Cybersecurity Guidelines

OD-TI-002

ODINSA

CONTENTS

AUDIENCE

These guidelines apply to all employees of Odinsa, Odinsa Gestor Profesional, Odinsa Vías, and Odinsa Aeropuertos, as well as contractors and third parties who have access to the Company's technological resources.

1. DOCUMENT CONTEXT

This document is part of the cybersecurity model, which includes the following elements, among others:

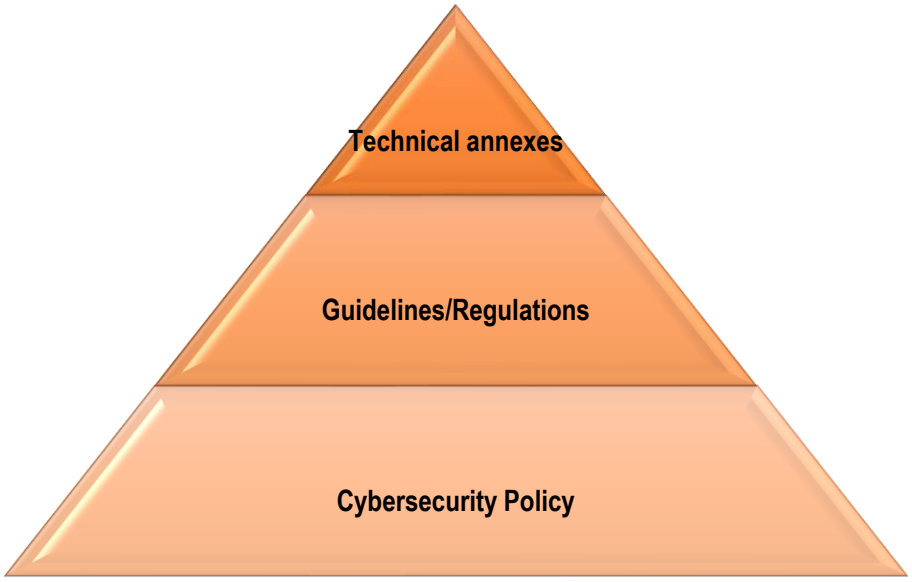

Illustration 1 – Elements of the cybersecurity model

Cybersecurity Policy: The Cybersecurity Policy is a high level document that demonstrates management's commitment to cybersecurity and establishes the framework for action that guides the behavior guidelines for employees and third parties involved in information management and operations, as well as the protection measures for the security of the technologies that enable the business.

Guidelines/Regulations: These refer to the set of orders, guidelines, principles, or specific rules on a particular security related topic, and must be aligned with the Cybersecurity Policy.

Technical Annexes: Technical documents corresponding to guides[1], procedures[2], and standards[3] for the implementation of cybersecurity policies.

2. DEFINITIONS

Information Assets: A set of data collected and transformed that has strategic, operational, economic, technical, legal, or regulatory value for the business, therefore, it must be protected.

Cyber Assets: Programmable electronic devices and elements of communications networks, including hardware, software, data, and information. As well as those elements with routable communication protocols that allow local or remote access to them.

Cybersecurity Committee: A multidisciplinary group led by the Cybersecurity area that ensures the implementation of actions to ensure compliance with the Cybersecurity Policy.

Confidentiality: The property of information not to be made available or disclosed to unauthorized individuals, entities, or processes. ISO/IEC 27002:2013

Control: Means to manage risk, including policies, procedures, guidelines, practices, or organizational structures that may be administrative, technical, managerial, or legal in nature.

Availability: The property of information being accessible and usable upon request by an authorized entity, when required. ISO/IEC 27002:2013

Cybersecurity Event: The identified presence of a system state or a service that indicates a possible noncompliance with the Cybersecurity Policy, a failure of controls, or a previously unknown situation that may be relevant to security.

Fraud: Any intentional act or omission designed to deceive others; carried out by one or more persons for the purpose of improperly appropriating, taking advantage of, or obtaining another's property, whether material or intangible, to the detriment of another and generally due to the lack of knowledge or malice of the affected party.

Cybersecurity Incident: Indicated by a single event or a series of unexpected or unwanted cybersecurity events that have a significant probability of compromising business operations and threatening information security.

Integrity: The property of information relating to its accuracy and completeness. ISO/IEC

[1] **Guides**: A guide is a general declaration used to recommend or suggest an approach to implementing policies and guidelines. Guides are essentially recommendations that should be considered when implementing security. Although they are not mandatory, they will be followed unless there are documented and approved arguments for not doing so.
[2] **Procedures**: They specifically define how policies, standards, best practices, and guidelines will be implemented in a given situation. Procedures are generally developed, implemented, and monitored by the process or system owner. Procedures will follow the organization's policies, standards, best practices, and guidelines as closely as possible.
[3] **Standard**: A standard is a document established by consensus that serves as a pattern, model, or guide that is used repeatedly. Security standards are often updated periodically since they depend directly on technology.

27002:2013

Business Continuity Plan: A documented and tested **plan** to respond appropriately to an emergency in business processes, thereby minimizing the impact on business operations.

Owner: The person responsible for the information asset to be protected.

Risk: Combination of the probability of an event and its consequences.

Information Systems: The set of technologies, processes, business applications, and software available to people within an organization.

Third Parties: Third parties are understood to be customers, contractors, outsourcing companies, and temporary workers.

User: The person who uses the information to carry out their job functions.

3. OBJECTIVE

Establish the set of guidelines, regulations, principles, directives, and rules to ensure the Company's cybersecurity, in accordance with the provisions of the Cybersecurity Policy and ensuring compliance with the objectives and legal obligations under the Company's current legal framework.

4. CYBERSECURITY ORGANIZATION

The Company establishes the structure for managing cybersecurity with clearly defined roles and responsibilities in order to ensure the proper functioning of the security program for information and operational technologies.

4.1. Cybersecurity Structure

The cybersecurity structure will consist of:

4.1.1. Board of Directors

Responsible for the adoption and proper implementation of cybersecurity policies and regulations, the establishment of an organizational structure that provides guidance and direction for cybersecurity management, the provision of the necessary resources for the implementation of cybersecurity measures, and the exercise of appropriate leadership before employees to reduce digital risks.

4.1.2. Strategic Cybersecurity Committee:

- Approve the organizational strategy that provides direction for cybersecurity management.
- Approve the Cybersecurity Policy and its guidelines.
- Manage the cybersecurity risk map and evaluate the effectiveness of the treatment measures adopted.
- Verify the adoption of recommendations issued by oversight bodies, auditors, insurance companies, risk areas, among others.
- Report to the Board of Directors and Senior Management.

4.1.3. Tactical Cybersecurity Committee

- Propose guidelines to implement the cybersecurity policy.
- Identify risks and vulnerabilities in the environment by constantly monitoring the cyber environment.
- Oversee the implementation of security measures.
- Propose the penetration testing program and drills for cyberattacks.
- Adjust the training and awareness program for all members of the organization.
- Design and implement expanded communication and training programs to strengthen the culture and capabilities of the cybersecurity management system.
- Communicate and report on the state of the organization's cybersecurity to Senior Management and other key members of the organization.

4.1.4. Operational Cybersecurity Committee

Responsible for the operation of the Company's security program for information and operational technologies (Technology Team). Must have suitable and clearly defined personnel in order to comply with and support cybersecurity activities. Their responsibilities include:

- Lead the implementation of the Company's security program for information and operational technologies.
- Lead the development of cybersecurity projects and initiatives.
- Coordinate and direct specific actions that help provide a secure environment and establish resources that are consistent with the Company's goals and objectives.
- Recommend specific roles and responsibilities related to cybersecurity.
- Approve the use of specific methodologies, tools, and processes for cybersecurity.
- Participate in the formulation and evaluation of action plans to mitigate and/or eliminate cybersecurity risks.
- Share documents generated within the Tactical Cybersecurity Committee that have a company wide impact.
- Ensure that the Company is taking the necessary actions to address risks to information assets.
- Promote the dissemination and awareness of cybersecurity within the Company.
- Follow up on security incidents reported by the Security area.

4.1.5. Company Information Security and Cybersecurity Officer, Cybersecurity Leader

Responsible for the Company's security program for information and operational

technologies, reporting to the assigned management level or, failing that, to the Tactical Cybersecurity Committee on policies, objectives, and compliance. The Company owns the information assets. The holding and handling of information is delegated to the Technology Team*, which is responsible for the custody and security of the information that the Company generates, considering its purpose and use. Their responsibilities include:

- Develop, implement, and administer an information technology and operational security program.
- Ensure that the implementations of cybersecurity controls through the processes are appropriate.
- Coordinate that the commitment to cybersecurity education and awareness is effectively supported and promoted throughout the Company.
- Ensure that the Company's cybersecurity incidents are monitored and reviewed, identifying appropriate preventive and corrective actions.
- Advise the Company on how to include cybersecurity in the initial phases of all information technology projects.
- Review policies, regulations, procedures, and specifications as stipulated and submit changes for approval to the corresponding instances.
- Participate in the definition of cybersecurity controls for the Company's technology platform.
- Evaluate, monitor, and report relevant cybersecurity incidents to the committee.
- Ensure that response plans for cybersecurity incidents or disruptions in information and communications technology are developed, maintained, and regularly tested for functionality.
- Ensure that access controls for each information system or operation are in accordance with the assessed level of risk.
- Verify that the tools for controlling access to information function in accordance with information classification regulations and guidelines.
- Define and approve the cybersecurity awareness plan for internal or external personnel.
- Conduct periodic security assessments of the technology platform.
- Report to the Tactical Cybersecurity Committee on the progress of security projects and initiatives.
- Evaluate significant changes in the exposure of information assets and cyber assets to security threats.

4.1.6. Owners of Information Assets and Cyber Assets – Area Leaders

Responsible for the information assets assigned to them, as well as for the classification, control, and monitoring of their use and management. Their responsibilities include:

- Monitor the practices of employees and third parties under their control and take the necessary actions to ensure compliance with cybersecurity policies and procedures.
- Ensure that security incidents involving personnel under their charge are reported.
- Keep up to date the inventory of information assets and cyber assets of the processes under their responsibility.
- Determine the classification level of each of the information assets and cyber assets for which they are responsible, according to their impact on the business and its

strategic objectives.

- Ensure that security controls are in accordance with the classification of the information or the criticality of the operational infrastructure.
- Define access and backup criteria for their assets.
- Execute or delegate the approval of access requirements, and the backup of information or the assignment of tasks to the person responsible for the information.
- Approve confidentiality agreements on information with third parties.
- Determine requirements for the availability of information.
- Assess information risk.
- Ensure that contracts with third parties that access the technology platform include clauses on compliance with the Company's information security and cybersecurity policies, procedures, and specifications, user account requirements for services and applications, and penalties in case of noncompliance.
- Identify the time requirements for safeguarding information assets.
- Monitor the access levels of employees and third parties to their information assets to ensure the confidentiality and integrity of the information stored, safeguarded, or processed therein.
- When there are employee departures or position changes, ensure that the information that is delivered and received is in accordance with corporate information storage guidelines.

4.1.7. Custodians of Information Assets and Cyber Assets

Responsible within the Company for safeguarding the information asset and cyber asset, enforcing the access restrictions and classifications given by the owner. The custodian can be any employee, supplier, contractor, or other authorized person. Their responsibilities include:

- Implement and document cybersecurity controls.
- Administer access to information in accordance with the criteria defined by the owners.
- Participate in the definition of security controls for the assets under their charge.
- Identify, investigate, and report cybersecurity incidents.
-

4.1.8. Users

Any employee, supplier, contractor, or other authorized person who uses the Company's information in the performance of their daily work activities. Their responsibilities include:

- Use the Company's information and IT resources solely for the performance of their work.
- Company information may not be used for personal purposes.
- Report cybersecurity incidents.
- Comply with cybersecurity policies, regulations, and procedures.
- Attend cybersecurity training and evaluations.
- Make proper use of the operations infrastructure and ensure its availability.
- Classify the information and operational infrastructure in accordance with its importance.

Comply with everything described in section 17 (Related Documentation).

4.1.9. Technology Department

Responsible for managing the necessary measures to mitigate cybersecurity risks and report any related events to the Tactical Cybersecurity Committee.

4.1.10. Human Resources Department

-
- Inform the Technology department in a timely and ongoing manner of employee hires, departures, and leaves of absence.
- Train Company employees on cybersecurity related aspects as part of the induction process.
- Carry out the selection process in accordance with the defined procedure.
- Include confidentiality clauses on information in the contracts of the Company's employees and third parties, together with the Legal department.
- Define the disciplinary process for noncompliance with security and cybersecurity policies.
- Include in the clearance certificate upon the employee's departure from the Company the return of IT resources and information assets under their custody.
- Conduct assessments of the cybersecurity knowledge of the Company's employees.

4.1.11. Legal Departments

- Identify and include in contracts with third parties the legal and contractual requirements associated with information security and cybersecurity.
- Collaborate in the incident response administration process when necessary due to legal proceedings or requests from competent authorities.
- Maintain contact with authorities and stakeholders to stay abreast of changes in government regulations in countries of influence.

4.1.12. Audit Area and Oversight Bodies

- Implement and execute a cybersecurity audit plan with the support of the Technology* team and/or external specialists. This plan should focus on reviewing all security requirements (policies and procedures). The results should generate a program that includes, at a minimum: actions to be taken, timelines, and responsible parties. The program must be approved by the Tactical Cybersecurity Committee.

4.1.13. Service Desk

- Respond to and support or escalate cybersecurity incidents to a second and third level.

5. HUMAN RESOURCE SECURITY

The Company's Human Resources department, or the company it delegates to manage its human resources, must notify the Technology department of all changes in direct and indirect personnel such as new hires, transfers, departures, and vacations, and must ensure that employees, contractors, and third party users understand and comply with their cybersecurity responsibilities.

5.1. Pre employment Security

All persons joining the Company must have an adequate job description and the terms and conditions of hiring.

All job candidates, contractors, and third party users must be screened appropriately (if a security check is required), especially for jobs that require access to sensitive, confidential, or restricted information. Therefore, a background verification process must be used that is proportional to the security classification of the information that the employee to be hired will access. The same treatment must be applied to candidates who administer and operate cyber assets in the Company's operations.

Employees, contractors, and third party users of information and operating technologies must sign an agreement regarding their roles and responsibilities in relation to cybersecurity.

5.2. Security During Employment

Together with the Company's Information Technology department, or the company it delegates to manage its information technology, the Processes department and the Company's Human Resources department must develop an effective and continuous information protection awareness program for all personnel. Specific training in technology risk management must also be defined and deployed for those individuals who are in charge of special protection responsibilities and the basic concepts with which every employee must comply.

It is the responsibility and duty of each Company employee to attend the cybersecurity awareness courses scheduled by the Company and to apply security in accordance with the policies and procedures established by the Company.

Any employee found to be in violation of cybersecurity policies and procedures will be subject to an administrative investigation to establish the circumstances and reasons that caused it. Based on the conclusions of this investigation, the relevant administrative, regulatory, and legal actions will be taken.

The employment contract must contain a paragraph that outlines this responsibility.

5.3. Security Upon Termination or Change of Contract

The Company's Human Resources department must ensure that all employees, consultants, contractors, and third parties who leave the Company or change jobs have signed a confidentiality agreement, which will remain in effect until the Company considers it appropriate, even after the termination of the job or contract.

The Company's Human Resources department must ensure that the departure or mobility of employees, contractors, or third parties is managed until the complete return of all assets and the withdrawal of access rights.

The leader of the area to which the departing employee belongs must ensure that the assets that will be returned are delivered for administration.

Access rights and user accounts for all employees, contractors, and third parties will be blocked once the established relationships have been finalized to prevent subsequent access to the organization's processes and systems.

All employees who change roles must have their access to systems reviewed and eliminated if necessary. Information stored, processed, or transmitted by these employees in repositories other than the Company's official ones will be deleted (this includes information stored on personal computers, mobile devices, email, and collaboration systems).

The only impediment to the destruction of information is of a legal and/or judicial order, which will determine the minimum period for storage of the information (retention period).

6. MANAGEMENT OF INFORMATION ASSETS AND CYBER ASSETS

The Company must have accurate knowledge of the information assets and cyber assets it possesses as a fundamental part of cybersecurity risk management, for which it must have:

- An inventory of information assets and cyber assets, with their respective risks, threats, vulnerabilities, and controls.
- The assignment of owners of information assets and cyber assets with the responsibility of controlling their development, maintenance, processing, classification, and security.
- The classification of information assets and cyber assets, taking into account their value to the business and in accordance with the criteria of confidentiality, integrity, and availability, for which the Company must establish classification criteria that include at least these three key variables in security.
- The management of storage media to protect information, and the identification of whether the use of encryption mechanisms is necessary to protect its confidentiality.

7. ACCESS CONTROL

The Company's Information Technology department, or the company it delegates to manage its information technology, must implement the applicable access control measures in accordance with the classification of information assets and cyber assets, in order to prevent tampering, loss, leakage, consultation, unauthorized use, or fraudulent access.

Access control for sensitive data and information must be based on the principle of least privilege, which means that access will not be granted unless explicitly permitted. Additionally, the following requirements must be met:

- Ensure that users are only assigned the privileges and rights necessary for the performance of their functions.
- Document user profiles and rights of access.
- Record events in case an audit is required.
- The Company shall define procedures, guidelines, and standards to:
- Manage user access covering all stages of the user lifecycle, from initial registration to the elimination or deactivation of the registration of those who no longer need access, including authorization levels and responsibilities.
- Review user access rights.
- Define user responsibilities regarding equipment and access to digital assets.
- Control access to information systems and platforms, including restrictions on access to information, the use of systems administration tools, and the management of user passwords.
- For resources such as shared folders, access and permission management are the responsibility of the asset owner, who assigns or removes access for third parties as needed.
- Third party access control.

8. CRYPTOGRAPHY

The Company's Information Technology department, or the company it delegates to manage its information technology, must establish the use of cryptographic systems and techniques to protect access keys to systems, data, and services, for the transmission of classified information, and/or for the safeguarding of relevant information based on the results of the risk evaluation conducted by the organization, in such a way as to ensure its confidentiality and integrity.

The Company shall secure asset information through encryption of its portable equipment and removable media on which corporate information is stored.

If an employee or a third party uses portable media not owned by the Company, such media may be read and will be restricted from downloading Company information, which restriction may be lifted with the express authorization of the owner of the information asset.

9. PHYSICAL AND ENVIRONMENTAL SECURITY

The Company must minimize the risks of damage and interference to information and its operations by establishing secure areas and security perimeters that allow for the implementation of controls to protect the organization's critical or sensitive information processing facilities against unauthorized physical access.

Likewise, equipment must be protected against physical and environmental threats to reduce the risk of unauthorized access to information and to protect it against loss or theft.

10. SECURITY IN INFRASTRUCTURE OPERATIONS

The Company's Information Technology department, or the company it delegates to manage its information technology, must ensure the correct and secure operation of information processing facilities and means of communication through the appropriate, effective, and efficient management of information and communications technology, including aspects associated with:

- Backups.
- Tape verification.
- Data recovery and change reversal.
- Change management.
- Antivirus systems administration.
- User and password administration.
- Resource access administration.
- Remote access administration.
- Performance measurement.
- IT resource capacity and availability management.
- Audit trail and information recording system management.
- Platform assurance.
- Separation of development, testing, and production environments.
- Segregation of duties.
- Protection against malicious code.
- Control of software in operation.
- Technical vulnerability management.

11. NETWORK AND TELECOMMUNICATIONS SECURITY

The Company's Information Technology department, or the company it delegates to manage its information technology, must ensure the protection of information communicated over voice and data networks and the protection of the support infrastructure. Secure network management, which may extend beyond organizational boundaries, requires careful consideration of data flow, legal implications, monitoring, and protection, for which it must:

- Ensure that network service providers implement measures in compliance with security requirements.
- Incorporate special controls 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.
- Ensure that information exchanges by the Company are based on formal exchange policies, procedures, and controls in line with exchange agreements and comply with any relevant legislation.

12. SECURITY IN SYSTEMS MANAGEMENT

The Company's Information Technology department, or the company it delegates to manage its information technology, must provide security measures in information systems from the requirements phase, and these must be incorporated into the development, implementation, and maintenance stages, which includes:

- The definition of cybersecurity related requirements that information systems must meet.
- Cybersecurity requirements must be included in the requirements for new systems or improvements to existing information systems, and must be justified, agreed upon, and documented as part of the entire information system project.
- The assurance of development environments, as well as access to the file system and source code.
- Assurance of the control of changes to systems, and the technical review of systems after changes are made to the operating system.
- The incorporation of information security policies into software development outsourcing processes.
- The proper use of test data.

13. RELATIONSHIP WITH SUPPLIERS

The Company must maintain an appropriate level of cybersecurity in its relationships with third parties, ensuring the protection of information assets that are accessible to them. The implementation of agreements must be checked, compliance with standards must be monitored, and changes must be managed to ensure that services are delivered to meet all requirements agreed upon with third parties.
The Company shall establish and agree on all cybersecurity requirements relevant to each supplier that accesses, processes, stores, communicates, or provides IT infrastructure components that support organizational information. To this end, the Legal department shall provide the clauses that regulate the relationship with suppliers for the cybersecurity issues mentioned in this document.

Agreements with suppliers must include requirements to address cybersecurity risks associated with the supply chain of information and communications technology services

and products.

The Company must verify the implementation of agreements associated with cybersecurity, monitor compliance, and manage changes to ensure that the services provided meet all agreed requirements.

14. CYBERSECURITY INCIDENT MANAGEMENT

All employees or third parties must communicate any observed or suspected cybersecurity events to the Technology staff.

The Company's Information Technology department, or the company it delegates to manage its information technology, must define the procedures, guides, and standards for cybersecurity incident management, which must include:

- The timely notification of cybersecurity events and weaknesses in order to undertake corrective actions.
- The escalation, assessment, and response to reported cybersecurity incidents.
- The proper collection of evidence for investigations and future legal actions.
- The proper management of knowledge acquired in response to information security and cybersecurity incidents as a source of learning for the analysis and resolution of future incidents.

15. BUSINESS CONTINUITY SECURITY

The Company must have a business continuity program that includes cybersecurity as a key element in all phases of the program: the identification of scenarios and risks; business impact analysis; the identification, definition, and implementation of continuity and recovery strategies; the documentation and implementation of response plans, including business continuity, disaster recovery, and crisis management plans; as well as the respective testing of strategies and plans.

The Company must preserve cybersecurity during the activation, evaluation, and operational phases of business continuity procedures and plans, as well as during the return to normalcy. Cybersecurity management requirements must be integrated into the continuity of critical business processes, with special attention to legislation, operations, personnel, materials, transportation, services, and additional, alternative, and/or differently arranged installations.

16. COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS

Any service or technological infrastructure solution must ensure that its selection is in accordance with contractual conditions, and with external and internal legislation and regulation, for proper compliance with the legal regimes to which the organization is subject.

16.1. Compliance with Legal and Contractual Requirements

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements, which must be advised by the organization's legal advisors or appropriately qualified professionals.

16.1.1. Identification of Applicable Legislation

All contractual and legal requirements that may affect the Company's information systems must be defined in advance and documented in accordance with the guidelines or methodologies employed by the Company. Specific controls, protective measures, and individual responsibilities that comply with the requirements must also be defined and documented. The Company's Legal department must participate in the identification of applicable legislation.

16.1.2. Intellectual Property Rights

The Company's intellectual property, both its own and that of third parties (copyrights on software or documents, design rights, trademarks, patents, licenses, source code, among others), shall be appropriately protected. Copyrighted material must not be copied without the owner's authorization.
Employment contracts must include clauses that indicate to all employees their legal responsibilities regarding copyright, in order to avoid possible violations of the legislation.

For compliance with software licensing, the following is established:

- A tool or procedure must be in place to control the current licenses of the software officially used by the Company.
- Evidence of the licenses that are the property of the Company, manuals, or master disks must be maintained.
- The number of users allowed by a given license must not be exceeded.
- At least one annual review must be conducted to ensure that only licensed software is used.
- Before sending information by email, using information available on the Internet, music, or using information from any type of document, the respective approval or payment must be obtained from the copyright owner.

16.1.3. Protection of Information Records

For information records associated with accounting records, database records, transaction records, audit records, and operational procedures, the retention periods and types of storage media such as paper, microfiche, magnetic media, optical media, etc. must be defined. In addition, they must be protected against loss, destruction, falsification, unauthorized access, and publication, in accordance with legislative, regulatory, contractual, and commercial requirements.

16.1.4. Data Protection and Privacy of Personal Information

The Company must ensure the privacy and protection of personal information that can be identified, as required by the applicable laws and regulations. Security standards are mandatory for employees with access to personal data and to information systems.

16.1.5. Controls on the Implementation of Cryptographic Techniques

The use of encryption software licenses must comply with the relevant agreements, laws, and regulations.

16.2. Cybersecurity Reviews

The Company must conduct regular reviews of the security of information systems. Reviews must be conducted in accordance with appropriate security policies, and technical platforms and information systems should be audited for compliance with appropriate security implementation standards and documented security controls.

16.2.1. Compliance with Security Policies and Regulations

Company managers must ensure that all security procedures within their area of responsibility are performed correctly in order to comply with security policies and regulations; in the case of noncompliance, corrective actions will be evaluated and proposed. The results of these reviews will be kept for audit review.

16.2.2. Compliance Verification

Information systems must be checked periodically to ensure that they comply with security implementation regulations. Periodic audits must be performed with the help of automated tools, and technical reports must be generated that reflect the cybersecurity risk assessment, vulnerabilities, and degree of risk exposure.

16.2.3. Considerations Regarding Information Systems Audits

The following aspects must be complied with when conducting internal or third party audits:

- Activities related to audit processes must be approved by the Security leader and the information owner.
- The scope, coordination, and control of the entire process must be determined in advance.
- The integrity of the information must be preserved throughout the entire process.
- The resources necessary to perform the audit must be explicitly defined.
- Additional processing requirements must be identified in advance.
- All access must be monitored and stored to produce a record of the activities performed during the process.
- All procedures, requirements, and responsibilities must be formally documented.
- Audit tools must be protected from misuse.

17. RELATED DOCUMENTATION

- Cybersecurity Policy
- Personal Data Processing Policy
- Guide to the Proper Use of IT Resources
- Security Guide for the Classification of Information Assets
- Information Security Specifications - End Users
- Information Security Standard - Application Acceptance

BIBLIOGRAPHY

ISO International Organization for Standardization. (2013). *ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls.*

DOCUMENT HISTORY

VERSION CONTROL

Number	Date	Description of change or modification
1	November 16, 2016	Initial issue
2	April 11, 2022	Adjustments for improvement opportunities in the Cybersecurity Process Audit
3	August 30, 2023	Approval body Strategic Cybersecurity Committee