POLICY

Integrated Management System

INFORMATION SECURITY

Document Reference | PL03_V8

TABLE OF CONTENTS

1. References	ISO/IEC 27001:2013 | 4.1 | 5 | A.5.1.1 e A.5.1.2. ISO/IEC 20000:2018 | 8.7.3. | 6.3.(c) ETSI EN 319 411-1 ETSI EN 319 411-2 ETSI EN 319 421 ETSI EN 319 401 Regulation (EU) No. 910/2014 General Data Protection Regulation (Regulation 2016/679 of the European Parliament and of the Council) Law 58/2019, of 8 August - Data Protection
2. Associated Documents	PL05|SGSI – Acceptable usage (in Portuguese language) DS20|SGSI – ISMS scope definition (in Portuguese language) PL10_GTS – Privacy Policy DS24_SGSI – Definition of the scope of the ISMS (in Portuguese language)
3. Associated Registers	RG01 – Document registration (in Portuguese language) RG02 – Inventory (in Portuguese language) MA04_GTS - Document registration (in Portuguese language)
4. Distribution List	Public
5. Document History	2013-10-07 **|** Version 1 2014-02-04 **|** Version 2 2015-01-12 **|** Version 3 2015-05-26 **|** Version 4 2016-12-29 **|** Version 5 2017-11-02 **|** Version 6 2019-11-25 **|** Version 7 2021-01-26 | Version 8
6. Document Classification	D | Public

7. Revision Record:

Version Number	Creation	Approval	Reason
	26-01-2020	**26-01-2020**	
8	**CSG**	**Leadership**	Transition to the 2018 version of the standard
	Sandra Fernández	Tolentino Pereira	

8. Strategic Business Framework

The strategic business options of ACIN are part of a dynamic of expanding coverage of increasingly selective activities and markets, where the differentiating factors of quality, safety, reliability, suitability and credibility are key to success.

Therefore, ACIN chooses Information Security as a management tool that will support the achievement of its business objectives.

9. Information Security Rationale

The market in which ACIN operates is governed by the national and international legislation applicable to its commercial activity, with regard to the management and security of the information that its customers place under custody on the electronic platforms.

ACIN is determined to systematically follow the evolution of this legal environment and to integrate it into its management systems, as well as to comply with and enforce the requirements and contractual provisions of and for its direct and indirect customers.

10. Information Security Significance

The information that ACIN's customers place under its custody is an indispensable asset for "business survival".

The information security policy of ACIN is a commitment assumed by its Administration to ensure the implementation and continuous improvement of a system for its management, hereinafter referred to as the Information Security Management System (ISMS), ensuring the availability of the necessary resources for its effectiveness and guaranteeing its review, in accordance with the minimum periodicity established.

The ISMS of ACIN will be implemented in accordance with the requirements of ISO/IEC 27001:2013, and its Statement of Applicability will be defined on the basis of the list of controls presented in Annex A of that standard.

11. Information Security Scope of Protection

The scope of protection of the Information Security Management System (ISMS) covers the products and services provided by the application platforms of ACIN, taking into account the exceptions presented in document DS24_ISMS-Definition of the scope of the ISMS.

12. Commitment to Information Security

- ✓ Confidentiality

Guarantee that customer information entrusted to the custody of the electronic platforms of ACIN, within the scope of protection, is only accessed by those who are formally authorised for that purpose.

- ✓ Integrity

Guarantee of protection of the accuracy of the information received, processed, stored and transmitted under the responsibility of ACIN, on its electronic platforms within the scope of protection.

- ✓ Availability

Guarantee that the information processed within the scope of protection is accessible, and when necessary, to carry out a business process activity, within the formally defined service levels, and respecting the commitment to confidentiality and integrity.

- ✓ Data Privacy

Guarantee of the privacy and the trust of its holders and partners, promoting total protection on the privacy and security of personal data.

- ✓ Non-Repudiation

Guarantee that the author does not deny having created and signed the document.

- ✓ Authenticity

Guarantee of the validity of the transmission, the message and its sender. The objective is that the recipient can confirm the origin and authorship of a given document.

13. Risk Management

In order to ensure readiness and compliance of its ISMS, ACIN is committed to identifying, analysing, qualifying and treating risks arising from various sources of threats.

All information security risks are properly assessed and documented at scheduled intervals.

ACIN's risk management policy defines the methodology adopted to treat the risks identified, being based on the best practices defined by international reference standards, and constitutes a management tool of the company.

14. Incident Management and Business Continuity Management

All events that may jeopardise information security commitments will be treated as possible security incidents and, as such, included in the incident management procedures of ACIN.

The respective diagnosis of causes, consequences, control measures and mitigation of the resulting risk will be treated according to the best practices, with the activation of disciplinary processes and legal actions foreseen for matters revealing fraud or violation of responsibilities assumed by third parties.

The availability of information, without neglecting the responsibility of the other information security commitments, will be ensured by the implementation of responses to disruptive incidents and that fall within the scope of the Business Continuity Plan of ACIN.

15. Supplementary Policies

Whenever deemed relevant to the effectiveness of the ISMS, ACIN will define thematic policies that describe the practices implemented in various matters within the scope of protection, as well as the implementation of controls arising from the need to treat risk.

These thematic policies will be approved by the ISMS leadership, by proposal of its coordinator.

16. Integration with other Management Systems

ACIN ensures that the ISMS will always be the management system that ensures the treatment of issues related to Information Security, regardless of the management systems implemented while maintaining an integrated management system approach.

As a result of the current implementation of the ISO/IEC 20000-1:2011 Management System, ACIN undertakes to align the interests and scopes of both systems, with a view to a future integrated system.

17. Training and Awareness-raising

Raising awareness, training and systematic training of the employees of ACIN on information security matters is a strong commitment arising from the commitment of the company for the effectiveness of the ISMS.

These initiatives are included in an annual Training Plan that will be audited on the effectiveness of its execution.

18. Disclosure and Publication

The disclosure of the formalisation of the decisions taken by the ISMS Leadership is ensured through a process of internal communication.

The internal publication of documents relevant to the implementation of information security is considered essential for the employees of the company to feel co-responsible, comply and ensure compliance with the determinations of the ISMS, and support training actions included in the annual Training Plan.

The involvement of subcontracting entities providing services results in ACIN integrating the respective employees in actions considered to be relevant, to which we should add the commitment to promote the disclosure of policies and practices with these entities, based on duly formalized agreements for that purpose.

19. Commitment to Continuous Review and Improvement

The Leadership of ACIN is committed to ensure the management review of the Information Security Management System (ISMS) at planned intervals, or whenever significant changes occur in the company, in order to ensure its adequacy and effectiveness, certifying in this act the evidence of commitment to the continuous improvement of the ISMS.

20. Roles and Responsibilities

Aware of the importance of ensuring the implementation, operability, review and continuous improvement of the ISMS, the management of ACIN has appointed one of its members to assume the Leadership of this system.

With the respective duties and responsibilities described in the *ACIN Roles and Responsibilities Manual*, the Leadership appoints an employee responsible for coordinating the ISMS.

21. Organisation Context

The following external and internal aspects that ACIN considers relevant for achieving the expected results and objectives have been identified and are presented in document DS24-Definition of the scope of the ISMS.