INFORMATION SECURITY – 2023 Highlights

Information security is a key part of the strategic and operational management of our businesses to reduce any exposure to risks associated with the matter.

Our concern extends to our businesses, given that a cyber-attack on the gas supply service, for instance, can affect supply to customers, hospitals, and industries, causing significant damage to society.

For this reason, we dedicate significant effort to the development of mechanisms for protecting the data and systems that manage our operations.

The management of this issue has been structured to integrate all our companies.

The Chief Information Security Officer (CISO) operates in a matrix manner, reporting simultaneously to the Finance and Investor Relations Vice Presidency while collaborating with the Business Information Security Officers (BISOs) of each subsidiary.

Governance on the matter consists of reporting and frequent alignment of identified risks and process improvements with portfolio companies on a tactical basis. **Strategic reports are made monthly to the Executive Board and quarterly presented to the Board of Directors, contributing to better management of information and cyber security of our operations and data protection, placing the matter at the heart of the Company's strategic discussion.**

The current governance and operating model brings several benefits to Grupo Cosan companies, such as operational cost synergy, a unified threat intelligence center, a multidisciplinary team (technicians, specialists, and business interactions), and technologies. In this regard, we have developed standardized strategies, policies, rules, risk management methods, and education programs (Guardian Program) that are compatible and replicable for all portfolio companies.

Guardian Program

An institutional initiative that brings the information security agenda to the heart of the company. It aims to present, discuss, and introduce concepts and habits related to information security to all people working in the Group.

In 2023, we continued with our planning initiated in 2021 with strategic projections until 2025, with an annual review seeking alignment with best market practices.

12 phishing tests

16 cyber-attack simulation and crisis management

98% of adherence to the Knowledge Trail applied to all employees

In the last three years, no incidents or cases of internal data leaks have been recorded.

We have consolidated the operation of information and cyber security for our operational and industrial environments (OT Security) along with the implementation of phase 2 (industrial expansion). The database protection project stood out this year with the completion of its first phase, thus enhancing security and monitoring 24x7 focusing on critical systems affecting operations. **We exceeded our 2023 goal and raised our maturity to level 3.3 (scale of 0 to 5 based on CMMI and NIST Framework), which means significant governance, with more critical processes and controls, cyber crisis tests and simulations, and vulnerability management with technological intelligence, with constant improvement of 24x7 monitoring with responses to incidents and more sophisticated attacks.**

The Security Maturity Program provides for annual independent assessment.

Evolution in security maturity rating is a goal tied to variable compensation for all employees, including leaders and executives. This program includes key international frameworks such as NIST-CSF, ISO 27001/2, and CIS Controls.

Guardian

Awareness among teams and the identification of possible attack attempts are key assumptions to support our protection measures. **Throughout the year, actions and practices of continued education, awareness, and engagement were carried out to assess employees' behavior regarding malicious links and equip the team with information and care on the subject, covering everyday situations (personal life) and the most well-known threats targeted at corporate environments.**

The new Guardian program started in the second half of 2023, extending as a strategic part until 2025. This strategy is born with the purpose of integrating the initiative into the executive agenda, as well as positioning Guardian as an institutional narrative and an integral part of business security, with CEOs and senior executives of the businesses as the main spokespersons.