Information Security Manual and Policies
_____(document internal code)

VERSION	DATE	CHANGE CONTROL	APPROVED
1	01-10-2018	ACTUALIZATION	GENERAL MANAGER

CONTENTS

1. INTRODUCTION

With the definition of computer security policies and standards, the aim is to establish within XXXXXXXXXXXXX a culture of quality operating in a reliable manner. Computer security is a process where risks must be evaluated and managed, supported by policies and standards that cover the Entity's needs in terms of security.

The computer security policies and standards established in this document are the fundamental basis for the protection of computer assets and all information and Communications in XXXXXXXXXXXXX so that it meets the criteria of Confidentiality, Integrity, and Availability.

Information security is a priority for XXXXXXXXXXXXX and therefore it is the responsibility of all Collaborators to ensure that activities that contradict the essence and spirit of each of these policies are not carried out.

1 REACH.

The information security policies cover all the administrative and control aspects that must be fulfilled by the Directors, Collaborators and Third Parties that work or have a relationship with XXXXXXXXXXXXX, in order to achieve an adequate level of protection of the security and quality characteristics of the information. related information.

1. DEFINITIONS.

- **Information asset:** any component (human, technological, software, documentary or infrastructure) that supports one or more business processes of XXXXXXXXXXXXX and, consequently, must be protected.
- **Confidentiality Agreement:** it is a document in which the officials of XXXXXXXXXXXXX or those provided by third parties express their willingness to maintain the confidentiality of the Entity's information, committing not to disclose, use or exploit the confidential information to which they have access by virtue of the work they develop within it.

- **Threat:** potential cause of an unwanted incident, which can cause damage to a system or the company.
- **Information security risk analysis:** systematic process of identifying sources, estimating impacts and probabilities, and comparing these variables against evaluation criteria to determine the potential consequences of loss of confidentiality, integrity and availability of information.
- **Authentication**: it is the procedure for verifying the identity of a user or technological resource when trying to access a processing resource or information system.
- **Capacity Planning**: it is the process to determine the capacity of the resources of the technological platform that the entity needs to satisfy the processing needs of said resources efficiently and with adequate performance.
- **Wiring centers:** These are rooms where communication devices and most of the cables should be installed. Like data centers, wiring centers must meet requirements for physical access, wall, floor, and ceiling materials, electrical power supply, and temperature and humidity conditions.
- **Computer Center:** it is a specific area for the storage of multiple computers for a specific purpose, which are connected to each other through a data network. The data center must meet certain standards in order to ensure physical access controls, wall, floor and ceiling materials, electrical power supply and adequate environmental conditions.
- **Encryption**: is the transformation of data through the use of cryptography to produce unintelligible data (encrypted) and ensure its confidentiality. Encryption is a very useful technique to prevent information leakage, unauthorized monitoring, and even unauthorized access to information repositories.
- **Information Security Committee:** the Information Security Committee is the body that must establish the management and control criteria, which allow the implementation of the most appropriate mechanisms for the protection of information of XXXXXXXXXXXXX, applying the principles of confidentiality, integrity and availability of the same and of the

computer resources or of another nature that support it, in accordance with the strategic planning of the company.

- **Confidentiality:** it is the guarantee that the information is not available or disclosed to unauthorized persons, entities or processes.
- **Control:** is any activity or process aimed at mitigating or avoiding a risk. It includes policies, procedures, guides, organizational structures and good practices, which can be of an administrative, technological, physical or legal nature.

- **Cryptography:** is the discipline that brings together the principles, means and methods for data transformation in order to hide the content of your information, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorized use.
- **Custodian of the information asset:** it is the organizational unit or process, designated by the owners, in charge of maintaining the protection measures established on the information assets entrusted.
- **Copyright:** is a set of rules and principles that regulate the moral and patrimonial rights that the law grants to authors for the sole fact of creating a literary, artistic or scientific work, whether published or not yet published. published.

- **Disaster or contingency:** interruption of the ability to access information and process it through computers or other means necessary for the normal operation of a business.
- **Availability**: it is the guarantee that authorized users have access to information and associated assets when they require it.
- **Computer equipment:** electronic device capable of receiving a set of instructions and executing them by performing calculations on numerical data or compiling and correlating other types of information.
- **Standard:** A rule that specifies an action or response to be followed in a given situation. Standards are mandatory guidelines that seek to enforce policies. Standards are designed to promote the implementation of the organization's high-level policies before creating new policies.
- **Security standards:** are approved products, procedures and metrics that define in detail how security policies will be implemented for a particular environment, taking into account the strengths and weaknesses of the available security features. They must be reflected in a document that describes the implementation of a guide for a specific component of hardware, software or infrastructure.
- **Risk assessment:** process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

- **Information security event:** identified presence of a system, service, or network condition, indicating a possible information security policy violation or failure of safeguards, or a previously unknown situation that may be relevant to safety.

- **Guidance:** A guidance is a general statement used to recommend or suggest an approach to implementing policies, standards, and good practices. The guidelines are essentially recommendations that should be considered when implementing security. Although not mandatory, they will be followed unless there are documented and approved reasons for not doing so.
- **I**nformation classification guidelines: guidelines for cataloging the entity's information and distinguishing between information that is critical and information that is less critical or not critical and, accordingly, establishing differences between security measures to apply to preserve the criteria of confidentiality, integrity and availability of information.
- **Ethical hacking:** is the set of activities to enter the data and voice networks of the institution in order to achieve a high degree of penetration into the systems, in a controlled manner, without any malicious or criminal intent and without causing damage. in the systems or networks, with the purpose of showing the effective level of risk to which the information is exposed and proposing eventual corrective actions to improve the level of security.

- **Impact:** the consequence that occurs in the company when a threat materializes.
- **Security Incident:** is an adverse event, confirmed or suspected, that has violated information security or that attempts to violate it, regardless of the information affected, the technological platform, the frequency, the consequences, the number of times it occurred or the origin (internal or external).
- **Integrity**: is the protection of the accuracy and completeness of assets.
- **Inventory of information assets**: it is an ordered and documented list of the information assets belonging to the Entity.
- **Software license:** it is a contract that specifies all the rules and clauses that govern the use of a certain software product, taking into account aspects such as: scope of use, installation, reproduction and copying of these products.
- **Removable media:** is any removable hardware component that is used for information storage; Removable media include tapes, removable hard drives, CDs, DVDs, and USB thumb drives, among others.
- **Best Practice:** A specific security rule or platform that is accepted throughout the industry as providing the most effective approach to a particular security implementation. Best practices are established to ensure that the security features of regularly used systems are uniformly configured and managed, ensuring a consistent level of security throughout the organization.

- **Security organization:** it is a function that seeks to define and establish a balance between the responsibilities and the requirements of the roles associated with the administration of information security.
- **User profiles:** they are groups that concentrate several users with similar information needs and identical authorizations on technological resources or information systems to which they are granted access according to the functions performed. Modifications to a user profile affect all users protected within it.

- **Policies:** all the intentions and directives formally expressed by the Role.
- **Processes:** a process is defined as each set of activities that receive one or more inputs to create a value product for the customer or for the company itself (concept of internal quality customer). Typically, a business activity has multiple business processes that serve to develop the activity itself.

- **Procedures**: Procedures are the operational steps that officials must perform to achieve certain objectives. Procedures are technology or process independent and refer to specific platforms, applications, or processes. They are used to outline the steps that must be followed by an agency to implement security related to that specific process or system. Procedures are generally developed, implemented, and monitored by the process or system owner; procedures will follow organization policies, standards, best practices, and guidelines as closely as possible, while conforming to procedural or technical requirements established within the dependency where they apply.
- **Intellectual property:** is the recognition of a particular right in favor of an author or other rights holders, over the works of the human intellect. This recognition is applicable to any property considered to be of an intellectual nature and worthy of protection, including scientific and technological inventions, literary or artistic productions, trademarks and identifiers, industrial designs, and geographical indications.
- **Information owner:** is the organizational unit or process where information assets are created.
- Technological resources: are those hardware and software components such as: servers (for applications and network services), workstations, portable equipment, communications and security devices, data network services and databases, among others. others, whose purpose is to support the administrative tasks necessary for the proper functioning and optimization of work within XXXXXXXXXXXXX
- **Audit Records:** these are files where the events that have been identified in the Entity's information systems, technological resources and data networks are recorded. Such events may include, but are not limited to, user identification, events and actions performed, terminals or locations, successful and unsuccessful access attempts, configuration changes, use of utilities, and system failures.

- **Responsible for the information asset** is the person or group of persons, designated by the owners, in charge of ensuring the confidentiality, integrity and availability of information assets and deciding how to use, identify, classify and protect said assets. assets in your charge.
- **Risk:** combination of the probability of an event and its consequences.

- **Information security:** Preservation of confidentiality, integrity and availability of information, also involves other properties such as: authenticity, traceability, non-repudiation and reliability.

- **ISMS:** Information Security Management System
- **Information system:** it is an organized set of data, operations and transactions that interact for the storage and processing of information that, in turn, requires the interaction of one or more information assets to carry out their tasks. An information system is any software component either of internal origin, that is, developed by XXXXXXXXXXXXX, or of external origin, either acquired by the entity as a standard market product or developed for its needs.
- **Environmental control systems:** these are systems that use air conditioning, an air treatment process that allows certain characteristics of the air to be modified, fundamentally humidity and temperature, and additionally, it also allows its purity and movement to be controlled.
- **Malicious software:** is a variety of software or programs of hostile and intrusive codes that are intended to infiltrate or damage technological resources, operating systems, data networks or information systems.
- **Stakeholders:** For the practical use of the Company's Risk Management System, it is any natural or legal person with whom there is a direct or indirect relationship (employees, Board of Directors, associates, suppliers, clients, payment agencies, banks and others).
- **Third parties:** all persons, legal or natural, such as suppliers, contractors or consultants, who provide services or products to the entity.
- **IT:** refers to information technology.
- **ICT:** refers to information and communication technologies.
- **Vulnerabilities:** are the weaknesses, security holes or weaknesses inherent to the information assets that can be exploited by external factors and not controllable by the Entity (threats), which constitute sources of risk.

1. OBJECTIVE

Establish the organizational, technical, physical, and legal measures necessary to protect information assets against unauthorized access, disclosure, duplication, system interruption, modification, destruction, loss, theft, or misuse that may occur intentionally. or accidental, in any scenario where XXXXXXXXXXXXX has not authorized it. In this way, as a non-mandatory good practice, we comply with what is required in this matter, concatenated in the ISO 27001 standards, External Circulars of the Financial Superintendence 052 of 2011, 052 of 2007, 042 of 2012: Law 5271999 Law of electronic commerce, and derivatives of the previous ones

1.1. SPECIFIC OBJECTIVES

- Minimize the risk of the entity's missionary processes.
- Comply with the principles of information security.
- Comply with the principles of the administrative function.
- Maintain the trust of officials, contractors and third parties.
- Support technological innovation.
- Implement the information security management system.
- Protect information assets.
- Establish policies, procedures and instructions on information security.
- Strengthen the culture of information security in officials, third parties, apprentices, interns and clients of XXXXXXXXXXXXX
- Guarantee business continuity against incidents.

1. INFORMATION SECURITY MANUAL.

For XXXXXXXXXXXXX, information is a fundamental asset for the provision of its services and efficient decision-making, which is why there is an express commitment to protect its most significant properties as part of a strategy aimed at business continuity, administration of risks and the consolidation of a safety culture.

Aware of current needs, XXXXXXXXXXXXX implements an information security management model as a tool that allows identifying and minimizing the risks to which information is exposed, helps reduce operating and financial costs, establishes a culture of security and guarantees compliance with current legal, contractual, regulatory and business requirements.

Collaborators, external personnel, suppliers and all those who have responsibilities over the sources, repositories and information processing resources of XXXXXXXXXXXXX, must adopt the guidelines contained in this document and in the documents related to it, in order to maintain confidentiality, integrity and ensure the availability of information.

- **1. MANAGEMENT COMMITMENT.**

- The General Management of XXXXXXXXXXXXX approves the Information Security Manual as a sign of its commitment and support in the design and implementation of efficient policies that guarantee the security of the entity's information.

- The Senior Management of XXXXXXXXXXXXX demonstrates its commitment through:

- Review and approval of the Information Security Policies contained in this document.

- Active promotion of a safety culture.

- Facilitate the dissemination of this manual to all Collaborators of XXXXXXXXXXXXX.

- Ensuring adequate resources to implement and maintain information security policies.

- Verification of compliance with the policies mentioned here.

1. BREACH OF SECURITY POLICIES.

The information security policies aim to establish and strengthen the culture of information security among the Collaborators, external personnel and suppliers of XXXXXXXXXXXXX. For this reason, it is necessary that the violations of the Information Security Policies be classified, in order to apply corrective measures in accordance with the defined classification levels and mitigate possible effects on information security. Corrective measures may range from administrative actions to disciplinary or criminal actions, depending on the circumstances, if they so merit.

1. ORGANIZATIONAL STRUCTURE OF INFORMATION SECURITY.

- XXXXXXXXXXXXX will establish an information security scheme where there are defined roles and responsibilities that consider information security administration, operation and management activities.

- Senior Management of XXXXXXXXXXXXX must define and establish the roles and responsibilities related to information security at management and operational levels.

- Senior Management must define and establish the contact procedure with the authorities if required, as well as those responsible for establishing said contact.

- Senior Management must review and approve the Information Security Policies contained in this document.

- Senior Management must actively promote a culture of information security in the Entity.

- Senior Management must facilitate the disclosure of the Information Security Policies to all the entity's officials and personnel provided by third parties.

- The Technology Directorate must assign the functions, roles and responsibilities to its officials for the operation and administration of the technological platform of XXXXXXXXXXXXX. Said functions, roles and responsibilities must be documented and appropriately segregated.

- Collaborators and personnel provided by third parties who perform work in or for XXXXXXXXXXXXX, have the responsibility to comply with the policies, regulations, procedures and standards regarding information security.

9. BASE LINE OF THE POLICY

9.1 LIABILITY

It is the responsibility of the Technology Role to make use of the Information Security Policy, as part of its governance and management tools, to define the standards, procedures and guidelines that guarantee its compliance and that of the other Areas, to comply with what to its full role in matters of Information Security.

9.2 COMPLIANCE

Compliance with the Information Security Policy is mandatory. If officials, consultants, contractors, third parties violate these policies, the organization reserves the right to take appropriate action.

- XXXXXXXXXXXXX has decided to define, implement, operate and continuously improve an Information Security Management System, supported by clear guidelines aligned to the needs of the business, and to the regulatory requirements that apply to its nature.
- Responsibilities regarding information security will be defined, shared, published and accepted by each one of the employees, contractors or third parties.
- XXXXXXXXXXXXX will protect the information generated, processed or safeguarded by the business processes and information assets that are part of them.
- XXXXXXXXXXXXX will protect the information created, processed, transmitted or protected by its business processes, in order to minimize financial, operational or legal impacts due to its incorrect use. For this, the application of controls according to the classification of the information owned or in custody is essential.
- XXXXXXXXXXXXX will protect your information from threats from staff.
- XXXXXXXXXXXXX will protect the processing facilities and the technological infrastructure that supports its critical processes.
- XXXXXXXXXXXXX will control the operation of its business processes, guaranteeing the security of technological resources and data networks.
- XXXXXXXXXXXXX will implement access control to information, systems and network resources.
- XXXXXXXXXXXXX will guarantee that security is an integral part of the life cycle of information systems.
- XXXXXXXXXXXXX will guarantee, through proper management of security events and weaknesses associated with information systems, an effective improvement of its security model.
- XXXXXXXXXXXXX will guarantee the availability of your business processes and the continuity of your operation, based on the impact that events can generate.
- XXXXXXXXXXXXX. will guarantee compliance with the established legal, regulatory and contractual obligations.

9.3 EXCEPTIONS

Exceptions to any compliance with the Information Security Policy must be approved by the Technology Role, prior approval of the General Management. All exceptions to the Policy must be formally documented, recorded and reviewed.

9.4 POLICY ADMINISTRATION

The modifications or additions to the Information Security Policy will be proposed by the interested Areas and will be approved by the General Manager. These policies must be reviewed at least once a year or when necessary.

- **9.4.1. PHASES OF IMPLEMENTATION OF INFORMATION SECURITY POLICIES**

- **Development of policies:** In this phase, the Entity must make the areas responsible for creating the policies, structuring them, writing them, reviewing them and approving them; Therefore, in order to successfully complete this phase, it is required that verification and investigation activities be carried out on the following aspects:
- **Justification for the creation of the policy:** It must be identified why the Entity requires the creation of the information security policy and determine the control to which its implementation refers.
- **Scope:** The scope must be determined. To what population, areas, processes or departments does the policy apply? Who must comply with the policy?
- Roles and Responsibilities: Those responsible and the roles for the implementation, application, monitoring and authorization of the policy must be defined.
- **Review of the policy**: It is the activity through which the policy, once it has been drafted, goes through an evaluation procedure by other individuals or group of individuals who evaluate the applicability, the drafting and suggestions are made on the development and creation of the same.
- **Approval of the Policy:** The person or role of senior management that has the competence to formalize the information security policies by signing and publishing them must be determined within the entity. It is important that the Entity's Senior Management shows interest and support in the implementation of said policies.
- **Compliance:** Phase through which all those written policies must be implemented and related to information security controls, this in order that there is consistency between what is written in the policies against the implemented and documented security controls.
- **Communication**: Phase through which the policies are made known to the Entity's officials, contractors and/or third parties. This phase is very important since a large part of their compliance depends on knowledge of the content of the policies; This phase of the implementation will also allow obtaining feedback on the effectiveness of the policies, thus allowing pertinent exceptions, corrections and adjustments to be made. All contracting officers and/or third parties of the entity must know the existence of the policies, the mandatory nature of their compliance and the physical location of such document or documents, so that they can be consulted at the time they are required.
- Monitoring: It is important that the policies are monitored to determine their effectiveness and compliance. Example indicator mechanisms must be created to verify periodically and with evidence that the policy works and whether or not it should be adjusted.
- Maintenance: This phase is responsible for ensuring that the policy is updated, integrated and contains the necessary adjustments obtained from the feedback.

- Withdrawal: Phase through which a security policy is eliminated as soon as it has fulfilled its purpose, or the policy is no longer necessary in the Entity. This is the last phase to complete the life cycle of security policies and requires that this withdrawal be documented in order to have references and background on the subject.

9.4.2. DESCRIPTION OF THE POLICIES AND STANDARDS

Information is an asset that the company considers essential for the company's activities and must be protected in accordance with the principles of confidentiality, integrity and availability. Through this Policy, the company's information security objectives are disseminated, which are achieved through the application of security controls, to manage an acceptable level of risk. This document has the objective of guaranteeing the continuity of the services, minimizing the probability of exploiting threats, and ensuring the efficient fulfillment of business objectives and legal obligations in accordance with the current legal system and the security requirements aimed at preventing infractions. and security breaches

9. GENERAL POLICIES.

10.1. Responsibility for computer assets and resources.

XXXXXXXXXXXXX puts at the service of the officials the use of the necessary means for the normal development of the tasks of their respective positions, for which it adopts and communicates the policies of acceptable use, controls and measures aimed at guaranteeing the security and continuity of the service which lends

10.2. Acceptable use of computing assets and resources.

All collaborators, consultants, contractors, third parties, who use information assets owned by XXXXXXXXXXXXX, are responsible for complying with and accepting with integrity the acceptable use policy to make rational and efficient use of assigned resources.

10.3. computer users.

The head of Human Management must notify the Technology Role of all news regarding direct and indirect personnel who are users of computer assets and resources, such as income, transfers, licenses, withdrawals and vacations.

10.3.1. New Users.

All new staff of XXXXXXXXXXXXXX, must be notified by the Technology Role, to assign the corresponding rights as a computer user (Computer Equipment, Network User Creation, User Profile in the Active Directory) and corporate email account.

10.3.2. Partial withdrawal of the user.

When the computer user is absent from his work due to vacations, disabilities or licenses, this situation must be reported by the immediate Manager to the Technology Role to partially inactivate the rights of the computer user.

10.3.3. Final withdrawal of the user.

In case of definitive withdrawal of the Collaborator in XXXXXXXXXXXXX, the Technology Role will annul and cancel all the rights granted as a computer user.

10.3.4. Obligations of the Users.

- All users of information services are responsible for the username and password they receive for the use and access of resources.

- All users must be authenticated by the access control mechanisms provided by the Technology Role before being able to use the technological infrastructure in XXXXXXXXXXXXX.

- Users must not provide information to external personnel about the access control mechanisms to the facilities and technological infrastructure of XXXXXXXXXXXXX, unless they have the approval of the General Management.
- Each user who accesses the technological infrastructure of XXXXXXXXXXXXX must have a unique and personalized user identifier (ID). Therefore, the use of the same ID by several users is not allowed.
- Officials are responsible for all activities carried out with their user identifier (ID). Users must not disclose or allow others to use their user IDs, just as you are prohibited from using other users' IDs.

- Users must keep their computer equipment locked when they are not at their workplace.

10.3.5. User rights.

Computer security training: Every employee at XXXXXXXXXXXXXX must have induction on the Computer Security Policies and Standards, where the obligations for users and the sanctions they may incur in case of non-compliance are disclosed.

10.3.6. User sanctions.

- Serious violations are the theft, damage, disclosure of proprietary or confidential information from XXXXXXXXXXXXX, or being found guilty of a computer crime.

- The entry and exit of visitors to the work areas in XXXXXXXXXXXXX must be registered at the reception, indicating the date and time of entry and exit of the same.

- Any person who has access to the facilities of XXXXXXXXXXXXX and who enters with computer equipment, communications equipment, storage media and tools that are not owned by the entity, must be registered at the time of entry, in the reception role or goal, which can be removed the same day. Otherwise, you must process the corresponding exit authorization before the Technology Role.

- The Server room is a restricted Role, so only Technology Role personnel can access it.

10.4. Physical access controls.

10.5. Physical and environmental security.

- The user or official must report immediately to the Technology Role when a real or potential risk is detected on computer or communications equipment, such as waterfalls, electric shocks, falls or blows or fire hazard.

- The user or official has the obligation to protect the storage units that are under their responsibility, even when they are not used and contain confidential or important information.

- It is the responsibility of the user or official to avoid at all times the leakage of information from the entity that is stored in the personal computer equipment assigned to him.

10.6. Protection and location of equipment.

- Officials must not move or relocate computer or communications equipment, install or uninstall devices, or remove seals from them without the authorization of the Technology Role. If this service is required, they must request it.

- The Technology Role will be in charge of generating the receipt and obtaining the signature of the IT official as the person responsible for the IT assets assigned to him and of keeping them in the location authorized by Technology.

- The assigned computer equipment must be for the exclusive use of the functions of the employees of XXXXXXXXXXXXX.

- It will be the official's responsibility to request the necessary training to manage the computer tools used in their team, in order to avoid risks due to misuse and to make the most of them.

- It is the responsibility of the employees to store their information only in the different hard drive partition intended for program files and operating systems: Documents / My Documents

- Avoid placing objects on top of the computer equipment or covering the ventilation outlets of the monitor or the CPU.

- The official must ensure that the connection cables are not stepped on when placing other objects on top of or against them in the event that a cable relocation request is not fulfilled with the Technology staff.

- It is forbidden for the official other than the Technology staff to open or uncover the computer equipment.

10.6. Equipment maintenance.

- Only personnel authorized by the Technology Role may carry out services and repairs to computer equipment.

- Officials must make sure to store the information in the BACKUP folder created in each computer equipment in order to back up the information generated with scheduled backups to this folder the information they consider relevant when the

equipment is sent for repair and erase that sensitive information found in the equipment, thus preventing the involuntary loss of information, derived from the repair process.

10.7. Use of removable devices.

- Access to external storage devices such as USB Flash Drives, Portable Drives, External CD and DVD Drives is restricted in XXXXXXXXXXXXX.

- If any role or dependency for very specific requirements of the type of application or information services have the need to have one of them, it must be justified and authorized by the Technology Role with the respective approval of the Head of the Unit.

- The official who is allowed to use these devices will be responsible for the proper use of them.

10.8. Management of operations in computer equipment.

- Collaborators must protect the information used in the technological infrastructure of XXXXXXXXXXXXX. In the same way, the reserved or confidential information that must be saved, stored or transmitted, either within the company's internal network to other dependencies and/or regional or external networks such as the Internet.

- Users and Collaborators of XXXXXXXXXXXXX who make use of computer equipment must know and apply the measures for the prevention of malicious code such as viruses, Trojan horses or network worms.

- When an unauthorized official or a visitor requires the need to enter the Server room, they must request it through an internal communication duly signed and authorized by the Director of Technology and for a visitor, the visit must be requested in advance, and where the type is specified. of activity to be carried out, and always have the presence of an official from the Technology Role.

- The computer equipment, peripheral or information technology accessory that suffers any damage, abuse, carelessness or negligence by the responsible user, a report of non-compliance with security policies will be filed.

- The technology role support technician ensures, through the Secure Deletion instructions, the elimination of information from the computer equipment that must be reassigned to new employees.

- The technology role support technician ensures with the application of the safe deletion instructions that the computer equipment that suffers irreparable damage and must be removed from the asset inventory in XXXXXXXXXXXXX, the activities and controls necessary for formatting must be applied. and destruction of the same in order to ensure that their elimination is carried out safely.

10.3. Clean desktop and screen policy.

In order to reduce the risk of unauthorized access, loss and damage to information during and outside of users' normal business hours, the following guidelines should be observed:

- The personnel of XXXXXXXXXXXXX must keep their desktop free of the entity's own information, which may be accessed, copied or used by third parties or by personnel who do not have authorization for its use or knowledge.

- XXXXXXXXXXXXX staff must lock their computer screen with the screen saver, when they are not using the equipment or when they have to leave their job for any reason.

- When printing documents of a confidential nature, they should be removed from the printer immediately.

10.3. Use of printers and the Printing service.

- Ensure the correct and safe operation of the printers and the printing service, following the following guidelines:

- The documents that are printed on the DAPRE printers must be of an institutional nature.

- It is the user's responsibility to know the proper handling of the printing equipment (scanner and photocopier) so that its correct operation is not affected.

- No user should carry out repair or maintenance work on the printers. In the event of any failure, it must be reported to the Technology Role.

10.9. Use of Email.

The use of the Internet must be exclusively destined to the execution of the activities of the organization and must be used by the employee to carry out the functions established for his position, for which the following parameters are defined for its use:

- The Technology Role will be in charge of providing the corporate mail service, as well as monitoring its correct use and operation. For this purpose, it will assign an account that has an associated mailbox, in which all messages sent and received are stored.
- Each user must continually purge their mailbox in order to always keep space available for new messages.

- The information contained in the mail is considered private information and therefore must be handled as a private and direct communication between the sender and the recipient.

- The email account is non-transferable, and the account cannot be shared.

- Each user is responsible for the information sent or forwarded from their email account.

- Although the entity has a virus checking service for incoming email messages, email users should be careful when deciding to open attachments placed in messages from unknown or suspicious senders. If messages with this feature arrive, the Technology Role must be informed.
- he employees of XXXXXXXXXXXXX may not use e-mail addresses other than the official accounts to attend to the affairs of the Entity.

- Corporate email users should not send emails with attached documents whose weight exceeds 8 Megabytes.

- It is forbidden to send or reply to chain messages to a person or group of people.

- Corporate email users must not promote through the corporate account certain goods or services that are not related to the objectives of XXXXXXXXXXXXX.

- The use of email for purposes other than the objectives of XXXXXXXXXXXXX is prohibited.

- Corporate email users must not misrepresent, hide, suppress or substitute the identity of an email user.

- It is prohibited to intercept, disclose or assist third parties to intercept or disclose electronic communications.

10.10. Controls against viruses or malicious software.

- The Technology Department must ensure that antivirus software is installed on all computer equipment and that it is updated through a scheduled task.

- To prevent computer virus infections, users of computer equipment at XXXXXXXXXXXXX must not use software that has not been provided and validated by the Technology Role.

- All computer files that are provided by external or internal personnel considering at least software programs, databases, documents and spreadsheets that have to be decompressed, the user must verify that they are virus-free using authorized antivirus software before running.

- Any user who suspects a computer virus infection must immediately stop using the equipment and notify the Technology Role for the review and eradication of the virus.

10.11. Shared resources.

The use of shared folders on the XXXXXXXXXXXXX network is a practice that, although it can be a useful work tool, has some implicit risks that can affect the principles of confidentiality, integrity and availability of information, therefore its use and application It's controlled.

For this purpose, the following guidelines are defined for its safe use:

- The support technician establishes and implements, in approved cases, the configuration of access to the folder, prior formal request of the same through the technology role.

- The users to whom the shared resource is authorized and available are responsible for the actions and access to the information contained in said folder.

10.12. Controls for the Generation and Restoration of Backup Copies (Backups).

Procedure for generating and restoring backup copies to safeguard the critical information of the entity's significant processes. The following aspects are considered as a minimum:

- The technology department will carry out the backup copy to the BACKUP folder created on each computer through a scheduled task.
- The storage of information in this folder is the responsibility of each user.
- The information in shared folders and with access restricted to authorized users will be backed up.
- Backup copies will be made weekly on Fridays at 5:30 p.m.

- **0.13. Internet browsing.**

- Internet access provided to users and officials of XXXXXXXXXXXXX is exclusively for activities related to the needs of the position and functions performed.
- Users of the Internet browsing service, by accepting the service, are accepting that:
- They will be subject to monitoring of the activities carried out on the Internet, they know that there is a prohibition on access to unauthorized pages, they know that there is a prohibition on the transmission of unauthorized reserved or confidential files.

- They know that there is a prohibition to download software without the authorization of the Technology Role.

- The use of the Internet is for the performance of their functions and position in XXXXXXXXXXXXX and not for personal purposes.

- The Technology Directorate, through traffic monitoring and analysis tools, will detect users who misuse Internet services.

- The Role of Technology is empowered to block all those Internet sites that it considers are not compatible with the work of officials. If there are exceptions due to duly justified causes, the Head of the corresponding Unit must submit the request by means of a

memorandum, explaining the causes of the exception to the Technology Role for its study and approval.

- Wi-Fi access will be allowed to visitors and suppliers who require it, upon request to the Technology Role of the official in charge of visiting staff.

- Entering pornographic pages, downloading music and video, especially with the services provided by specialized pages for this purpose, as well as using or participating in online entertainment games is prohibited.

- Do not use the radio and TV services through the Internet, in case this information is required for the development of the functions in charge, the Head of the corresponding Unit must present the request by means of a memorandum, stating the causes of the exception before the Technology Roll for study and approval.

- Do not access pages related to social networks during the working day.

- The download of files from the Internet must be for work purposes and in a reasonable way so as not to affect the Internet service, specifically the user must comply with the requirements of the Internet use policy described in this manual.

10.14. Controls to Grant, Modify and Withdraw Access to Users.

- The creation of a new user within the Information systems in XXXXXXXXXXXXX, must be sent to the Technology Role accompanied by the request duly signed by the Head of Area, otherwise the request will not be processed.

- The Technology Role, headed by the Technology Director, will be responsible for executing the registration, cancellation or profile changes of users.

- The creation of entry cards for new users for the headquarters of XXXXXXXXXXXXX must be sent to the Director of Technology by the Head of Human Resources with the data of the user to be created and the access privileges they must have.

10.15. Administration and use of passwords.

- The assignment of passwords is done individually, so the use of shared passwords is prohibited.

- When a user forgets, blocks or loses his password, he must go to the Technology Role to be given a new password.

- It is forbidden for passwords to be found in legible form on any printed medium and to leave them in a place where unauthorized persons can discover them.

- Regardless of the circumstances, passwords should never be shared or revealed. Doing this makes the user who lent their password responsible for all actions carried out with it.

- Any user who suspects that his password is known by another person must change it immediately.

10.16. Software Acquisition.

- It is considered a serious offense for officials to install any type of program (software) on their computers, workstations, servers, or any equipment connected to the XXXXXXXXXXXXX network, which is not authorized by the Technology Role.

- The management control for the licenses and the inventory of the Media will be the responsibility of the Technology Role.

- The Technology Role must maintain an inventory of physical equipment and installed programs and may delete or install authorized and legally licensed programs or software.

10.17. Computer Security Compliance Policy.

One of the functions of the Technology Role is to propose and review compliance with security standards and policies, which guarantee preventive and corrective actions for the safeguarding of computer equipment and facilities, as well as automated information databases in general.

Intellectual property rights, the systems developed by internal or external personnel that control the Technology Role are the intellectual property of XXXXXXXXXXXXX.

10.18. Compliance clauses.

- The Technology Role will carry out actions to verify compliance with the Information Security Policies and Standards Manual.

- The Technology Role may implement control mechanisms to identify trends in the use of computer resources by internal or external personnel, to review the activity of the processes executed and the structure of the files that are processed. The misuse of computer resources that is detected will be reported to the General Management.

- The managers and those responsible for the processes established in XXXXXXXXXXXXX must support the reviews of the compliance of the systems with the appropriate computer security policies and standards and any other security requirements.

10.19. Computer security violations.

- The use of hardware or software tools to violate computer security controls is prohibited.

- No officer of XXXXXXXXXXXXX should test or attempt to test known Computer Security flaws.

- Do not intentionally write, generate, compile, copy, collect, propagate, execute or attempt to introduce any type of code (program) known as viruses, worms or Trojan horses, designed to self-replicate, damage or affect performance or access to the computers, networks or information of XXXXXXXXXXXXX.

11.1. SECURITY ORGANIZATION

11.1.1. Security Organization Policy

The Technology Role is responsible for defining, coordinating and controlling the necessary management to mitigate the risks associated with information security in XXXXXXXXXXXXX and will report to the INFORMATION SECURITY COMMITTEE, said committee is made up of the Technology Role, which chairs ; the Risk Role and the roles that may eventually be required, in order to comply with and support Information Security activities.

11.2.1. Security Organization Policy Standards

11.2.1.2. Responsibilities for information security.

XXXXXXXXXXXXX is the owner of the information. Its possession and management are delegated to those responsible for the Areas, who are responsible for the custody of the information they generate and use, considering its purpose and use. For this reason, those

responsible for Role must be aware of the risks to which the information in their charge is exposed, so that they exercise the appropriate leadership with their officials to reduce them.

11.2.2. Contact with authorities and interest groups.

XXXXXXXXXXXXXX, you must maintain contact with the authorities and interest groups to keep up to date with changes in electronic government regulations in Colombia and identify trends in Information Security.

11.2.3. Independent review on information security.

Internal Audit must implement and execute an internal information security audit plan. This plan should be focused on reviewing all security requirements (policies and procedures). The results must generate a safety program, which includes at least: actions to be carried out, timetables and those responsible. The program must be approved by the Information Security Committee.

11.2.4. Security in Accesses by Third Parties.

The Technology Role must carry out a risk assessment to identify the risk of access by third parties to the information of XXXXXXXXXXXXX. Each Role must verify the implementation of agreements, monitor compliance with them and manage changes to ensure that the services provided meet the requirements agreed with third parties.

Any request for access or use of the Technological component of XXXXXXXXXXXXX by a third party requires the performance of a risk analysis prior to the use of said resources. This analysis must be carried out by the Information Security Committee together with the administrator of the Technological platform.

The risk analysis must be carried out on any third party that requires interaction with the technological components, information systems and data networks of XXXXXXXXXXXXX.

The identification and analysis of risks must be carried out taking into account the following aspects:

- The type of service and the physical and logical access to be used.
- The type of information and its criticality.
- The staff of the third party that will interact.

- The level of impact that access to resources by the third party will have.
- The relevant legal and regulatory requirements associated with the third party and with the activities to be carried out.

In the case of submitting a contract with a third party (customers or suppliers), the Information Security policies apply equally to third parties, and they must also comply with national and international laws and regulations regarding copyright and intellectual property., electronic commerce and electronic data interchange. Any lack of information security policies by an external party will be subject to the measures established by XXXXXXXXXXXXX. Any technological change must be previously informed to XXXXXXXXXXXXX and authorized by the Company.

In relations with clients, the third party is the one who defines the initial parameters of Information security in accordance with its internal policies and it is the duty of the Information Technology Management

11.3. CLASSIFICATION AND CONTROL OF INFORMATION ASSETS

11.3.1. Policy for the classification and control of information assets

The information must be inventoried and have the security risks and exposures identified; In order to avoid financial, operational and/or image losses for the company, the information must be classified as secret, restricted or general. Secret and restricted information must be supported by a confidentiality or non-disclosure agreement when shared with third parties.

11.3.2. Information asset classification and control policy standards

11.3.2.1. Liability over assets.

XXXXXXXXXXXXX puts at the service of the officials the use of the necessary means for the normal development of the tasks of their respective positions, for which it adopts and communicates the policies of acceptable use, controls and measures aimed at guaranteeing the security and continuity of the service which lends

Regarding the owners of information assets, information users must act as owners of the entity's physical and electronic information, thus exercising the power to approve or revoke

access to their information with the appropriate profiles for that purpose. They must generate an inventory of said assets for the areas or processes they lead, accepting the indications of the information classification guides; likewise, they must keep the inventory of their information assets updated. They must periodically monitor the validity of users and their information access profiles. They must be aware that the institute's information processing resources are subject to audits and compliance reviews by control entities.

11.3.2.2. Asset classification methodology.

To ensure that information assets receive the appropriate level of protection, the Technology Role is responsible for defining the methodology for classifying information assets, these must be classified according to need, priorities and the degree of protection expected in the management thereof.

11.4 ACCEPTABLE USE OF ASSETS AND RESOURCES

11.4.1. Acceptable Use Policy for Assets and Information Resources

All officials, consultants, contractors, third parties, who use information assets owned by XXXXXXXXXXXXX, are responsible for complying with and accepting the Acceptable Use Policy with integrity in order to make rational and efficient use of assigned resources. Standards for the acceptable use of information assets Information Security Policy

11.4.2. Use of computer systems and equipment.

The organization has a disclaimer rule that must be used when logging into the computer equipment:

"Caveat! This system (hardware, software and peripherals), as well as the information contained therein, is the property of the company and its use is restricted solely for business purposes, reserving the right to monitor it at any time. Any unauthorized use, modification or access to this system will give rise to the corresponding disciplinary and/or legal actions. The entry and use of this system implies your consent to this policy."

The Technology Role must provide the necessary mechanisms and strategies to protect the confidentiality, integrity and availability of technological resources, inside and outside the facilities of XXXXXXXXXXXXX. It must carry out preventive and corrective maintenance of the resources of the technological platform. It must ensure that the computer equipment loading and unloading areas are isolated from the computer center and other information processing areas. You must generate secure configuration standards for the computer equipment of the institute's officials and configure said equipment accepting the generated standards. You must establish the conditions that must be met by personal computer equipment provided by third parties that require connection to the institute's data network and verify compliance with said conditions before granting these computers access to network services. You must isolate computers from sensitive areas, such as the Treasury Role, to protect their access from other employees on the company network. You must generate and apply guidelines for the safe disposal of the computer equipment of the institute's officials, either when they are discharged or change users. You must review physical access during non-business hours to the areas where information is processed.

The Internal Audit Role is responsible for including within the annual audit plan the random verification of the computer equipment of all dependencies and service points of the entity.

The Risk Role must evaluate and analyze the verification reports of computer equipment from the different areas of the institute, particularly sensitive areas.

11.4.3. Email.

The organization, as a sign of respect for the principles of freedom of expression and privacy of information, does not generate any expectation of privacy in any element that it stores, sends or receives through the electronic mail system owned by the company; accordingly, you may deny access to email services, inspect, monitor and/or cancel an assigned mailbox. Communications by email between the company and its public of interest must be made through the mail approved and provided by the company. It is not allowed to use personal accounts to communicate with the public of interest of the organization, nor to transmit any other type of business information. Officials who, according to their functions, require an email account, this is assigned to them once they are linked. The Human Management Role is responsible for informing the Technology Role of the links that require the creation of an email account; In the same way, it must promptly inform the withdrawals of officials for the suspension of this service. This account will be active for the duration of the employee's relationship with the company, except in cases of force majeure or misuse that may eventually cause the suspension or cancellation of the account. Once the person is unlinked, the account will be removed from the server through a request sent to the service desk. The maximum capacity for email storage is defined by the Technology Role and depends on the type of user. However, in case of special needs, the interested party may request an

increase in capacity. Similarly, if necessary (for business or technical reasons), the maximum capacities of mailboxes may be unilaterally modified by the company.

The monitoring system will filter the files attached to email messages to verify the absence of viruses. The delivery of any message to its final recipient is subject to the success of this check. The organization has a disclaimer rule that must always be used in messages. To avoid legal claims, all users of the company's mail must make public the waiver of legal responsibility for sending the information. The approved disclaimer is:

"The information contained in this message and its attachments is strictly confidential. If you received this communication by mistake, please immediately notify this circumstance by forwarding it to the sender's email and delete it, since its unauthorized use will carry the sanctions and legal measures that may apply. The company is not responsible for the presence in this message or in its annexes, of any virus or malware that may cause or cause damage to your equipment, programs or affect your information.

The information contained in this message and its attachments is strictly confidential. If you received this communication in error, please immediately notify the sender of the situation by replying to it to sender email address and delete this message as its unauthorized use shall derive in applicable penalties and legal actions. The Company is not liable for the presence of any virus or malware in this message or its attachments that cause or may cause damage to your equipment, software or that affects your information."

- The mailbox is personal and non-transferable, and it is up to the collaborator to ensure security by protecting their access code. The user is solely responsible for the proper use of their email account. Consequently, by accepting the mailbox granted by the organization, the user agrees to:
- • Respect the privacy of the accounts of other users of the service, both inside and outside the corporate network. The user may not use fictitious identities or those belonging to other users to send messages.
- • The collaborator who owns the email or account assigned by the organization, will use the email to send and receive messages necessary for the development of the tasks of their position or the investigations assigned to them; Only people responsible for Role can approve mass mailings to company officials.
- • The use of electronic mail owned by the company must be used only for the organization's own purposes. In its use, the collaborator will always act with respect and courtesy; may not create, distribute or forward messages that offend the dignity, privacy and good name of people, institutions, or to carry out any type of harassment, defamation, slander, with the intention of intimidating, insulting or any other form of hostile activity ; In the same way, it is prohibited to spread political, religious ideas, propaganda, among others.

- • The company refrains from sending or receiving messages from its users with inappropriate, defamatory, illicit, obscene, indecent content or that contain news dissemination without fully identifying its author; Additionally, officials may not send anonymous, advertisements or literature of any kind, surveys, contests, pyramid schemes, chain letters, unwanted messages, or any that contain duplicative or unsolicited messages, or other information unrelated to the work they perform. in your charge.
- • Company officials will refrain from using the account to send or forward spam messages (unsolicited, unwanted or unknown sender, usually advertising type, sent in large numbers), hoax (it is an attempt to make believe that something false is real), with content that may be offensive or harmful to other users (such as viruses or pornography), or that is contrary to institutional policies and regulations.
- • Avoid sending from your mailbox elements (texts, software, music, images or any other) that contravene the provisions of current legislation and internal regulations on intellectual property and copyright. In particular, it is necessary to avoid the distribution of software that requires a license, illegal software keys, programs to break licenses (crackers), and in general, any element or data object without the specific permission of the author when this is required. The violation of this obligation automatically causes the suspension of the service and may be the cause of sanctions to the user, to the detriment of the responsibilities that may eventually arise before the law.
- Carry out periodic maintenance of your mail, when the system warns you of available space. These warnings are made several times, so you must be attentive and inform the computer services desk, when you require debugging.
- • Use the corporate email account for work purposes, research and those strictly related to the activities of their work. Officials must avoid using the mailbox for commercial purposes other than those related to the interest of the company.
- • The collaborator must purge the content of the inbox on the server on a monthly basis to prevent messages from remaining in it for an excessive amount of time, leading to congestion or blockage.
- • Respect the privacy of the accounts of other users of the service, both inside and outside the corporate network.
- • Avoid sending copies of replies to all the recipients of a received message, and in particular when it comes to messages that were originally addressed to a large group of users; except in the case of a response that, due to its nature or content, necessarily requires to be known by all of them.
- • Avoid opening unexpected messages that contain attachments, even if they come from people you know. It could be a virus. In particular, do not open messages whose subject contains English words unless you are expecting it.

- • As far as possible, it is necessary to avoid using capital letters, especially in the "Subject:" field, as well as the excessive use of exclamation marks (&, %, $, #, ?, i, !, ¿), this can cause mail systems to identify it as spam, and the message may not reach the recipient, or arrive with spam identification.
- • If you use the mail service through the company website, it is recommended that you do not leave messages stored for a long time on the mail server. Keep in mind to download them frequently, preferably daily. Please note that the size of your mailbox is limited; once this limit is exceeded, the system will not process any more emails. Delete messages if you need to and empty the trash whenever possible.

11.4.5. Use of tools that compromise security.

Doing or attempting to do, without permission of the owner or host of the system or Technology Role, any of the following acts:

- Access the system or network.
- Monitor data or traffic.
- Probe, copy, test firewalls or hacking tools.
- Attack the vulnerability of the system or networks.
- Violate system or network security measures or authentication routines.

11.4.5.1. Shared resources.

The use of shared folders on users' computers is a practice that, although it can be a useful work tool, has some implicit risks that can affect the principles of confidentiality, integrity and availability of information, therefore its use and application must be controlled. For this purpose, the organization defines the following guidelines for its safe use:

- The use of shared folders on desktop computers should be avoided.
- The network administrators establish and implement, in approved cases, the configuration of access to the folder, following a formal request from the same through the Service Desk.
- The user who authorizes and provides the shared resource is responsible for the actions and access to the information contained in said folder.
- The type of access and the strictly necessary roles on the folder (reading, writing, modifying and deleting) must be defined.
- The time limit during which the information will be published, and the resource shared in the team must be clearly specified.
- If it is confidential or critical information for the company, the folders intended for this purpose must be used on the user file server, so that they are included in the daily backup copies of information or implement tools for the continuous backup of information. on said equipment.

- Access to shared folders should be limited to the users who need them and should be protected with passwords.
- Access to these folders should not be allowed to users who do not have updated corporate antivirus.

11.4.5.2. Web sites to share documents.

The owner of the site will be responsible for its security and access to the information that is hosted.
- The site owner will be responsible for granting the required permits.
- The owner of the site will define a delegate who has full control over the site, as a contingency, for the assignment of the required permissions in his absence.

11.4.5.3. Cloud computing.

No information of XXXXXXXXXXXXXX may use cloud computing technologies if it is not previously authorized by the Technology Role.

11.4.5. I use laptops and mobile devices.

Officials, contractors and third parties agree to make appropriate use of mobile devices to access corporate mobility services provided by the company, such as virtual desktops and applications, mail, unified communications, virtual private networks (VPN), among others. others, according to the following guidelines:
- The mobile device must be in a pocket, briefcase or place not visible in public places.
- The mobile device must be configured to automatically lock in inactivity time through available configuration means such as password, fingerprint pattern, voice recognition, among others.
- Use of antivirus application.
- Use of secure and encrypted channels when connecting to shared, freely accessible, non-secure networks.

11.4.5. Access of teams other than those assigned.

All Company officials, from their role and competence, have the obligation to:
- Deactivate the password autosave option in the different web browsers.
- Do not leave passwords in any web information storage system.

- Creation of secure passwords, do not include personal information such as names, dates of birth, etc.
- Logged out of virtual desktop when not in use.

The Technology Role must implement the necessary measures to protect against the risk of using mobile equipment and communication. Special care will be taken to ensure that business information is not compromised, taking into account the risks involved in working with mobile equipment in unprotected environments. The use of mobile services connected to networks must have adequate protection. Remote access to business information over public networks using mobile computing services should only take place after successful identification and authentication and with the establishment of adequate access control mechanisms.

11.4. INFORMATION SECURITY RISK TREATMENT AND MANAGEMENT

11.4.5. Information Security Risk Treatment and Management Policy

The Technology Role is responsible for analyzing information security risks, based on business objectives and in accordance with the Risk Management Policy and with the approval of the Information Security Committee. Area managers are responsible for prioritizing and treating information security risks in accordance with the company's risk appetite.

11.4.5. Information Security Risk Treatment and Management Policy Standards

A risk assessment should be carried out periodically to take into account changes in security requirements and the risk situation, such as changes in assets, threats, vulnerabilities and impacts. You must decide when a risk is acceptable, either for reasons of business objectives or unprofitable costs. Possible treatments for identified risks include:

- Avoid risk.
- Reduce the probability of occurrence.
- Reduce the impact.
- Transfer risks.
- Retain risks.

11.4. STAFF SAFETY

11.6.1. Staff Responsibility Policy

The Human Management Role must notify the Technology Role of all news regarding direct and indirect personnel such as admissions, transfers, delegations, withdrawals and vacations.

11.6.2. Staff Security Policy Standards

11.6.2.1. Security prior to the hiring of personnel and personnel provided by third parties.

For every person who joins the company, the Human Management Role must ensure safety responsibilities prior to hiring. This task must be reflected in an adequate job description and in the terms and conditions of the contract.

11.6.2.2. Security during the contract.

The Human Management Role must develop an effective and continuous information protection awareness program for all personnel. Specific training in technological risk management is also required for those individuals who are in charge of special protection responsibilities and the basic concepts that all employees must comply with. It is the responsibility and duty of each collaborator of XXXXXXXXXXXXX to attend the information security awareness courses scheduled by the company and to apply security according to the policies and procedures established by the company.

11.6.2.3. Termination or change of position.

The Human Management Role must ensure that all officials, consultants, contractors, third parties, who leave the company or change jobs, have signed a confidentiality agreement, compliance with which will be in force until XXXXXXXXXXXXX deems it convenient, even after the end of the job or the contract. The Human Management Role will ensure that the departure or mobility of officials, contractors or third parties is managed until the complete return of all assets and withdrawal of access rights.

11.7. PHYSICAL, ENVIRONMENTAL AND SURROUNDING SAFETY

11.7.1. Physical and Environmental Security Policy

The data processing center and technological equipment room must be in areas physically protected against unauthorized access, damage or interference and must comply with physical security policies.

11.7.1.1. Standards of the Physical and Environmental Security Policy

11.7.1.1.1. Physical access controls.

Access to restricted ICT areas should only be allowed for:
- Development of technological operations.
- Cleaning tasks (monitored by personnel from the Technology Management Role).
- Equipment tests.
- Equipment storage.
- Implementation or maintenance of environmental controls.

The Technology Role must provide the necessary physical and environmental conditions to certify the protection and correct operation of the technological platform resources located in the computing center; There must be environmental control systems for temperature and humidity, fire detection and extinction systems, electrical discharge systems, surveillance and monitoring systems, and alarms in case inappropriate environmental conditions are detected. These systems must be permanently monitored. If something is not within your competence for this purpose, you must manage it. You must ensure that the technological platform resources of XXXXXXXXXXXXX located in the computer center are protected against electrical failures or interruptions. You must certify that the computer center and the wiring centers that are under your custody are separated from areas that have flammable liquids or that are at risk of flooding and fire. It must ensure that the maintenance tasks of electrical, voice and data networks are carried out by suitable and properly authorized and identified personnel; Likewise, control of the preventive maintenance schedule must be kept. It is in charge of the acquisition, installation and environmental protection of the Technological equipment and components of the Companies. It is also in charge of the installation, configuration and maintenance of environmental control devices in the data centers. You must prepare and formalize preventive maintenance schedules for the equipment and components under your responsibility, with an annual review of compliance,

and you must coordinate its execution with the Computer Center Administrator. You must establish a test schedule for environmental control systems, taking into account the type of system, criticality and impact of each computer center.

Role managers who are in restricted areas must monitor the effectiveness of physical access controls and surveillance equipment implemented in their areas. They must authorize any temporary entry to their areas, evaluating the relevance of the entry; likewise, they must delegate to Rol personnel the registration and supervision of each entry to their areas. They must ensure that the passwords for alarm systems, safes, keys and other security mechanisms for access to their areas are only used by authorized officials and, except in emergency situations or other types of events that by their nature require it, these are not transferred to other officials of the institute.

Officials and personnel provided by third parties must fully comply with the physical controls implemented. They must carry the card that identifies them as such in a visible place while they are in the institute's facilities; In case of loss of the card or access card to the facilities, they must report it as soon as possible. They must not attempt to enter areas to which they are not authorized.

Any event reported by an environmental control system connected to the security role's alarm panel must be notified by every official to the Technology role.

At least every 30 days cleaning work must be carried out in the computer centers. Only personnel authorized by the Technology Role should enter the computer center to perform these tasks. Said Role must periodically verify that the computer center is in a perfect state of cleanliness and organization.

Computer centers and wiring centers must not house obsolete equipment or spare parts, waste or electronic elements and, in general, any combustible material such as clothing, stationery, boxes; that may generate some type of negative event that affects the technological component of the computing center.

11.7.1.1.2. Clean desk.

Implementing a clean desk policy will help reduce the risk of unauthorized access or damage to media and documents. Computers must be locked after ten (10) minutes of inactivity, the user will have to authenticate before resuming their activity. All officials, consultants, contractors, third parties, must block the session when leaving their computer.

11.7.1.1.3. Equipment safety.

To prevent the loss of information, damage or compromise of information assets and the interruption of the activities of XXXXXXXXXXXXX, the equipment must be connected to the regulated outlet intended for this purpose.

11.7.1.1.4. Equipment removal.

The equipment installation and removal processes must be taken into account, in such a way that they are done in a controlled and safe manner. Protecting equipment, even when used outside the office, is necessary to reduce the risk of unauthorized access to information and to protect against loss or theft.

11.8. INFORMATION ACCESS CONTROL

11.8.1. Information Access Control Policy

The Technology Role, according to the classification of information assets, must implement the applicable security measures according to the case, in order to avoid adulteration, loss, leakage, consultation, use or unauthorized or fraudulent access. The access control of data and sensitive information must be based on the principle of least privilege, which implies that access will not be granted unless it is explicitly allowed. You must periodically verify the access controls for users provided by third parties, in order to check that said users are allowed access only to those network resources and technology platform services for which they were authorized.

Officials and personnel provided by third parties, before having logical access for the first time to the XXXXXXXXXXXXX data network, must have the duly authorized user account creation format and the Confidentiality Agreement previously signed. The end-user computer equipment that connects or wishes to connect to the Company's data networks must comply with all the requirements or controls to be authenticated in them and may only perform the tasks for which they were authorized. Officials and personnel provided by third parties, before having logical access for the first time to the XXXXXXXXXXXXX data network, must have the duly authorized user account creation format and the Confidentiality Agreement previously signed. The end-user computer equipment that connects or wishes to connect to the Company's data networks must comply with all the requirements or controls to be authenticated in them and may only perform the tasks for which they were authorized.

11.8.2. Information Access Control Policy Standards

11.8.2.1. User access management.

The Technology Role will establish formal procedures to control the definition of profiles and the assignment of access rights to users, previously defined by the Role responsible for the process. Such procedures should cover all stages of the user's life cycle, from their initial registration to the deletion or deregistration of those who do not need access. Special attention and monitoring should be given, where appropriate, to the need to control privileged access assignments. You must establish a formal procedure for the administration of users in the institute's data networks, technological resources and information systems, which includes the creation, modification, blocking or elimination of user accounts. You must define guidelines for the configuration of passwords that will apply to the technological

platform, network services and information systems of XXXXXXXXXXXXX; These guidelines must consider aspects such as length, complexity, periodic change, historical control, blocking due to the number of failed authentication attempts, and password change on first access, among others. You must establish a procedure that ensures the elimination, reassignment or blocking of the access privileges granted to technological resources, network services and information systems in a timely manner, when employees leave, take leave, vacation, are transferred or they change positions. It must be ensured that the users or user profiles assigned by default to the different resources of the technological platform are disabled or eliminated.

11.8.2.2. User Registration.

All users must have a unique personal or legal identification, which will be used to track activities of individual or legal responsibility. Regular user activities should not be performed through privileged accounts. In exceptional circumstances, for the benefit of the company, a shared identifier may be used, for a group of users with specific work; this must be authorized and duly approved by the Technology Role. The user must have authorization from the respective Role to use the information system or service. It must be verified that the level of access granted is adequate for the purposes of the company and that they maintain an adequate segregation of functions. Additionally, they must take and certify the training and thus guarantee the proper use of the information system or service.

11.8.2.3. User Responsibilities.

An effective security requires the cooperation of authorized users, who must know their responsibilities for the maintenance of effective access controls, in particular, those with reference to the use of passwords, The Role of Technology will implement the necessary procedures that allow controlling the creation, modification, deactivation and elimination of users, administration of passwords and access permissions to technological resources and information. Additionally, it is necessary to implement a procedure for periodic review of user access permissions. Officers, contractors, and third parties understand the terms of access and must keep personal passwords confidential and group passwords only among group members. This statement can be included in the terms and conditions of employment. They must also comply with good practices in the selection and use of the password.

11.8.2.4. Network access control.

Officials should only be provided with access to services for which they have been specifically authorized to use. Appropriate authentication methods must be used to control access to remote users. Additional controls should be implemented for access over wireless networks.

Adequate network segregation must be established, separating network environments from users and services.

11.8.2.5. Access control to applications and information systems.

The use of programs that may be capable of overriding system and application controls should be restricted and strictly controlled. Idle sessions should be closed after a defined period of inactivity, and restrictions on connection times should be used to provide additional security for high-risk applications. Default tool or product user accounts should be disabled immediately after installation of the systems or software. Vendor default passwords must be changed immediately after installation of systems or software. The Technology Role must integrate applications with Active Directory.

The owners of information assets must authorize access to their information systems or applications, in accordance with the established profiles and the needs of use, following the established procedures. They must periodically monitor the profiles defined in the information systems and the privileges assigned to the users who access them.

The Technology Role will designate those responsible and establish procedures to control the installation of operating software, will ensure that it has the support of the providers of said software and will ensure the functionality of the information systems that operate on the technological platform when the operating software is updated. You must establish a procedure for assigning access to systems and applications. You must establish separate physical and logical environments for development, testing, and production, each with its own platform, servers, applications, devices, and versions independent of the other environments, preventing development and testing activities from putting integrity at risk. of production information. You must ensure, through the necessary controls, that users use different profiles for development, test and production environments, and that menus display the appropriate identification messages to reduce the risk of errors. It must establish the procedure and access controls to the production environments of the information systems; Likewise, it must be ensured that internal or external developers have limited and controlled access to data and files found in production environments. It must provide source file repositories of the information systems; These must have controlled access and restricted privileges, in addition to a record of access to said files.

Developers must ensure that the information systems built require authentications for all resources and pages, except those specifically classified as public. They must certify the reliability of authentication controls, using centralized implementations for those controls. They must certify that no passwords, connection strings, or other sensitive information is stored in clear text and that password integrity controls are implemented. Authentication controls should be set up in such a way that when they fail, they do so in a secure manner, avoiding specifically stating what the failure was during the authentication process, and instead generating general failure messages. They must ensure that entered passwords are

not displayed on the screen, as well as disable the functionality of remembering password fields. They must certify that the accounts are disabled after a set number of failed attempts to enter the developed systems. They must ensure that if password reassignment is used, only a link or temporary passwords are sent to email accounts previously registered in the applications, which must have an established validity period; Temporary passwords should be forced to change after use. They must certify that the last access (failed or successful) is reported to the user in his next successful access to the information systems. They must ensure the re-authentication of users before carrying out critical operations in the applications. They must, at the application level, restrict access to files or other resources, to protected URL addresses, to protected functions, to services, to application information, to attributes and policies used by access controls and to relevant information of the application. configuration, only to authorized users. They must establish that periodically the authorization of the users in the applications is re-validated and it is ensured that their privileges have not been modified.

11.9. INFORMATION SECURITY INCIDENT MANAGEMENT

11.9.1. Information Security Incident Management Policy

All officials, consultants, contractors, third parties, must note and communicate any weak point they have observed, or suspect exists in the systems or services through the service desk.

11.9.2. Information Security Incident Management Policy Standards

11.9.2.1. Notification of events and information security weaknesses.

The Technology Role must ensure that information security events and weaknesses associated with information systems are communicated in such a way that corrective action can be

taken. A formal information security event reporting procedure should be established, along with an incident response and escalation procedure, which determines the response to be given when a report of an information security event is received.

11.9.2.2. Information security incident management.

Responsibilities and procedures should be established to deal with information security events and weaknesses effectively. Once they have been communicated through a continuous improvement process, the problem resolution group will be responsible for analyzing the cause and evaluating according to the problem management process. When an information security event is first detected, it may not be obvious whether the event will result in legal action. For this reason, there is a danger that necessary evidence will be intentionally or accidentally destroyed before becoming aware of the seriousness of the incident. The legal services of XXXXXXXXXXXXX and/or the control entities must be used in the first phases of any legal action being considered, as well as advice on the necessary evidence. When an action against a person or organization, after an information security incident, involves legal measures (both civil and criminal), evidence should be collected, preserved and presented in a manner that conforms to current legal standards. When collecting evidence, the chain of custody will be preserved and accepted forensic analysis tools and procedures will be used.

11.10. SECURITY MANAGEMENT FOR TELECOMMUNICATIONS AND ICT INFRASTRUCTURE

11.10.1. Telecommunications and ICT Infrastructure Management Policy

The Technology Role must provide the correct and safe operation of the information processing facilities and means of communication, through an effective and efficient Telecommunications and ICT Infrastructure Management.

11.10.2. Telecommunications and ICT Infrastructure Management Policy Policy Standards

11.10.2.1. Operating procedures and responsibilities.

The Technology Role must clearly define and document responsibilities for the management and operation of computer and network facilities, supported by appropriate operational instructions including incident response procedures. It must also define controls that guarantee the appropriate technological operation. These controls must include at least the following procedures:

- Backups.
- Verification of tapes.

- Data recovery and reversal of changes.
- Administration of antivirus systems.
- Administration of users and passwords.
- Administration of access to resources.
- Remote access management.
- Performance measurement.
- Capacity and availability of IT resources.
- Management of audit trails and information registration systems.
- Platform insurance.

11.10.2.2. Change management.

The Technology Role must implement the necessary controls to guarantee the segregation of duties and adequate monitoring of the changes made to critical IT assets. The documentation must include, among others:

- Person requesting the change.
- Responsible for authorization.
- Description of the change.
- Justification of the change for the business.
- Checklist for risk assessment, compromised systems and/or devices. o Impact level.
- Testing, approval of post-implementation reviews. o Training, when necessary.

11.10.2.3. Segregation of functions.

Technology management tasks and responsibilities must be segregated to reduce and prevent opportunities for unauthorized access to the network and any modification or misuse of information system assets. Special care will be taken so that a person cannot access, modify or use the assets by themselves, without prior authorization.

11.10.2.4. Separation of Environments.

Where applicable, development, test, and production environments should be separated to reduce the risks of unauthorized access or changes, prevent failures, and implement controls.

11.10.2.5. Planning and Acceptance.

Future capacity requirements must be defined in order to reduce the risk of system overload. Operational requirements for new systems must be established, documented, and tested

prior to acceptance. Restitution requirements for services supported by different applications should be coordinated and reviewed frequently. IT administrators must be alert to the risks associated with these technologies, as well as consider taking special measures for their prevention or detection.

11.10.2.6. Protection against malicious code.

The Technology Role must implement detection, prevention and recovery controls to protect against malicious code. It must provide tools such as antivirus, antimalware, antispam, antispyware, among others, which reduce the risk of contagion of malicious software and support the security of the information contained and managed in the technological platform and the services that run on it. You must ensure that the antivirus, antimalware, antispam and antispyware software has the required use licenses, thus certifying its authenticity and the possibility of periodic updating of the latest service provider signature databases. You must certify that the information stored in the technological platform is scanned by antivirus software, including the information that is contained and transmitted by the email service. You must ensure that users cannot make changes to the settings of anti-virus, anti-spyware, anti-spam, anti-malware software. You must certify that the antivirus, antispyware, antispam, antimalware software has the latest updates and security patches, to mitigate the vulnerabilities of the technological platform.

Users must be aware of the dangers of malicious code. At XXXXXXXXXXXXX the use of unlicensed software and its installation on any of the company's equipment is not permitted. Users of technology resources must not change or delete antivirus, antispyware, antimalware, antispam software settings defined by the Technology Role; therefore, they will only be able to perform virus scanning tasks on different media. They must run antivirus, antispyware, antispam, antimalware software on files and/or documents that are opened or executed for the first time, especially those found on external storage media or from email. They must ensure that the attached files of emails downloaded from the Internet or copied from any storage medium, come from known and safe sources to avoid the spread of computer viruses and/or the installation of malicious software in technological resources. Users who suspect or detect any malicious software infection must notify the Help Desk, so that through it, the Technology Role can take the corresponding control measures.

11.10.2.7. Backups.

Backup copies of information and software should be made. To ensure integrity and availability, regular checking of mechanisms and information must be done in accordance with the agreed backup policy, maintaining the required levels of confidentiality. The Technology Role

must store the backup copies outside of the XXXXXXXXXXXXX facilities in order to guarantee their recovery in the event of a major event at the main headquarters.

The Company will certify the generation of backup copies and storage of your critical information, providing the necessary resources and establishing the procedures and mechanisms for carrying out these activities. The areas that own the information, with the support of the Technology Role, in charge of generating backup copies, will define the strategy to be followed and the retention periods for the backup and storage of information.

The Technology Role, through its officials, must generate and adopt the procedures for the generation, restoration, storage and treatment of backup copies of information, ensuring their integrity and availability. It must have the necessary resources to allow the identification of the storage media, the information contained in them and their physical location to allow quick and efficient access to the media that contain the protected information. You must carry out the procedures to perform recovery tests on the backup copies, in order to verify their integrity and possibility of use if necessary. You must define the conditions of transport or transmission and custody of the backup copies of the information that are stored externally.

Those responsible for the mandatory resources, the owners of technological resources and information systems must define, together with the Technology Role, the strategies for the generation, retention and rotation of backup copies of information assets.

It is the responsibility of the users of the technological platform to identify the critical information that must be backed up and store it according to its classification level.

11.10.2.8. Security management in event registration and monitoring of resources of information systems

The Technology Role will carry out permanent monitoring of the use given by officials and personnel provided by third parties to the resources of the technological platform and the institute's information systems. In addition, it will ensure the custody of the audit records, complying with the retention periods established for said records.

The Internal Auditor must determine the retention periods of the audit records (logs) of the institute's technological resources and information systems. She must periodically review the audit records of the technological platform and information systems in order to identify security gaps and other monitoring activities.

Developers must generate audit records (logs) of the activities carried out by end users and administrators in the developed information systems. Integrity checks should be used on such records. Events such as: validation failures, failed and successful authentication attempts, access control failures, control evasion attempts, system exceptions, administrative functions and security configuration changes, among others, must be recorded in the audit logs., in accordance with established guidelines. They must avoid

storing unnecessary data from the built systems in the audit logs that provide additional information to that strictly required.

11.10.2.9. Security management in peripherals and storage media

The Information Security Committee must establish the conditions for the use of peripherals and storage media on the technological platform of XXXXXXXXXXXXX It must authorize the use of peripherals or storage media on the technological platform of the institute in accordance with the official's position profile applicant.

The Technology Role must implement the controls that regulate the use of peripherals and storage media in the institute's technological platform, in accordance with the established guidelines and conditions. You must generate and apply guidelines for the safe disposal of the institute's storage media, either when they are removed or re-assigned to a new user.

Officials and personnel provided by third parties must abide by the conditions of use of peripherals and storage media established by the Technology Role. They must not modify the configuration of established peripherals and storage media. They are responsible for the custody of assigned institutional storage media.

11.10.2.10. Security management with cryptography

The Technology Role must establish that the authorization of the users in the applications is periodically re-validated, and it is ensured that their privileges have not been modified. You must verify that any information system or application that requires the transmission of reserved or restricted information has data encryption mechanisms. You must develop and establish a procedure for handling and managing encryption keys. You must develop and establish standards for the application of cryptographic controls.

Developers must encrypt reserved or restricted information and certify the reliability of storage systems for such information. They must ensure that the cryptographic controls of the built systems comply with the established standards.

11.10.2.11. Safety management in the operation

The Technology Role, in charge of the operation and administration of the technological resources that support the processes of XXXXXXXXXXXXX, will assign specific functions to its officials, who must carry out the operation and administration of said technological resources, maintaining and updating the documentation of the operational processes. for the execution of activities. Likewise, it will ensure the efficiency of the controls implemented in the operational processes associated with the technological resources in order to protect the confidentiality, integrity and availability of the information handled and will ensure that the changes made to the technological resources will be properly controlled and duly authorized.

It will provide the processing capacity required in the institute's technological resources and information systems, making growth projections and provisions in the technological platform with a defined periodicity. It must carry out, through its officials, the documentation and update of the procedures related to the operation and administration of the technological platform. It must provide its employees with configuration and operation manuals for the operating systems, firmware, network services, databases and information systems that make up the technological platform. It must provide the necessary resources for the implementation of controls that allow the separation of development, testing and production environments, taking into account considerations such as: controls for the exchange of information between development and production environments, the non-existence of compilers, editors or sources in the production environments and a different access for each one of the environments. It must carry out studies on the demand and growth projections of managed resources on a regular basis, in order to ensure the performance and capacity of the technological platform. These studies and projections must consider aspects of resource consumption of processors, memories, disks, printing services, bandwidth, internet and data network traffic, among others. It must issue a concept and generate recommendations about the security solutions selected for the technological platform.

11.10.2.12. Security management in the exchange of information

XXXXXXXXXXXXXX, will ensure the protection of information at the time it is transferred or exchanged with other entities and will establish the necessary procedures and controls for the exchange of information; Likewise, Confidentiality and/or Information Exchange Agreements will be established with the third parties with whom said exchange is carried out. The institute will promote the use of computer and telecommunications technologies to carry out the exchange of information; however, it will establish guidelines for the exchange of information in physical media.

The Technology Role, with the support requested from the competent Areas, must define the models of Confidentiality and/or Information Exchange Agreements between the institute and third parties, including the commitments acquired and the civil or criminal penalties for non-compliance with said agreements. agreements. Among the aspects to consider should be included the prohibition of disclosing the information delivered to third parties with whom these agreements are established and the destruction of said information once it fulfills its mission. You must establish in the contracts that are established with third parties, the Confidentiality Agreements or Exchange Agreements, making explicit the responsibilities and legal obligations assigned to said third parties for the unauthorized disclosure of information of beneficiaries of the institute that has been delivered to them due to the fulfillment of mission objectives. It must offer secure information exchange services or tools, as well as adopt controls such as information encryption, which allow compliance with the procedure

for the exchange of information (digital or magnetic media), in order to protect said information against disclosure or modifications. unauthorized.

The Information Security Committee must define and establish the information exchange procedure with the different third parties that, as part of the operation, receive or send information from the institute's beneficiaries, which includes the use of reliable means of transmission and the adoption of controls, in order to protect its confidentiality and integrity. You must ensure that the exchange of information with external entities is carried out in compliance with the Security Policies for the exchange of information described here, the Information Exchange Agreements and the procedure defined for said exchange of information. You must authorize the establishment of the information transmission link with third parties, so that later the functional areas carry out the transmission activities required in each case**.**

The owners of information assets must ensure that the information or its beneficiaries are protected from unauthorized disclosure by third parties to whom this information is delivered, verifying compliance with the related clauses in contracts, confidentiality agreements or agreements. exchange established. They must ensure that the data required of the beneficiaries can only be delivered to third parties, with the prior consent of the owners thereof, except in cases provided by law or at the request of the control entities. They must verify that the exchange of information with third parties leaves a record of the type of information exchanged, the sender and receiver of the same and the date of delivery/reception. They must authorize the request/sending of information by/to third parties, except in the case of requests from control entities or compliance with current legislation. They must ensure that the Exchange of (digital) information is only carried out if it is authorized and in compliance with the Policies for network administration, logical access and protection of personal data, as well as the information exchange procedure.

The sending or receiving user of physical information, with the support of the Administrative Coordinator, must accept the procedure for the exchange of information (storage media and documents) with third parties and the adoption of controls in order to protect sensitive information against disclosure., loss or modifications. You must certify that all sending of physical information to third parties (document or magnetic medium) uses only authorized transport services or courier services, and that these allow tracking of deliveries.

The third party with whom information is exchanged must properly handle the information received, in compliance with the Institute's Security Policies, the established contractual conditions and the Information Exchange Procedure. He must safely destroy the information provided, once it fulfills the function for which it was sent and demonstrates the completion of the destruction activities.

Role managers must give clear instructions on what information can be transmitted through which communication channel.

11.10.2.13. Security management in communications

The Technology Role will establish, through the Technology Role, the necessary control mechanisms to provide the availability of the data networks and the services that depend on them; Likewise, it will ensure that there are security mechanisms that protect the integrity and confidentiality of the information that is transported through said data networks. In the same way, it will promote the security of the data networks, the control of the traffic in said networks and the protection of the reserved and restricted information of the institute. You must implement controls to minimize the security risks of the information transported through data networks. You must keep the data networks segmented by domains, groups of services, groups of users, geographical location or any other classification that is considered convenient for the institute. You must identify the required security mechanisms and network service levels and include them in the network service agreements, when these are contracted out. It must establish the technical standards for the configuration of the security and network devices of the technological platform of the institute, adopting good practices of secure configuration. You must identify, justify and document the services, protocols and ports allowed by the institute in its data networks and disable or eliminate the rest of the services, protocols and ports. You must install protection between the internal networks and any external network, which is outside the control and administration capacity of the institute. You must ensure the confidentiality of data network addressing and routing information The third party with whom information is exchanged must properly handle the information received, in compliance with the Institute's Security Policies, the established contractual conditions and the Information Exchange Procedure. He must safely destroy the information provided, once it fulfills the function for which it was sent and demonstrates the completion of the destruction activities.

Role managers must give clear instructions on what information can be transmitted through which communication channel.

11.10.2.13. Security management in communications

The Technology Role will establish, through the Technology Role, the necessary control mechanisms to provide the availability of the data networks and the services that depend on them; Likewise, it will ensure that there are security mechanisms that protect the integrity and confidentiality of the information that is transported through said data networks. In the same way, it will promote the security of the data networks, the control of the traffic in said networks and the protection of the reserved and restricted information of the institute. You must implement controls to minimize the security risks of the information transported through data networks. You must keep the data networks segmented by domains, groups of services, groups of users, geographical location or any other classification that is considered convenient for the institute. You must identify the required security mechanisms and network service levels and include them in the network service agreements, when these are contracted out. It must establish the technical standards for the configuration of the security and network devices of the technological platform of the institute, adopting good practices of secure configuration. You must identify, justify and document the services, protocols and

ports allowed by the institute in its data networks and disable or eliminate the rest of the services, protocols and ports. You must install protection between the internal networks and any external network, which is outside the control and administration capacity of the institute. You must ensure the confidentiality of data network addressing and routing information

11.10.2.14. Vulnerability security management

The Technology Role will periodically review the appearance of technical vulnerabilities on the resources of the technological platform by performing periodic vulnerability tests, with the aim of correcting the findings produced by said tests. These two areas make up the Vulnerability Committee in charge of reviewing, assessing and managing the technical vulnerabilities found. You must periodically review the appearance of new technical vulnerabilities and report them to the administrators of the technological platform and the developers of the information systems, in order to prevent exposure to their risk. Must generate and execute or monitor action plans for the mitigation of technical vulnerabilities detected in the technological platform

The Risk Role must carry out the corresponding procedures to carry out vulnerability tests and ethical hacking with an established frequency, by an entity independent of the Role object of the tests, in order to guarantee the objectivity of their development. It must generate the guidelines and recommendations for the mitigation of vulnerabilities, the results of the vulnerability tests and ethical hacking.

The Information Security Committee must review, assess and manage the technical vulnerabilities found, relying on technological tools for their identification.

11.10.2.15. Security management in test data protection

The Technology Role of will protect test data that will be delivered to developers, ensuring that it does not reveal sensitive information from production environments. You must certify that the information to be delivered to the developers for their tests will be masked and will not reveal confidential information from the production environments. You must delete the information from the test environments once they have finished.

11.10.2.16. Security management with third parties

XXXXXXXXXXXXXX will establish control mechanisms in its relationships with third parties, in order to ensure that the information to which they have access or services that are provided by them, comply with the information security policies, standards and procedures.

The officials responsible for the execution and/or signing of contracts or agreements with third parties will ensure the disclosure of information security policies, standards and procedures to said parties.

The Legal Role, together with the Information Security Committee, must generate a base model for Service Level Agreements and Information Security requirements, with which third parties or service providers must comply; Said model must be disclosed to all areas that acquire or supervise technological resources and/or services. They must prepare models of Confidentiality Agreements and Information Exchange Agreements with third parties. Said agreements must give rise to both civil and criminal liability for the contracted third party.

The Technology Role must establish the appropriate connection conditions for the computer equipment and mobile devices of third parties in the institute's data network. You must establish the conditions for secure communication, encryption and transmission of information to and from third-party service providers. You must mitigate the risks related to third parties that have access to the information systems and the technological platform. You must evaluate and approve access to the institute's information required by third parties. You must identify and monitor the risks related to third parties or the services provided by them, extending this activity to the supply chain of the technology or communications services provided.

The Supervisors of contracts with third parties must disclose the information security policies, standards and procedures to said third parties, as well as ensure that access to information and to the storage or processing resources of the same, by third parties is carried out securely, in accordance with information security policies, standards and procedures.

11.10.2.17. Security incident management and its corresponding report

XXXXXXXXXXXXXX will promote among officials and personnel provided by third parties the reporting of incidents related to information security and its means of processing, including any type of information storage medium, such as the technological platform, information systems, media physical storage and people. It will assign persons responsible for the treatment of information security incidents, who will be responsible for investigating and solving reported incidents, taking the necessary measures to prevent recurrence and escalating incidents according to their criticality. They are the only ones authorized to report security incidents to the authorities; likewise, they are the only communication channels authorized to make official pronouncements before external entities.

The owners of information assets must inform the Information Security Committee of security incidents that they identify or that they recognize as possible.

The Information Security Committee must establish responsibilities and procedures to ensure a quick, orderly and effective response to information security incidents. You must evaluate all security incidents according to your particular circumstances and escalate to the Information Security Committee those in which it is considered pertinent. Qualified personnel must be designated to adequately investigate reported security incidents, identifying the causes, carrying out an exhaustive investigation, providing solutions and finally preventing their recurrence. You must create knowledge bases for the security incidents presented with their respective solutions, in order to reduce the response time for future incidents, starting from said knowledge bases (for this, the report of operational risk events applies). You must analyze the security incidents that are escalated and activate the contact procedure with the authorities, when you deem it necessary.

All officials of XXXXXXXXXXXXXX and personnel provided by third parties report any event or incident related to information and/or technological resources as soon as possible. In case of learning of the loss or unauthorized disclosure of information classified as internal use, reserved or restricted, officials must notify the Risk Office so that it can be registered and given the necessary paperwork.

11.10.2.18. Redundancy security management

The Information Security Committee must analyze and establish the redundancy requirements for critical information systems for the institute and the technological platform that supports them. You must evaluate and test technology redundancy solutions and select the solution that best meets the requirements.

The Technology Role must manage the technological redundancy solutions and carry out periodic tests on said solutions, to ensure compliance with the institute's availability requirements.

11.10.2.19. Security management in the Business Continuity Plan

XXXXXXXXXXXXXX, will provide sufficient resources to provide an effective response of officials and processes in case of contingency or catastrophic events that occur in the institute and that affect the continuity of its operation. In addition, it will respond effectively to catastrophic events according to their magnitude and degree of impact; Operations will be restored with the lowest possible cost and loss, maintaining information security during such events. The Company will maintain adequate communication channels with officials, suppliers and interested third parties.

The Continuity Committee must recognize the situations that will be identified as emergencies or disasters for the institute, the processes or the areas and determine how to act on them. You must lead on issues related to business continuity and disaster recovery. You must carry out the business impact analysis and the continuity risk analysis to subsequently propose possible recovery strategies in the event that the contingency or continuity plan is activated, with the information security considerations that may apply. You must select the most convenient recovery strategies for the institute. You must validate that the contingency, recovery and return to normality procedures include information security considerations. You must ensure periodic testing of the disaster recovery plan and/or business continuity, verifying the security of the information during its implementation and the documentation of said tests.

The Information Security Committee must develop a disaster recovery plan for the computer center and a set of contingencies, recovery and return to normal procedures for each of the services and systems provided. They must actively participate in disaster recovery testing and report the results to the General Manager.

Those responsible for Role must identify and, within their areas, generate the documentation of the continuity procedures that could be used in the event of an adverse event, taking into account information security. These documents must be tested to certify their effectiveness.

11.10.2.20. Security management in the provision of third-party services

XXXXXXXXXXXXXX, will maintain the agreed levels of information security and provision of supplier services, in accordance with the agreements established with them. Likewise, it will ensure the adequate management of changes in the provision of services of said providers.

The Technology Role must verify at the time of connection and, when considered pertinent, compliance with the connection conditions of third-party computer equipment and mobile devices in the institute's data network. You must verify the conditions of secure communication, encryption and transmission of information to and from third-party service providers.

The Information Security Committee and the Client Role of the contract must periodically monitor compliance with the Service Level Agreements, Confidentiality Agreements, Information Exchange Agreements and the Information Security requirements of third parties. Service providers. You must manage changes in the provision of services by providers, maintaining the service and security compliance levels established with them and monitoring the appearance of new risks

11.10.2.21. Security management in remote connection

The Technology Role must analyze and approve the methods of remote connection to the technological platform of XXXXXXXXXXXXX It must implement the methods and security controls to establish remote connections to the technological platform of XXXXXXXXXXXXX It must restrict remote connections to the resources of the technological platform ; This access should only be allowed to authorized personnel and for established periods of time, in accordance with the tasks performed. You must verify the effectiveness of the controls applied over remote connections to the resources of the technological platform of XXXXXXXXXXXXX on a permanent basis.

The Internal Audit Role must, within its autonomy, carry out audits on the controls implemented for remote connections to the technological platform of XXXXXXXXXXXXX

Users who make a remote connection must have the approvals required to establish said connection to the devices of the technological platform of XXXXXXXXXXXXX and must abide by the conditions of use established for said connections. Users should only establish remote connections on previously identified computers and, under no circumstances, on public computers, hotels or internet cafes, among others.

11.10.2.22. Token security management

XXXXXXXXXXXXX, will provide the conditions for handling security tokens for the processes that use them and will ensure that officials make responsible use of them.

Each user role of security tokens must assign an administrator official of the same with the power to authorize access requests.

The Security Token Administrators must process the requests for said tokens according to the requirements of each entity that provides them and attach the necessary documentation. They must receive them and carry out the necessary activation in the respective portals or sites of use in order to carry out operations through them. Users and profiles must be created in each portal or site of use, according to the activities to be carried out by each created official. Users and serials of the devices that are assigned for their use must be delivered to the designated officials, formalizing the delivery by means of a certificate and a security document (or envelope) for their custody. They must give notice to the issuing entities in case of theft or loss of these in order to carry out the respective blocking and replacement of the same. They must make the change of these, when there is a malfunction, expiration, change of functions or change of the owner, reporting to the issuing entity and returning the assigned devices.

The Users of the security tokens must have a user account in the portals or sites for their use; These tokens will be part of the physical inventory of each user to whom they have been assigned. they must return the assigned token in operating status to the Token Administrator when the employment relationship with XXXXXXXXXXXXX is terminated or there is a change of position, to obtain the peace and salutation, which will be required to

legalize the termination of the relationship with the institute. They must notify the Administrator of the tokens in case of theft, loss, malfunction or expiration so that this, in turn, communicates with the issuing entities of said tokens. They must not allow third parties to observe the key that generates the token, and they must not accept help from third parties for the use of the token. They must be responsible for the electronic transactions that are carried out with the user account, password and the assigned token, in the development of the activities as officials of the XXXXXXXXXXXXXX In the event that any irregular event occurs with the tokens, the users must assume administrative responsibility, disciplinary and economic They must keep the assigned tokens in a dry place and not put them in water or other liquids. They should avoid exposing the tokens to magnetic fields and extreme temperatures. They must prevent the tokens from being hit or subjected to physical exertion. Do not open the tokens, remove the battery or circuit board, as it will cause malfunction. They must not use the tokens outside the facilities of XXXXXXXXXXXXX to avoid loss or theft of these

11.10.2.23. Network security management.

Special attention should be given to managing network security, which may extend beyond the physical limits of XXXXXXXXXXXXX

Special procedures and measures are required to protect the passage of sensitive information to public domain networks.

The Technology Role must ensure that network service providers implement measures in compliance with security features, service level agreements and management requirements. Special controls must be established to safeguard the integrity and confidentiality of data passing through public networks or wireless networks and to protect connected systems and applications. The availability of network services and connected computers must also be guaranteed.

11.10.2.24. Electronic Commerce Services.

An assessment should be made to identify the risk associated with the use of electronic commerce services, including online transactions, and the requirements for controls. Completeness and availability of published information should be considered

11.10.2.24. Electronic Commerce Services.

An assessment should be made to identify the risk associated with the use of electronic commerce services, including online transactions, and the requirements for controls. The completeness and availability of information published electronically through publicly available systems should be considered.

11.10.2.25. System usage monitoring.

The level of monitoring required for services will be determined through a risk assessment. XXXXXXXXXXXXX will comply with the legal requirements that apply to its monitoring activities. The activities of both the operator and the system administrator must be recorded. The activities to monitor include privileged operations, unauthorized access and alerts or system failures, among others.

11.10.2.26. Audit Records.

Audit logs of user activities, operation and administration of the system must be prepared and maintained for an agreed period.

11.10.2.27. Protection of registration information.

Services and log activity information must be protected from unauthorized access or tampering.

11.10.2.28. Treatment of media with information.

Means must be controlled and protected to prevent unauthorized disclosure, modification, removal or destruction of assets and interruption of business activities. The Technology Role must implement the controls that guarantee that the elimination of any technological device or component that contains sensitive information is physically destroyed, or that the information is destroyed, erased or overwritten, by means of techniques that do not make it possible to recover data. the original data, instead of using a normal erase or formatting.

11.10.2.25. System usage monitoring.

The level of monitoring required for services will be determined through a risk assessment. XXXXXXXXXXXXX will comply with the legal requirements that apply to its monitoring activities. The activities of both the operator and the system administrator must be recorded. The activities to monitor include privileged operations, unauthorized access and alerts or system failures, among others.

11.10.2.26. Audit Records.

Audit logs of user activities, operation and administration of the system must be prepared and maintained for an agreed period.

11.10.2.27. Protection of registration information.

Services and log activity information must be protected from unauthorized access or tampering.

11.10.2.28. Treatment of media with information.

Means must be controlled and protected to prevent unauthorized disclosure, modification, removal or destruction of assets and interruption of business activities. The Technology Role must implement the controls that guarantee that the elimination of any technological device or component that contains sensitive information is physically destroyed, or that the information is destroyed, erased or overwritten, by means of techniques that do not make it possible to recover data. the original data, instead of using a normal erase or formatting.

11.10.2.29. Password Protection

- Email is not a secure medium. For this reason, the password should not be sent by this means, nor should it be mentioned in a conversation.

- Passwords should not be stored in readable format in batch files, automatic login scripts, software macros, terminal function keys, computers without access control, or in other places where unauthorized persons can discover and use them.

- Each password is personal and non-transferable. Officials and third parties working for XXXXXXXXXXXXX must not disclose your account password to other officials and/or third parties.

- It is forbidden to try to access the computer and communications services through the account of another official.

- Officials and third parties working for XXXXXXXXXXXXX must immediately notify the Information Security Committee if they suspect that someone has gained unauthorized access to their account. The password must be changed immediately.

- Individuals who are not members of XXXXXXXXXXXXX should not be allowed to gain access to the companies' computer and communications services. All officials and third parties (contractors, service providers and outsourcing) must ensure that this type of situation does not occur within XXXXXXXXXXXXX

- Each user is responsible for the custody of their password and account. You should avoid as much as possible typing the password while someone is watching what you type on the keyboard. It is an unspoken rule of good user not to look at the keyboard while someone is typing their password.

11.10.2.30. virus control

It is part of the Information Security policy of XXXXXXXXXXXXX the non-tolerance to the spread of viruses, treated with efficient measures throughout the document.

11.10.2.31. Confidentiality of information

It is part of the Information Security policy of XXXXXXXXXXXXX to manage information confidentially, treated with efficient measures throughout the document

11.10.2.31. Compliance Verification

It is part of the Information Security policy of XXXXXXXXXXXXX the management of verification of compliance with all the standards required in terms of Information Security, treated with efficient measures throughout the document.

11.10.2.32. unused equipment

Employees and contractors should at a minimum adopt the following practices when leaving their equipment unattended:

- Leave the equipment located in a safe area
- Lock your computer equipment with a password-protected screen saver when said equipment is going to be unattended for more than three (3) minutes.

11.10.2.33. Backup – Information Back Up

It is part of the Information Security policy of XXXXXXXXXXXXX the management of information backups, treated with efficient measures throughout the document

11.10.2.34. Removal of Access Rights

In the case of voluntary retirement, dismissal, transfer or other type of activity associated with the culmination or modification of the contract, service agreement or other type of written agreement of the officers of the companies or third parties that have access privileges, these rights they must be removed/inactivated or updated as established.

The following procedure must be carried out:

- The Human Management Role must report the news (only for the withdrawal of personnel hired directly, through a temporary company or for services) of officials immediately upon learning of the employee's news.
- The Technology Role must make the corresponding adjustments. The maximum term to eliminate/inactivate or modify the accesses of an official is no more than 3 calendar days from when the news was reported.
- The Information Security Committee and the Internal Auditor will also review the Information components and assets in order to validate compliance with the policy.

11.10.2.35. Security of equipment outside the company

- Laptops should not be used in homes to connect to the Internet or other networks in the absence of virus controls and PC firewalls installed, properly configured, and continuously operational.

- During any move, equipment (and storage media) must not be left unattended. Laptops must be carried as permanently guarded carry-on baggage.

- The computer equipment (regardless of its owner) used outside of XXXXXXXXXXXXXX and in the Company's own functions, must be exclusively used to provide business support and must be subject to an equivalent degree of protection to the equipment that is inside the company. company facilities.

All computer equipment, Technological devices and any type of electronic media that contains Critical Information for the business of XXXXXXXXXXXXXX must be reviewed, analyzed and the information contained safely eliminated before the media is reassigned or destroyed when business requirements are not require its use.

The Technology Role is the one who establishes the different people responsible for the destruction of media depending on the type and function (backup media, computer equipment, etc.). He must establish procedures for media destruction, and they must be subject to approval by the Information Security Committee. All media destruction processes must be formalized and recorded through the media destruction memorandum.

Prior to the destruction of a magnetic medium, the Official in charge must verify if it is necessary to make a backup copy of the Information found on the medium prior to its destruction or reassignment.

When a computer equipment is delivered to a third party or reassigned and it has a storage unit (hard disk), it must be reviewed by the Technology Role and the information must be deleted in such a way that it cannot be recovered. If the device does not have a storage unit (e.g., communications equipment) it must be reset to the factory settings.

Information stored on storage devices such as hard drives and USB drives must be deleted by using specialized tools that allow partitions to be formatted safely so that previously stored information cannot be restored. The tool to be used is approved by the Information Security Committee.

In the event that the means are assigned or donated to a third party for charitable purposes, they must follow the guidelines described here in accordance with the provisions of this policy.

The Information Security Committee will carry out periodic reviews of compliance with the provisions of this policy.

11.10.2.37. Control of technological changes.

The Technology Role establishes two types of change: Scheduled or operational changes and urgent changes.

Scheduled changes: These are changes that must be implemented as a result of a requirement, update or improvement of a technological component.

Urgent changes: These types of changes require priority and/or immediate attention and can be justified outside of the normal cycle of changes. They can be generated due to a failure or malfunction of an Information Technology component and that can significantly impact business processes. These types of changes can be executed by the corresponding Technology Role prior to the endorsement of the designated person. Once they are implemented, they must be made official and documented within 36 business hours of being applied.

A formal change control procedure must exist according to the type of change and must be followed to control modifications to the IT component. No change can be implemented without prior compliance with what is established in the procedure.

Any change to the Technological platform or Information Systems must be subject to prior approval of its application by the functional role involved and affected by the change. The composition of the "change control approval group" will depend on the type of component, criticality and impact that the change may generate. The officials involved in the approval correspond to the matrix responsible for Information Systems and Infrastructure.

Any change must be tested in a separate environment before being put into production. The results of the tests must be documented by the Platform administrator or by the Functional Role in the case of Information Systems.

Each Administrator of the technological platform or Information System must keep a historical record of the changes applied to each IT component that it manages.

Changes to the information in the database must be approved by the corresponding functional role and therefore it is not allowed to create or modify data by officials of the Information Technology Role without prior request and authorization.

Any application of a change in the IT platform that affects the services of XXXXXXXXXXXXX must be reported to an official of each affected Company before making the change. This official is appointed by the Technology Role.

11.10.2.38. Monitoring of Technological Components.

All business processes, activities and services that are supported by Information Technology must be analyzed by the Technology Role. The Administrators of each component Platform must establish the capacity requirements of the systems involved in the business process, activity or service requirements specification stage. To this end, the following criteria for evaluating capacity requirements must be taken into account as a minimum:

- Size and type of service provided by the Technological Component.
- Estimation of the capacity required to provide the service adequately and efficiently.
- Carry out an analysis of the information and data to be managed by the system.
- Establish the level of impact of the implementation of systems and operations.

All critical components must be reviewed periodically, taking into account at least the following monitoring factors:

- Ability
- Performance
- Availability

The Technology Role must establish the review frequency, the indicators, the metrics and the thresholds defined for each Technology Component in order to determine its capacity and performance.

11.10.2.39. Controls in Networks

All devices without exception that are entered into the corporate data networks (including computer equipment, printers, scanners, communications devices, among others) must be previously registered and configured by the Technology Role.

When a Technological component is registered for use in corporate networks, a network name and IP address will be assigned according to the mechanism established by the Technology Role. The basic information of the owner of the component, description and function must be registered by the Administrator of said Component or his designee.

The definition and design of network addressing, as well as the approval of the assignment of fixed IP addresses in the network, is the responsibility of the Technology Role.

Every Technological Component that is entered into the corporate networks must comply with the security requirements and minimum standards established by each Network Administrator.

Joint component with the Information Security Committee. In the event that a device does not meet the established standards, it must be disconnected from the network until it is configured with the defined requirements. The Information Security Committee will carry out periodic reviews of the configurations and standards applied in the different Technological Components in order to evaluate and ensure compliance with the Information Security requirements.

Any entry or connection to corporate networks, modem or remote access by a third party must be previously approved by the Information Security Committee. A risk analysis must be carried out and the respective security requirements must be established prior to the connection made by the third party. Everything must be documented.

11.10.2.40. Recycled paper and order in the workplace.

All employees must keep their desks and work areas free of any material that contains any information considered confidential, unless it is being used by authorized personnel; This must guarantee the adequate insurance of the same during non-working hours and/or absence from his job.

• Assurance of confidential information

All information printed and/or on magnetic media that is not being used must be properly secured, using filing cabinets, safes or furniture intended for storage.

- Information leakage

Any official who has access to confidential information in physical media must prevent its unauthorized disclosure to people who work in environments or work modules close to or outside the company.

• No recycling of paper with confidential information

Any document containing information classified as confidential may not be recycled; must be destroyed using means that prevent the reconstruction of said information.

11.10.2.41. Review of Access Permissions Network Services

The Administrators of each Network service or whoever the Technology Role designates must carry out quarterly reviews of the different users who have access to each of the components. These reviews should include at a minimum:

- Users authorized in the Information systems and who no longer work for the Companies.
- Users with Administration role.
- Users who present inactivity in the account greater than 60 days.
- Generic users.
- Users who do not meet the password creation and complexity standards.

The evidence and support of the reviews must be duly identified and documented; stored in custody together with the documents related to the review. This information must be available for review and audit purposes.

Once the revisions are carried out, each person responsible for the Technological Component must adjust the permits and carry out the measures that result.

11.10.2.42. Access to Resources in Information Systems

For each information system of the companies there must be an owner or proprietor of the information who must belong to the functional role and must be responsible for the administration of the security module.

The Business Managements must define the access schemes and the user privileges for those who are authorized to use the information systems.

Quarterly reviews must be carried out on the access profiles defined and registered in the application in production, determining the exceptions on the following points of greatest risk:

- Users authorized in the Information systems and who no longer work for the Company.
- Compliance with the standard for creating users.
- Review of access profiles according to the activities of each user created in the information system.

The evidence and support of the reviews must be duly identified, segregated and in custody, with forms and documents related to the review of user profiles. This information must be available for review and audit purposes.

The session in the workstations from which the business information systems are accessed must have a defined period of time without transaction, after which the session must be cancelled. This time is defined by each owner of the Information system and must be approved by the Technology Role.

Contractors or third parties that are authorized to access the business information systems, will be restricted in access to data classified as "sensitive" as well as confidentiality and privacy clauses registered in the contract together with the respective penalty schemes for breach of these will be formalized for the purpose.

11.10.2.43. Financial Systems Interfaces.

No end user interface that has an impact on the financial information system should be controlled by personnel from the Technology Role. You must also keep up-to-date documentation on the operation of each of the interfaces that have a financial impact.

Any changes to interfaces with a financial impact must comply with the change control policy and procedure.

The data structures with their characteristics variable name, length and format type of the files used in the interface process will be updated and available for consultation permanently.

No interface can be uploaded to the Information systems without carrying out the minimum validations that guarantee the integrity and consistency of the data.

All interfaces must have checksum mechanisms that involve validations on the most critical fields.

All interface processing must have a record of inconsistencies.

11.10.2.44. Management of Vulnerabilities in the Technological Platform.

For all the assets of the technological platform that supports the operation of the business, assurance procedures must be executed that guarantee a required level of availability, confidentiality and integrity of the information stored, processed or transported in each of the assets.

The Information Security Committee will define the assurance guidelines for each of the technological platforms that support the operation of the business in XXXXXXXXXXXXX.

It is the responsibility of each of the areas in charge of technological assets to apply the previously defined assurance guidelines to each of its assets.

The Information Security Committee, through a contracted third-party expert, will be responsible for executing passive vulnerability analysis tests on XXXXXXXXXXXXX critical technological assets once a year.

It is the responsibility of each of the areas in charge of technological assets to request the corporate information security role to run passive vulnerability analysis tests on their assets each time a total change or critical modification is made to the asset. These tests will be included in the annual analysis schedule. Critical modification is understood as: change or reinstallation of the asset's operating system, changes in the security policies of the asset, change of a physical component of the asset's information processing.

It is the responsibility of each of the areas in charge of technological assets to execute the pertinent actions that mitigate the risks caused by the threats detected in the vulnerability analysis.

It is the responsibility of the areas in charge of technological assets to maintain a low or acceptable level of risk in the assets.

The corporate information security role will report periodically to technology management Computing the status of the technology platform assurance indicator.

11.10.2.45. Clock synchronization.

The clocks of the systems within XXXXXXXXXXXXX must be synchronized with an agreed time. It must be established according to an accepted standard, mitigating the risk of failures in the information for different hours of the systems.

11.11. SECURITY MANAGEMENT FOR THE ACQUISITION, DEVELOPMENT AND MAINTENANCE OF INFORMATION SYSTEMS

11.11.1. System Acquisition, Development and Maintenance Policy

The Technology Role must provide security measures in information systems from the requirements phase, and they must be incorporated in the development, implementation and maintenance stages. You must establish methodologies for software development, including the definition of security requirements and good practices for secure development, in order to provide developers with a clear vision of what is expected

All information systems or software developments must have an owner role

The areas that own information systems, together with the Information Security Committee, must establish the specifications for the acquisition or development of information systems, considering information security requirements. They must define what sensitive information can be removed from their systems and request that they support the removal of such information, such as personal or financial data, when these are no longer required.

Developers must define what sensitive information can be removed from their systems and request that they support the removal of such information, such as personal or financial data, when it is no longer required. They must certify that all information systems acquired or developed use development tools licensed and recognized in the market. They should disable autocomplete features on data request forms that require sensitive information. They must establish the duration time of the active sessions of the applications, terminating them once this time has elapsed. They must ensure that recurring connections to information systems built with the same user are not allowed. They must use the protocols suggested by the Technology Role and the Risk Office in the applications developed. They must certify the transmission of information related to payments or online transactions to the operators in charge, through secure channels.

11.11.2 Standards of the Systems Acquisition, Development and Maintenance Policy

11.11.2.1. System security requirements.

The Technology Role must ensure that all activities related to the development and maintenance of information systems consider the management of security risks. All security requirements must be identified during the requirements stage, as well as justified, agreed and documented, as part of the entire information system project.

11.11.2.2. Security of system applications.

Standards must be developed that indicate how the different systems, applications and developments must be secured, to minimize the appearance of errors, losses and unauthorized modifications or improper uses of the information in the applications. Appropriate controls must be designed into applications to ensure proper processing. Validation of input data, internal processing, and resulting data should be included. The applications that are developed in XXXXXXXXXXXXXX must meet minimum security requirements, in accordance with good practices in information security and this security policy. The design and operation of the systems must comply with commonly accepted safety standards and current regulations.

11.11.2.3. Security of file systems.

Access to the file system and source code of programs must be controlled. The update of the application software, the applications and the libraries, should only be carried out by the administrators.

11.11.2.4. Security of development and support processes.

Strict control is required in the implementation of changes. Change control procedures must validate that security and control processes are not compromised; Likewise, they must ensure that support programmers have access only to the parts of the system necessary to carry out their work, which said changes are approved with an adequate procedure and with the corresponding documentation.

The owners of the information systems are responsible for carrying out the tests to ensure that they comply with the security requirements established before the systems go into production, using established methodologies for this purpose, documenting the tests carried out and approving the steps into production. These tests must be carried out for the delivery of new functionalities, for functionality adjustments or for changes to the technological platform on which the applications work. They must approve the migrations between the development, testing and production environments of new information systems and/or changes or new functionalities.

The Technology Role must implement the necessary controls to ensure that migrations between the development, testing and production environments have been approved, in accordance with the change control procedure. You must have version control systems to manage changes to information systems. It must be ensured that the information systems acquired or developed by third parties have a licensing agreement which must specify the conditions of use of the software and the intellectual property rights. It must generate methodologies for testing the developed software, containing guidelines for the selection of scenarios, levels, types, test data and documentation suggestions. It must be ensured that the technological platform, the development tools and the components of each information

system are updated with all the patches generated for the versions in use and that they are running the latest approved version of the system. It must include within the change management procedure and controls the handling of changes in the application software and the institute's information systems.

The Information Security Committee must verify that the security tests on the information systems are carried out in accordance with the defined methodologies, with duly documented tests.

The developers of information systems must consider the good practices and guidelines for secure development during their life cycle, from design to start-up. They must provide an adequate level of support to solve problems that arise in the application software; said support must contemplate acceptable response times. They must build the applications in such a way that they perform input data validation and output data generation reliably, using centralized and standardized validation routines. They must ensure that the information systems built validate the information provided by users before processing it, considering aspects such as: data types, valid ranges, length, lists of accepted characters, characters considered dangerous and path alteration characters, among others. others. They must provide options to disconnect or close the session of the applications (logout) that allow the complete termination of the session or associated connection, which must be available in all the pages protected by authentication. They must ensure the handling of sensitive or critical operations in the applications developed, allowing the use of additional devices such as tokens or the entry of additional verification parameters. They must ensure that the applications provide the minimum information of the established session, stored in cookies and complements, among others. They must ensure that no sensitive information is disclosed in error responses, including system details, session identifiers, or user account information; likewise, they must implement generic error messages. They must remove all the functionalities and files that are not necessary for the applications, prior to putting them into production. They must prevent the disclosure of the directory structure of the built information systems. They should remove unnecessary information in the response headers that refers to the operating systems and versions of the software used. They should avoid including database connection strings in application code. Such connection strings should be in separate configuration files, which are recommended to be encrypted. They must certify the closing of the connection to the databases from the applications as soon as these are not required. They must develop the necessary controls for file transfers, such as requiring authentication, monitoring the types of files to be transmitted, storing transferred files in dedicated repositories or databases, removing execution privileges from transferred files, and ensuring that such files have only read privileges. They must protect the source code of the built applications, in such a way that it cannot be downloaded or modified by users. They must ensure that the applications developed are not allowed to execute commands directly in the operating system.

11.12. COMPLIANCE AND LEGAL REGULATIONS

11.12.1. Policy for Compliance and Legal Regulations

Any solution of services or technological infrastructure must guarantee that its selection is in accordance with the contractual conditions, legislation and external and internal regulations, for the due compliance with the legal regimes to which the organization is subject.

11.12.2. Standards of the Policy for Compliance and Legal Regulations

11.12.2.1. Legal compliance.

All contractual and legal requirements that may affect XXXXXXXXXXXXX information systems must be previously defined and documented in accordance with the methodology used by the company. The specific controls, protection measures and individual responsibilities that meet the requirements must also be defined and documented. The legal role of XXXXXXXXXXXXX will advise the Security Committee on said specific legal aspects.

The information security policies of XXXXXXXXXXXXX were designed to adjust or exceed, without contravening, the protection measures established in the laws and regulations, if any official and/or third party of XXXXXXXXXXXXX considers that any information security policy is in conflict with existing laws and regulations, has the responsibility to immediately report said situation to the Information Security Committee, who will attend to the situation.

4.12.2.2. Intellectual property.

The intellectual property of XXXXXXXXXXXXX, both its own and that of third parties (copyright of software or documents, design rights, registered trademarks, patents, licenses, source code, among others) will be adequately protected. Copyrighted material must not be copied without the permission of the owner.

11.12.2.3. Data Protection.

Security standards are mandatory for officials with access to personal data and information systems. They should consider the following aspects:

- Scope of application of the procedure with detailed specification of the protected resources.

- Measures, standards, procedures, rules and standards aimed at guaranteeing the level of security required by law.
- Functions and obligations of personnel with access to databases.
- Structure of personal databases and description of the information systems that process them.
- Incident notification, management and response procedure.
- Data backup and recovery procedures.
- Periodic controls that must be carried out to verify compliance with the provisions of the security procedure that is implemented.
- Measures to adopt when a support or document is going to be transported, discarded or reused. The procedure will be kept up to date at all times and must be reviewed whenever relevant changes occur in the information system or in its organization.

11.12.2.4. Compliance with security policies and regulations.

Company managers must ensure that all security procedures within their role of responsibility are carried out correctly, in order to comply with security policies and standards; in case of non-compliance, corrective actions will be evaluated and proposed. The results of these reviews will be maintained for your audit review.

11.12.2.5. Technical compliance.

It must be periodically verified that the information systems comply with the security implementation standards. Periodic audits must be carried out with the help of automated tools and technical reports must be generated that reflect the evaluation of information security risks, vulnerabilities and their degree of exposure to risk.

11. RELATED DOCUMENTATION

In support of the principles of Information Security, it supports in context:

- Code of Good Corporate Governance.
- Quality Management System and Environmental Policy of the organization.
- Human Management Policy.
- Information and communication technology policy.

12. PRIVACY POLICY AND PROTECTION OF PERSONAL DATA

In compliance with Law 1581 of 2012, which establishes provisions for the protection of personal data, XXXXXXXXXXXXXX, will strive for the protection of the personal data of its beneficiaries, suppliers and other third parties from which it receives and manages information. The terms, conditions and purposes will be established for which the entity, as responsible for the personal data obtained through its different service channels, will process the information of all the people who at some point, for reasons of the activity carried out by the institute, have provided personal data. In case of delegating the processing of personal data to a third party, the Company will require the third party to implement the necessary guidelines and procedures for the protection of personal data. Likewise, it will seek to protect the privacy of the personal information of its officials, establishing the necessary controls to preserve that information that the institute knows and stores about them, ensuring that said information is used only for the institute's own functions and is not published, disclosed or delivered to officials or third parties without authorization.

The Areas that have contact with personal data must obtain authorization for the treatment of this data in order to collect, transfer, store, use, circulate, delete, share, update and transmit said personal data in the development of the activities of the Company. They must ensure that only those with a legitimate employment need can access such data. They must establish contractual and security conditions for the entities linked or allies delegated for the processing of said personal data. They must abide by the technical guidelines and procedures established for the exchange of these data with the third parties delegated for the processing of said personal data. They must abide by the technical guidelines and procedures established to send messages to beneficiaries, suppliers or other third parties, via email and/or text messages.

The Information Security Committee must establish the controls for the treatment and protection of the personal data of the beneficiaries, officials, suppliers and other third parties from whom they receive and manage information.

The Technology Role must implement the necessary controls to protect the personal information of beneficiaries, officials, suppliers or other third parties stored in databases or any other repository and prevent its disclosure, alteration or elimination without the required authorization.

Direct or indirect officials must keep the corresponding discretion, or absolute confidentiality with respect to the information of the institute or its officials of which they become aware in the exercise of their functions. It is the duty of the users to verify the identity of all those people, to whom information is delivered by telephone, by fax, by email or by certified mail, among others.

- The users of the applications for clients of XXXXXXXXXXXXXX must assume individual responsibility for the access code to said portals that is provided to them; Likewise, they must periodically change this access code. They must have security controls in their

computer equipment or private networks to access the portals. They must accept the provision of personal data that the institute may make to third parties delegated for the processing of personal data, to judicial entities and other State entities that, in the exercise of their functions, request this information; Similarly, they must accept that they may be subject to internal or external audit processes.

- **11. ROLES AND RESPONSIBILITIES**

- **15.1. MANAGEMENT COMMITMENT**

- The Board of Directors of XXXXXXXXXXXXX approves this Information Security Policy as a sign of its commitment and support in the design and implementation of efficient policies that guarantee the security of the entity's information. The entity's Board of Directors and Senior Management demonstrate their commitment through:
- Review and approval of the Information Security Policies contained in this document.
- Active promotion of a safety culture.
- Facilitate the dissemination of this manual to all employees of the entity.
- Ensuring adequate resources to implement and maintain information security policies.
- Verification of compliance with the policies mentioned he

15.2. INFORMATION SECURITY COMMITTEE

- The Information Security Committee is made up of the person in charge of the Technology Role –who chairs it- and by the person in charge of the Risk and Internal Control Role, together with the people previously requested on an eventual basis.
- It must update and present to the Board of Directors the Information Security Policies, the methodology for the analysis of security risks and the methodology for the classification of information, as it deems pertinent.
- The Information Security Committee must analyze the security incidents that are escalated and activate the contact procedure with the authorities, when it deems it necessary.
- The Information Security Committee must verify compliance with the information security policies mentioned here.

- **15.3. ROLE OF TECHNOLOGY**

- The Technology Office must lead the generation of guidelines to manage the information security of XXXXXXXXXXXXX and the establishment of technical, physical and administrative controls derived from security risk analysis.

- The Risk Office must periodically validate and monitor the implementation of the established security controls.

15.4. AUDITOR

- Must plan and execute internal audits of the Information Security Management System of XXXXXXXXXXXXX in order to determine if the policies, processes, procedures and controls established are in accordance with the institutional requirements, security requirements and applicable regulations.
- You must execute total or partial reviews of the processes or areas that are part of the scope of the Information Security Management System, in order to verify the effectiveness of corrective actions when nonconformities are identified.
- You must report the findings of the audits to the responsible areas.

15.5. ALL OFFICERS OF XXXXXXXXXXXXX

- Full compliance by role, action or omission of this document and additional ones.
- All collaborators will act with the periodic measurements that the Consultant chosen for this purpose will carry out from now on, to certify compliance with this Risk Management System.

16. PRIVACY POLICY AND PERSONAL DATA PROTECTION

In compliance with Law 1581 of 2012, by which provisions are issued for the protection of personal data, XXXXXXXXXXXXX through the Risk Role, will strive for the protection of the personal data of its beneficiaries, suppliers and other third parties of which receive and manage information. The terms, conditions and purposes will be established for which XXXXXXXXXXXXX, as responsible for the personal data obtained through its different service channels, will process the information of all the people who at some point, for reasons of the activity carried out by the Entity have provided personal data.

In case of delegating the processing of personal data to a third party, XXXXXXXXXXXXX will require the third party to implement the necessary guidelines and procedures for the protection of personal data. Likewise, it will seek to protect the privacy of the personal information of its employees, establishing the necessary controls to preserve that information that the Entity

knows and stores about them, ensuring that said information is used only for business functions and is not published, revealed or delivered to officials or third parties without authorization.

16.1. Privacy regulations and protection of personal data.

- The areas that process personal data of beneficiaries, officials, suppliers or other third parties must obtain authorization for the treatment of these data in order to collect, transfer, store, use, circulate, delete, share, update and transmit said data personnel in the development of the Entity's activities.
- The areas that process personal data of beneficiaries, officials, suppliers or other third parties must ensure that only those people who have a legitimate work need can have access to said data.
- The areas that process personal data of beneficiaries, officials, suppliers or other third parties must establish contractual and security conditions for the linked entities or delegated allies for the processing of said personal data.
- The areas that process personal data of beneficiaries, officials, suppliers or other third parties must abide by the technical guidelines and procedures established for the exchange of these data with the third parties delegated for the processing of said personal data.
- The areas that process personal data of beneficiaries, suppliers or other third parties must abide by the technical guidelines and procedures established to send messages to beneficiaries, suppliers or other third parties, through email and/or text messages
- Users must keep the corresponding discretion, or absolute reserve with respect to the information of XXXXXXXXXXXXX or its officials of which they become aware in the exercise of their functions.
- It is the duty of the users to verify the identity of all those people, to whom information is delivered by telephone, by fax, by email or by certified mail, among others.

ANNEX 1. INFORMATION SECURITY AGREEMENT

INFORMATION SECURITY RESPONSIBILITY AGREEMENT FOR XXXXXXXXXXXXX STAKEHOLDERS

I, _____, identified with ___ No. _____, as legal representative of _____ with NIT, or on my own behalf __, by virtue of the relationship with XXXXXXXXXXXXX as _____, receive in full, in accordance with the Security regulations of Competent Information, the responsibility for the proper use of physical or digital information derived from my relationship with XXXXXXXXXXXXX, for which I sign this Information Security Responsibility Agreement, by which I declare to know and accept that:

- I am responsible for not disclosing, revealing or altering my personal password, confidential information, procedures, formats, and other technical and administrative aspects that are generated within the system, derived from the delivery of the user and password of the institution, to protect information against unauthorized or incorrect use, even after my employment relationship with the Institution to which I belong has ended.
- The password is an important mechanism for the protection of systems and applications. For which I understand that its management is personal and non-transferable. And I agree not to disclose the access code(s) assigned to me to any person.
- I understand that the username and password assigned to me are exclusively for my use and for work purposes. And I am aware that any activity in the systems, misusing my passwords is my responsibility.
- It is my responsibility to inform myself, understand, support and comply with the security regulations that govern the protection of information assets.
- In case of loss, forgetfulness or theft of the User Identifier and password, I undertake to communicate with the persons responsible for the respective entity, immediately.
- I will be responsible for the administrative, civil and criminal consequences established in the Law, for the loss, forgetfulness or theft of the User Identifier and password, as well as for those derived from the improper use of the information.
- I will be responsible for delivering the user identifier and password at the time of my cessation of functions, vacations, commissions and temporary absences to the institution by means of delivery receipt certificate so that these are disabled in the system.

- I acknowledge that I am responsible for the use of my User Identifier and password, if the loss, forgetfulness or theft occurs or is presumed until the time it is notified by written communication (email, official letter) to the Institution.
- I agree to inform the authority as appropriate, immediately, of any suspicious behavior or situation that may endanger the information assets in the public finance management system.
- I understand that XXXXXXXXXXXXX may review any information I have generated. I am aware that periodic audits will be made of the handling that I do of the information.

- It is my responsibility to comply with the information security recommendations requested by XXXXXXXXXXXXX
- I must comply with the secure deletion procedures, demonstrating it to XXXXXXXXXXXXX
- In general, I must comply with ISO 27001 standards, External Circulars of the Financial Superintendence 052 of 2011, 052 of 2007, 042 of 2012; Law 5271999 Law of electronic commerce, and derived from the previous ones, when managing any type of information of XXXXXXXXXXXXX, under penalty of the legal and commercial measures that the omission of this point implies.

In proof of having read and accepted the foregoing, I sign this document on the _____ day of the month of _____ of _____ in the city of _____.

CLIENT'S SIGNATURE _____

NAME _____

C.C _____ **Fingerprint Right Index**

LEGAL REPRESENTATIVE OF _____**NIT** _____

ANNEX 2. THIRD PARTY COMPLIANCE INFORMATION SECURITY

Separate document, integral to this document

CHANGE CONTROL

CHANGE CONTROL			
01-10-2017	v1	**INCLUSION**	Document Creation
		MODIFICATION	NA

PLASPEL S.A.S. EMPAQUES DE PLASTICO Y PAPEL			

		EXCLUSION	NA