ATENTO

Yes, policies and procedures are our **responsability**

POL.SI.001.V05.ENG

Security Information and Cybersecurity Policy

Version 05

08/25

#PoliciesThatGuideUs

Table of contents

1. PURPOSE

This Information and Cybersecurity Policy establishes the high-level principles and guidelines for the protection of the IT and technological resources of Grupo Atento, serving as the central document of the Information Security and Privacy Management System (SGSIP). The purpose of this policy is to ensure the confidentiality, integrity, and availability of information, as well as the acceptable and secure use of technological resources, in accordance with best practices and applicable legal and regulatory requirements, including ABNT NBR ISO/IEC 27001, and aligned with the strategic objectives of Grupo Atento.

2. ORGANIZATIONAL CONTEXT

Grupo Atento recognizes the critical importance of information security, data privacy, and the proper and secure use of its technological resources for the sustainability of the business and the protection of its stakeholders' interests.

The organization operates in a dynamic environment, carrying out continuous analysis of internal and external contexts that may impact and generate changes, as well as opportunities for the Information Security and Privacy Management System (SGSIP).

In this context, the increasing reliance on information systems and technological infrastructures to deliver the services that support Grupo Atento's business is highlighted. The effective and responsible use of these resources is essential to guarantee confidentiality, integrity, and availability of the information processed and stored, in addition to mitigating the risks associated with the inappropriate or malicious use of technology.

The analysis of the organizational context also considers the expectations of clients, partners, regulators, and other stakeholders regarding information security, personal data privacy, and the integrity of processes that depend on reliable technological resources, used ethically and in compliance with established standards. This Policy, therefore, encompasses both the protection of information and the guidelines for the appropriate use of Grupo Atento's technological resources.

3. SCOPE

This Policy covers all processes and information systems, electronic and IT equipment, as well as network resources of Grupo Atento. It applies broadly and without restrictions to all technological resources made available or used by Grupo Atento, including, among others: IT equipment, software, operating systems, storage media, nominal and service network accounts, email, web browsing, and data transmission.

This Policy applies to all areas of Grupo Atento, as well as to all employees (permanent or temporary), service providers, consultants, clients, and other partners who interact with Grupo Atento's processes, information systems, or technological resources.

The purpose of this scope is to ensure that all individuals and all information and technology assets within Grupo Atento's ecosystem are subject to the guidelines established in this Information and Cybersecurity Policy, consolidating in a single normative document the responsibilities and controls for protecting information and ensuring the appropriate use of technological resources.

In summary, this Policy applies to:

- All processes of Grupo Atento.
- All information systems of Grupo Atento.
- All technological resources owned, used, or made available by Grupo Atento.
- All employees of Grupo Atento.
- All service providers with access to Grupo Atento's information or systems.
- Consultants, clients, and other partners who interact with Grupo Atento's technological resources, information systems, or processes.

4. REFERENCES

This Policy is integrated into the Information Security and Privacy Management System (SGSIP) and refers to the following high-level documents:

- ISO/IEC 27001:2022
- ISO/IEC 42001:2023
- MAN.SI.001 – Information Security Management System Manual
- POL.LEG.012 – Global Privacy Policy
- POL.ITD.004 – Responsible Use of AI Policy
- Royal Decree 311/2022, of May 3 – regulating the National Security Scheme (ENS).
- Organic Law 3/2018, of December 5 – on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD).
- Regulation (EU) 2016/679, of April 27, 2016 – General Data Protection Regulation (GDPR).
- Law 6/2020, of November 11 – regulating certain aspects of trusted electronic services.
- Law 34/2002, of July 11 – on Information Society Services and Electronic Commerce (LSSI).
- Law 9/2014, of May 9 – on Telecommunications.

Other normative documents — such as standards, procedures, and specific policies — complement this Policy and are referenced in the SGSIP Manual (MAN.SI.001) and related records.

5. PRINCIPIOS DE CIBERSEGURIDAD

Grupo Atento adopts the following fundamental principles for information management and cybersecurity, which serve as the foundation for all security measures implemented:

- Information Security as a Comprehensive Process: A set of practices and processes implemented to protect Grupo Atento's information assets. It encompasses the fundamental principles of confidentiality, integrity, availability, authenticity, and traceability, serving as the basis for all security measures adopted to mitigate risks and ensure business continuity. This principle is intrinsically linked to the security and privacy objectives mentioned in Section 7 of this Policy and detailed in the Information Security and Privacy Management System Manual (MAN.SI.001 – Information Security Management System Manual). Security is considered part of day-to-day operations, applied from the initial design of ICT systems and throughout their entire lifecycle.
- Confidentiality: Ensuring that information is accessible only to authorized entities. This is achieved through the implementation of access controls (defined in POL.SI.005 – Access Control Policy) and password protection (NOR.SI.011 – Password Management Standard), guaranteeing that only authorized personnel can access sensitive data. Practical example: ensuring that customer data and confidential internal information are not accessed by unauthorized individuals, while allowing service agents to access only the information necessary to perform their work.
- Integrity: Ensuring the accuracy and completeness of information and processing methods, protecting them against unauthorized or accidental modifications. This involves ensuring that data remains accurate, complete, and reliable throughout its lifecycle. Measures such as Vulnerability Management (NOR.SI.020 – Vulnerability Management and Patch Application Standard) and change controls contribute to this principle. Practical example: ensuring that customer service records and system configurations are not improperly or unauthorizedly altered.
- Availability: Ensuring that information and systems are accessible and usable by authorized entities whenever required. This principle is supported by practices such as NOR.SI.012 – Backup and Information Restoration Standard and business continuity plans, guaranteeing continued operations in the event of incidents. Practical example: keeping customer service systems and communication platforms accessible whenever required for business operations.
- Authenticity: Ensuring the truthfulness and legitimacy of an entity — whether a person, a process, or a system — as well as the reliability of the source from which the data originates. This principle is essential to trust in user identities and the origin of information.

- Traceability: Ensuring that the actions of an entity or person within systems and on information can be exclusively attributed to that entity or person. This is achieved through detailed activity and event logging, enabling the reconstruction of actions for audit and accountability purposes.
- Privacy (Personal Data Protection): Applying the laws, standards, and regulations in force in the country where personal data is processed, including, prominently, the General Data Protection Regulation (GDPR) and the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD) in Spain. It ensures the protection of employees', customers', and suppliers' personal data, as well as the collection of necessary consents and the implementation of appropriate security measures.
- Responsible Use of Technological Resources: Using Grupo Atento's technological resources in an ethical, legal, and compliant manner, in accordance with company policies, as established in the Global Acceptable Use of Technological Resources Standard (NOR.SI.019). This is essential to prevent security incidents, protect information, and avoid the misuse of company assets. Practical example: using Grupo Atento's computers and network solely for professional purposes, in compliance with company policies, while avoiding the installation of unauthorized software or access to malicious websites (as detailed in NOR.SI.019).
- Robust Access Control, Including Password Management: A key aspect of information security is the implementation of robust access controls to ensure that only authorized users, processes, or devices can access information and information assets. This includes effective password management, which must be robust and managed in accordance with the Password Management Standard (NOR.SI.011). The detailed requirements for logical access management are defined in the Access Control Standard (NOR.SI.005), which establishes the processes for requesting, approving, granting, revoking, modifying, and reviewing user accounts.
- Determination of the Required Security Level: The organization will determine the level of security required for each information system, in compliance with applicable national regulatory frameworks, such as Article 40 of Royal Decree 311/2022, which regulates the National Security Scheme (ENS) in Spain, and the general criteria outlined in its Annex I. This determination will be based on assessing the impact on security dimensions (Confidentiality, Integrity, Availability, Authenticity, and Traceability), using methodologies aligned with relevant national frameworks such as the CCN-STIC 803 Guide for system categorization.
- Governance and Responsible Use of Artificial Intelligence (AI): Grupo Atento is committed to the development, implementation, and responsible use of Artificial Intelligence systems. To achieve this, the organization ensures that AI is managed ethically, transparently, and securely, with the objective of minimizing risks such as bias and undesirable impacts on individuals and society. This includes a commitment to human oversight where necessary. Grupo Atento will establish and maintain an AI Management System (AIMS), aligned with the principles of ISO/IEC 42001:2023 (Information Technology — Artificial Intelligence — Management System). This system will integrate the management of AI-specific risks and opportunities with the Information Security Management System (ISMS), reinforcing the protection of confidentiality, integrity, and availability of information and ensuring the quality of data used in AI systems. The guidelines and procedures for the development, implementation, and responsible use of AI within Atento are defined in POL.ITD.004 – Responsible Use of AI Policy.

6. LEADERSHIP

Grupo Atento's top management demonstrates its strong commitment to information security and cybersecurity through the establishment, implementation, maintenance, and continual improvement of the Information Security Management System (ISMS). This commitment is reflected in the definition of this Information and Cybersecurity Policy, the allocation of necessary resources, and the continuous communication of the critical importance of information security to all employees and stakeholders.

The organizational responsibilities and authorities regarding information security are clearly defined and communicated across the organization, ensuring a multidisciplinary approach and active participation in protecting information assets. The specific details of roles, responsibilities, and authorities relating to information security — including associated expectations — are set forth in job descriptions and detailed in the Information Security and Privacy Management System Manual (MAN.SI.001).

Leadership at all levels of the organization is responsible for ensuring strict compliance with this Policy, as well as with the standards, procedures, and other normative documents on information security within their respective areas of expertise and responsibility.

7. PLANNING

Grupo Atento establishes, implements, and maintains the planning necessary to achieve information security and privacy objectives, in accordance with this Policy. This planning addresses the following key elements:

- Actions to address risks and opportunities: Through its strategic planning and process mapping, Grupo Atento understands internal and external scenarios and conducts periodic assessments of the Information Security and Privacy Management System (SGSIP). This analysis allows for the periodic identification and evaluation of risks to information assets and the opportunities inherent to the processes that make up the SGSIP. The details of the risk assessment and treatment process — including the methodology used and the implemented controls, are defined in specific normative documents. It is essential that this planning considers the principles of confidentiality, integrity, and availability discussed in Section 5 of this Policy.
- Information security and privacy objectives and planning to achieve them: Top management, through strategic planning, considers internal and external scenarios and stakeholder expectations to determine the SGSIP objectives. These objectives are established, documented, and communicated, aligned with business objectives, and consider applicable legal and regulatory requirements. Planning to achieve these objectives involves defining actions, responsibilities, deadlines, and necessary resources, as detailed in the Information Security and Privacy Management System Manual (MAN.SI.001). These objectives must reflect the protection of confidentiality, assurance of integrity, and availability of information, as well as compliance with privacy principles.
- Service planning: Grupo Atento carries out planning for IT services that support the business, considering information security and privacy. Top management periodically analyzes the performance of the SGSIP, considers risks and opportunities, and proposes action and improvement plans when necessary, ensuring service continuity and maintaining an appropriate level of security and privacy. The details of operational planning and control are described in MAN.SI.001. This plan must ensure the availability of services and the integrity of the information managed by them.

This planning is dynamic and is reviewed and updated periodically to ensure its effectiveness and alignment with changes in the business environment, legal and regulatory requirements, and information security and cyber threat scenarios. Clear emphasis on security principles — such as the confidentiality of sensitive information processed in IT services, the integrity of business data supported by these services, and their availability for operations — must remain a primary consideration in this planning.

8. SECURITY CONTROLS

Grupo Atento implements and maintains Information Security and Cybersecurity controls to ensure the confidentiality, integrity, and availability of information, in compliance with the principles established in this Policy and with applicable laws and regulations. Grupo Atento is committed to implementing controls that cover, among others, the following areas:

- Access controls: ensure that access to information and information assets is authorized and restricted to authorized users, processes, or devices. Details are defined in specific normative documents, such as POL.SI.005 – Access Control Policy and NOR.SI.011 – Password Management Standard, as referenced in the SGSIP Manual (MAN.SI.001).
- Vulnerability management: identify, analyze, and address security vulnerabilities in systems and applications. Procedures are defined in NOR.SI.020 – Vulnerability Management and Patch Application Standard and in the SGSIP Manual (MAN.SI.001).
- Malware protection: implement measures to protect systems against malicious software. NOR.SI.018 – Global Antivirus and Malware Prevention Standard details the protective measures.
- Network security: protect network infrastructure against unauthorized access and threats. NOR.SI.016 – Firewall Management Standard and NOR.SI.063 – Content Filtering Standard establish the applicable requirements.

- Encryption: use cryptography to protect the confidentiality and integrity of information in transit and at rest. NOR.SI.023 – Cryptography Usage Standard defines the guidelines.
- Backup and restoration: perform periodic backups and test restoration capabilities to ensure information availability in the event of incidents. NOR.SI.012 – Backup and Information Restoration Standard details the procedures.
- Information classification: classify information according to its sensitivity level and implement appropriate security controls. NOR.SI.036 – Information Classification Standard defines the criteria.
- Information security and privacy incident management: establish processes to identify, analyze, respond to, and recover from incidents. NOR.SI.009 – Information and Cybersecurity Incident Management Standard details the processes.
- Information security and privacy awareness: promote awareness and training programs for employees regarding risks and responsibilities. Details are described in Section 9.3 of the SGSIP Manual (MAN.SI.001).
- Physical and environmental security: implement controls to protect physical facilities and the IT environment. These practices are defined in internal normative documents.
- Personal data protection: implement measures to ensure the protection and privacy of personal data in compliance with applicable regulations.
- Proprietary information security: define security rules for mobile devices and equipment connecting to the internal network.
- Acceptable and unacceptable use: establish acceptable use conditions and prohibited activities, including copyright violations, insecure file sharing, and the introduction of malicious code into the network.
- AI governance and responsible use: Grupo Atento is committed to the development, implementation, and responsible use of AI in an ethical, transparent, and secure manner, mitigating risks such as bias and undesirable social impacts. This includes human oversight where necessary. Grupo Atento will establish and maintain an AI Management System (AIMS) aligned with ISO/IEC 42001:2023, integrating AI-specific risks and opportunities into the ISMS.

The specific details for implementing and managing these controls are described in complementary policies, standards, and procedures, which form part of Grupo Atento's Information Security and Privacy Management System (SGSIP), as detailed in the SGSIP Manual (MAN.SI.001).

9. AWARENESS AND COMMUNICATION

Grupo Atento promotes periodic awareness programs to ensure that all employees, third parties, and other stakeholders are familiar with this Information Security Policy and their responsibilities. Communication of the Policy and relevant information on information security is carried out through various channels.

10. PERFORMANCE EVALUATION

The performance of the ISMS is continuously monitored, measured, analyzed, and evaluated. This includes monitoring security objectives, analyzing incidents, reviewing the results of internal audits, and top management's critical review.

Internal audits are conducted periodically to verify compliance with ISMS requirements and this Policy. Results are reported for corrective actions and improvements.

Top management conducts critical reviews of the ISMS at planned intervals, ensuring its ongoing relevance, adequacy, and effectiveness.

11. IMPROVEMENT

Grupo Atento is committed to the continual improvement of the adequacy, sufficiency, and effectiveness of the ISMS. Nonconformities are addressed with corrective actions to eliminate their causes and prevent recurrence. Opportunities for improvement are constantly evaluated.

12. COMPLIANCE AND SACTIONS

Failure to comply with the requirements set forth in this Policy, as well as with any standards, procedures, or operational guidelines derived from it, will result in the application of disciplinary measures. Grupo Atento considers information security a fundamental priority, and any violation of the policies and standards established herein exposes the company to significant risks.

Disciplinary measures may include termination of employment, without prejudice to other applicable labor or legal actions. Any intentional violation of this Policy or infraction committed with the purpose, intent, or effect of fraud will be considered an aggravating factor and may result in immediate termination of employment.

In addition to employment-related consequences, violations of this Policy may result in civil and/or criminal actions under applicable law. The imposition of corrective actions is not an exclusive remedy, and Grupo Atento may exercise all legal rights available, without prejudice to employment-related decisions.

The application of these measures will follow the guidelines established in PRO.SI.002 – Information Security Sanctions Procedure of Grupo Atento, ensuring a fair, transparent, and consistent process across all global operations.

13. SUPPLIER MANAGEMENT

Suppliers and service providers must comply with Grupo Atento’s information security requirements, as defined in this Policy and other relevant documents. Confidentiality agreements are established when necessary.

14. EXCEPTIONS

All exceptions to this Policy must be reviewed, evaluated, and approved by the Information Security area, with final authorization from the Global CISO and the CIO.

15. VERSION

Version	Date	Reviewer	Modifications
01	08/25	CISO GLOBAL	Creation

16.