



Prosegur Group's Business Continuity Policy

1. Purpose

The objective of the Prosegur Group's Business Continuity Policy. (the **"Prosegur"**) (the **"Business Continuity Policy"**) is to establish the basic principles for developing, implementing, controlling, reviewing, maintaining and improving the Business Continuity Management System (**"BCMS"**) of the Company and its group that enable an adequate and timely response to the materialization of a risk (security, technological, cyber, health, environmental, etc.) material or catastrophic situation on employees, critical assets (including armoured vehicles and offices and buildings), technology, information or critical suppliers of the Company and its Group.

The Company is aware and acknowledges that the materialization of such risks could interrupt its activities and significantly affect the provision of services by the Company and its Group. To this end, this Policy aims to establish the basic principles of the BCMS of the Company and its Group with the aim of trying to minimise the consequences that may arise from the occurrence of such risks, restoring the aforementioned services to previous levels and within the agreed times.

2. Scope and scope

This Business Continuity Policy applies to the Company and to the companies in its group in which Prosegur has control (the **"Group"**). Notwithstanding the foregoing, Group companies which, in accordance with specific regulatory provisions, have to have their own business continuity policy are excluded from its scope of application. In any case, these policies must be in accordance with the principles included in this Business Continuity Policy.

3. General principles

The Business Continuity Policy is based on a set of principles and commitments that are set out below:

- Ensuring the integrity and protection of people is the priority objective, both in normal situations and in the event of a crisis.
- Minimise the impact on essential businesses or lines of activity that could arise from the materialisation of risks.
- The BCMS shall provide for the necessary mechanisms to identify, prevent, manage, reduce, mitigate and/or control and quantify (based on impact analyses) critical continuity risks (including ICT risks) in accordance with the defined risk tolerance and appetite and in accordance with the principle of proportionality, taking into account the impact on continuity of services; activities and operations of the Company and the Group that may be affected. The BCMS must allow the identification of the assets necessary to allow business continuity, including assets.
- Develop and implement this Business Continuity Policy in Business Continuity Plans in an appropriate manner for each of the main business lines of the Group companies that are bound by this Policy, establishing in a protocolized and detailed manner the response to the materialization of the different material risks and that said Business Continuity Plans include appropriate communication procedures, both internal and external, which enable the correct execution of the same and the timely provision of information to all interested parties.
- Review and update the BCMS and Business Continuity Plans on a regular basis or in the event of significant changes in regulations, lines of business, processes or critical assets of the organization according to the applicable requirements and taking into account the context and needs of each business or after the results of the analyses or tests.

- As part of the process of confirming the degree of reliability and continuous improvement of the BCMS, carry out tests of the Business Continuity Plans on a regular basis.
- Ensure the participation of the Management of each of the business lines and all the areas involved in the critical processes of the organization, for the identification and analysis of the associated risks, as well as the review and continuous improvement of the OH&S.
- For the main business lines of the Group's companies, set up a Business Continuity Committee made up of people and area managers with the appropriate knowledge and experience, who will have the coordination and support responsibilities necessary for the maintenance of the BCMS and the effective management of processes in the event of an incident.
- Provide appropriate communication plans to be communicated to third parties and other interested parties, including the procedures, responsibilities and activities developed in the field of Business Continuity in the organization, through the different communication channels and procedures, both internal and external, established by the company.
- Establish and implement business continuity strategies and measures that ensure the recovery of critical activities and processes in a protocolized, coordinated, and efficient manner in the event of an incident.
- To promote the knowledge and learning of the management and staff affected by the BCMS, in the field of Business Continuity, through the implementation of a training plan.
- Ensure compliance with the applicable legislation and regulations in force on Business Continuity and, in particular, with the DORA and NIS2 regulations or similar, as applicable to the different companies of the Group.
- To collaborate with the authorities in the event of disaster or need, as part of the spirit of service that permeates all the actions of the Group's companies and their responsibility towards the society in which they operate.
- Ensure that the critical suppliers of the main business lines of the Group's companies (and, in particular, the critical ICT suppliers) have, in turn, a Business Continuity Plan that allows them to reasonably continue providing the critical services provided to the Company and its Group.
- The Group companies that are bound by this Policy will apply the principles and commitments set out in this policy in accordance with the principle of proportionality, taking into account their size and overall risk profile, as well as the nature, scale and complexity of their services, activities and operations

4. Approval, dissemination and knowledge of this Policy

This Business Continuity Policy was approved by the Company's Board of Directors on October 29, 2025.

This Policy will be published on the Company's corporate website and intranet.

The content of this Policy may be included among the training subjects for its own staff and in additional dissemination actions, as determined at any given time.

5. Preparation

Owner:	Head of the Business Continuity Management System of the Prosegur Group		
Reviewed by:	Prosegur CISO Global Management	Corporate Legal Area	
Approved by:	Board of Directors of Prosegur Compañía de Seguridad, S.A.	Date:	29/10/2025