




## **TP MAR INFORMATION SECURITY POLICY**

**PUBLIC TP**

It may be shared internally and to third parties without additional authorization from the owner of the information.



|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 2 of 16  |

**CONTENT**

|    |  |    |
|----|--|----|
| 1. | OBJETIVE.....  | 4  |
| 2. | SCOPE .....  | 4  |
| 3. | RESPONSIBILITY .....   | 4  |
| 4. | AUTHORITY.....   | 4  |
| 5. | DEFINITION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM. .... | 4  |
| 6. | PILLARS OF THE POLICY .....                                    | 5  |
| 7. | OBJECTIVES OF THE INFORMACTION SECURITY SYSTEMS.....           | 6  |
| 8. | SPECIFIC CONTENT OF THE POLICY. ....                           | 6  |
| 9. | CHANGE CONTROL AND APPROVAL CYCLE.....                         | 15 |




|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 3 of 16  |

**REVISION LOG**

| DATE            | CHANGES | DESCRIPTION   | APPROVAL CYCLE  |
|-----------------|---------|---|---|
| <b>Apr/2024</b> | No      | Document review without changes                                   | <b>Created by:</b> Liliana Villar<br><b>Approved by:</b> Luis Gonzalez      |
| <b>Aug/2024</b> | Yes     | Policy update in accordance with ISO 27001:2022 version controls. | <b>Created by:</b> Liliana Villar<br><b>Approved by:</b> Luis Gonzalez      |
| <b>Nov/2024</b> | No      | Review without changes, minor adjustments in the document.        | <b>Created by:</b> Liliana Villar<br><b>Approved by:</b> Luis Gonzalez      |
| <b>Apr/2025</b> | Yes     | Update of logo and cover of the policy.                           | <b>Created by:</b> Estefania Castañeda<br><b>Approved by:</b> Luis Gonzalez |



|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 4 of 16  |

## 1. **OBJETIVE**

Establish guidelines and procedures that describe how the organization manages and protects its sensitive data and information assets.

## 2. **SCOPE**

The guidelines of this policy are mandatory for all TP MAR employees, including direct and indirect employees, contractors, subcontractors and suppliers, who provide support to the organization both from the physical facilities and from teleworking.

## 3. **RESPONSIBILITY**

- Senior Management is responsible for ensuring the resources and support necessary for compliance with this policy.
- The ISMS Team is responsible for conducting annual reviews of the Information Security Management System (ISMS), including all documented information and related activities.
- Service providers, such as vendors, suppliers, and contractors, must be aware of and comply with the organization's policies.
- The communication and PR team will ensure communication and outreach in physical or digital form within the organization and accessibility to relevant internal and external stakeholders.
- Operating unit leaders are responsible for taking this policy into account in all aspects of their critical business functions and services.


## 4. **AUTHORITY**

- Approval: Senior Management
- Review and update: Information Security Management System (*ISMS*) Leader.

## 5. **DEFINITION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM.**

An Information Security Management System (ISMS) is a systematic approach to managing sensitive information so that it remains secure. It involves establishing policies, procedures, and processes to manage risks and ensure the confidentiality, integrity, and availability of information assets.




|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 5 of 16  |

## 6. PILLARS OF THE POLICY

- Confidentiality: Protection of sensitive data and information from unauthorized access or disclosure, both internal and external.
- Integrity: Ensuring that data and information are accurate, complete, reliable, and not modified or manipulated in any way.
- Availability: Ensuring that data and information is available to authorized users when they need it, and that it is not subject to downtime or interruptions.
- Privacy: Identify and ensure compliance with requirements related to personally identifiable information of all stakeholders in the organization, in accordance with contractual laws and/or regulations.
- Accountability: Ensuring that individuals are responsible and accountable for their actions in relation to information security, and that appropriate action is taken in the event of non-compliance.
- Compliance: Ensure that the organization complies with applicable laws, regulations, and standards related to information security, such as TP Global, SOC 1, SOC 2, GDPR, HIPAA, PCI DSS, ISO 27701, and ISO 27001.
- Risk Management: Ensuring that the organization identifies, assesses, and manages information security risks, that appropriate controls and measures are in place to mitigate these risks.
- Continuity: Ensuring that the organization can continue to operate and deliver services in the event of a disruptive incident, such as environmental risks, political risks, loss of utilities, technology-related outages, and cyberattacks.
- Awareness: Ensure that all employees and stakeholders are aware of the organization's information security policies and procedures and are trained on how to identify and respond to security threats and incidents.



|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 6 of 16  |

## **7. OBJECTIVES OF THE INFORMATION SECURITY SYSTEMS**

- Maintain appropriate security levels for the processes established in the organization and promote continuous improvement.
- Mitigate and manage information security risks (clients, collaborators, suppliers, or third parties) through internal organizational controls aligned with international standards or regulatory requirements for Information Security and Privacy.
- Implement security controls for the organization's technological infrastructure, networks, and other services.
- Manage technological and infrastructure change controls, contributing to the fulfillment of the organization's information security requirements. \*Compliance with TP Policy controls.
- Conduct the Business Impact Analysis (BIA) process to identify the requirements of critical business processes that the Business Continuity Plan must address.
- Execute Business Continuity Plans to share with stakeholders.
- Manage quarterly tests on the Business Continuity Plans.

## **8. SPECIFIC CONTENT OF THE POLICY.**

### **8.1. Organizational Controls.**


#### **8.1.1. Information security policies.**

- 8.1.1.1. Information Security has a set of policies approved by management. These Will be made available to employees and external entities.
- 8.1.1.2. Information security policies are reviewed annually or when significant changes occur, to ensure their relevance and effectiveness.
- 8.1.1.3. Information security policies are approved by senior management, published, and communicated to all organizational personnel, as well as stakeholders.

#### **8.1.2. Information Security Roles and Responsibilities.**

- 8.1.2.1. All information security responsibilities will be defined and assigned.



|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 7 of 16  |

8.1.2.2. Conflicting duties and responsibilities should be segregated to reduce opportunities for unauthorized, unintentional modification, and/or misuse of organizational assets.

8.1.2.3. Management responsibilities Management should require all personnel to implement information security in accordance with the established information security policy and organization-specific procedures.

8.1.2.4. Contacts with relevant authorities and special interest groups should be kept up to date and documented.

8.1.2.5. The organization must analyze and collect all threat-related information.

8.1.2.6. Information security must be included from the beginning of each project.

### **8.1.3. Inventory of information and assets**

8.1.3.1. The organization must develop and maintain an inventory of information and assets including owners.

8.1.3.2. Rules that allow for acceptable use and procedures for handling information and other assets should be documented and implemented.

8.1.3.3. Personnel and stakeholders must, as appropriate, return all assets of the organization in their custody in the event of termination or change of employment, contract, or agreement.


### **8.1.4. Classification of the organization's information.**

8.1.4.1. Information should be classified according to the information security needs of the organization for the purpose of confidentiality, integrity, availability, and relevant stakeholder requirements.

8.1.4.2. The organization must implement and execute procedures for the labeling of the information in accordance with the structure adopted by TP.

8.1.4.3. Transfer guidelines, processes, or agreements should be developed between the organization and third parties.



|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 8 of 16  |

#### **8.1.5. Access Control.**

- 8.1.5.1. TP must establish processes and guidelines for the control of physical and logical access to information and other assets associated with information security based on security and business requirements.
- 8.1.5.2. The entire lifecycle of identities must be managed.
- 8.1.5.3. The rights of access to the information and associated assets must be adapted, reviewed, modified and eliminated in accordance with the organization's specific policy and guidelines for access control.

#### **8.1.6. Information security in supplier relationships.**

- 8.1.6.1. To address information security in the relationship with suppliers, you must define and implement processes and procedures, to manage information security risks related to the use of suppliers' products or services.
- 8.1.6.2. TP must establish and agree on information security requirements with all suppliers based on the type of relationship with the supplier.
- 8.1.6.3. Processes and procedures for the management of information security risks, associated with the supply chain of TIC products and services, must be defined and implemented.
- 8.1.6.4. Vendors must be monitored by the organization, regularly review, evaluate, and manage changes in vendors' information security practices and in the organization's service delivery.


#### **8.1.7. Information security for the use of cloud services.**

- 8.1.7.1. The organization must establish processes for acquiring, using, managing, and egressing cloud services will be established in accordance with information security requirements.

#### **8.1.8. Planning and preparation for the management of information security incidents.**

- 8.1.8.1. Response to Information security incidents must be planned, prepared for and managed, defining, establishing and communicating processes, roles and responsibilities in the face of incident management.
- 8.1.8.2. The organization must evaluate information security events and decide whether they should be classified as information security incidents.



|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 9 of 16  |

8.1.8.3. For all information security incidents, the organization must respond in accordance with documented policies and procedures.

8.1.8.4. The organization must learn to acquire knowledge from information security incidents, that will be used to strengthen and continuously improve information security controls.

8.1.8.5. Policies and procedures must be established, implemented for the identification, collection, acquisition and preservation of relevant evidence with information security events.

#### **8.1.9. Information security during outage.**

8.1.9.1. TP must plan how to maintain information security at the appropriate level during the outage.

#### **8.1.10. TIC readiness for business continuity.**

8.1.10.1. The organization must have planning, implementation, maintenance and testing with the capacity of the objectives and requirements of business continuity and ICT.

#### **8.1.11. Legal, regulatory, statutory and contractual requirements.**

8.1.11.1. The organization must identify, document, and keep up to date the legal, statutory, regulatory, and contractual requirements.

#### **8.1.12. Intellectual Property Rights.**

8.1.12.1. Procedures that protect intellectual property rights should be implemented.


#### **8.1.13. Records protection.**

8.1.13.1. The organization's records must be protected from loss, destruction, falsification, unauthorized access, and disclosure.

#### **8.1.14. Privacy and Protection of Personally Identifiable Information (PII).**

8.1.14.1. Requirements related to the preservation of privacy and the protection of personally identifiable information, must be identified and complied with in accordance with laws, regulations, and contractual requirements.



|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 10 of 16 |

#### **8.1.15. Independent review of information security.**

8.1.15.1. The organization must independently review the security of the information, including all relevant aspects such as: people, documented information, processes and technologies. This review should be carried out at least once a year or when significant changes occur.

#### **8.1.16. Compliance with information security policies, rules, and standards.**

8.1.16.1. The organization must conduct annual reviews on compliance with the information security policy, guidelines and standards.

8.1.16.2. Annual reviews should be conducted on information security and its implementation in the organization, to ensure compliance with controls, policies, procedures, and objectives.

8.1.16.3. The operating procedures where the facilities where the information is processed must be documented and made available to the personnel who require it.

### **8.2. Human Resources Controls.**

#### **8.2.1. Verifications and conditions of employment.**

8.2.1.1. Background checks on all candidates must be conducted prior to joining the organization considering applicable laws, regulations, and ethics, and that are proportionate to the requirements of the business.

8.2.1.2. Contractual work agreements should set out the responsibilities of the staff and the organization in terms of information security.


#### **8.2.2. Information security awareness.**

8.2.2.1. Individuals within the organization and relevant stakeholders should receive appropriate training and education on information security, and regular updates to specific information security policies and procedures, according to their role within the organization.

#### **8.2.3. Disciplinary process.**

8.2.3.1. The organization must formalize and communicate a disciplinary process, to take appropriate action against personnel and other relevant stakeholders, who have committed any type of violation of the information security policy.



|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 11 of 16 |

#### **8.2.4. Liabilities after cancellation or change of employment.**

8.2.4.1. The organization must implement responsibilities and duties related to information security, so that they remain valid after termination or change of employment, which will be defined, applied and communicated to all personnel and other interested parties.

8.2.4.2. Confidentiality or non-disclosure agreements that reflect the organization's needs for information protection should be identified, documented, reviewed periodically, and signed by staff and other relevant stakeholders.

#### **8.2.5. Remote Work.**

8.2.5.1. The organization must implement security measures when personnel are working remotely to protect information that they have access to, process, or store outside of the organization's premises.

#### **8.2.6. Information security event reports.**

8.2.6.1. The organization should provide a mechanism for staff to communicate observed or suspicious information security events in a timely manner, through communication channels implemented in the organization.

### **8.3. Physical controls.**

8.3.1.1. Physical security perimeters shall be defined and used to protect areas containing information and other associated assets.

8.3.1.2. Controls must be implemented at entrances and access points that protect secure areas of the organization.


8.3.1.3. The organization must design and implement physical security for offices, rooms, and facilities.

8.3.1.4. The organization must implement monitoring controls that continuously detect unauthorized physical access.

8.3.1.5. To protect against physical and environmental threats, the organization must implement strategies to protect the organization from natural disasters and other intentional or unintentional physical threats to infrastructure.

8.3.1.6. Safe areas must be ensured for the development of business and organizational activities.




|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 12 of 16 |

- 8.3.1.7. The organization must properly define and enforce the guidelines stipulated for desks and removable storage media, and clear screen rules for information processing facilities.
- 8.3.1.8. The organization must define the location of the computers in a safe and secure way.
- 8.3.1.9. Off-site equipment must be protected by the organization.
- 8.3.1.10. Storage media must be managed throughout the life cycle of acquisition, use, transport and disposal in accordance with the classification scheme and handling requirements of the organization.
- 8.3.1.11. The organization's processing facilities must be protected against power failures and other interruptions caused by failures in supporting utilities.
- 8.3.1.12. Cabling carrying power, data, or supporting information services must be protected from interception, interference, or damage.
- 8.3.1.13. The organization must ensure the maintenance of equipment to guarantee the availability, integrity and confidentiality of the information.
- 8.3.1.14. Equipment containing storage media, confidential data, and licensed software must be securely deleted before disposal or reuse of the equipment.

#### **8.4. Technological controls.**


- 8.4.1.1. The stored information must be processed or accessed through protected user terminal devices.
- 8.4.1.2. The assignment of privileged access rights must be managed and restricted.
- 8.4.1.3. The organization must control access to information and other associated assets in accordance with the access management policy.
- 8.4.1.4. Read and write access to source code, development tools, and software library must be managed correctly and appropriately.
- 8.4.1.5. The organization must implement secure authentication technologies and procedures based on restricted access to information and the established policy on access control.



|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 13 of 16 |

- 8.4.1.6. The capacity of the resources must be managed, monitored and adjusted in line with current and projected capacity requirements.
- 8.4.1.7. Protection against malware must be implemented and supported through proper user awareness.
- 8.4.1.8. The organization must obtain information regarding the technical vulnerabilities of the information systems that are in use, the organization's exposure to such vulnerabilities must be evaluated and appropriate actions must be taken.
- 8.4.1.9. Configuration management must be established, documented, implemented, and monitored for configurations, including hardware, software, services, and network security.
- 8.4.1.10. The organization's information that is stored in systems, devices or any storage medium must be deleted when it is no longer needed.
- 8.4.1.11. The organization must apply data masking which will be used in accordance with the policy established by the organization on access controls and other related specific policies and business requirements, and local laws.
- 8.4.1.12. To prevent data leakage, the organization must apply preventive measures against data leakage from systems, networks and any other device that processes, stores or transmits sensitive information.
- 8.4.1.13. Backups of software information and systems should be maintained and tested periodically in accordance with the established and agreed policy on information backups.
- 8.4.1.14. Information processing facilities the organization must implement sufficient redundancy to meet availability requirements.
- 8.4.1.15. Logs must be generated, stored, protected, and analyzed for logins, activities, exceptions, failures, and other relevant events.
- 8.4.1.16. The organization must monitor networks, systems, and applications for the detection of abnormal behavior and implement pertinent actions to evaluate possible information security incidents.
- 8.4.1.17. The clocks of the information processing systems that are used by the organization must be synchronized with the approved time sources.



|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 14 of 16 |

- 8.4.1.18. The use of privileged utility programs that can override controls on systems and applications must be strictly restricted and controlled by the organization.
- 8.4.1.19. Procedures and controls must be implemented to securely manage the installation of software on operating systems.
- 8.4.1.20. The security of networks and devices must be protected, managed, and controlled to safeguard information in systems and applications.
- 8.4.1.21. Network Services Security The organization must identify, implement, and monitor security mechanisms, service levels, and network service requirements.
- 8.4.1.22. Information services, users, and information systems groups must be segregated into the organization's network groups.
- 8.4.1.23. Access to the organization's external websites must be filtered and managed to reduce the exposure of malicious content.
- 8.4.1.24. The organization must define and implement rules for the effective use of cryptography, including the management of cryptographic keys.
- 8.4.1.25. Guidelines and rules for the life cycle of secure software and systems development must be established and applied.
- 8.4.1.26. Application security requirements must be identified, specified, and approved when developing or acquiring applications.
- 8.4.1.27. The organization must establish, document, maintain, and apply secure systems engineering principles to any information system development activity.
- 8.4.1.28. Secure coding principles should be applied to software development.
- 8.4.1.29. Security testing processes in development and acceptance should be defined and implemented in the development lifecycle.
- 8.4.1.30. The outsourced development organization must direct, monitor, and review related activities.
- 8.4.1.31. The separation of development, test, and production environments must be separated and secured.
- 8.4.1.32. Changes to information processing facilities and information systems should be subject to organizational change management procedures.



|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 15 of 16 |


8.4.1.33. The organization must protect, properly manage the information of the tests.

8.4.1.34. The organization must plan and agree between the evaluator and the appropriate management to protect the information systems during audit tests and other assurance activities that involve the evaluation of the operating systems.

## 9. CHANGE CONTROL AND APPROVAL CYCLE.

| DATE       | VERSION | DESCRIPTION   | APPROVAL CYCLE  |
|------------|---------|---|---|
| 08/05/2012 | 1       | First version of the ISMS policy definition and objectives                  | <b>Created:</b> Ana Gomez<br><b>Reviewed:</b> Ivan Fernando Diaz<br><b>Approved:</b> Carlos Carrizosa                                   |
| 19/03/2014 | 2       | ISMS Policy and Objectives Review 2013/2014                                 | <b>Created:</b> Ana Gomez<br><b>Reviewed:</b> Ivan Fernando Diaz<br><b>Approved:</b> Omar Ladino  |
| 07/04/2015 | 3       | Document review and update  | <b>Created:</b> Ana Gomez<br><b>Reviewed:</b> Ivan Fernando Diaz<br><b>Approved:</b> Omar Ladino  |
| 09/02/2016 | 4       | Document review and update  | <b>Created:</b> Ana Gomez<br><b>Reviewed:</b> Ivan Fernando Diaz<br><b>Approved:</b> Omar Ladino  |
| 14/08/2017 | 5       | Document review and update  | <b>Created:</b> Ana Gomez<br><b>Reviewed:</b> Ivan Fernando Diaz<br><b>Approved:</b> Omar Ladino  |
| 30/08/2018 | 6       | Revision and updating of the document (logo)                                | <b>Created:</b> Ana Gomez<br><b>Reviewed:</b> Ivan Fernando Diaz<br><b>Approved:</b> Omar Ladino  |
| 29/04/19   | 7       | Broadening the scope of the policy and integrating with Management Systems. | <b>Created:</b> Gustavo Olaya- Yesenia Brand<br><b>Reviewed:</b> Ivan Diaz- Ana Gomez<br><b>Approved:</b> Carlos Carrizosa- Omar Ladino |
| 28/10/2020 | 8       | Revision and minor corrections to the text                                  | <b>Created:</b> Luis González – William Ricaurte<br><b>Reviewed:</b> Alvaro Guerrero<br><b>Approved:</b> Carlos Carrizosa               |
| 13/09/2021 | 9       | Revision and minor corrections to the text                                  | <b>Created:</b> Luis González<br><b>Reviewed:</b> Alvaro Guerrero<br><b>Approved:</b> Carlos Carrizosa                                  |
| 27/09/2022 | 10      | Expansion and improvement of the content of the policy.                     | <b>Created:</b> Jose Montañez<br><b>Reviewed:</b> Luis Gonzalez<br><b>Approved:</b> Claudio Esteves                                     |
| 01/02/2023 | 11      | The scope in relation to teleworking is expanded.                           | <b>Created:</b> Jose Montañez<br><b>Reviewed:</b> Luis Gonzalez<br><b>Approved:</b> Claudio Esteves                                     |



|  |                                      |                |
|--|--------------------------------------|----------------|
|  | <b>INFORMATION SECURITY POLICY</b>   | Code: SI-PO-01 |
|  |                                      | Version: 14    |
|  | Capability: 7.4 Information Security | Page: 16 of 16 |

|            |    |   |  |
|------------|----|---|--|
| 24/03/2023 | 12 | Expansion and improvement of the content of the policy.           | <b>Created:</b> Luis Gonzalez-Liliana Villar<br><b>Reviewed:</b> Javier Albiol Fernandez<br><b>Approved:</b> Claudio Esteves |
| 21/08/2024 | 13 | Policy update in accordance with ISO 27001:2022 version controls. | <b>Created:</b> Liliana Villar<br><b>Reviewed:</b> Javier Fernandez<br><b>Approved:</b> Claudio Esteves                      |
| 18/11/2024 | 13 | Review without changes, minor adjustments in the document         | <b>Created:</b> Liliana Villar<br><b>Reviewed:</b> Javier Fernandez<br><b>Approved:</b> Claudio Esteves                      |
| 01/04/2025 | 14 | Update of logo and cover of the policy.                           | <b>Created:</b> Estefania Castañeda<br><b>Reviewed:</b> Javier Fernandez<br><b>Approved:</b> Claudio Esteves                 |