phishing.
- Management of organisational changes that affect information security.

And makes the following commitments:

- Comply with legal and contractual requirements applicable to information security.

- Prevent and detect viruses and other types of malware, establishing agreements with specialised organisations.
- Apply a continual improvement approach to information security.
- Develop security training and awareness plans for employees and collaborators.
- Conduct periodic security incident simulations to assess the organisation's preparedness.
- Ensure that any violation of this policy has clear consequences, reflected in contracts with employees, suppliers and subcontractors.
- Act at all times in accordance with strict principles of professional ethics.
- Commit to sustainability and climate change mitigation, reducing the company's environmental impact and promoting good sustainability practices.

This policy provides the framework for continual improvement of the information security management system and for establishing and reviewing its objectives. It is communicated throughout the Organisation via the internal corporate management platform and company website, and is reviewed annually or whenever substantial changes occur in the Information Security Management System.

The Policy is available to the general public.

Management