

	<b>POLÍTICA DE EMPRESA</b> <b>(Calidad, Medio Ambiente, Seguridad y Salud y Ciberseguridad)</b>	Documento: 003000020
		Revisión: 18
		Publico

El Grupo AKO es un grupo de empresas líder en Soluciones para la regulación, el control y la monitorización de la temperatura y la energía para la industria, refrigeración y construcción, que ayuda a sus clientes a garantizar la continuidad operativa, la seguridad de las personas y el cumplimiento normativo de sus instalaciones. Consciente de su responsabilidad con los clientes, colaboradores, partners, sociedad, accionistas y otras partes interesadas, contribuyendo al desarrollo sostenible del planeta y generando confianza a largo plazo.

Asumimos como valores la Seguridad y Salud Ocupacional de nuestros colaboradores, la Calidad de nuestros trabajos, la protección y el cuidado del medio ambiente, y la protección de la información y de los activos digitales (ciberseguridad). Para mantenerlos y reforzarlos, nos comprometemos a los siguientes 10 puntos clave:

1. Trabajar con calidad, de manera segura, saludable y responsable con las personas y el medio ambiente, cumpliendo e integrando los requisitos de las normas ISO 9001 e ISO 14001, no solo como exigencia normativa, sino como herramienta para garantizar fiabilidad, mejora continua y excelencia en el servicio al cliente. Y estableciendo un Sistema de Gestión de la Seguridad de la Información conforme a ISO 27001, como marco de referencia para el establecimiento y seguimiento de objetivos y la mejora de nuestros procesos.
2. Garantizar que nuestras actividades se desarrollen en cumplimiento de la legislación aplicable, de los requisitos de nuestros clientes y de otros compromisos asumidos por AKO Electromecánica, incluidos los establecidos en el Real Decreto 244/2016 y la Orden ICT/155/2020 (o las normas que las sustituyan o modifiquen) y incluyendo los requisitos relacionados con protección de datos y seguridad de la información cuando aplique.
3. Identificar y evaluar los peligros, riesgos y aspectos inherentes a nuestros procesos, así como los riesgos de seguridad de la información y ciberseguridad, a fin de prevenir y controlar incidentes, accidentes, enfermedades, impactos al entorno y eventos que puedan comprometer la confidencialidad, integridad o disponibilidad de la información.
4. Garantizar el respeto de los Derechos Humanos y trabajar con nuestros proveedores y partners para aplicar de forma eficiente nuestra política de responsabilidad en la cadena de suministro, incorporando criterios de ciberseguridad y protección de la información en la selección, evaluación y seguimiento de terceros.
5. Optimizar y fomentar el ahorro y la eficiencia energética en nuestras instalaciones y en las de nuestros clientes, como contribución eficaz en la lucha contra el cambio climático, aplicando asimismo prácticas tecnológicas eficientes y seguras.
6. Promover una cultura organizacional que fomente la consulta y participación activa de nuestros colaboradores en el desarrollo de las actividades del sistema de gestión, impulsando además la concienciación y la responsabilidad en ciberseguridad.
7. Proteger los activos de información (personales, comerciales y técnicos) mediante controles adecuados de acceso, uso, conservación y destrucción, así como mediante un enfoque de seguridad por diseño y por defecto en los procesos y soluciones, garantizando sistemas robustos, conectados y seguros que no comprometen la infraestructura tecnológica de nuestros clientes.

	<b>POLÍTICA DE EMPRESA</b> <b>(Calidad, Medio Ambiente, Seguridad y Salud y Ciberseguridad)</b>	Documento: 003000020
		Revisión: 18
		Publico

8. Motivar y capacitar a nuestros colaboradores y partners para que efectúen sus labores cumpliendo las disposiciones de calidad, seguridad, salud ocupacional, medio ambiente y ciberseguridad, incluyendo la formación periódica y la comunicación de buenas prácticas.
9. Establecer, probar y mejorar de forma continua los procesos de gestión de incidentes (incluidos los de ciberseguridad), continuidad de negocio y recuperación ante desastres, para minimizar impactos en nuestros clientes y en la operación del negocio, restaurando servicios y operaciones en el menor tiempo posible.
10. Realizar inspecciones, auditorías y revisiones periódicas para evaluar nuestro desempeño y mejorar continuamente la eficacia de nuestro sistema de gestión (calidad, medio ambiente, seguridad y salud y seguridad de la información), mediante la aplicación de métodos y tecnologías modernas de prevención, detección y respuesta.

AKO se compromete a garantizar la confidencialidad, integridad y disponibilidad de la información, estableciendo objetivos medibles de seguridad de la información y promoviendo la mejora continua del Sistema de Gestión de Seguridad de la Información.

Esta política será comunicada, entendida y aplicada dentro de la organización, y estará disponible para las partes interesadas pertinentes.

Esta política es responsabilidad de todas las personas que forman parte de AKO. Su cumplimiento solo es posible desde una cultura compartida de responsabilidad, colaboración y mejora continua.

La dirección y los líderes de la organización asumen un papel activo en su comunicación, aplicación y ejemplo, porque en AKO la calidad, la seguridad y la confianza no se declaran: se practican cada día.

Sant Pere de Ribes, marzo 2026

Director General  
Josep Lluís Bescós

	<p align="center"><b>POLÍTICA DE EMPRESA</b>  <b>(Calidad, Medio Ambiente, Seguridad y Salud y Ciberseguridad)</b></p>	Documento: 003000020
		Revisión: 18
		Publico

## Quality, Environment, Safety and Health, and Cybersecurity Policy

The AKO Group is a leading group of companies in solutions for the regulation, control, and monitoring of temperature and energy for industry, refrigeration, and construction, helping its clients ensure operational continuity, the safety of people, and regulatory compliance of their facilities. Aware of its responsibility towards clients, collaborators, partners, society, shareholders, and other stakeholders, contributing to the sustainable development of the planet and building long-term trust.

We embrace as our values the Occupational Safety and Health of our collaborators, the Quality of our work, the protection and care of the environment, and the protection of information and digital assets (cybersecurity). To maintain and strengthen them, we commit to the following 10 key points:

1. Work with quality, in a safe, healthy, and responsible manner towards people and the environment, complying with and integrating the requirements of ISO 9001 and ISO 14001 standards, not only as a regulatory requirement but as a tool to ensure reliability, continuous improvement, and excellence in customer service. And establishing an Information Security Management System in accordance with ISO 27001, as a reference framework for setting and monitoring objectives and improving our processes.
2. Ensure that our activities are carried out in compliance with applicable legislation, our customers' requirements, and other commitments assumed by us, including those set out in Royal Decree 244/2016 and Order ICT/155/2020 (or any regulations that amend or replace them) and including requirements related to data protection and information security where applicable.
3. Identify and assess hazards, risks, and aspects inherent to our processes, as well as information security and cybersecurity risks, in order to prevent and control incidents, accidents, illnesses, environmental impacts, and events that may compromise confidentiality, integrity, or availability of information.
4. Ensure respect for Human Rights and work with our suppliers and partners to efficiently implement our supply chain responsibility policy, incorporating cybersecurity and information protection criteria in the selection, assessment, and monitoring of third parties.
5. Optimize and promote savings and energy efficiency in our facilities and in those of our customers, as an effective contribution to the fight against climate change, also applying efficient and secure technological practices.
6. Promote an organizational culture that encourages consultation and the active participation of our employees in the development of the management system activities, while also strengthening awareness and responsibility in cybersecurity.
7. Protect information assets (personal, commercial, and technical) through appropriate controls for access, use, retention, and destruction, as well as through a security-by-design and security-by-default approach in processes and solutions, ensuring robust,

	<b>POLÍTICA DE EMPRESA</b> <b>(Calidad, Medio Ambiente, Seguridad y Salud y Ciberseguridad)</b>	Documento: 003000020
		Revisión: 18
		Publico

connected, and secure systems that do not compromise our customers' technological infrastructure.

8. Motivate and train our employees and partners to carry out their work in compliance with quality, safety, occupational health, environmental, and cybersecurity provisions, including periodic training and the communication of good practices.
9. Establish, test, and continuously improve incident management processes (including cybersecurity incidents), business continuity, and disaster recovery, to minimize impacts on our customers and business operations, restoring services and operations in the shortest possible time.
10. Conduct periodic inspections, audits, and reviews to assess our performance and continuously improve the effectiveness of our management system (quality, environment, health and safety, and information security) through the application of modern prevention, detection, and response methods and technologies.

AKO is committed to ensuring the confidentiality, integrity, and availability of information, establishing measurable information security objectives, and promoting the continuous improvement of the Information Security Management System.

This policy will be communicated, understood, and applied within the organization, and will be available to relevant interested parties.

This policy is the responsibility of everyone who is part of AKO. Compliance is only possible through a shared culture of responsibility, collaboration, and continuous improvement. Management and the organization's leaders take an active role in communicating it, implementing it, and setting an example, because at AKO, quality, safety, and trust are not merely stated: they are put into practice every day.

Sant Pere de Ribes, March 2026

Managing Director  
Josep Lluís Bescós