INFORMATION SECURITY AND BUSINESS CONTINUITY POLICY

General information

Document control

Security Classification:	**Public**
Version:	**2.1**
Edition date:	**06705/2025**
File:	**POL-1-Política_Seguridad_Información_y_Continuidad_Negocio_v2.1_EN.docx_EN**
Code:	**POL-1-**

Formal state

Prepared by:	**Reviewed by:**	**Approved by:**
Name: JGM Date: 30/04/2025	Name: AGB Date: 06/05/2025	Name: GGM Date: 06/05/2025

Version control

Version	Parts that change	Description changes	Author change	Date of change
1.0	Original	Creating the document	ABD	10/25/2018
1.1	No changes	Annual review	ABD	09/19/2019
1.2	1	Annual Review Review of document terminology	AGB	11/26/2020
1.3	No changes	Annual review	ANM	12/15/2021
1.4	No changes	Annual review	AGB	02/02/2023
1.5	No changes	Annual review	AGB	09/02/2024
2.0	Changes throughout the document	Security policy is adapted to take into account business continuity	JGM	08/01/2025
2.1	2	The wording of this policy is improved to bring it more in line with the ENS.	JGM	30/04/2025

Index

Information Security Policy and Business Continuity

1. Introduction

This document contains the Information Security and Business Continuity Policy (hereinafter ISBCP) of Uanataca, SAU, hereinafter UANATACA, in accordance with the Information Security Management System (hereinafter ISMS), and the Business Continuity Management System (hereinafter BCMS), which it implements in its activities related to the provision of certification services.

It meets the requirements of a Qualified Trust Service Provider, certified by UANATACA as certified in accordance with the applicable regulations with the Spanish supervisory body.

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

2. Information Security Policy

UANATACA is aware of the need to protect the services it provides and the information it keeps, as well as its commitment to maintaining, through principles of risk management, quality, sustainability and continuous improvement, an environment of maximum security and legal guarantee.

UANATACA's Management recognizes the importance of identifying and protecting its information assets, as well as their associated risks, and especially those of its clients, avoiding the loss, disclosure, modification and unauthorized use of all its information, committing to develop, implement, maintain and continually improve the ISMS and the BCMS.

It is the responsibility of the UANATACA Management:

1. Accept as assets of the organization, the different UANATACA application services such as certificate issuance services, time stamping, remote identification, electronic signature, certified mail, and custody, including the information received from interested parties, the evidence generated, as well as the systems and networks that support it.
2. Periodically establish objectives regarding information security management and business continuity, and the actions necessary for their development.
3. Establish a systematic risk analysis, evaluating the impact and threats.
4. Implement the necessary actions to reduce identified risks that are considered unacceptable, according to the criteria established by the Technological Safety and Risk Committee.
5. Apply the necessary controls and their corresponding monitoring methods.
6. Comply with the requirements assumed by UANATACA, legal, regulatory, client and contractual security obligations, as well as meet the expectations of interested parties.
7. Promote awareness and training in information security for all UANATACA staff.
8. Provide the necessary resources to ensure the security of the company's information and business continuity.
9. Manage the risks arising from the processing of personal data.

Information security and business continuity are characterized as the preservation of:

a) availability, ensuring that authorized users have access to information and its associated assets when they require it.

b) Confidentiality, ensuring that only those who are authorized can access the information;

c) integrity, ensuring that information remains unchanged and traceable;

d) authentication, ensuring that only authorised persons have access to information and assets.

e) traceability, ensuring that all security-related events are recorded allowing for follow-up actions that contribute to incident detection and response;

f) legal compliance with all laws, regulations or contracts with our customers that relate to privacy, information security and business continuity.

This information security and business continuity policy shall be further developed in additional documentation indicating the following minimum requirements:

- organisation and implementation of the security process;
- risk analysis and management;
- personnel management;
- professionalism;
- access authorisation and control;
- protection of premises;
- procurement of security products and contracting of security services;
- least privilege;
- system integrity and updating;
- protection of information in storage and in transit;
- prevention of other interconnected information systems;
- logging of activity and detection of malicious code;
- security incidents;
- business continuity;
- continuous improvement of the security process.

The responsibility for management systems will fall on the Technological Security and Risk Committee, with the ultimate responsibility of Management as the highest authority of Uanataca.

Additionally, the Security and Technological Risks Committee will act as the party directly responsible for:

- Maintaining the information security and business continuity policy, by providing advice and guidance for its implementation;
- define security roles and functions, defining for each, their duties and responsibilities, as well as the procedure for their appointment and renewal;
- ensure the resources necessary to make the management system available;
- categorise, on the basis of a principle of proportionality, the balance between the importance of the information it handles and the services it provides and the security effort required.

3. Information Security Objectives

The goals and objectives will be in accordance with UANATACA's policy and the analysis of the context. The security and business continuity objectives are grouped around the following work blocks, continuously improving the degree of effectiveness of the controls implemented to support adaptation to the constant evolution of risk and the technological environment.

- Establish security as an integral process consisting of all human, material, technical, legal and organizational elements related to the information system.
- Establish a continuous and updated process of analysis and risk management.
- Protection of knowledge, information and data.
- Protection of information and communications technologies.
- Protection of facilities, buildings and rooms.
- Protection of company assets against internal and external threats, deliberate or accidental, following principles of confidentiality, integrity and availability.
- Protecting business continuity by preventing, responding to and recovering from unwanted security events.
- Compliance with legal and regulatory standards, compliance with any other business, sector or contractual requirements that affect security.
- Generating a work environment where the different UANATACA actors are aware, recognized and involved with these objectives, through communication of the policy and its understanding.

4. Security Policy Administration

This information security and business continuity policy is administered by UANATACA in its capacity as a Trusted Electronic Service Provider in accordance with the provisions of Regulation 910/2014 of July 23, 2014 regarding electronic identification and trust services for electronic transactions in the internal market.

This document will be kept up to date and will be reviewed whenever relevant changes occur in the information or organization of this document. The content will always be in accordance with the current legislative provisions on security, with UANATACA acting appropriately in accordance with the applicable legislation.

5. On the scope and area of application

This information security and business continuity 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.

Likewise, the management of UANATACA has established the functions and responsibilities necessary to comply with and enforce this policy at all times, placing special emphasis on the procedures and security measures to be adopted by those professionals who have access to the service platforms, sensitive business data and personal data. Consequently, this policy shall be mandatory for all UANATACA personnel, and also for any third party involved or participating in the execution of activities related to the provision of said services.

6. Communication

This 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.