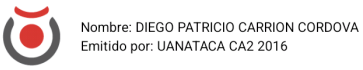
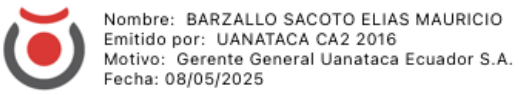
# UANATACA ECUADOR S. A.

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

| | |
|---|---|
| Código: | GES-PO-01 |
| Versión: | 0.2 |
| Fecha de la versión: | 2025-05-01 |
| Creado por: | Equipo de Seguridad de la Información<br>  |
| Revisado y aprobado por: | Gerente General<br>  |
| Nivel de confidencialidad: | Uso Interno |

## Historial de modificaciones

| Fecha | Versión | Creado por | Descripción de la modificación |
|---|---|---|---|
| 2023.09.08 | 0.1 | Consultora Road Quality - Equipo de proyecto SGSI | Descripción básica del documento |
| 2024.09.09 | 0.2 | Equipo de Proyecto | No hay modificaciones |
| 2025.05.01 | 0.2 | Comité de Seguridad de la Información | Se actualiza la política de seguridad de la información |
| | | | |
| | | | |
| | | | |
| | | | |

## Tabla de contenido

**1. Objetivo, alcance y usuarios 3**

**2. Documentos de referencia 3**

**3. Terminología básica sobre seguridad de la información 3**

**4. Gestión de la seguridad de la información 3**

4.1. Objetivos y medición 3
4.2. Requisitos para la seguridad de la información 4
4.3. Controles de seguridad de la información 4
4.4. Continuidad de negocio 4
4.5. Responsabilidades 4
4.6. Comunicación de la Política 5

**5. Apoyo para la implementación del SGSI 5**

**6. Validez y gestión de documentos 5**

## 1. Objetivo, alcance y usuarios

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

Esta Política se aplica a todo el Sistema de Gestión de Seguridad de la Información (SGSI), según se define en el Documento sobre el alcance del SGSI.

Los usuarios de este documento son todos los Colaborador de UANATACA ECUADOR S.A, como también terceros externos a la organización.

## 2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas 5.2, 5.3, 6.2, 7.4 y A.6.3
- Documento sobre el alcance del SGSI
- Manual de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Lista de requisitos legales, normativos, contractuales y de otra índole

## 3. Terminología básica sobre seguridad de la información

**Confidencialidad**: característica de la información por la cual solo está disponible para personas o sistemas autorizados.

**Integridad**: característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida.

**Disponibilidad**: característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.

**Seguridad de la información**: es la preservación de la confidencialidad, integridad y disponibilidad de la información.

**Sistema de gestión de seguridad de la información**: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

# 4. Gestión de la seguridad de la información

## 4.1. Política de Seguridad de la Información

La política de Uanataca Ecuador es la siguiente:

UANATACA es una Entidad de Certificación de Información y Servicios Relacionados para firma electrónica, comprometida con la protección de la información, garantizando la confidencialidad, integridad y disponibilidad de sus servicios.

Este compromiso se refleja en la creación de un entorno digital seguro y confiable para nuestros clientes y demás partes interesadas, asegurando la protección de la identidad digital y el tratamiento responsable de los datos. Cumplimos con todos los requisitos legales, regulatorios y contractuales aplicables, así como con las exigencias del ecosistema normativo al que pertenecemos.

Fomentamos una cultura de mejora continua orientada a optimizar nuestros procesos y fortalecer de forma permanente los controles de seguridad de la información, garantizando la eficacia del sistema y su resiliencia frente a posibles riesgos.

## 4.2. Objetivos y medición

Los objetivos generales alineados a la Política para el sistema de gestión de seguridad de la información son los siguientes:

- Fomentar mayor seguridad en el ambiente informático minimizando los riesgos que atenten contra la confidencialidad, integridad y disponibilidad de la información.
- Promover un ambiente de confianza del cliente y partes interesadas mediante la protección de la identidad, confidencialidad e integridad de los datos.
- Cumplir a cabalidad los requisitos legales y el ecosistema al cual pertenecemos que aplique a la organización relacionada con seguridad de la información.
- Generar estrategias de mejora continua para implementar en los procesos y controles del sistema de gestión a fin de optimizar la seguridad de la información.
- Desarrollar un plan de capacitación para nuestros colaboradores en temas de seguridad de la información para mantener personal idóneo.

El Comité de Seguridad de la Información es el responsable de revisar estos objetivos generales del SGSI y de establecer nuevos.

Los objetivos para controles individuales de seguridad o grupos de controles son propuestos por los líderes de los procesos y son aprobados por el Comité en la Declaración de aplicabilidad.

Todos los objetivos deben ser revisados en la revisión por la Dirección.

Uanataca medirá el cumplimiento de todos los objetivos. El Compliance officer es el responsable de definir el método para medir el cumplimiento de los objetivos; la medición se realizará al menos al menos una vez al año y analizará y evaluará los resultados y los reportará a Gerencia General, como material para la revisión por la dirección. El Compliance officer es responsable de registrar los detalles sobre los métodos de medición, periodicidades y resultados en el Informe de medición.

### 4.3. Requisitos para la seguridad de la información

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información, como también con las obligaciones contractuales.

En la ***Lista de requisitos de partes interesadas, legales, normativos, contractuales y de otra índole*** se detalla una lista de requisitos contractuales y legales.

### 4.4. Controles de seguridad de la información

El proceso de escoger los controles (protección) está definido en el Manual ***de evaluación y tratamiento de riesgos.***

Los controles seleccionados y su estado de implementación se detallan en la ***Declaración de aplicabilidad.***

### 4.5. Continuidad de negocio

La gestión de la continuidad de negocio está reglamentada en la ***Política de continuidad de negocio.***

### 4.6. Responsabilidades

Las responsabilidades para el SGSI son las siguientes:

- El Compliance officer es el responsable de garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política y de garantizar que todos los recursos necesarios estén disponibles.
- El Compliance officer, es el responsable de la coordinación operativa del SGSI, como también de informar su desempeño.

- La Gerencia General debe revisar el SGSI al menos una vez por año o cada vez que se produzca una modificación significativa; y debe elaborar actas de dichas reuniones. El objetivo de las verificaciones por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGSI.
- El Área de TI implementará programas de formación y concienciación de empleados sobre seguridad de la información.
- La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.
- Todos los incidentes o debilidades de seguridad deben ser informados al Compliance officer.
- El Compliance officer definirá qué información relacionada con la seguridad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo.
- El Compliance officer, en conjunto con el proceso de Talento Humano, es el responsable de adoptar e implementar el Plan de formación y concienciación, que corresponde a todas las personas que cumplen un rol en la gestión de la seguridad de la información.

La alta dirección se encargará de invertir en recursos y estrategias para llegar cumplir los compromisos establecidos en esta política y los requisitos del sistema.

### 4.7. Comunicación de la Política

El Coordinador de Talento Humano debe asegurarse de que todos los empleados de Uanataca, como también los participantes externos correspondientes, estén familiarizados con esta Política.

## 5. Apoyo para la implementación del SGSI

A través del presente, la Gerencia General declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

## 6. Validez y gestión de documentos

Este documento es válido hasta un año.

El propietario de este documento es el Compliance officer que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de empleados y participantes externos que cumplen un rol en el SGSI pero que no están familiarizados con el presente documento.
- No cumplimiento del SGSI con las leyes y normas, las obligaciones contractuales y con los demás documentos internos de la organización.
- Ineficacia de la implementación y mantenimiento del SGSI.
- Responsabilidades ambiguas para la implementación del SGSI.