POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DEL NEGOCIO

Información general

Control documental

Clasificación de seguridad:	**Público**
Versión:	**2.1**
Fecha edición:	**06/05/2025**
Fichero:	**POL-1-Política_Seguridad_Información_y_Continuidad_Negocio_v2.1_ES.docx**
Código:	**POL-1-**

Estado formal

Preparado por:	**Revisado por:**	**Aprobado por:**
Nombre: JGM Fecha: 25/04/2025	Nombre: AGB Fecha: 06/05/2025	Nombre: GGM Fecha: 06/05/2025

Control de versiones

Versión	Partes que cambian	Descripción cambio	Autor cambio	Fecha cambio
1.0	Original	Creación del documento	ABD	25/10/2018
1.1	Sin cambios	Revisión anual	ABD	19/09/2019
1.2	1	Revisión Anual Revisión de terminología del documento	AGB	26/11/2020
1.3	Sin cambios	Revisión anual	ANM	15/12/2021
1.4	Sin cambios	Revisión anual	AGB	02/02/2023
1.5	Sin cambios	Revisión anual	AGB	09/02/2024
2.0	Cambios en todo el documento	Se adapta la política de seguridad para que tenga en cuenta la continuidad del negocio	JGM	08/01/2025
2.1	2	Se mejora la redacción de esta política para que se adecué mejor a lo indicado en el ENS	JGM	25/04/2025

Índice

Política de Seguridad de la Información y continuidad del negocio

1. Introducción

Este documento contiene la Política de Seguridad de la Información y Continuidad del Negocio (en lo sucesivo PSICN) de Uanataca, S.A.U., en lo sucesivo UANATACA, de acuerdo con el Sistema de Gestión de la Seguridad de la Información (en adelante SGSI), y el Sistema de Gestión de Continuidad del Negocio (en adelante SGCN), la cual implementa en sus actividades relacionadas a la prestación de servicios de certificación.

La misma cumple con los requisitos propios de un Prestador de Servicios de Confianza Cualificado, constado UANATACA acreditada de acuerdo con la regulación aplicable ante el Organismo de supervisión español.

Este documento es el resultado del compendio de documentos relativos a los procesos que garantizan la seguridad de la información de los procesos del Prestador de Servicios de Confianza.

2. Política de seguridad de la información

UANATACA es consciente de la necesidad de la protección de los servicios que presta y de la información que custodia, así como del compromiso de mantener, mediante principios de gestión del riesgo, calidad, sostenibilidad y mejora continua, un entorno de máxima seguridad y garantía jurídica.

La Dirección de UANATACA reconoce la importancia de identificar y proteger sus activos de información, así como sus riesgos asociados, y en especial los de los clientes, evitando la pérdida, la divulgación, modificación y utilización no autorizada de toda su información,

comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el SGSI y el SGCN.

Es responsabilidad de la Dirección de UANATACA:

1. Aceptar como activos de la organización, los diferentes servicios de aplicaciones de UANATACA como los servicios de emisión de certificados, sellado de tiempo, identificación remota, firma electrónica, correo certificado, y custodia, incluyendo la información recibida de las partes interesadas, las evidencias generadas, así como los sistemas y redes que la soportan.
2. Establecer periódicamente objetivos sobre la gestión de la seguridad de la información y la continuidad del negocio, y las acciones necesarias para su desarrollo.
3. Establecer la sistemática de análisis del riesgo, evaluando el impacto y las amenazas.
4. Implementar las acciones necesarias para reducir los riesgos identificados que se consideren inaceptables, según los criterios establecidos por el Comité de Seguridad y Riesgos Tecnológicos.
5. Aplicar los controles necesarios y sus correspondientes métodos de seguimiento.
6. Cumplir con los requisitos asumidos por UANATACA, legales, reglamentarios, de cliente y las obligaciones contractuales de seguridad, así como cumplir con las expectativas de las partes interesadas.
7. Promover la concientización y formación en materia de seguridad de la información a todo el personal de UANATACA.
8. Aportar los recursos necesarios para garantizar la seguridad de la información y la continuidad del negocio de la empresa.
9. Gestionar los riesgos que se derivan de tratamiento de datos personales.

La seguridad de la información y la continuidad del negocio se caracterizan como la preservación de:

a) la disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

b) la confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información;

c) la integridad, asegurando que la información se mantiene invariable y trazable;

d) la autenticación, asegurando que solo las personas autorizadas tengan acceso a la información y a los diferentes activos.

e) la trazabilidad, asegurando que se registran todos los eventos relacionados con la seguridad permitiendo el seguimiento de acciones que contribuyan a la detección y respuesta de incidentes;

f) el cumplimiento legal de todas las leyes, regulaciones o contratos con nuestros clientes que están relacionados con la privacidad, y la seguridad de la información y continuidad del negocio.

Esta política de seguridad de la información y continuidad del negocio se desarrollará en documentación adicional donde se indiquen los siguientes requisitos mínimos:

- organización e implantación del proceso de seguridad;
- análisis y gestión de los riesgos;
- gestión de personal;
- profesionalidad;
- autorización y control de los accesos;
- protección de las instalaciones;
- adquisición de productos de seguridad y contratación de servicios de seguridad;
- mínimo privilegio;
- integridad y actualización del sistema;

- protección de la información almacenada y en tránsito;
- prevención ante otros sistemas de información interconectados;
- registro de la actividad y detección de código dañino;
- incidentes de seguridad;
- continuidad de la actividad;
- mejora continua del proceso de seguridad.

La responsabilidad de los sistemas de gestión recaerá sobre el Comité de Seguridad y Riesgos Tecnológicos, siendo responsabilidad última de la Dirección como máximo responsable de Uanataca.

Adicionalmente, el Comité de Seguridad y Riesgos Tecnológicos, actuará como responsable directo:

- en el mantenimiento de la política de seguridad de la información y de continuidad del negocio, por brindar consejo y guía para su implementación;
- definirá los roles y funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación;
- asegurará los recursos necesarios para que el sistema de gestión esté disponible;
- categorizará, en base a un principio de proporcionalidad, el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido.

3. Objetivos de la seguridad de la información

Las metas y objetivos estarán de acuerdo con la política de UANATACA y el análisis del contexto. Los objetivos de seguridad y de continuidad del negocio se agrupan entorno a los siguientes bloques de trabajo, mejorando de forma continua el grado de eficacia de los controles implantados para soportar una adaptación a la constante evolución del riesgo y del entorno tecnológico.

- Establecer la seguridad como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información.
- Establecer un proceso continuo y actualizado de análisis y la gestión de los riesgos.
- Protección del conocimiento, la información y los datos.
- Protección de las tecnologías de la información y las comunicaciones.
- Protección de las instalaciones, edificios y estancias.
- Protección de los activos de la compañía, frente a amenazas internas y externas, deliberadas o accidentales, siguiendo principios de confidencialidad, integridad y disponibilidad.
- Protección de la continuidad del negocio, mediante la prevención, reacción y recuperación ante eventos no deseados de seguridad.
- Cumplimiento con los estándares legales y normativos, el cumplimiento de cualquier otro requisito de negocio, sectorial o contractual, que afecten a la seguridad.
- Generando un ambiente de trabajo donde se conciencie, reconozca y se implique a los diferentes actores de UANATACA con estos objetivos, a través de la comunicación de la política y su entendimiento.

4. Administración de la Política de Seguridad

La presente política de seguridad de la información y continuidad del negocio es administrada por UANATACA en su condición de Prestador de Servicios Electrónicos de Confianza de acuerdo con las previsiones del Reglamento 910/2014 del 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Este documento se mantendrá actualizado y será revisado siempre que se produzcan cambios relevantes en la información u organización de este. El contenido se adecuará en todo momento a las disposiciones legislativas vigentes en materia de seguridad, actuando UANATACA adecuadamente conforme a la legislación aplicable.

5. Del alcance y ámbito de aplicación

Esta política de seguridad de la información y continuidad del negocio se aplicará a la ejecución de las actividades relacionadas con los servicios de confianza y de certificación de UANATACA, esto es gestión del ciclo de vida de los certificados electrónicos (emisión, validación, mantenimiento y revocación). Sellado de tiempo. Servicio de custodia centralizada de certificados y servicio de firma remota.

Así mismo la dirección de UANATACA ha establecido las funciones y responsabilidades necesarias para cumplir y hacer cumplir en todo momento esta política, haciendo especial énfasis en los procedimientos y medidas de seguridad a adoptar por aquellos profesionales que tienen acceso a las plataformas de servicios, a datos sensibles de negocio y a datos de carácter personal. En consecuencia, la presente política será de cumplimiento obligatorio para todo el personal de UANATACA, y también para cualquier tercero que intervenga o participe en la ejecución de las actividades relacionadas con la prestación de dichos servicios.

6. Comunicación

La presente política será notificada a todos los empleados, terceros y partes interesadas que participen en la ejecución de actividades relacionadas con la prestación de los servicios de confianza y de certificación. En la medida en que sea aplicable, será incluida dentro de los planes de formación del personal y terceros vinculados.