INFORMATION SECURITY POLICY

FUND & CLAIM S.L, a company dedicated to the provision of advisory services in legal matters of all kinds, including economic, tax, financial and business fields, and to the extent permitted by law, both to individuals and legal entities. Has decided to implement an Information Security Management System based on the ISO 27001 standard with the aim of preserving the confidentiality, integrity and availability of information and protecting it from a wide group of threats.
This Management System is intended to ensure the continuity of business lines, minimize damage, maximize return on investments and business opportunities and continuous improvement.

The Management of **FUND & CLAIM S.L** is aware that information is an asset that has a high value for the Organization and therefore requires adequate protection.

The Management of **FUND & CLAIM S.L** establishes the following as basic objectives, starting point and support for the objectives and principles of information security:

- The protection of personal data and privacy of people
- Safeguarding organizational records
- The protection of intellectual property rights
- Documentation of the information security policy
- The assignment of security responsibilities
- Training and training for information security
- The registration of security incidents
- Business continuity management
- The management of changes that may occur in the company related to security

The Management of **FUND & CLAIM S.L**, through the development and implementation of this Information Security Management System, acquires the following commitments:

- Develop products and services that comply with legislative requirements, identifying the legislation applicable to the business lines developed by the organization and included in the scope of the Information Security Management System.
- Establish and meet contractual requirements with interested parties.
- Define security training requirements and provide the necessary training in this area to interested parties by establishing training plans.
- Prevent and detect viruses and other malicious software, by developing specific policies and establishing contractual agreements with specialized organizations.
- Manage business continuity, developing continuity plans in accordance with methodologies of recognized international prestige.
- Establish the consequences of violations of the security policy, which will be reflected in the contracts signed with interested parties, suppliers and subcontractors.
- Act at all times within the strictest professional ethics.

This Policy provides the framework for continuous improvement of the Information Security Management System and for establishing and reviewing the objectives of the Information Security Management System. It is communicated to the entire Organization through the document manager installed in the organization and its publication on information panels, being reviewed

annually for its adequacy and extraordinarily when special situations and/or substantial changes occur in the Information Security Management System. being available to the general public.

Madrid, december 20th 2023

El Responsable de Seguridad de la Información