GENERAL INFORMATION SECURITY POLICY	Camanchaca	
	CODE	PO-CM-GTI-001
	VERSION	004
	APPROVAL DATE	30-08-23

I. Policy

This General Policy is based on the following principles adopted by Camanchaca, which must be integrated into the functions of every employee:

Strategic Principles:

1) Promote Information Security practices as an integral part of the organization's values and requirements for clients, associates, and the community.
2) Center the Information Security strategy on business requirements and objectives through a management and governance model that includes people, processes, and procedures.
3) Involve key Information Security stakeholders (information asset owners and related strategic roles) to ensure high standards of asset protection in a collaborative environment.
4) Keep the Information Security control framework current and updated, and align it with information security and corporate security controls.
5) Manage Information Security risks, whether operational, organizational, or contributed by third parties, keeping exposure within acceptable limits.
6) Ensure that cybersecurity controls are proportionate, balance cost-benefit, and facilitate and support innovation.

Operational Principles:

7) Effectively communicate the existence and characteristics, as well as the performance and compliance of Information Security controls, to all stakeholders.
8) Align corporate Information Security controls with current legislation and regulations.
9) Establish a cybersecurity culture among all personnel, including those in plants and operational environments, as well as third parties and suppliers involved in production, including due diligence obligations in employment contracts.
10) Provide an Information Security control framework that helps protect and monetize information technologies, operational technologies, and related assets.
11) Apply controls with a focus on operational continuity and integrate Information Security controls into the organization's continuity plans.
12) Address Information Security events and incidents in a timely manner to reduce financial, reputational, regulatory, and environmental impact.

II. Roles and responsibilities

Information Security Committee: This is the entity defined for the governance of IT (Information Technology) and OT (Operational Technology) cybersecurity. This includes the responsibility to sanction, validate, and approve the normative framework required for IT and OT cybersecurity management and all supervision and control activities related to Information Security programs. This committee will meet quarterly and will be composed of: Corporate IT Manager, Corporate Finance Manager, Corporate Audit Manager, IT Business Continuity Manager, Cybersecurity Engineer, and Legal Affairs Manager (optional), Corporate General Manager (optional), and Business Unit General Managers (optional). Its scope of action and responsibilities will be defined in a specific regulation.

Board of Directors Committee: To oversee the company's cybersecurity and information security strategy, as well as participate in sessions to evaluate and analyze various risks, whether operational, financial, technological, etc.