



**Prosegur
Compañía de
Seguridad, S.A.
Information
Security and
Cybersecurity
Policy**

1. Scope

The Board of Directors of Prosegur Compañía de Seguridad, S.A. ("**PCS**" or the "**Company**") has the non-delegable power of determining its general policies and strategies, including the Information Security and Cybersecurity Policy for the Company and its subsidiaries (the "**Group**").

The Company's Board of Directors has approved this Information Security and Cybersecurity Policy (the "**Policy**"), which sets out the main aspects and commitments of the Company and its Group in relation to information security and cybersecurity.

In accordance with the Regulations of the Board of Directors, the Sustainability, Corporate Governance, Appointments and Remuneration Committee is responsible for overseeing the application of this Policy, assessing its effectiveness regularly and proposing the adoption of suitable measures to the Board of Directors to update it and resolve any weaknesses.

This Policy applies to all physical locations, employees, third parties with which the Company has contractual relations, and technology assets in the countries where the Company and its Group operate and will operate in future through organic and inorganic growth.

2. Purpose

The pillars on which the Company and its Group base the protection of its information and the assets associated with its processing and management are its commitment to the highest ethical standards and compliance with national and international best practices in information security and cybersecurity, and the values of the Company and its Group (proactivity, commitment, value creation, customer-centric approach, transparency, excellence, leadership, teamwork, and the brand).

As part of its commitment to transparency, the rules and main policies in the Company's corporate governance system, including this Policy, are permanently available to the market, shareholders, and investors on its corporate website (www.prosegur.com).

The purpose of this Policy is to establish the basic principles and general framework for managing information security and cybersecurity, improving resilience, ensuring an appropriate response to risks and associated cyber-risks, and preserving the values associated with information and information systems—confidentiality, integrity, availability, authenticity, inclusivity, and traceability—at all times.

3. Details

By establishing this Policy, the Company and its Group undertake to:

- 🌐 **Comply with all applicable legal and regulatory requirements**, particularly with regard to intellectual property rights, security and privacy.
- 🌐 **Define, develop and implement technical and organizational controls** to protect the assets and data of the Company, its Group and its customers.
- 🌐 Align security with the **business** objectives established by the Company and its Group.
- 🌐 **Define the general** guidelines for action to avoid threats **and react to** information security incidents.

- **Keep in contact with the authorities** through the appropriate channels.
- **Manage the assets** of the Company and its Group from acquisition through identification, classification, prioritization, custody, transport and disposal.
- **Keep its facilities protected** from physical and environmental threats through security controls.
- **Perform security audits** to review compliance over time, and to **certify our systems and products under the main standards**.
- **Monitor the systems and networks of the Company and its Group** to prevent unauthorized access, third-party attacks and other causes that might compromise them.
- **Inform and raise awareness** among all employees of the information security strategy, creating a culture of information security among employees, partners and suppliers.

The Board of Directors of the Company will approve any other corporate regulations, policies or programs it deems necessary or appropriate to ensure the correct functioning of the Company and its Group.

This *Information Security and Cybersecurity Policy* was approved by the Company's Board of Directors on July 27, 2023.