TABLE OF CONTENTS

1. PROCESS

Control – Information Security

2. INTRODUCTION

Threats that violate information security and cybersecurity can considerably affect the reputation of Grupo Aval Acciones y Valores S.A (Grupo Aval) and its subordinates, as well as its most important information assets. Aware of the consequences, and in response to its commitment to the preservation of the pillars of information security and cybersecurity, Grupo Aval and its subordinates develop this corporate policy to protect and guarantee the availability, confidentiality, integrity and privacy of information and the establishment, implementation, maintenance and continuous improvement of its information security and cybersecurity management system.

3. OBJECTIVE

3.1 General Objectives

Protect the strategic information assets of Grupo Aval and its subordinates, managing and complying with the general principles that preserve the Confidentiality, Integrity, Availability and Privacy of information through the definition of policies, identification of risks and controls, which establish roles and responsibilities of the key actors, who intervene in the Information Security Management System (ISMS).

3.2 Specific Objectives

- Establish guidelines to maintain the confidentiality, integrity, availability and privacy of information and cybersecurity in Grupo Aval and its subordinates.
- Define how information should be protected in a homogeneous manner based on the valuation of the critical information assets of Grupo Aval and its Subordinates.
- Ensure the management of information security and cybersecurity risks in Grupo Aval and its subordinates.
- Establish and implement controls that preserve the confidentiality, integrity, availability and privacy of information in Grupo Aval and its subordinates.
- Establish roles and responsibilities of supervisory authorities in matters of the information security and cybersecurity pillars of Grupo Aval and its subordinates.
- Ensure the application of information security and cybersecurity requirements in business continuity and disaster recovery in Grupo Aval and its subordinates.
- Define the general framework for managing the Information Security Management System (ISMS) that adapts to the requirements of the business and that is in accordance with the guidelines established in this corporate policy.

4. SCOPE

This Information Security and Cybersecurity Policy applies to all Grupo Aval Employees and their subordinates, temporary officers and suppliers who, in the exercise of their functions, use information and technological services of Grupo Aval or subordinates; they must adopt it in accordance with the nature, size, complexity and structure of their operations.

5. GLOSSARY

- **Information Asset:** knowledge or data that has value for the entity or individual.
- **Management:** President, Vice-Presidents of Grupo Aval and their subordinates, or whoever takes their place.
- **Senior Management:** are the people responsible for directing, executing and supervising the operations of the entity under the direction of the Board of Directors.
- **Threat:** A potential cause of an unwanted incident, which can cause damage to a system or organization[1]
- **Risk Appetite:** is the exposure to the level of risk that an entity is willing to assume in the development of its activity in order to achieve its strategic objectives and comply with its business plan.
- **Cyberthreat:** appearance of a potential or current situation that could become a cyberattack.[2]
- **Cyberspace:** a complex environment resulting from the interaction of people, software and services on the Internet through technological devices connected to said network, which does not exist in any physical form.[2]
- **Cyber Risk:** possible negative results derived from failures in the security of technological systems or associated with cyberattacks.[2]
- **Cybersecurity:** is the development of business capabilities to defend and anticipate cyberthreats to protect and secure data, systems, and applications in cyberspace that are essential to the operation of the entity.[2]
- **Employee:** workers including Senior Management, interns and trainees of Grupo Aval and/or their subordinates.
- **Confidentiality:** refers to the protection of information whose disclosure is not authorized.[1]
- **Control:** A measure taken by the entity and other parties to manage risks and increase the likelihood of achieving established objectives and goals.
- **Availability:** Information must be available at the time and in the format required now and in the future, as well as the resources needed to use it.[1]
- **Subordinate:** corresponds to the entities of Aval Group, among which Banco de Bogotá, Banco Popular, Banco de Occidente, Banco AV Villas, Corficolombiana and Porvenir stand out as their main business units.

[1] NTC-ISO 27000
[2] CE 007 of 2018

- **Information Security Standards and Good Practices:** set of measures implemented to ensure that the entity's information and that in its possession is accessed only by those who have a legitimate need for the performance of their business functions (confidentiality), that it is protected against unplanned modifications, made intentionally or unintentionally (completeness), that is available when required (availability) and that is only used for the purposes for which it was obtained (privacy and reservation) and solely and exclusively for business purposes.

- **Risk Assessment:** The entity's process for identifying and analyzing risks relevant to the achievement of its objectives, forming the basis for determining how risks should be managed.

- **Cybersecurity Event:** occurrence of a situation that may affect the protection or assurance of data, systems and applications in cyberspace that are essential for the operation of the entity.[2]

- **Cybersecurity Incident:** occurrence of a situation that affects the protection or assurance of the entity's data, systems and applications that are essential to the business.[2]

- **Information Security Incidents:** a single event or series of unexpected or unwanted information security events that have a significant probability of threatening information security[4].

- **Integrity:** Information must be accurate, consistent, and complete from creation to destruction.[1]

- **Impact Magnitude:** it is the loss (monetary or non-monetary) generated by the materialization of a risk, which can be measured qualitatively and quantitatively.

- **Information Security Pillars:** principles or characteristics of information security (Confidentiality, Integrity and Availability).

- **Privacy:** ownership of the information that guarantees the proper use of it, even if legitimately authorized to handle it.[3]

- **Probability of Occurrence:** is the possibility that a risk will materialize. Qualitative or quantitative analysis can be used to determine this probability.

- **Risk Management Assessment Process:** process of identifying and analyzing relevant risks that exist and impede the achievement of objectives; forming a basis for determining how they should be managed, transferred, controlled or assumed.

- **Information Responsible - RES:** is the employee for whom the information was created in order to perform their functions in the business and has the responsibility of managing it, classifying it and evaluating the risks that may affect it. He/she is also primarily responsible for implementing the Information Security Policy within his/her area and in

order to do so he/she must know the value of his/her information, the users who must have access to it and the privileges they require for its use.

- **Reserve:** refers to the fact that the information can only be used for the purposes for which it was obtained from the owner and solely and exclusively for business purposes. Involves the obligation not to use, disclose or distribute the acquired information for purposes other than those for which it was obtained from the owner and solely and exclusively for business purposes.

- **Risk:** the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

- **Emerging Risks:** understood as those new or unidentified risks that have never been previously considered by the entity, or known risks that are evolving unexpectedly, which may affect not only a company but an entire sector or the entire economy**.**

- **Generic Risk:** are all those risks identified by the second line of Grupo Aval/Subordinates.

- **Inherent Risk (IR):** the level of risk inherent to the activity, without taking into account the effect of controls. In other words, Inherent Risk is the probability that an entity may incur a material loss as a result of its exposure to, and the uncertainty arising from, potential adverse events. IR is intrinsic to each significant activity and is evaluated without taking into account the size of the activity in relation to the organization and before evaluating the quality of the risk management that it performs. To identify and evaluate the IRs to which an organization is exposed, it is essential to have a thorough knowledge of both the nature of the activities it carries out and the environment in which it operates.

- **Residual Risk:** Also known as net risk, it is the result of the mitigation of inherent risks by operational management and supervisory functions. In other words, it is the risk that remains after the controls have been carried out and preventive measures have been taken to respond to the risks identified.

- **Information Security:** preservation of the confidentiality, integrity and availability of information.[3-4] Also referred to as the set of policies, strategies, methodologies, resources, IT solutions, practices and competencies to preserve the pillars of the information that is stored, reproduced or processed in the entity's computer systems.[2]

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

[1] NTC-ISO 27000
[2] CE 007 of 2018
[3] Law 1581 of 2012
[4] NTC-ISO 27000

- **Vulnerability:** A weakness of an organization that potentially allows a threat to affect an asset.[1] also called the weakness of 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[2]

6. REGULATION

Grupo Aval and its subordinates must comply with the Information Security regulations in force in the country and with international regulations that they are obliged to adopt, as an example are:

- **Basic Legal Circular of the Finance Superintendence (CE 029/14) Part I Title IV Chapter V:** Minimum requirements for the management of information security and cybersecurity.
- **Basic Legal Circular of the Finance Superintendence (CE 029/14) Part I Title III Chapter I:** Access and information to the financial consumer.
- **Basic Legal Circular of the Finance Superintendence (CE 029/14) Part I Title I Chapter VI:** Rules relating to the use of cloud computing services.
- **Basic Legal Circular of the Finance Superintendence (EC 02/14) Part I, Title II, Chapter I:** Channels, Means, Security and Quality in the Management of Information in the Provision of Financial Services.
- **Law 1581 of 2012 (Habeas Data):** By which general provisions are issued for the treatment and protection of personal data.
- **Law 1273 of 2009:** Protection of information and data and the systems that use information and communication technologies are fully preserved.
- **Law 527 of 1999:** which defines and regulates access to and use of data messages, electronic commerce and digital signatures, and establishes certification bodies and other provisions
- **SOX Act**: Federal law of the United States of America issued in 2002 that aims to improve the internal control environment of companies listed on the stock exchanges of the United States; define and formalize responsibilities for compliance with the prevention of accounting and reporting errors.
- **Law 1266 of 2008**: By which the general provisions of habeas data are dictated and the management of the information contained in personal databases is regulated, especially financial, credit, commercial, services and that coming from third countries and other provisions are issued.

6.1 Other Frames of Reference

The following frameworks are used as best market practices. It is also clarified that the practices are not intended to be an exhaustive list:

- **NTC-ISO-IEC 27001:2013:** This standard specifies the requirements for establishing, implementing**,** maintaining, and continuously improving an Information Security management system, within the context of the organization. This standard also includes the requirements for the assessment and treatment of Information Security risks, adapted

[2] CE 007 of 2018
[3] Law 1581 of 2012
[4] NTC-ISO 27000

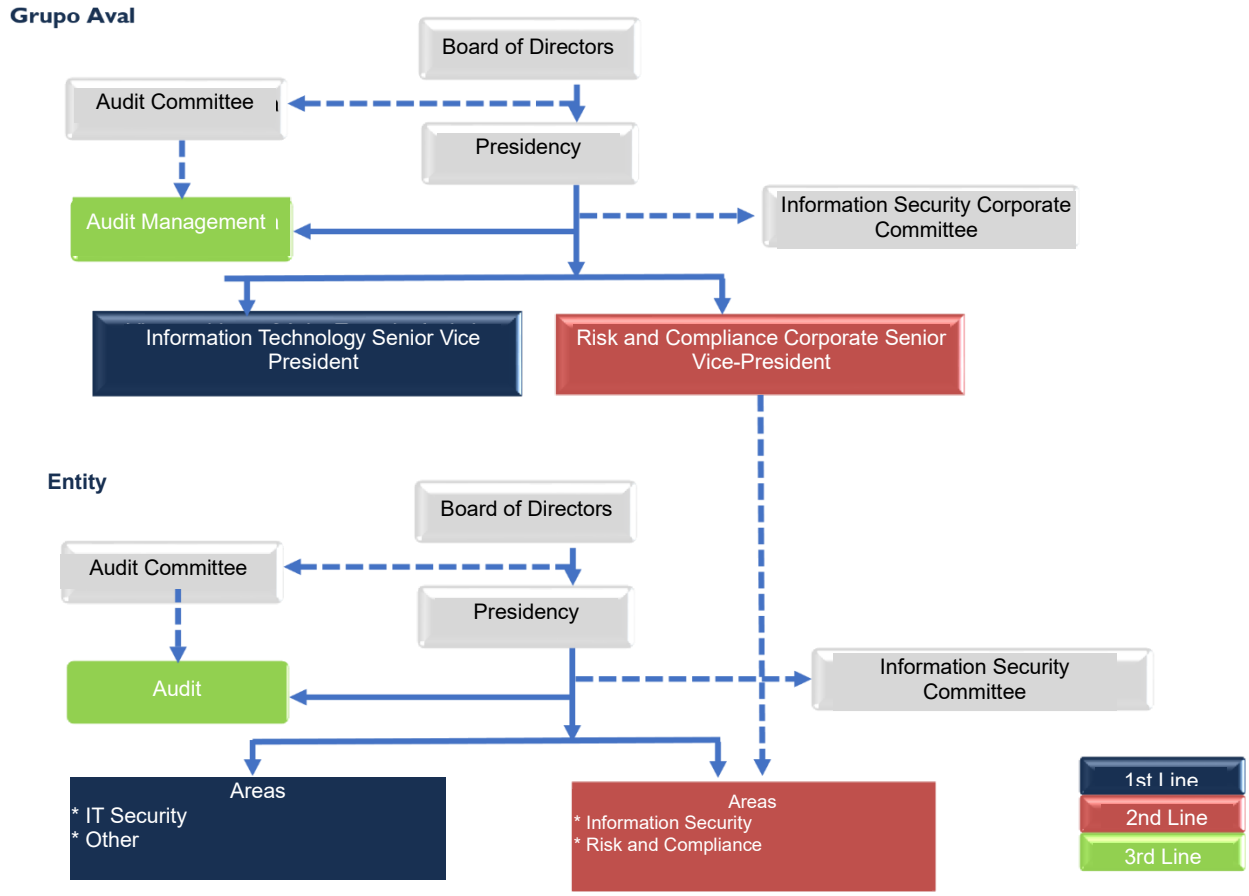
to the needs of the organization. The requirements set out in this standard are generic and are intended to be applied to all organizations, regardless of their type, size or nature.

- **ISO/IEC 27000:** is a group of international standards entitled: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. It aims to help organizations of all types and sizes to implement and operate an Information Security Management System (ISMS).
- **ISO/IEC 27701:** Standard that specifies requirements and provides guidance for establishing, implementing, maintaining, and continuously improving the Information Privacy Management System.
- **NIST Cybersecurity Framework:** A framework based on existing standards, guidelines, and practices for organizations to manage cybersecurity risk.

7. USER RESPONSIBILITIES

7.1 Government for Information Security and Cybersecurity Management

Grupo Aval and its subordinates must structure the functions and responsibilities for Information Security and Cybersecurity Risk and for management in this area, in accordance with the Corporate Policy for Comprehensive Risk Management; this framework defines the scheme of the three lines, considering (i) management by business line, (ii) an independent Information Security risk management function, and (iii) an independent review.



7.1.1 First Line

The first line is made up of the IT Security areas and all Grupo Aval Employees and their subordinates. The Information Security and Cybersecurity Policy recognizes the computer security areas and other Employees as primarily responsible for identifying, evaluating, managing, monitoring, and reporting information security and cybersecurity risks and incidents inherent to security products, activities, processes, and systems. Those who make up this line of defense must know their activities and processes, and have sufficient resources to effectively perform their tasks.

They must also comply with policies and procedures defined by the Organization, contributing to a solid culture of information security and cybersecurity.

7.1.2 Second Line

This line is made up of the Risk area or equivalents of each entity, which must establish the guidelines in this area and continuously monitor compliance with all risk obligations in information security and cybersecurity.

The Information Security Officer may also serve in the role of Chief Risk Officer, Chief Compliance Officer or equivalent. This officer must present the management results directly to Senior Management or the Audit Committee (or the Committee that the Board of Directors appoints). In the event of separation of duties, the relationship between the aforementioned officers and their respective functions must be clearly defined and known. Likewise, it must have sufficient resources to effectively perform all its functions and play a central and proactive role in the Information Security Management System. To do this, it must be fully familiar with current policies and standards, their legal and regulatory requirements, and Information Security risks arising from the business, including specific cybersecurity topics.

7.1.3 Third Line

The third line plays an important role in independently evaluating the management and controls of information security and cybersecurity risks, as well as the policies, standards and procedures of the systems, reporting to the Audit Committee or whoever is appointed. The internal audit persons who are required to conduct these reviews must be competent and appropriately trained and not involved in the development, implementation, and operation of the risk/control structure. This review may be conducted by audit staff or by personnel independent of the process or system being examined, but may also involve appropriately qualified external actors.

7.2 Roles and Responsibilities

To comply with the objectives of the Information Security and Cybersecurity Policy, the following key actors in information security management have been defined:

Actor	Activities	
	Execution	Supervisory
Board of Directors	• Approve the Information Security and Cybersecurity Policy. • Study and approve the Risk Appetite of the entities. • Ensure that there are sufficient technical and human resources to adequately manage information security and cybersecurity and others when applicable • Enforce compliance with government information security and cybersecurity rules and regulations. • Participate in awareness and training programs on information security and cybersecurity issues.	• Monitor Information Security and Cybersecurity in Group Aval and subordinates, understanding risks and ensuring that these are managed.
Senior Management	• Evaluate the monitoring of the level of maturity and monitoring of the proposed policies of the Information Security Management System. • Evaluate the reports submitted to it by the Information and Cybersecurity Security Office; on the results of the effectiveness evaluation of the Information Security and Cybersecurity program, proposals for improvement in Cybersecurity matters and summary of the incidents that affected the entity • Promote the application and appropriation of good information security and cybersecurity practices. • Ensure the information security and cybersecurity assessment of all information assets without exception. • Strengthen the information security culture of Grupo Aval Employees and their subordinates, who manage information assets. Each entity must evaluate the need to raise awareness of information security among its critical suppliers who access information assets.	• Supervise information security and cybersecurity in Grupo Aval and subordinates, understanding the risks and ensuring that they are managed. • Lead the GERI - Information Security Incident Response Executive Group, applies to Grupo Aval.

Information Security Corporate Committee	• Provide principles and corporate guidelines for information security and cybersecurity, take the relevant preventive and corrective actions for the entities of Aval Group. • Identify, evaluate and include information security and cybersecurity requirements in the corporate initiatives carried out for entities. • Make decisions related to the information security and cybersecurity of entities. • Socialize activities and projects that are of common interest and/or impact the entities. • Generate feedback from the security days and diagnoses of the ISMS carried out and contribute to the continuous improvement of the Information Security posture. • Define principles and corporate guidelines for information security and cybersecurity. • Define information security and cybersecurity requirements in corporate initiatives carried out for the entities. • Socialize activities and projects that are of common interest and/or impact the service companies	• Monitor compliance at the corporate level with the policies of the Information Security and Cybersecurity Management System in each entity. • Monitor internal compliance with the Information Security and Cybersecurity Management System Policies in each entity.
Risks Committee - Entities (Or whoever takes its place)	• Approve the guidelines that they deem appropriate, in each of the entities, for the improvement of Information Security Management. • Monitor the management carried out by the entities through the consolidated reports that are periodically presented to it. As a result of this review, it may propose the generation or modification of corporate guidelines that may affect one or all of the entities of the Conglomerate, as required.	• Know the result of the Information Security and Cybersecurity Management carried out by the direct subordinates, through a control panel. • Know the Information Security Incidents presented in the entities and that have had a significant impact, reported by the entities that make up the Organization and the action plans carried out to mitigate them.

Executive Committee of Information Security (CESI), applies to Grupo Aval.	• Inform information security and cybersecurity agreements and decisions. • Generate feedback from the security days and diagnoses of the ISMS carried out and contribute to the continuous improvement of the information security posture. • Inform principles and guidelines of information security and cybersecurity, verify the development of information security and cybersecurity projects, ensure the level of information security through the analysis of indicators and take the pertinent preventive and corrective actions to Grupo Aval. • Identify, evaluate and include information security and cybersecurity requirements in corporate initiatives. • Socialize activities and projects that are of common interest. • Promote the development of information security at Grupo Aval • Approve the changes and approvals of the information security architecture • Approve the action plans to mitigate the risks identified by the RES. • Approve the annual penetration testing schedule based on the proposal prepared by the IT security area.	• Monitor internal compliance with the Information Security and Cybersecurity Management System Policies at Grupo Aval.
Corporate Senior Vice presidency of Risk and Compliance (or whoever takes its place)	• Prepare information security and cybersecurity reports for the Executive Committee and any other committee that is defined. • Report the current status of the Information Security and Cybersecurity Management System in the entities to the Vice Presidency of Risk or whoever takes its place. • Define the guidelines for improvement in the processes of the Information Security and Cybersecurity Management System, in consensus with the entities. • Comply with the other responsibilities that are defined for Senior Management.	• Parent Entities: Receive and consolidate information on information security and cybersecurity of their subordinate to generate periodic monitoring reports in accordance with the defined communication protocol. • Keep the information security and cybersecurity guidelines approved by the Information Security Corporate Committee Grupo Aval -entities up to date. • Support and approve the guidelines for improvement in the processes of the Information Security and Cybersecurity Management System.

Information Technology Senior Vice Presidency	• Monitor the cybersecurity security indicators of the entities. • Define the cybersecurity guidelines of technology in consensus with the entities. • Follow up on projects to implement new cybersecurity controls in the entities. • Support entities in dealing with high-impact and/or cross-cutting incidents in the Group. • Convene the Executive Incident Response Group when required by an incident. • Comply with the other responsibilities that are defined for Senior Management.	• Parent Entities: Receive and consolidate cybersecurity information from their subordinates. • Keep the cybersecurity guidelines approved by the Corporate Cybersecurity Committee of the entities updated. • Support and approve the Group's technology cybersecurity guidelines.
Information Security Leader	• Submit the Management Report established by its direct Parent entity • Participate in the Information Security Executive Committee of its entity. • Adopt and socialize the best practices suggested in the Committee. • Promote the updating of the inventory of information security and cybersecurity risks. • Adopt the established guidelines. • Support the first line in the process of identifying risks and controls, determining their criticality and verifying compliance with the action plans established in the management of information security and cybersecurity incidents.	• Know the Information Security Incidents and the measures that have been implemented to mitigate them. • Monitor the result of the risk assessment. • Define and monitor key performance indicators on information security and cybersecurity management.
IT Security Leader	• Support the Information Security leader in the preparation of the Management report established by Grupo Aval. • Participate in its entity's Information Security Executive Committee when necessary. • Adopt and socialize the best practices suggested in the Committee. • Inform the Information Security Leader about new risks identified and in particular about new cybersecurity risks. • Adopt the established guidelines. • Support the second line in the process of identifying risks and controls, as well as in their evaluation. Implement and operate IT security and cybersecurity tools.	• Analyze high-impact Information Security and Cybersecurity incidents reported by their subordinates and their own and implement remediation plans • Ensure that measures are taken to respond to incidents and to prevent future incidents. Adopt the best practices in force in the market with respect to answers to incidents. • Define and monitor key performance indicators on IT Security and Cybersecurity management.

Responsible of information	• Identify, classify and protect the information under their responsibility, know the risks to which they could be exposed and ensure that the necessary mechanisms are provided so that these risks are mitigated to acceptable levels, considering cost-benefit for their business area and the organization. • Know the Information Security risks that applies to them. • With the support of the second line, identify key controls to mitigate the identified risks. • Carry out the execution of controls to mitigate risks (Self-control). • Define and execute action plans to mitigate information security risks under their responsibility. • Report to the IT Security and Information Security areas, any information security incident and in particular any material cybersecurity event.	Monitor and ensure that their work team complies with the security and cybersecurity policy.
Internal Audit	• Carry out the audit tests that it deems appropriate in accordance with the annual work plan approved by the Audit Committee in each entity.	Assess compliance with the company's Information Security and Cybersecurity Policy.

8. STATEMENT OF COMMITMENT

Grupo Aval and its subordinates are committed to the Information Security and Cybersecurity Policy, promoting a culture of compliance and control in accordance with the principles established by the Information Security and Cybersecurity management system, for which they must:

- Prevent damage to the image and reputation through the adoption and compliance with the Information Security and Cybersecurity Policy.
- Continuously promote a culture of information security and cybersecurity.
- Manage in a structured and strategic way the information security and cybersecurity risks associated with the business and its relationship with third parties.

Each employee, temporary employee and third party, is responsible for applying the criteria defined in this policy and for adjusting their actions in accordance with the corporate values and guidelines established in information security and cybersecurity, in the same way they are responsible for reporting the incidents of which they may become aware.

9. GENERAL GUIDELINES

Grupo Aval's Senior Management and its subordinates recognize the importance of adequately protecting information from threats that may affect business continuity, which is why it establishes the development of activities for the protection of information assets, management and administration of Information Security and cybersecurity risks, protection of personal data, security culture and the conduct that must be adopted by all Grupo Aval Employees and their subordinates, therefore, all temporary employees and suppliers who in the exercise of their

activities use technological information and services in Grupo Aval and their subordinates must ensure: compliance with the requirements and pillars of information security and cybersecurity, protecting the organization's information assets, preserving the confidentiality, integrity, availability and privacy of the information; therefore, Grupo Aval and its subordinates adopt the following policies on which the Information Security Management System (ISMS) is based and structured. Such Policies are expressions of management for a fair and transparent presentation and assessment of information security and cybersecurity risks. This allows for an adequate identification of the controls that reasonably mitigate the identified risks.

9.1Protect the Confidentiality, Integrity, Availability, Privacy, and Non-Repudiation of Information

All Grupo Aval Employees and their subordinates must protect and ensure the confidentiality, integrity, availability and privacy of the information, in such a way that the information:

Is only accessed by authorized personnel.
Is concise, precise, with an emphasis on accuracy.
Is available at the time it is required.
Is legitimately accessed and used for what it was authorized.

9.2 Adopt and Maintain a Strong Culture of Information Security and Cybersecurity

The three lines must take the lead in establishing a strong culture of information security and cybersecurity where:

- The first line must be an example and replicator of a solid culture and awareness in information security and cybersecurity, in compliance with defined organizational policies and procedures.
- The second line must define and execute awareness and culture activities, which cover all Employees, on the organizational policies and procedures of information security and cybersecurity.
- The third line should monitor the execution and compliance of information security and cybersecurity culture and awareness.

9.3 Implement and Maintain a Comprehensive Information Security and Cybersecurity Risk Management System

All Grupo Aval Employees and their subordinates must use a generally accepted internal control framework where it defines the elements that are expected to be present and functioning in an effective internal control system. To this end, it must be aligned with the corporate methodology of Operational Risk Management - SARO (inherent risk assessment, residual risk and heat map) and with the Corporate Methodologies of Information Security and Cybersecurity Risk Management.

9.4 Determine Risk Appetite, Level of Tolerance and Risk Capacity

Senior Management and the second line of Grupo Aval and its subordinates must determine the Risk Appetite, the level of tolerance and the maximum risk capacity, considering the effect of the nature of their operations and business lines, as well as the types and levels of

information security and cybersecurity risk that each entity is willing to assume at each of these levels. The Boards of Directors of the entities must approve the Risk Appetite, the level of tolerance and the maximum risk capacity.

9.5 Information Security and Cybersecurity Risk Assessment

Grupo Aval and its subordinates must have a process in place to identify, assess, document, manage, and mitigate information security and cybersecurity risks. This process is done at least once a year or when special circumstances occur, identifying risks and evaluating their probability and impact, which must be aligned with corporate methodologies for information security and cybersecurity risk management.

9.6Oversee the Administration of the Information Security and Cybersecurity Management System

Senior management and the second line must establish, approve, and periodically review the "Information Security and Cybersecurity Management System," and must supervise management to ensure that policies, processes, and systems are effectively implemented at all levels of decision-making.

9.7 Manage Change

Senior management and the second line must ensure that there is an approval process that fully assesses information security and cybersecurity risks in all new critical processes, activities, products, and systems, as well as that new threats are identified. For example, every time changes are made to an application that impacts the business, it is taken to a change committee where the possible risks that the implementation of said change would bring are evaluated.

9.8 Track and Report

Grupo Aval's second line and its subordinates are required to implement a process to regularly monitor Information Security risk profiles and exposures to significant losses. Additionally, it must carry out an information security diagnosis based on rules, standards and reference frameworks that support the management of information security and cybersecurity ISO 27000 and NIST Cybersecurity Framework in order to calculate the level of security and maturity of Grupo Aval and its subordinates, Corporate Indicators, Evolution of Risks and Evolution of Controls. Specifically, cybersecurity risks must be worked on in this same sense.

9.9 Control and Mitigate

The first and second lines of Grupo Aval and the subordinates must have a strong "control environment", structured through policies, procedures, standards, systems, adequate internal controls and the weighted mitigation or compensation of risks.

With the above, the first line of defense must have general access controls, privileges, updates in the following minimum aspects:

Physical access control monitoring.

Monitoring of logical access controls.
Password monitoring and protection.
Monitoring protection of configuration and remote access ports.
Restriction of the installation of applications by the end user.
Ensuring that operating systems are "patched" with updates or, failing that, that the controls implemented mitigate the possibility of an incident materializing.
Ensuring that software applications are updated regularly.
Restriction of administrative privileges (i.e., the ability to install software or change a computer's configuration settings).

9.10 Ensure that the Information Security and Cybersecurity Management System Operates in Contingency Situations

The second line or Information Security Leaders of Grupo Aval and their subordinates must ensure that the necessary controls on the pillars of information security and cybersecurity are included and implemented in the Business Continuity plans.

9.11 Ensure Compliance with Applicable Law

It is the obligation of the three lines of Grupo Aval and its subordinates to comply with all the regulations of the current regulators that apply to each entity related to Information Security and Cybersecurity.

9.12 Security in New Technologies and Emerging Risks

It is important to implement an information security and cybersecurity plan, in relation to new technologies. To monitor, develop and implement remediation strategies for emerging risks, where it is necessary to:

- Establish security policies on the technologies implemented in Grupo Aval and its subordinates.
- Adopt procedures for information classification, user management and administration, definition of responsible and owners, of the information to be processed in new technologies to determine and apply information security and cybersecurity controls.
- Establish the management and monitoring of cyber risks and third-party risks that arise from the implementation of new technologies, such as operational, financial, regulatory, organizational and technological risks.
- Include in the business continuity plan the security requirements and controls to resume operations oriented on automated systems and digital services.
- Supervise compliance with the work performed by automated systems, ensuring that these systems adhere to regulatory requirements and the organization's policies regarding security.

9.13 Information Security and Cybersecurity Management System Evaluation Model

For the identification of risks and the application of information security and cybersecurity controls, Grupo Aval and its subordinates adopt and publicize the information security and cybersecurity evaluation model. The purpose of this model is to evaluate the level of maturity

of the information security management system and identify opportunities for improvement to strengthen it, based on the domains and controls proposed in the NTC-ISO 27001:2013 standard and the NIST Cybersecurity Framework.

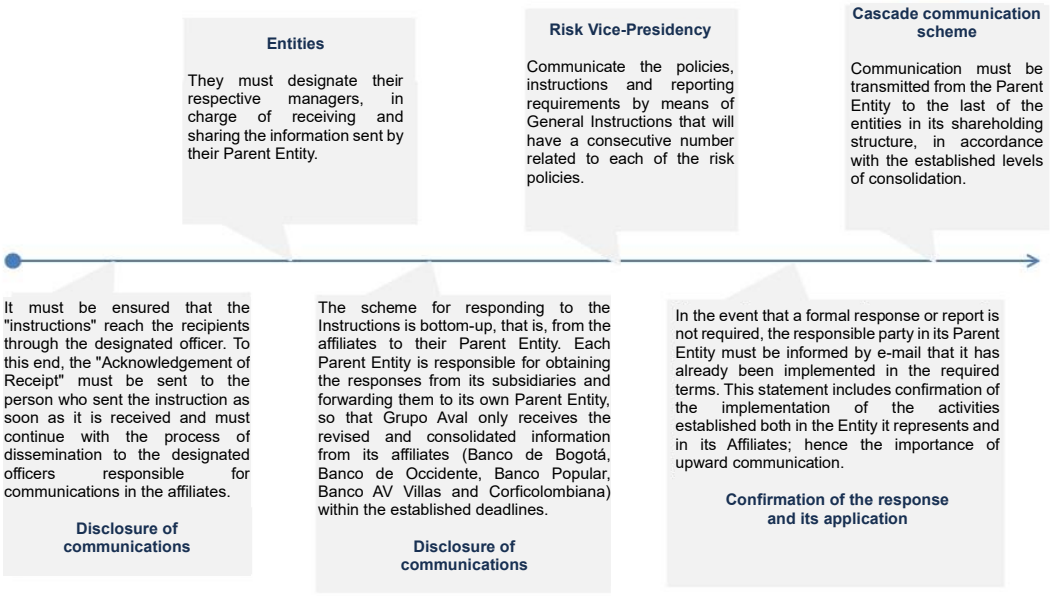
9.14 Communication Information Security Leaders

In order to promote the standardization of the application of compliance with this policy throughout the Group, the following will be established as an official information mechanism:

General Instructions, which will include activities, generally methodological, Prior evaluation, analysis and agreement with the competent specialists of each of the entities, the Corporate Information Security Team (Grupo Aval) issues general instructions to Presidents, Information Security Leaders and when applicable process owners of the four banks, Corficolombiana and Porvenir. They in turn disseminate the General Instruction to their peers in the respective affiliates and sometimes to other areas of interest as indicated in the Instruction. The foregoing in compliance with the communication protocol defined by the Senior Corporate Vice Presidency of Risk and Compliance of Grupo Aval.

Concepts are clarifications or expansion of information, useful to comply with general instructions, generally communications through institutional email. The Corporate Information Security Team issues concepts to the Information Security Leaders of the four banks, Corficolombiana and Porvenir, as well as additional subsidiaries in special cases, and these in turn disclose the concepts to the Information Security Leaders of the respective subsidiaries following the communication protocol.

Within the corporate communication process, Grupo Aval and its subordinates have established the communication protocol to ensure that the information issued reaches the required levels in a clear and timely manner, as follows:



9.15 Reports

In order to facilitate compliance monitoring, different management reports will be requested that constitute effective support for the administration; these must be truthful, understandable, complete and timely.

Likewise, subordinates must inform Grupo Aval of those information security and cybersecurity incidents that have significantly affected the confidentiality, integrity, availability and privacy of the entity's information at the time they occur, making a brief description of the incident, its impact and the measures adopted to manage them. Additionally, each entity must have a consolidated database of information security and cybersecurity incidents classified by type of incident, impact and remediation plan, as well as that this report is protected given the sensitivity of this information.

9.16 Training

As part of the induction process for a new Employee and at least annually for all Employees, training and/or updating on information security and cybersecurity must be carried out. Training can be provided continuously, virtually or face-to-face to Grupo Aval Employees and their subordinates, with the purpose of strengthening the concepts and ensuring the continuity and sustainability of the Information Security Management System. Each entity should assess the need to raise awareness of information security among its critical suppliers who access information assets.

9.17 Investigations and Sanctions

Grupo Aval and its subordinates acknowledge that in the event of non-compliance with this policy and other activities arising from it, the entities and persons responsible for their non-compliance may be subject to disciplinary action by Grupo Aval in accordance with the entity's internal policies related to the management of Information Security Incidents. The foregoing, without prejudice to the possible liability that may arise from non-compliance with the regulations applicable to Information Security.

9.18 Application to Grupo Aval Acciones y Valores S.A.

This Corporate Information Security and Cybersecurity Policy applies to Grupo Aval. Any exceptions will be documented and supported by the Corporate Senior Vice President of Risk and Compliance.