Cybersecurity

At Largo, we understand the importance of securing our information systems against malicious attacks, and of protecting any confidential information that we may have collected from our employees and stakeholders.

Our **Information Security Policy** in Brazil defines our strategy for protecting the integrity, availability and confidentiality of information. This strategy is based on the detection, prevention, monitoring and incident response and strengthens cybersecurity risk management and building a robust foundation for the increasingly digital future for Largo. This policy is based on the ISO 27001 and 27002 standards.

We implement robust technical and organizational measures to prevent unauthorized access, data loss, and cyber threats. To date, we have recorded no information security breaches, including incidents involving third parties.

Our **Data Protection and Privacy Program** is designed to ensure compliance with applicable legislation, including Brazil's General Personal Data Protection Law (LGPD). This program includes periodic assessments of departments that handle personal data and the development of action plans to address identified risks. We also provide targeted training on data protection principles to relevant teams.

To enhance our resilience, Largo has established a comprehensive **Cybersecurity Contingency Plan**, which includes a **Disaster Recovery Policy** that outlines procedures for incident response, business continuity, and system recovery across a range of scenarios. In addition, we maintain cyber insurance coverage as a risk mitigation measure.

Employees play an active role in our cybersecurity posture. We operate a formal IT ticketing system that allows employees to report suspicious activity, enabling proper documentation, investigation, and escalation to senior IT personnel.

To foster a strong security culture, we run an internal information **security awareness program**, known as *Hacker Rangers*, aimed at educating employees on cybersecurity risks and best practices in everyday operations.

Largo continuously evaluates and improves its cybersecurity and data protection protocols to remain aligned with evolving threats, technological advancements, and regulatory requirements.