Information Security	SEG's Information Security Management System is managed throughout the ISO 27001/2 standards and provides to all basic day-to-day services a set of implemented controls necessary to ensure a high level of security through the constant pursuit of minimizing risks, preserve confidentiality, availability, integrity and increase the capacity for resilience in situations related to incidents and therefore to ensure continuous improvement and business continuity.
Cybersecurity	The company is equally committed to maintaining robust cybersecurity measures to safeguard its systems and data from unauthorized access, breaches, and threats. The responsibility for implementing and overseeing cybersecurity policies lies with the Chief Information Security Officer (CISO).
Data Protection	SEG is also aware of its role in Data Protection and in the use of AI capabilities. Data protection is concerned with proper handling, processing, storage and usage of personal data. The objective is to comply with applicable data protection laws and to ensure the rights of individuals with respect to their personal data. The responsibility for implementing and monitoring compliance with data protection regulations lies with the CISO supported by the Data Protection Manager.
Compliance	SEG aims to maintain a strong reputation between all their stakeholders throughout a rigorous compliance process with all contractual, legal and regulatory requirements in the sphere where it operates.
Artificial Intelligence (AI)	The company also recognizes its responsibility in ensuring that the use of AI aligns with ethical standards and complies with relevant legal and regulatory requirements. Oversight of AI governance is managed by the Data Protection Manager.
Certification	IATF 16949 and TISAX Certification helps SEG to demonstrate a commitment to Information security, strengthening trust and credibility among partners and customers.
Stakeholders	We actively engage all employees, partners, suppliers, and relevant stakeholders in understanding and adhering to our Information Security and Data Protection policies and procedures. By fostering a culture of vigilance and responsibility, we ensure that everyone contributes to maintaining the highest standards of Information Security and Data Protection.