INFORMATION SECURITY POLICY

uanataca

trust service provider

General Information

Documental Control

Security Classification:	**Public**
Version:	**1.4**
Edition date:	**02/02/2023**
File:	**POL-1-Information Security Policy _EN_v1.4**
Code:	**POL-1-**

Formal Status

Prepared by:	**Reviewed by:**	**Approved by**
Name: Alejandro Grande Date : 02/02/2023	Name: Donald David Márquez Date: 02/02/2023	Name: Gabriel García Date: 03/02/2023

Versions Control

Version	Changes	Description of Change	Author of change	Date of change
1.0	Original	Document Creation	Albert Borrás	25/10/2018
1.1	No changes	Annual Review	Albert Borrás	19/09/2019
1.2	1	Annual Review Wording Review	Alejandro Grande	26/11/2020
1.3	No changes	Annual Review	Aylen Mondillo	15/12/2021
1.4	No changes	Annual Review	Alejandro Grande	02/02/2023

Index

Information Security Policy

1. Introduction

This document contains the Information Security Policy (hereinafter PSI) of Uanataca, S.A., hereinafter UANATACA, in accordance with the Information Security Management System (hereinafter ISMS), which it implements in its activities related to the provision of certification services.

It complies with the requirements of a Qualified Trust Service Provider, which UANATACA accredited in accordance with the regulations applicable before the Spanish National Supervisor.

This document is the result of the compendium of documents related to the processes that guarantee the information security of the Trusted Service Provider's processes.

2. Information Security Policy

UANATACA's management recognizes the importance of identifying and protecting its information assets, and especially those of its customers, avoiding the loss, disclosure, modification and unauthorized use of all its information, committing itself to develop, implement, maintain and continuously improve the Information Security Management System (ISMS).

It is the responsibility of the Management of UANATACA:

1. To periodically establish objectives on Information Security management, and the necessary actions for its development.
2. Establish a systematic risk analysis, assessing impact and threats.

3. Implement the necessary actions to reduce the identified risks that are considered unacceptable, according to the criteria established by the Safety Committee.
4. Apply the necessary controls and their corresponding monitoring methods.
5. Comply with the requirements assumed by UANATACA, legal, regulatory, customer and contractual security obligations.
6. Promote information security awareness and training for all UANATACA personnel.
7. Provide the necessary resources to guarantee the continuity of the company's business.

Information Security is characterized as the preservation of:

a) its availability, ensuring that authorized users have access to information and its associated assets when required.
b) its confidentiality, ensuring that only those authorized can access the information;
c) its integrity, ensuring that the information remains unchanged and traceable.

The management of UANATACA appoints the Information Security Manager as directly responsible for the maintenance of the information security policy, for providing advice and guidance for its implementation.

3. Information Security Objectives

The information security objectives are defined by the Information Security Committee at regular meetings, on the basis of documentation and records provided by the ISMS, which will be approved by the Strategic Committee or by the Management.

Goals and objectives will be in accordance with UANATACA Policy and context analysis.

The safety objectives are grouped around the following working blocks:

- Protection of knowledge, information and data
- Protection of information and communication technologies.
- Protection of installations, buildings and rooms.
- Protection of the company's assets.
- Protection of business continuity.
- Compliance with legal and regulatory standards.

This documentation (which includes non-conformities, corrective and preventive actions, internal audits, training records, etc.) must serve as a reference for establishing measurable and quantifiable objectives aimed at the continuous improvement of the service.

The objectives are included in the tool that supports the information security management system.

4. Security Policy Administration

This Security Policy is administered by UANATACA in its capacity as a Trust Service Provider in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. It also complies with the requirements of the Information Security Management System implemented by UANATACA.

Modifications to this document and their corresponding approvals are made through the Document Management procedure and if necessary, according to the provisions of the UANATACA Change Management Policy, considering the roles and responsibilities foreseen in the decision-making process. Similarly, responsibilities for the implementation of the security policy are assigned through the aforementioned procedure.

5. Scope and application

This security policy will apply to the execution of activities related to UANATACA's trust and certification services, i.e. Management of the life cycle of electronic certificates (issuance, validation, maintenance and revocation). Time stamping. Centralized certificate custody service and remote signature service. Consequently, this policy will be compulsory for all UANATACA personnel, and also for any third party that intervenes or participates in the execution of activities related to the provision of such services.

6. Communication

This Security Policy will be notified to all employees, third parties and interested parties involved in the execution of activities related to the provision of trust and certification services. To the extent applicable, it will be included in the training plans of staff and related third parties.