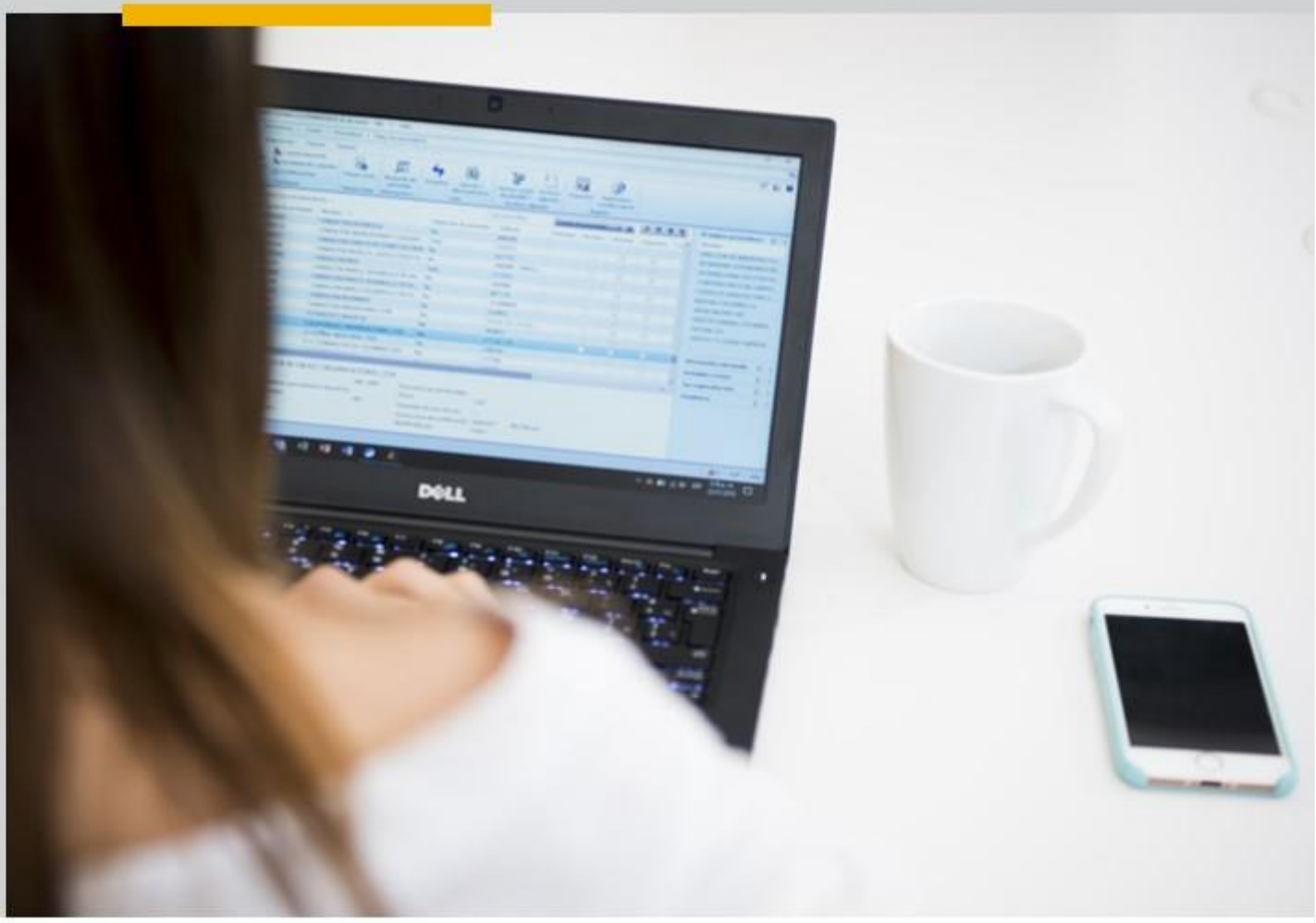

Cybersecurity Policy

ODIN-TI-001

ODINSA

Empresa de concesiones del GRUPO ARGOS

CONTENTS

1. OBJECTIVE

Establish the frameworks that will guide the conduct of employees and third parties involved in information management and operations, as well as the measures to protect the technologies that enable the business. Through this policy, guidelines are defined for implementing lines of action that guarantee the cybersecurity of ODINSA and its affiliated companies.

2. SCOPE

This policy applies to all geographies in which ODINSA and its affiliated companies operate. Additionally, it is mandatory for all employees and for all persons or entities that interact with the Companies' information and operational technologies.

3. POLICY

CYBERSECURITY POLICY

The Company, in compliance with laws and regulations for the protection of physical, digital, and cyber information assets[1] in the countries where it operates and in line with technology guidelines, identifies, manages, and mitigates associated risks by implementing cybersecurity best practices[2], seeking to guarantee the confidentiality, integrity, and availability of information, information technologies, and operational technologies, to ensure business sustainability and personal safety.

Regarding cybersecurity, the Company, its employees, and third parties that interact with digital assets commit to:

- Ensure that the cybersecurity policy is aligned with the Company's objectives and that it serves as a mechanism to contribute to the organization's continuity, sustainability, and value.
- Actively support cybersecurity within the organization in order to comply with

[1] Cyber asset: 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.

[2] Cybersecurity: refers to the protection of computer systems, networks, and connected devices against digital threats, such as data theft, service interruption, or unauthorized access, through the use of appropriate technologies, processes, and practices.

applicable regulations and achieve defined objectives, bearing in mind that cybersecurity is a responsibility shared by all members of the organization.

- Adopt an approach based on risk management that allows Odinsa and its affiliates, and its employees, to carry out their activities freely, safely, and reliably in the digital environment.
- Use all information that is stored, created, or transmitted using Odinsa's resources and those of its affiliates for the exclusive use of the organization and for business purposes.
- Maintain an updated inventory of existing information assets and cyber assets with their corresponding classification and owner.
- Establish controls to prevent the loss, damage, theft, or malfunction of information assets and cyber assets that could lead to the interruption of activities or impact the organization, through the identification, assessment, and treatment of risks, threats, and vulnerabilities in its information and operational systems.
- Ensure the establishment of measures for the proper functioning of its technological infrastructure in order to ensure the confidentiality, integrity, and availability of information assets and cyber assets, including measures that guarantee the non repudiation of actions by internal and external actors in the digital environment.
- Require employees and third parties that interact in the digital environment to know and apply the controls to protect information assets and cyber assets in order to reduce the risk of human error, theft, fraud, or misuse.
- Access only the information related to the functions of their position and responsibilities. Third parties that require access to information systems shall access only the information necessary for the performance of the object of their contracts.
- Disseminate and promote, in a planned manner, the objective of cybersecurity, its characteristics, and the individual responsibilities required to achieve it, including annual training plans, as well as ongoing activities and induction processes for new staff.
- Effectively manage cybersecurity incidents to minimize the risk of loss of availability, confidentiality, reliability, and integrity of information assets and cyber assets and to identify the controls to be implemented.
- Ensure that all critical processes and Company information systems that contain information assets have continuity plans that ensure resilience and recovery within the timeframes required by the business.
- Ensure that the use, operation, and handling of information systems comply with the requirements of applicable national and international laws regarding software licensing, copyright, information privacy, retention of information records, and all current legal provisions.
- Respect the privacy of customers, employees, suppliers, and other third parties with whom Odinsa and its affiliates interact, and take reasonable measures that ensure the security of personal data that is collected, stored, processed, disclosed, and transmitted.
- Coordinate with the Technology department for the development, adoption, or

procurement of new applications or technology services, ensuring compliance with cybersecurity guidelines and standards and proper integration with the Company's solution ecosystem.

- Respect the cybersecurity policy and its guidelines. Any violation by employees and third parties that interact with digital assets will trigger measures to address the resulting security incidents and will be subject to disciplinary action by the Human Resources departments.
- Ensure information security and business continuity based on the investigation of users' digital behavior by the internal control areas and the cybersecurity area.

4. CYBERSECURITY GOVERNANCE

ODINSA and its affiliated companies have defined the following organizational structure with instances, roles, and responsibilities to ensure adequate compliance with the information security and cybersecurity policy:

Strategic Cybersecurity Committee:

- Approve the organizational strategy that provides direction for managing information security and cybersecurity.
- Approve the information security and 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.

Members:

- Administrative Vice Presidency
- Finance Vice Presidency (Risk)
- Audit or (Compliance)
- Airport Vice Presidency
- Road Concessions Vice Presidency
- Summa Technology
- Cybersecurity

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 awareness and training program for all members of the organization.
- Communicate and report on the state of the organization's cybersecurity to Senior Management and other key members of the organization.

  Members:
  - Risks
  - Human Resources (Communications)
  - Operations Management for Operators
  - Process Management
  - Summa Technology
  - Cybersecurity

Information and cyber asset owners: Responsible for the assets assigned to them, as well as for the classification, control, and monitoring of the use and management of these assets.

Information and cyber asset custodians: Responsible within each company for safeguarding the assets, enforcing the access restrictions and classifications defined by the owner.

Control Areas (Technology, Risks, Audit): Responsible for managing and evaluating the measures adopted to mitigate the risk associated with cybersecurity.

Cybersecurity Officer: Responsible for developing the comprehensive cybersecurity management model, framing the cybersecurity policy within this ecosystem through risk management associated with information security and cybersecurity.

Users: Any employee, supplier, contractor, or other authorized person who uses the companies' information in the performance of their daily work activities.

5. ANNEXES AND REFERENCES

- NIST Cybersecurity Framework CSF.
- ISO 27000 Regulations.
- Laws and Regulations.
- Information Security and Cybersecurity Guidelines and Annexes.
- Personal Data Processing Policy.

6. EXCEPTIONS

Not applicable

7. POLICY REVIEW FREQUENCY

Each year or whenever required.

8. APPROVAL

Approval Body: Strategic Cybersecurity Committee
Review Body: Tactical Cybersecurity Committee.

9. VERSION CONTROL

Number	Date	Description of change or modification
1	November 16, 2016	Initial issue
2	August 30, 2023	Approval body Strategic Cybersecurity Committee