UNIVERSIDAD NACIONAL DE CHIMBORAZO

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SGSI

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Riobamba, Abril de 2026

# CONTENIDO


1. ANTECEDENTES ..... 3
2.OBJETIVO DE LA POLÍTICA ..... 4
3.POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ..... 5
3.1.DESCRIPCIÓN DE LA POLÍTICA ..... 5
3.2.DECLARACIÓN DE LOS OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN ..... 5
3.3.ROLES Y RESPONSABILIDADES ..... 6
3.4.ALCANCE Y USUARIOS ..... 8
3.4.1.ALCANCE ..... 8
3.4.2.USUARIOS ..... 8
3.5.COMUNICACIÓN DE LA POLÍTICA ..... 8
3.6.EXCEPCIONES Y SANCIONES ..... 9
3.6.1.EXCEPCIONES ..... 9
3.6.2.SANCIONES ..... 10
4.GLOSARIO DE TÉRMINOS ..... 10
5.DOCUMENTOS DE REFERENCIA ..... 11
6.CONTROL DE VERSIONES ..... 12
7.LEGALIZACIÓN ..... 12

## 1. ANTECEDENTES

La Universidad Nacional de Chimborazo (UNACH), en cumplimiento de su misión institucional y de las disposiciones legales aplicables al sector público ecuatoriano, reconoce que la información constituye un activo estratégico fundamental para el desarrollo de todos sus procesos institucionales, incluyendo los procesos gobernantes, los procesos sustantivos de docencia, investigación y vinculación con la sociedad, así como los procesos de apoyo y aquellos de carácter transversal que articulan la gestión institucional en su conjunto.

El uso intensivo de tecnologías de la información, la digitalización de procesos y el tratamiento de información académica, administrativa, científica y de datos personales de la comunidad universitaria exponen a la institución a riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información. Estos riesgos pueden incidir directamente en la continuidad operativa, la prestación de los servicios institucionales y la confianza de la comunidad universitaria.

En este contexto, la seguridad de la información se alinea con el direccionamiento estratégico definido en el Plan Estratégico Institucional 2022–2026, constituyéndose en un habilitador transversal para el cumplimiento de los objetivos institucionales.

En el ámbito de la docencia, el Objetivo Estratégico Nro. 1 orientado a mejorar la calidad de la formación profesional implica la gestión continua de información académica, como calificaciones, evaluaciones, contenidos educativos, plataformas virtuales de aprendizaje, sistemas institucionales de gestión académica, entre otros. La implementación del Sistema de Gestión de Seguridad de la Información (SGSI) permitirá proteger dicha información, garantizando que se mantenga confidencial, íntegra y disponible cuando se la requiera, asegurando su adecuado uso dentro de los procesos institucionales y fortaleciendo la confiabilidad en la gestión académica.

En el ámbito de la investigación, el Objetivo Estratégico Nro. 2 implica la generación y gestión de información científica de alto valor institucional. En este sentido, el SGSI contribuirá a proteger dicha información mediante la implementación de controles orientados a prevenir la alteración no autorizada, la pérdida de información, la divulgación indebida y los riesgos asociados a la gestión del conocimiento y la propiedad intelectual.

En el ámbito de la vinculación con la sociedad, el Objetivo Estratégico Nro. 3 contempla la interacción e intercambio de información con diversos actores internos y externos. En este contexto, el SGSI permitirá que estos flujos de información se gestionen de manera segura y controlada, reduciendo riesgos relacionados con accesos no autorizados, uso indebido de la información y exposición de información sensible.

En el ámbito de las condiciones institucionales, el Objetivo Estratégico Nro. 4 resalta la necesidad de contar con infraestructura tecnológica segura y servicios confiables. En este marco, el SGSI permitirá gestionar de manera estructurada los riesgos que pueden afectar la información, los sistemas y los servicios institucionales, mediante la implementación de controles que contribuyan a garantizar la continuidad de las operaciones y la protección de los activos de información críticos.

Bajo esta perspectiva, la seguridad de la información se configura como un habilitador estratégico transversal que permite proteger los activos de información institucionales, asegurar la continuidad de los servicios y fortalecer la confianza de la comunidad universitaria y de las demás partes interesadas.

En coherencia con este enfoque, la seguridad de la información se integra también con la Política de Aseguramiento de la Calidad, en particular con el principio 5.11 Seguridad y protección de datos, el cual

establece que: "*Crea un ambiente donde todas las partes interesadas pueden interactuar con plena confianza en que mantienen control sobre el uso de sus datos, y que la institución tratará sus datos con cuidado y confidencialidad adecuados*". En este sentido, la implementación del SGSI contribuye a garantizar un tratamiento seguro, responsable y confiable de la información institucional.

La seguridad de la información se gestiona mediante un enfoque sistemático basado en riesgos, que incorpora controles organizativos, de personas, físicos y tecnológicos, así como mecanismos orientados a asegurar la continuidad de los servicios y la protección de los activos de información. Este enfoque fortalece la confianza institucional, la confiabilidad de la información y el cumplimiento de los objetivos estratégicos.

En cumplimiento del Acuerdo Nro. MINTEL-MINTEL-2024-0003, mediante el cual se expide el Esquema Gubernamental de Seguridad de la Información (EGSI v3.0), la UNACH establece la presente Política de Seguridad de la Información como un instrumento de alto nivel orientado a definir el marco general, los principios, la dirección estratégica y las reglas básicas para la gestión de la seguridad de la información.

La ausencia de una política formal o su falta de actualización puede incrementar la exposición a riesgos en los distintos ámbitos de la gestión universitaria, así como generar posibles incumplimientos de obligaciones normativas, en un entorno donde la información constituye un recurso esencial para la operación institucional.

Finalmente, la presente política refleja el compromiso expreso de la Máxima Autoridad con la implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información, garantizando la protección de los activos de información de la institución y la adecuada gestión de los riesgos que puedan afectarlos, con el fin de asegurar la continuidad y confiabilidad de los procesos universitarios.

## 2. OBJETIVO DE LA POLÍTICA

El objetivo de la presente Política de Seguridad de la Información es establecer el marco institucional que oriente la gestión integral de la seguridad de la información en la UNACH, definiendo los principios, lineamientos y compromisos que garanticen la protección adecuada de todos los activos de información institucionales.

Esta política tiene como finalidad asegurar que la información, en cualquiera de sus formatos o medios, sea gestionada de manera segura durante todo su ciclo de vida, garantizando en todo momento su confidencialidad, integridad y disponibilidad, así como el cumplimiento de los requisitos legales, normativos y contractuales aplicables, en especial los relacionados con la protección de datos personales.

Asimismo, la presente política establece la dirección estratégica para la implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información, conforme a los lineamientos del Esquema Gubernamental de Seguridad de la Información y la norma ISO/IEC 27001:2022, alineándose con la Política de Aseguramiento de la Calidad y los objetivos estratégicos definidos en el Plan Estratégico Institucional de la UNACH.

A través de esta política, la UNACH busca prevenir, reducir y gestionar los riesgos que puedan afectar los activos de información de la institución, fortalecer la cultura organizacional en seguridad de la información, promover el uso responsable de los recursos tecnológicos y asegurar la continuidad de los procesos gobernantes (estratégicos y de dirección), sustantivos (docencia, investigación y vinculación), habilitantes de apoyo y asesoría, y transversales que articulan la gestión institucional en su conjunto, generando confianza en la comunidad universitaria y en las demás partes interesadas.

## 3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

### 3.1. DESCRIPCIÓN DE LA POLÍTICA

La UNACH a través de su Rectorado y de los órganos de gobernanza establecidos para la seguridad de la información, reconoce que la información constituye un activo estratégico esencial para el cumplimiento de sus funciones académicas, administrativas, de investigación y de vinculación con la sociedad.

En este contexto, la presente Política de Seguridad de la Información establece el marco general que guía la gestión de la seguridad de la información en la UNACH, definiendo los principios, directrices y reglas básicas que deben ser observadas por todos los estudiantes, docentes, servidores, trabajadores, proveedores y terceros que accedan, utilicen, administren o procesen información institucional.

***La Universidad Nacional de Chimborazo se compromete a proteger sus activos de información institucionales y los datos personales que trata en el ejercicio de sus funciones. Para ello, implementa, mantiene y mejora de manera continua su Sistema de Gestión de Seguridad de la Información (SGSI), conforme al Esquema Gubernamental de Seguridad de la Información (EGSI v3.0), a la Norma ISO/IEC 27001:2022 y a la Ley Orgánica de Protección de Datos Personales, integrando la seguridad de la información en los procesos institucionales y en la toma de decisiones estratégicas.***

***La protección de los activos de información institucional se basa en un enfoque de gestión de riesgos que permite identificar, analizar, evaluar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad, con el fin de reducir el impacto de eventos adversos y mantener niveles de riesgo aceptables para la institución.***

Asimismo, esta política promueve el fortalecimiento de una cultura organizacional de seguridad de la información, basada en la responsabilidad individual y colectiva, el cumplimiento normativo, la concienciación permanente y la adopción de buenas prácticas, contribuyendo a la confianza de la comunidad universitaria y de las demás partes interesadas.

### 3.2. DECLARACIÓN DE LOS OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

La UNACH establece los siguientes objetivos de seguridad de la información, alineados con el Esquema Gubernamental de Seguridad de la Información (EGSI v3.0) y la norma ISO/IEC 27001:2022, en concordancia con la Política de Aseguramiento de la Calidad y los objetivos estratégicos del Plan Estratégico Institucional.

Estos objetivos constituyen la base para la planificación, implementación, operación y mejora continua del SGSI. Su formulación y gestión se realizará de forma coherente con la presente política, considerando criterios de medición, monitoreo periódico y actualización cuando corresponda, en función de los resultados de la gestión de riesgos y de los cambios en el contexto institucional.

**Objetivo 1: Fortalecer la cultura institucional de seguridad de la información**
Fortalecer la cultura organizacional de la UNACH en materia de seguridad de la información, promoviendo el conocimiento, la concienciación y la adopción de buenas prácticas por parte de de estudiantes, docentes, servidores, trabajadores, proveedores y otras partes interesadas, de manera que la seguridad de la información se incorpore como un comportamiento habitual y transversal en todas las actividades institucionales.

**Objetivo 2: Gestionar de manera sistemática los riesgos de seguridad de la información**
Identificar, analizar, evaluar y tratar los riesgos de seguridad de la información que puedan afectar a los activos de información institucionales, mediante la aplicación de una metodología formal de gestión de riesgos, con el fin de prevenir, reducir o mitigar los impactos negativos sobre su confidencialidad, integridad y disponibilidad.

**Objetivo 3: Proteger los activos de información durante todo su ciclo de vida**
Garantizar la protección adecuada de los activos de información de la UNACH durante todo su ciclo de vida, desde su creación u obtención hasta su eliminación o disposición final, mediante la implementación de controles organizativos, de personas, físicos y tecnológicos, proporcionales al nivel de riesgo identificado.

**Objetivo 4: Gestionar eficazmente los incidentes de seguridad de la información**
Establecer y mantener procesos formales para la detección, reporte, análisis y respuesta de incidentes de seguridad de la información, con el propósito de minimizar su impacto en los procesos académicos y administrativos, asegurar la continuidad de las operaciones institucionales y fortalecer la mejora continua del SGSI.

**Objetivo 5: Asegurar el cumplimiento legal, normativo y contractual**
Garantizar el cumplimiento de los requisitos legales, normativos y contractuales aplicables a la seguridad de la información y a la protección de datos personales, en particular los establecidos en la Ley Orgánica de Protección de Datos Personales y su normativa conexa, la normativa de control interno emitida por la Contraloría General del Estado, el Esquema Gubernamental de Seguridad de la Información (EGSI v3.0), las normas ISO/IEC adoptadas por la institución, así como cualquier otra normativa vigente aplicable.

**Objetivo 6: Impulsar la mejora continua del Sistema de Gestión de Seguridad de la Información**
Promover la mejora continua del SGSI mediante el monitoreo del desempeño, la medición de indicadores, la ejecución de evaluaciones internas, la revisión por la Alta Dirección (Rectorado) y la implementación de acciones correctivas y de mejora, asegurando la eficacia y sostenibilidad del sistema en el tiempo.

### 3.3. ROLES Y RESPONSABILIDADES

Con el fin de garantizar el uso adecuado y la protección efectiva de los activos de información de la UNACH, se establecen los siguientes roles y responsabilidades, los cuales aseguran una gestión clara, coordinada y eficaz de la seguridad de la información en toda la institución.

**Alta Dirección (Rectorado)**
El Rectorado, como encargado del proceso Gestión Estratégica Universitaria, es responsable de:

- Aprobar la Política de Seguridad de la Información y sus actualizaciones.
- Proveer los recursos humanos, técnicos y financieros necesarios para la implementación, operación y mejora continua del SGSI.
- Demostrar liderazgo y compromiso con la seguridad de la información, integrando sus principios en la gestión institucional.
- Garantizar que el SGSI esté alineado con los objetivos estratégicos de la UNACH.

**Comité de Seguridad de la Información, Protección de Datos Personales y Tecnologías de la Información y Comunicaciones**

El Comité es el órgano de gobernanza responsable de:

- Asegurar que la seguridad de la información se gestione de manera adecuada y coherente en toda la institución.
- Supervisar el cumplimiento de la presente política y de los lineamientos del SGSI.
- Revisar los resultados de la gestión de riesgos, evaluaciones internas, auditorías e incidentes de seguridad.
- Proponer y recomendar acciones de mejora al Rectorado.
- Validar excepciones debidamente justificadas a la presente política.

**Oficial de Seguridad de la Información (OSI)**

El Oficial de Seguridad de la Información es responsable de:

- Coordinar la implementación, mantenimiento y mejora continua del SGSI.
- Asesorar al Rectorado y al Comité en temas relacionados con la seguridad de la información.
- Elaborar y mantener actualizada la documentación del SGSI.
- Coordinar la gestión de incidentes de seguridad de la información.
- Elaborar y presentar informes periódicos sobre el estado de la seguridad de la información.
- Promover actividades de capacitación y concienciación en seguridad de la información.

**Dirección de Tecnologías de la Información y Comunicación (DTIC)**

La Dirección de Tecnologías de la Información y Comunicación es responsable de:

- Implementar, operar y mantener los controles tecnológicos de seguridad de la información.
- Proteger la infraestructura tecnológica, redes, sistemas y plataformas institucionales, y demás componentes tecnológicos que soportan los procesos de gestión de tecnologías de la información.
- Gestionar los accesos a los sistemas de información conforme a los principios de mínimo privilegio y necesidad de conocer.
- Apoyar técnicamente la gestión de incidentes de seguridad de la información.

**Dirección de Talento Humano**

La Dirección de Talento Humano es responsable de:

- Incorporar los lineamientos de seguridad de la información en los procesos de vinculación, permanencia y desvinculación del personal.
- Apoyar la ejecución de programas de capacitación, concienciación y sensibilización en seguridad de la información.
- Garantizar que los servidores conozcan y cumplan sus responsabilidades en materia de seguridad de la información.

**Responsables de Unidades Organizativas / Autoridades, Directores, Coordinadores**

Los responsables de las unidades organizativas son responsables de:

- Garantizar que el personal bajo su responsabilidad cumpla la Política de Seguridad de la Información y la normativa relacionada.
- Asegurar la correcta protección de la información generada, procesada o almacenada en su unidad.
- Apoyar los procesos de evaluación de riesgos, auditorías y evaluaciones internas del SGSI.

**Usuarios (Estudiantes, Docentes, Servidores, Trabajadores, Proveedores y Terceros)**

Todos los usuarios que utilicen los activos de información de la UNACH son responsables de:

- Cumplir la presente Política de Seguridad de la Información y la normativa institucional aplicable.

- Proteger la confidencialidad, integridad y disponibilidad de la información a la que tengan acceso.
- Utilizar los activos de información exclusivamente para fines institucionales autorizados.
- Reportar oportunamente cualquier incidente, evento o debilidad de seguridad de la información.

### 3.4. ALCANCE Y USUARIOS

La presente Política de Seguridad de la Información es de aplicación obligatoria en la UNACH y forma parte integral del SGSI, conforme a lo establecido en el Esquema Gubernamental de Seguridad de la Información.

#### 3.4.1.ALCANCE

Esta política aplica a:

- Todos los procesos gobernantes (estratégicos y de dirección), procesos sustantivos o agregadores de valor (docencia, investigación y vinculación), procesos habilitantes de apoyo y asesoría (que brindan soporte a los procesos sustantivos), y procesos transversales que atraviesan tanto los ejes sustantivos como la estructura institucional en su conjunto.
- La información institucional, considerada el activo principal del Sistema de Gestión de Seguridad de la Información.
- Los activos de soporte de la información, incluyendo sistemas de información, aplicaciones, bases de datos, infraestructura física y tecnológica, redes, plataformas tecnológicas, servicios de tecnologías de la información y la comunicación, así como el personal involucrado en su operación, administración y gestión.
- Todas las actividades relacionadas con el ciclo de vida de la información, desde su creación, recepción o recolección, hasta su almacenamiento, uso, transferencia, archivo y eliminación.
- El alcance específico del SGSI se encuentra definido en el Documento de Alcance del Sistema de Gestión de Seguridad de la Información de la UNACH, el cual forma parte de la documentación oficial del SGSI.

#### 3.4.2.USUARIOS

Son usuarios de la presente política, y por tanto están obligados a su cumplimiento:

- El Rectorado y las autoridades universitarias.
- El personal académico y administrativo de la UNACH (docentes, servidores y trabajadores en general).
- Los estudiantes que accedan a los activos de información institucionales.
- Los proveedores, contratistas y terceros, internos o externos, que tengan acceso directo o indirecto a los activos de información de la UNACH.
- Cualquier otra parte interesada que, en el marco de sus funciones, actividades o relaciones contractuales, acceda a los activos de información institucionales.

### 3.5. COMUNICACIÓN DE LA POLÍTICA

La UNACH garantizará que la Política de Seguridad de la Información sea comunicada, difundida y comprendida por todos los usuarios a los que aplica, como parte fundamental del fortalecimiento de la cultura institucional en seguridad de la información y del cumplimiento del Sistema de Gestión de Seguridad de la Información.

La comunicación de la política se realizará a través de los siguientes medios y mecanismos:

- **Publicación oficial** de la Política de Seguridad de la Información en los repositorios y canales institucionales autorizados, tales como, el portal web oficial y gaceta universitaria de la UNACH.

- **Difusión mediante correo electrónico institucional**, dirigido a la comunidad universitaria, informando la aprobación, vigencia y obligatoriedad de la política.

- **Socialización a través de talleres, charlas, inducciones y jornadas de sensibilización**, dirigidas a, funcionarios institucionales y cuando corresponda, a proveedores y terceros.

- **Inclusión de la política en los procesos de inducción y capacitación** para personal de nuevo ingreso, así como en los programas periódicos de concienciación en seguridad de la información.

- **Disponibilidad permanente de la política**, asegurando que los usuarios puedan consultarla de manera oportuna y actualizada.

El Oficial de Seguridad de la Información (OSI), con el apoyo de la Dirección de Tecnologías de la Información y Comunicación, la Dirección de Talento Humano y la Coordinación de Comunicación Institucional, será responsable de coordinar y verificar la adecuada difusión de la presente política, así como de asegurar su comunicación efectiva a todos los niveles de la institución. Para ello, deberá mantener evidencias documentadas que respalden su socialización, comprensión y disponibilidad para las partes interesadas.

La política será comunicada nuevamente cada vez que se realicen actualizaciones relevantes o cambios significativos en su contenido, asegurando que todos los usuarios conozcan y comprendan dichas modificaciones.

### 3.6. EXCEPCIONES Y SANCIONES

La UNACH establece que la presente Política de Seguridad de la Información es de cumplimiento obligatorio para todos los usuarios definidos en su alcance.

#### 3.6.1.EXCEPCIONES

Podrán concederse de manera excepcional y temporal, únicamente cuando existan razones técnicas, operativas o institucionales debidamente justificadas.
Toda excepción deberá cumplir con las siguientes condiciones:

- Estar formalmente documentada, indicando el alcance, la justificación, los riesgos asociados y las medidas de control compensatorias aplicables.
- Contar con la evaluación y recomendación del Oficial de Seguridad de la Información (OSI).
- Ser analizada y aprobada por el Comité de Seguridad de la Información, Protección de Datos Personales y Tecnologías de la Información y Comunicaciones.
- Establecer un plazo de vigencia definido, al término del cual la excepción deberá ser revisada, renovada o eliminada.
- Mantener un nivel de riesgo aceptable para la institución, conforme a la metodología de gestión de riesgos del SGSI.

Las excepciones aprobadas deberán ser registradas y monitoreadas como parte del Sistema de Gestión de Seguridad de la Información.

### 3.6.2.SANCIONES

El incumplimiento de la presente Política de Seguridad de la Información, de los procedimientos y lineamientos derivados de ella, o de las disposiciones del Sistema de Gestión de Seguridad de la Información, dará lugar a la aplicación de medidas correctivas y sanciones, conforme a la normativa legal vigente y a los reglamentos internos de la UNACH.

La UNACH promoverá la aplicación de sanciones de manera proporcional, justa y documentada, asegurando el debido proceso y fomentando, de manera prioritaria, la corrección, prevención y mejora continua en la gestión de la seguridad de la información.

## 4. GLOSARIO DE TÉRMINOS

- **Activo de información:** Toda información o dato que tiene valor para la UNACH, en cualquier formato o medio. Para su gestión, también se consideran los elementos que la soportan, como sistemas, aplicaciones, bases de datos, infraestructura física y tecnológica, redes y el personal que interviene en su manejo. Su importancia se determina según el impacto que pueda generar su pérdida, alteración, divulgación no autorizada o indisponibilidad en los ámbitos académico, administrativo, legal, financiero o reputacional.

- **Alta Dirección (Rectorado):** Primera autoridad ejecutiva de la Institución, responsable de definir la dirección estratégica, aprobar políticas y asignar los recursos necesarios para la implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información.

- **Concienciación:** Proceso continuo y sistemático orientado a lograr que los funcionarios reconozcan la importancia de la seguridad de la información, comprendan los riesgos asociados al manejo de la información y adopten comportamientos responsables y alineados a las políticas institucionales.

- **Confidencialidad:** Propiedad de la información que garantiza que esta solo sea accesible, divulgada o utilizada por personas, entidades o procesos debidamente autorizados.

- **Disponibilidad:** Propiedad de la información que asegura que los activos de información y los servicios asociados se encuentren accesibles y operativos cuando sean requeridos por los usuarios autorizados.

- **EGSI v3.0:** Esquema Gubernamental de Seguridad de la Información, marco normativo obligatorio para las instituciones del sector público ecuatoriano, que establece principios, lineamientos, controles y buenas prácticas para la gestión y protección de la información institucional.

- **Incidente de seguridad de la información:** Evento, o conjunto de eventos, no deseado e inesperado que tiene una alta probabilidad de comprometer la confidencialidad, integridad o disponibilidad de la información institucional.

- **Integridad:** Propiedad de la información que garantiza su exactitud, completitud, consistencia y protección frente a modificaciones no autorizadas o accidentales.

- **LOPDP:** Ley Orgánica de Protección de Datos Personales, normativa legal ecuatoriana que regula el tratamiento de datos personales y establece los derechos, obligaciones y responsabilidades de los responsables y encargados del tratamiento.

- **Oficial de Seguridad de la Información (OSI):** Responsable de liderar, coordinar y supervisar la implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información en la institución.

- **Protección de datos personales:** Conjunto de principios, derechos, obligaciones y medidas técnicas y organizativas destinadas a garantizar el tratamiento lícito, leal, transparente y seguro de los datos personales.

- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza explote una vulnerabilidad de un activo de información y genere un impacto negativo sobre la confidencialidad, integridad o disponibilidad de la información.

- **SGSI:** Sistema de Gestión de Seguridad de la Información, conjunto de políticas, procesos, procedimientos, roles, responsabilidades y controles destinados a gestionar de manera sistemática los riesgos de seguridad de la información.

- **Sensibilización:** Conjunto de acciones orientadas a generar conciencia, modificar comportamientos y promover buenas prácticas en el manejo y protección de la información institucional.

- **Tratamiento de datos personales:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automáticos o manuales, tales como recolección, almacenamiento, uso, comunicación, eliminación o destrucción.

## 5. DOCUMENTOS DE REFERENCIA

Para la elaboración, implementación y cumplimiento de la presente Política de Seguridad de la Información, la UNACH se fundamenta en los siguientes instrumentos normativos, legales, técnicos e institucionales, que constituyen el marco de referencia obligatorio para la gestión de la seguridad de la información:

- **Ley Orgánica de Protección de Datos Personales (LOPDP):** Norma legal aplicable a los procesos de tratamiento de datos personales que se desarrollan en la UNACH y que orienta las actividades de sensibilización relacionadas con la protección de los derechos de los titulares de datos personales.

- **Acuerdo Ministerial Nro. MINTEL-2024-0003 – Esquema Gubernamental de Seguridad de la Información (EGSI v3.0):** Marco rector de seguridad de la información para las instituciones del sector público ecuatoriano, que establece los dominios, objetivos de control y lineamientos obligatorios que sustentan las acciones de comunicación y sensibilización del SGSI.

- **Plan Estratégico Institucional (PEI) 2022–2026 de la Universidad Nacional de Chimborazo:** Instrumento de planificación que define la misión, visión, objetivos estratégicos y lineamientos de desarrollo institucional.

- **Política Institucional de Aseguramiento de la Calidad de la Universidad Nacional de Chimborazo:** Documento que establece los principios, lineamientos y estructura para la gestión de la calidad en los procesos institucionales.

- **Políticas de Seguridad de la Información de la Universidad Nacional de Chimborazo**, aprobadas por el Vicerrectorado Administrativo y actualmente vigentes.

- **Normas Técnicas Ecuatorianas (NTE INEN):**

- **NTE INEN-ISO/IEC 27001:2022**, requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.
- **NTE INEN-ISO/IEC 27002:2022**, controles de seguridad de la información y guía para su implementación.
- **NTE INEN-ISO/IEC 27005:2022**, lineamientos para la gestión de riesgos de seguridad de la información.

## 6. CONTROL DE VERSIONES

| VERSIÓN | FECHA | DETALLE DE LA MODIFICACIÓN |
|---|---|---|
| **0.0** | 24/01/2026 | Elaboración de la Política de Seguridad de la Información del SGSI |
| **1.0** | 26/03/2026 | Actualización del contenido del documento, reforzando su correspondencia con los objetivos estratégicos institucionales. |
| **2.0** | 30/03/2026 | Actualización del contenido del documento conforme a la recomendación de Procuraduría Institucional, asegurando la alineación con los criterios legales y de cumplimiento institucional. |

## 7. LEGALIZACIÓN

| ACCIONES | FECHA | RESPONSABLE | FIRMA |
|---|---|---|---|
| **Elaboración** | 11-02-2026 | Ing. Diego Gustavo Caiza Méndez. Mgs<br>**Oficial de Seguridad de la Información** | Validar únicamente en FirmaEC.<br>Firmado electrónicamente por:<br>DIEGO GUSTAVO CAIZA MENDEZ |
| **Revisión de los miembros en la Primera Sesión Ordinaria del Comité mediante ACTA No. CSI-PDP-TIC-2026-001** | 06-03-2026 | Ing. Marcia Janeth Romero Riera. Mgs<br>**Presidenta del Comité de Seguridad de la Información, Protección de Datos Personales y Tecnologías de la Información y Comunicaciones** | Firmado electrónicamente por:<br>MARCIA JANETH ROMERO RIERA<br>Validar únicamente con FirmaEC |
| **Aprobación** | 14-04-2026 | Ph.D. Myriam Murillo Naranjo<br>**Rectora de la Universidad Nacional de Chimborazo** | Validar únicamente en FirmaEC.<br>Firmado electrónicamente por:<br>MYRIAM ELIZABETH MURILLO NARANJO |