# Safety Protocol Information.

| | |
|---|---|
| **Purpose** | Summary of the Information Security Protocol |
| **Scope** | All processing of personal data and other information carried out by MONTEPINO LOGÍSTICA SOCIMI. S.A. and its investee companies (hereinafter referred to as "MONTEPINO"). |
| **Responsible** | General Management, Information Security Officer and Data Protection Officer |

Versions

| **Version** | Date | Content of the modification |
|---|---|---|
| **0.0** | 10/12/2020 | Initial Drafting |
| **0.1** | 14/12/2020 | Modification of the initial document |
| **0.2** | 24/03/2021 | Approval |
| **0.3** | 12/12/2023 | Update (various sections) |

## 1 COMMITMENT TO INFORMATION SECURITY

At MONTEPINO we consider information security as a strategic pillar to guarantee the continuity of our business, protect personal data and safeguard the interests of customers, employees, suppliers and investors. Information security is continuously reviewed and improved, taking into account the evolution of risks.

Within this framework, the suppliers and third parties that access, process or manage MONTEPINO's information, or that may have access to its systems, must comply with the information security requirements established by MONTEPINO, depending on the nature of the services provided and the level of access to MONTEPINO's information.

We have developed an Information Security Protocol that includes a set of policies, procedures and controls designed to protect our information assets against internal and external threats. This protocol is aligned with European and national data protection regulations, including the General Data Protection Regulation (GDPR).

## 2 PILLARS OF THE INFORMATION SECURITY PROTOCOL

- **Confidentiality:** Ensuring that information is accessible only to persons authorized to have access.

- **Integrity:** Ensuring that the information and methods of its processing are accurate and complete.

- **Availability:** Ensure that authorized persons have access to information and its associated assets, when required for the exercise of their functions.

## 3 MAIN MEASURES TAKEN

- Security controls to protect data and physical and logical access to the organization's systems and devices.
- Secure password management with multi-factor authentication.
- Regular backups and disaster recovery plans.
- Management and monitoring of security incidents, responding to them and implementing mitigation strategies.
- Classification and proper treatment of confidential information.
- Restriction of the use of external storage devices.
- Continuous training and awareness of all staff on good practices in cybersecurity.

## 4 GOVERNANCE AND COMPLIANCE

The Protocol establishes clear roles and responsibilities in terms of information security: General Management, Security Officer, Data Protection Officer and Users. These profiles collaborate in a coordinated manner to ensure regulatory compliance, risk assessment and response to possible threats or vulnerabilities.

In short, this Protocol responds to MONTEPINO's commitment to strict compliance with current regulations on information security and personal data protection, as well as to the implementation of good practices that guarantee operational continuity and the protection of the interests of all parties involved.