

Information for third parties interested in the Group's Cyber Security and Information Security policy

Contents

Version Control	3
Introduction	4
Scope	4
Rationale and objectives: commitments and initiative	5
Governance framework	6
Core principles	7
Governance	7
Suppliers (Technological risk).....	7
Information security	8
Cybersecurity operations	8
Cybersecurity monitoring	8
Technological and non-technological resilience.....	8
Information security reviews, cybersecurity, assessments and testing	8
Cyber security training and awareness (internal and external)	9
Project security and continuity	9
Technological change management	9
Crisis management and communication	9
Technological risk.....	9
Indicators and KRIs	10
Certifications and benchmark standards.....	10

Version Control

Version	Date	Description
1	31.05.2026	First summarised version of the Cyber Resilience Governance Framework

Introduction

Grupo Cooperativo Cajamar (hereinafter, the “Group”) has established a framework to guide its actions in the field of cyber resilience, understood as the ability to withstand, protect and defend information systems against attackers and technological risks, through a governance model comprising an Operational Resilience Strategy and three corporate policies: (i) Cybersecurity and Information Security Policy, (ii) Technology Risk Management Policy and (iii) Operational Resilience Policy.

Information is an essential asset for the Group’s operations. Therefore, our approach is aimed at ensuring the authenticity, confidentiality, integrity, availability and traceability of the information processed and held in the course of our business processes and services.

The strategy and framework for action in the areas of cybersecurity, information security, technology risk management and operational resilience are backed and supported by the Board of Directors and senior management, who are responsible for ensuring their proper implementation, execution and maintenance.

The Group implements this model with the aim of safeguarding its core functions, ensuring the continuity of its services and strengthening the confidence of customers, members and supervisory bodies, through an integrated approach that combines technology risk management, information protection and the ongoing strengthening of its operational resilience capabilities.

Scope

The governance framework comprising the Operational Resilience Strategy and the three Policies mentioned above is mandatory for all Group employees, regardless of their hierarchical level or their functional or geographical location. It also extends to interns, those on work experience, subcontractors and, in general, all those who work or provide services within the Group or in companies providing services to the Group when they use information owned and/or managed by the Group.

The scope also covers suppliers and third parties who access the Group’s systems, networks, services or information, in accordance with the terms set out in internal regulations and the relevant contractual and service level agreements.

Furthermore, the Technology Risk Management Policy applies to all technology systems, digital infrastructure, business processes, technology service providers and the organisation’s staff, including external contractors and strategic partners.

Rationale and objectives: commitments and initiative

The Group must comply with current legislation and with the requirements of supervisory bodies and competent authorities in the areas of information security, cyber security, digital operational resilience and personal data protection. To this end, its policies are based on the most relevant regulatory frameworks, notably DORA and its technical guidelines, the GDPR and the LOPDGDD, the EBA's guidelines on ICT risk, security, internal governance and outsourcing, the National Security Framework, TIBER-EU/TIBER-ES, the ECB's cyber resilience expectations and, where applicable, international standards such as NIST, among others.

In this context, the Group's cyber resilience model establishes a comprehensive framework for preventing, protecting against, detecting, responding to and recovering from technological risks and cyber threats, aligning these capabilities with the organisation's strategic objectives and risk appetite.

The Operational Resilience Strategy sets out the overall framework through which the Group manages ICT-related risk and strengthens its ability to prevent, respond to and recover from disruptions. To this end, it incorporates the definition of tolerances, objectives, indicators, technological architecture, incident management, resilience testing and communication mechanisms.

The Cybersecurity and Information Security Policy sets out the corporate framework for protecting the Group's information assets, ensuring their confidentiality, integrity, availability and traceability. Its aim is to ensure effective threat management, in line with the Group's strategy and based on a model of continuous improvement that strengthens the ability to anticipate, withstand and recover from incidents.

The Technology Risk Management Policy sets out the framework for identifying, assessing, managing, monitoring and reporting risks arising from the use of technology. Its aim is to ensure a structured and consistent approach to managing these risks, in line with the Group's risk appetite and designed to protect its processes, systems and services.

The Operational Resilience Policy sets out the Group's framework for business continuity and response to disruptive events that may affect its essential functions. Its aim is to ensure the ability to maintain or restore operations to acceptable levels through business continuity, disaster recovery and crisis management plans.

Governance framework

The Group has a governance model that enables it to comprehensively oversee, coordinate and control its capabilities in the areas of cybersecurity, technology risk management and operational resilience. This model sets out distinct roles and responsibilities, ensuring informed decision-making, consistent implementation of measures and ongoing monitoring of the control framework.

The governance framework provides for a formal and regular reporting system to the Group's governing bodies. In particular, on a regular basis and additionally whenever circumstances require, the Board of Directors receives structured information on developments in technological and cybersecurity risk, the status of the cybersecurity control environment, the main incidents and vulnerabilities, the results of audits and assessments, the progress of action plans, and the most relevant indicators and KRIs.

Set out below are the key responsibilities and functions of the bodies involved in the cyber resilience governance model, which should be taken into account by those bodies and departments that play a role within the cybersecurity governance framework.

- The Board of Directors bears ultimate responsibility for the Group's cybersecurity, technological risk and operational resilience framework. It is responsible for approving policies and strategies in this area, overseeing their implementation and periodically reviewing whether adequate resources, capabilities and training are in place to ensure their proper implementation.
- The Technology and Cybersecurity Committee is responsible for providing information, advice and recommendations to the Board of Directors on matters relating to technological risk, cybersecurity and technology strategy. It monitors key exposures, the progress of response and recovery plans, and technological issues relevant to the Group.
- The Risk Committee oversees and reviews the Group's overall risk profile, including risks arising from technology. Its role helps to ensure that risk-related decisions are taken with a holistic approach, consistent with the organisation's risk appetite and strategic objectives.
- The Management Committee acts as a link between the Group's governing bodies and its executive departments, driving forward action plans and monitoring the implementation of approved policies. In this area, it monitors developments in cybersecurity, operational resilience and technological risk, and facilitates the implementation of strategic guidelines into day-to-day management.
- The Cybersecurity and Operational Resilience Committee coordinates and monitors strategic initiatives relating to information security, cyber resilience and business continuity. It also reviews regulatory proposals, oversees improvement initiatives, regulatory reports, test plans and action plans arising from audits or certifications.
- The Technology Risk Committee monitors Group's most significant technological risks and assesses the associated treatment and remediation proposals. It also analyses alerts, indicators and risks relating to technology

suppliers, and assesses whether the measures adopted are appropriate in light of the level of risk defined by the organisation.

- The Cyber Resilience Department, led by the CISO, defines and maintains the Group's framework for information protection, cybersecurity, technological risk and operational resilience. Its responsibilities include advising governing bodies, defining controls and methodologies, managing incidents, monitoring threats, and promoting training and awareness.
- The Technology and Processes Division drives the practical implementation of the technical and organisational measures required to comply with the applicable regulatory framework in the areas of cybersecurity, information security and operational resilience. Its role is crucial in ensuring that control requirements are incorporated into the design, operation and development of technology services.
- The Internal Audit Division carries out independent reviews of the management and control systems relating to cybersecurity, technological risk, operational resilience, business continuity and crisis management. It helps to verify the effectiveness of the framework put in place and promote its continuous improvement.

Core principles

The core principles of the Group's cyber resilience model are organised into the following areas, which cover the governance, protection, operation and resilience of technological and business capabilities:

Governance

The governance framework sets out how oversight, decision-making and the allocation of responsibilities are organised in relation to cybersecurity, technological risk and operational resilience. Its purpose is to ensure that there are clear roles, oversight by the relevant bodies, and management that is aligned with the Group's strategy and control framework.

Suppliers (Technological risk)

This area focuses on ensuring that services provided by third parties are managed with appropriate levels of security, continuity and control. To this end, requirements are set out in agreements with suppliers, along with mechanisms for monitoring, assessing and verifying compliance with these requirements, in accordance with the applicable risk-based approach and the terms set out in each contractual relationship.

Information security

The aim of information security is to protect the confidentiality, integrity, availability, authenticity and traceability of the Group's information. This section sets out the principles and measures necessary to ensure the proper use of information assets and to prevent unauthorised access, alteration or disclosure.

Cybersecurity operations

Cybersecurity operations encompass measures aimed at preventing, detecting, containing and responding to threats or incidents affecting IT systems and services. These include, among other things, vulnerability management, asset protection, secure configuration and the implementation of technical security controls.

Cybersecurity monitoring

This area focuses on the continuous monitoring of technological activity to identify anomalous behaviour, threats, incidents or potential vulnerabilities. Its aim is to facilitate early detection and a timely response, thereby strengthening the organisation's preventive and reactive capabilities.

Technological and non-technological resilience

Technological and non-technological resilience encompasses the Group's ability to maintain or restore its essential functions in the event of disruptions, whether these stem from ICT systems or from people, processes, facilities or suppliers. Its aim is to ensure business continuity through appropriate plans, resources, and response and recovery measures.

Information security reviews, cybersecurity, assessments and testing

This area involves carrying out periodic reviews and tests designed to verify the robustness of the information security and cybersecurity framework, as well as its actual capacity to respond to crisis scenarios, including internal and external audits, breach analyses and technical reviews that enable the identification of weaknesses and the validation of existing controls; in addition, specific operational resilience tests—both technological and non-technological—are carried out, such as recovery tests, advanced TLPT-type exercises in accordance with TIBER-EU/TIBER-ES, and penetration tests, with the aim of practically assessing the effectiveness of the measures implemented across all phases of prevention, response and recovery, and identifying opportunities for continuous improvement.

Cyber security training and awareness (internal and external)

Training and awareness-raising aim to strengthen safety knowledge and culture among all those involved in the Group's activities. This area promotes compulsory and regular training to reduce errors, encourage safe behaviour and ensure that employees and relevant groups are aware of their responsibilities. Furthermore, the Group develops and runs regular security awareness programmes involving both staff and members of the Board of Directors, with the aim of ensuring a proper understanding of the risks associated with information security and their effective management.

Project security and continuity

This area aims to ensure that technology projects incorporate security and business continuity requirements, from their earliest stages, in line with the criticality of the services concerned. This helps to ensure that new initiatives, changes or developments are implemented in a safe and controlled manner, in line with the Group's resilience requirements.

Technological change management

Technology change management governs how changes to technology systems and services are to be assessed, approved, tested, documented and implemented. Its aim is to minimise risks, prevent unintended consequences and ensure that technological development takes place in a controlled manner.

Crisis management and communication

This area sets out the mechanisms required to trigger an organised response to serious situations that could disrupt the Group's normal operations. This includes coordinating actions, defining roles, and managing internal and external communication with stakeholders and, where appropriate, with the relevant authorities. These mechanisms enable recipients to report immediately any incidents, vulnerabilities or anomalous behaviours detected, ensuring that these are assessed, addressed and monitored and, where appropriate, that measures are put in place for containment, recovery, internal or external communication, and escalation to the relevant bodies.

Technological risk

Technological risk refers to the range of threats arising from the use, management or reliance on technology that may affect the Group's processes, services or assets. This area establishes the framework for identifying, assessing, managing, monitoring and reporting these risks in a structured manner that is aligned with the organisation's risk appetite.

Indicators and KRIs

Indicators and KRIs allow the Group to measure the effectiveness of the control framework and monitor exposure to risk in the areas of cybersecurity, technology and operational resilience. Their purpose is to facilitate regular monitoring, support decision-making and detect deviations or signs of deterioration at an early stage.

Certifications and benchmark standards

The Group is strengthening its cyber resilience framework by adopting internationally recognised standards and reference frameworks to enhance its security and resilience framework. These include certifications and accreditations such as ISO 27001, ENS Alto, PCI DSS and PCI PIN, which help to consolidate an approach based on control, continuous improvement and alignment with industry best practice.

This model enables the Group to offer reliable, secure and resilient services, even in adverse environments or in the event of technological incidents, thereby helping to protect its customers, ensure business continuity and comply with regulatory requirements.