

1. OBJECTIVE

To define the guidelines for the Information Security and Cybersecurity Management System (ISMS) at Grupo Aval Acciones y Valores S.A. and its subsidiaries (the Group), in order to preserve the pillars of information security: confidentiality, integrity, availability, and privacy of information assets, while ensuring compliance with regulatory, legal, and statutory requirements.

2. SCOPE

This policy applies to the Group, as well as to temporary employees and suppliers who, in the performance of their duties, use information and technological services and who must adopt this policy in accordance with the nature, size, complexity, risk appetite, and structure of their operations.

3. STATEMENT OF COMMITMENT

The Group is committed to implementing this policy, which is based on the structured and strategic management of risks associated with the business and its relationships with suppliers, as well as on the prevention of potential damage to its image and reputation.

4. GENERAL GUIDELINES

General

The following guidelines apply to the Group and provide direction for the management of information security and cybersecurity:

- Protect its assets against potential threats, vulnerabilities, events, and incidents that could affect information security.
- Promote ongoing training and individual accountability in the handling of information.
- Ensure secure relationships with suppliers and manage the information security and cybersecurity risks associated with its supply chain by requiring compliance with information security standards and promoting collaborative management of shared risks.
- Adopt emerging technologies with a security-first approach, assessing risks from the design phase and ensuring data protection throughout its entire lifecycle.
- Ensure the application of information security and cybersecurity requirements in business continuity and disaster recovery by leveraging the resilience strategy.
- Establish the general framework for managing the ISMS, ensuring its alignment with business requirements, the guidelines defined in this policy, and applicable laws and regulations.
- Establish guidelines for the consistent protection of information, taking into account the assessment and classification of critical information assets and the associated risk levels.
- Based on risk analysis, strategies, and projects, establish the implementation of controls that safeguard the pillars of information.
- Implement a risk management methodology, which must include the following stages: identification, measurement, monitoring, and control. This process must be carried out at least once a year or when special circumstances arise.
- Implement a process to regularly monitor risk profiles and exposures to significant losses.
- Conduct information security assessments based on recognized norms, standards, and/or reference frameworks that support information security and cybersecurity management—such

as the ISO 27001/IEC standard and the NIST Cybersecurity Framework—in order to evaluate the entities' current level of security and maturity.

- Comply with current regulations applicable to each Group entity regarding information security and cybersecurity.
- Comply with the communication protocol of the Corporate Vice-Presidency of Risk and Compliance, using mechanisms such as general instructions and guidelines.
- Ensure the timely submission of reports required for monitoring the ISMS, in accordance with the established deadlines and the communication protocol defined by the Corporate Vice-Presidency of Risk and Compliance.
- Immediately report to Grupo Aval any information security or cybersecurity incident that may affect or has affected the confidentiality, integrity, availability, or privacy of the entity's information. This notification must be made in accordance with the classification and severity criteria established by the Executive Incident Response Group (GERI) structure, ensuring its timely escalation.
- Maintain a consolidated and up-to-date database of all information security and cybersecurity incidents, as well as those related to the impact on personal data, in accordance with the information privacy pillar, classified by type of incident and/or security event, level of impact, and the remediation plan implemented. Likewise, the management of such incidents must include root cause analysis, lessons learned, and follow-up on remediation plans. This database must be properly labeled and/or protected, ensuring the confidentiality and sensitivity of the information it contains and enabling effective management of associated risks.
- Develop and periodically implement information security and cybersecurity culture plans, as well as communication strategies aimed at employees.
- Assess and manage the risks associated with the use of emerging technologies, including solutions based on Artificial Intelligence (AI), ensuring that their use complies with criteria for information security and cybersecurity, data protection, regulatory compliance, and the responsible use of information.
- Establish indicators with their respective thresholds for monitoring the Information Security and Cybersecurity Risk Management System.

Protection of confidentiality, integrity, availability, privacy, and non-repudiation of information

- Keep information protected through minimum acceptable controls in accordance with each entity's risk appetite.
- Implement validation mechanisms, continuous verification, and technologies that strengthen the integrity of data.
- Ensure the accessibility of information and services when needed through resilience strategies such as proactive monitoring, disaster recovery, and scalability.
- Protect personal data in both manual and automated processes, as well as in big data analytics using emerging technologies, ensuring transparency, consent, data processing in accordance with its lifecycle, and protection against bias, in compliance with ethical and regulatory principles.
- Maintain traceable records and evidence of every transaction or interaction with the information, using mechanisms such as digital signatures or technologies that guarantee the authenticity, integrity, and accountability of the actions performed.

Implement and maintain the Risk Management System

- Use the COSO (Committee on Sponsoring Organizations of the Treadway Commission) model as the internal control framework, in accordance with the Comprehensive Management Policy, ensuring its proper implementation and operation.
- Adopt a systematic, structured, and dynamic approach that enables continuous improvement of the system, informed decision-making, and the efficient allocation of resources.
- Implement and maintain a third-party risk management process that includes the identification, measurement, monitoring, and control of risks associated with suppliers and their supply chains, according to their level of criticality and impact on the Entity.
- Manage information security and cybersecurity risks in accordance with risk appetite, tolerance levels, and maximum capacity, taking into account the nature of operations and business lines.

Manage Change

- Ensure the existence of a change management process that incorporates security-by-design and security-by-default principles, including the identification of threats, as well as the assessment, classification, and mitigation of information security and cybersecurity risks associated with changes to processes, channels, products, services, applications, and critical information systems. This process must be aligned with the established risk management methodology and integrated into a change review and approval framework, where the resulting risks are assessed and their treatment defined.

Control and Mitigate

- Maintain a control environment aligned with the COSO model, structured through policies, procedures, standards, and systems, as well as clearly defined roles and responsibilities.
- Implement a continuous vulnerability management process that includes identification, analysis, prioritization, and treatment of vulnerabilities, ensuring timely remediation.
- Conduct periodic cybersecurity drills that simulate scenarios such as denial-of-service (DDoS) attacks, ransomware, malware, and attacks on cloud services, among others. These must be coordinated with business continuity and disaster recovery plans, as well as with the Corporate Cybersecurity Incident Management Protocol administered by Aval Valor Compartido (AVC) and must include validation of the recovery of critical services, business continuity, the effectiveness of response plans, and the ability to recover from cybersecurity incidents.
- Ensure the timely recovery of services and information assets in the event of information security and cybersecurity incidents, in accordance with established corporate guidelines.

Security in New Technologies and Emerging Risks

- Establish security policies or guidelines for the adoption and use of new technologies, taking into account the associated risks.
- Adopt procedures for identifying, classifying, managing, and administering users of critical information assets (crown jewels), as well as defining those responsible for and the owners of the information, to enable the determination and application of security controls in the use of new technologies.
- Incorporate security from the initial stages of design and development by applying security principles, as well as implementing post-deployment monitoring, detection, and recovery measures to ensure resilience.

- Establish the management and monitoring of cyber risks and supplier risks arising from the implementation of new technologies.
- Ensure that environments used for business continuity have minimum information security controls equivalent to those established for production environments, in order to minimize exposure to vulnerabilities and protect information during contingency scenarios in accordance with corporate guidelines.
- Oversee the performance of automated systems, ensuring that these systems comply with regulatory requirements and the organization's security policies.

4.1 INVESTIGATIONS AND SANCTIONS

The Group acknowledges that any breach of this policy, as well as of activities and procedures related to information security and cybersecurity, will be subject to a thorough investigation to determine the causes and corresponding responsibilities.

5. ROLES AND RESPONSIBILITIES

The Group must comprehensively structure the functions and responsibilities associated with risk management in accordance with the three-lines model, taking into account: (i) the management exercised by each business line, (ii) the management of risk and compliance areas, and (iii) the independent review function of management, in accordance with the provisions of the Comprehensive Policy for Risk Management and Compliance.

In this context, and to fulfill the objectives of this policy, the following key actors in information security and cybersecurity management have been identified:

Board of Directors of the entities or the body acting in its stead

Without prejudice to the functions assigned in other provisions, it is the responsibility of the Board of Directors or the body acting in its stead to:

- Approve the Information Security and Cybersecurity Policy and its updates.
- Provide the necessary resources for the proper management of the ISMS.
- Review and comment on the ISMS management reports.
- Issue a ruling on the periodic Information Security and Cybersecurity assessment conducted by the oversight bodies.
- Issue, when deemed appropriate, guidelines for improving Information Security and Cybersecurity Management.
- Participate in ISMS awareness and training programs.

Risk Committee and Cybersecurity Officer of the Board of Directors of Grupo Aval Acciones y Valores S.A.

- Monitor the results of information security and cybersecurity management and issue the corresponding recommendations when necessary.
- Recommend to the Board of Directors corrective and/or improvement actions regarding Information Security and Cybersecurity issues when there is a foreseeable risk that could impact Grupo Aval or its subsidiaries.

- Present to the Board of Directors the results of corrective and/or improvement actions taken when deemed necessary due to their materiality.

Senior Management of the Entities

- Assess the level of maturity and monitoring of the proposed ISMS policies.
- Evaluate the reports submitted by the Information Security and Cybersecurity leaders regarding the results of the effectiveness assessment of the information security and cybersecurity program, proposals for improvement in the area of cybersecurity, and relevant incidents that have affected the entity.
- Promote the implementation and adoption of best practices in information security and cybersecurity.
- Ensure that all information assets undergo information security and cybersecurity assessments.
- Strengthen the information security culture among employees who manage information assets, as well as promote awareness among critical suppliers with access to such assets.
- Oversee the management of information security and cybersecurity, ensuring that associated risks are properly understood and managed.
- Ensure, through the second line of defense, the existence of a change approval process that incorporates the principles of security by design and security by default.
- For Grupo Aval Acciones y Valores S.A., lead the Executive Information Security Incident Response Group (GERI).

Information Security Executive Committee (CESI) of Grupo Aval Acciones y Valores S.A.

- Approve the Information Security and Cybersecurity Manual and its updates.
- Oversee the management of Information Security and Cybersecurity, ensuring compliance with the guidelines issued by this Committee.
- Analyze and approve the execution of initiatives or requirements for the implementation of Information Security and Cybersecurity strategies.
- Provide guidelines on information security and cybersecurity for employees.
- Understand, support, and oversee the development of Information Security and Cybersecurity.

Corporate Information Security Committee (Grupo Aval and its entities)

The Corporate Information Security Committee is composed of Grupo Aval and its main entities. On behalf of Grupo Aval, the Senior Compliance Department serves as secretary. The representatives of the entities on this committee are the Information Security Officers; the committee's deliberations and conclusions are recorded in minutes.

Quorum for Deliberation and Decision-Making

A quorum for deliberation and decision-making exists when a simple majority of its members is present.

Functions:

- Define corporate principles, guidelines, and policies.
- Take the appropriate preventive and corrective actions regarding issues that arise within the Group's entities.

- Identify, evaluate, and incorporate requirements into corporate initiatives carried out for the entities, from a risk management perspective.
- Share information about activities and projects that are of common interest and/or impact the entities in terms of risk management.
- Centralize the analysis of specific risk situations to assess their impact.
- Assess risks and the rating methodology annually or as needed.

Corporate Vice-Presidency of Risk and Compliance at Grupo Aval Acciones y Valores S.A.

- Submit the Corporate Information Security and Cybersecurity Policy for approval by the Board of Directors and disseminate it to ensure proper risk management.
- Report on the current status of the Information Security Management System to Grupo Aval's Board of Directors Risk Committee regarding matters deemed to be of greatest relevance.
- Define, promote, and support guidelines for improving the processes of the Information Security and Cybersecurity Management System, in consultation with the entities.
- Fulfill any other responsibilities assigned to Senior Management.

Corporate Vice-Presidency of Technology, Grupo Aval Acciones y Valores S.A.

- Define, promote, and support the approval of cybersecurity guidelines related to the Group's technology, in coordination with the entities.
- Keep the cybersecurity guidelines approved by the Corporate Cybersecurity Committee up to date.
- Monitor the Group's information security and cybersecurity indicators.
- Monitor projects to implement new cybersecurity controls within the Group.
- Support the response to high-impact and/or cross-functional information security and cybersecurity incidents within the Group.
- Convene the Executive Incident Response Group as required by any incident.
- Receive and consolidate cybersecurity information from its subsidiaries.
- Report on the current state of Cybersecurity to Grupo Aval's Board of Directors Risk Committee on matters deemed to be of the highest importance.
- Fulfill any other responsibilities as defined by Senior Management.

Information Security Leader at the entities and within Grupo Aval

- Participate in the Information Security Executive Committee of your entity and adopt and disseminate the best practices defined therein.
- Submit the management reports and statements established by Grupo Aval Acciones y Valores S.A., as well as those determined by the parent company or within the entity.
- Facilitate the updating of the information security and cybersecurity risk inventory.
- Adopt the guidelines established in this policy and other corporate guidelines regarding information security and cybersecurity.
- Support front-line staff in the process of identifying risks and controls, determining their criticality, and verifying compliance with the action plans defined for managing information security and cybersecurity incidents.
- Be aware of information security incidents, as well as the measures implemented to mitigate them.
- Monitor the results of the risk assessment.

- Define and monitor key performance indicators for information security and cybersecurity management.
- Report to the Corporate Vice President of Risk and Compliance, or who acts as such, on the current status of the ISMS.

Cybersecurity Leader at the entities and at Grupo Aval

- Support the Information Security Leader in preparing the management report established by Grupo Aval Acciones y Valores S.A.
- Participate in the entity's Executive Information Security Committee as required and adopt and disseminate the best practices defined therein.
- Report to the entity's Information Security Leader on newly identified risks, particularly new cybersecurity risks.
- Adopt the guidelines established in this policy and other corporate guidelines regarding information security and cybersecurity.
- Support the second line in the process of identifying risks and controls, as well as in their assessment.
- Implement and operate IT security and cybersecurity tools.
- Analyze high-impact information security and cybersecurity incidents, both those occurring within the organization and those reported by its subsidiaries, and implement the corresponding remediation plans.
- Ensure that measures are taken to respond to reported incidents and to prevent future incidents.
- Adopt current industry best practices regarding incident response.
- Define and monitor key performance indicators related to IT security and cybersecurity management.

Information Officers at the entities and within Grupo Aval

- Identify, classify, and protect the information under their responsibility; understand the risks to which it is exposed; and ensure the implementation of mechanisms that mitigate those risks to acceptable levels, taking into account cost-benefit criteria for the business unit and the organization.
- Understand the information security and cybersecurity risks relevant to their management.
- Identify, with the support of the second line of defense, the key controls to mitigate the identified risks.
- Implement the controls defined for risk mitigation, within the framework of self-monitoring.
- Define and implement action plans to mitigate the information security and cybersecurity risks under their responsibility.
- Report any information security incidents, particularly significant cybersecurity events, to the information security and cybersecurity departments.
- Ensure that your team complies with the information security and cybersecurity policy.

Internal Audit (or who acts as such) at the entities and at Grupo Aval

- Conduct the audit tests deemed appropriate in accordance with the annual work plan approved by the Audit Committee at each Group entity.
- Assess compliance with the Information Security and Cybersecurity Policy.

6. REGULATION

The Group must comply with current regulations regarding information security and cybersecurity, both nationally and internationally, where applicable; these include:

- Laws: 527/1999, 1266/2008, 1273/ 2009, 1581/2012, 1978/2019, and 2300/2023.
- Sarbanes-Oxley Act (SOX).
- Decrees: 1377/2013 and 338/2022.
- Basic Legal Circular of the FinanceSuperintendence of Colombia.
- Any other applicable regulations.

Best Practices

- ISO/IEC 2700:2018 and ISO/IEC 27001:2022
- NIST Cybersecurity Framework
- The Group must consider compliance with the regulatory, legal, and statutory requirements applicable to the use of emerging technologies, including Artificial Intelligence (AI), in the areas of information security, personal data protection, and risk management.
- Any others applicable

7. GLOSSARY

Management: the president and vice-presidents of Grupo Aval and its subsidiaries, or who acts as such.

Senior Management: the person or group of persons responsible for directing the entity's operations. For some entities in certain jurisdictions, Management includes some or all persons involved in governance; for example, members of the Board of Directors.

Threat: A potential cause of an undesirable incident that could result in harm to a system or organization.

Cybersecurity: the development of organizational capabilities to defend against and anticipate cyber threats in order to protect and secure the data, systems, and applications in cyberspace that are essential to the entity's operations.

Confidentiality: Refers to the protection of information whose disclosure is unauthorized.

Availability: Information must be available at the time and in the format required now and in the future, as must the resources necessary for its use.

Information security standards and best practices: a set of measures implemented to ensure that the entity's information and any information in its possession is accessed only by those who have a legitimate need to perform their business functions (confidentiality), that it is protected against unplanned modifications, whether intentional or unintentional (integrity), that it is available when required (availability), and that it is used only for the purposes for which it was obtained (privacy and confidentiality) and solely and exclusively for business purposes.

Risk assessment: the organization's process for identifying and analyzing risks relevant to the achievement of its objectives, forming the basis for determining how those risks should be managed.

Event: the occurrence of a situation that may affect the protection or security of data, systems, and applications in cyberspace that are essential to the entity's operations.

Incident: the occurrence of a situation that affects the protection or security of the entity's data, systems, and applications that are essential to its business.

Integrity: Information must be accurate, consistent, and complete from its creation through its destruction.

Artificial intelligence (AI): technology that enables computer systems to perform tasks that normally require human intelligence, through data analysis, decision automation, or content generation.

Privacy: the property of information that guarantees its proper use, even when there is legitimate authorization to handle it.

Emerging risks: These refer to new or unidentified risks that have never been previously considered by the organization, or known risks that are evolving in unexpected ways, which may affect not only a single company but an entire sector or the entire economy.

Information security: the preservation of confidentiality, integrity, and availability of information. It is also defined as the set of policies, strategies, methodologies, resources, IT solutions, practices, and competencies designed to safeguard the pillars of information, whether stored, reproduced, or processed, within the entity's IT systems.

Information Security and Cybersecurity Management System: a set of interrelated or interacting elements (organizational structure, policies, activity planning, responsibilities, processes, procedures, and resources) that an organization uses to establish an information security policy and objectives and to achieve those objectives, based on a risk management and continuous improvement approach.

Subsidiaries: These are the entities of Grupo Aval, among which the following stand out as its main business units: Banco de Bogotá, Banco de Occidente, Banco AV Villas, Banco Popular, Corficolombiana, Porvenir, Aval Fiduciaria, AVC, GOU Payments, and Aval Casa de Bolsa.

Vulnerability: A weakness in an organization that potentially allows a threat to affect an asset; also referred to as a weakness in an asset or control that can be exploited by a threat. All threats arising from the interaction of systems in cyberspace are taken into account.