



INFORMATION SECURITY POLICY

Our organization prioritizes the protection of critical assets such as customer information, design data, production plans, process and project information, financial records, technological know-how, applications, and software systems in packaging production and service processes as a fundamental responsibility.

The Information Security Policy aims to ensure continuous improvement throughout the organization and maintain the highest level of information security, for this purpose we are committed to:

- Ensure the confidentiality, integrity, accessibility and continuity of corporate information within authorized limits.
- Observe and fully fulfil the information security requirements required by contractual obligations and business relationships with third parties.
- Protect the confidentiality of confidential, commercial, and proprietary information belonging to the institutions/organizations we serve and their customers.
- Ensure uninterrupted business continuity by minimizing the potential impact of information security risks on business continuity.
- Protect our systems against cyber threats and continuously improving them through regular monitoring and updates.
- Act in compliance with applicable national and international legislation, sectoral regulations, and obligations arising from agreements.
- Conduct training to raise information security awareness and develop technical and behavioural competencies.
- Ensure the security of personal information.
- Maintain and continuously improve the level of information processing security through the established control infrastructure.