**UNIVERSIDAD NACIONAL DE EDUCACIÓN**
Enrique Guzmán y Valle
"Alma Máter del Magisterio Nacional"

**RECTORADO**

**RESOLUCIÓN N° 2430-2026-R-UNE**

Chosica, 24 de setiembre del 2026

**VISTOS** los Oficios N° 333-2026-OPyP-UNE y N° 488-2026-OPyP-UNE, expedidos por la Oficina de Planeamiento y Presupuesto de la Universidad Nacional de Educación Enrique Guzmán y Valle.

**CONSIDERANDO:**

Que, a través de los Oficios N° 117-2026-OTI-UNE y N° 230-2026-OTI-UNE, el Director de la Oficina de Tecnologías de la Información remite a la instancia respectiva el Plan de Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) primera etapa, a fin de que se adopten las acciones correspondientes;

Que, mediante Oficios N° 0246-2026-UM/OPyP-UNE y N° 0335-2026-UM/OPyP-UNE, la Jefa de la Unidad de Modernización eleva al Director de la Oficina de Planeamiento y Presupuesto el PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PRIMERA ETAPA;

Que con los documentos del visto, el Director de la Oficina de Planeamiento y Presupuesto remite al Rectorado el expediente en mención y solicita que el Consejo Universitario se pronuncie al respecto;

Estando a lo acordado por el Consejo Universitario, en su sesión ordinaria virtual realizada el 30 de junio del 2026; y,

En uso de las atribuciones conferidas por los artículos 59° y 60° de la Ley N° 30220 - Ley Universitaria, concordante con los artículos 19°, 20° y 23° del Estatuto de la UNE, y los alcances de la Resolución N° 1436-2026-R-UNE;

**SE RESUELVE:**

**ARTÍCULO 1°.- APROBAR** el PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PRIMERA ETAPA, suscrito por la instancia pertinente y la oficina técnica respectiva, dando conformidad al contenido que se adjunta en treinta y cuatro (34) folios.

**ARTÍCULO 2°.- DAR A CONOCER** a las dependencias correspondientes los alcances de la presente resolución, a fin de que se adopten las acciones complementarias que resulten pertinentes.

Regístrese, comuníquese y cúmplase.

Universidad Nacional de Educación - Enrique Guzmán y Valle - SECRETARIA GENERAL

**Abg. Anita Luz Chacón Ayala**
**Secretaria General**

Universidad Nacional de Educación - Enrique Guzmán y Valle - RECTOR

**Dr. Tito Doroteo Acosta Castro**
**Rector**

ALCHA/YCA

UNIVERSIDAD NACIONAL DE EDUCACIÓN
ENRIQUE GUZMÁN Y VALLE

*Alma Máter del Magisterio Nacional*

# Plan de Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) primera etapa

**Versión: 1.0**

Oficina de Tecnologías de la Información

## CUADRO DE RESPONSABLES

| Etapa | Responsable | Firma y sello |
|---|---|---|
| Propuesto por: | **Lic. Victor Walter Gallegos Ferrel.** | |
| Cargo: | **Director de la Oficina de Tecnologías de la Información.** | |
| Revisado por: (Revisión Técnica) | **Lic. Adm. Julia Achahui Huayhua.** | Lic. Adm. Julia Achahui Huayhua<br>Jefa de la Unidad de Modernización |
| Cargo: | Jefa de la Unidad de Modernización. | |
| Revisado por: (Revisión Legal) | **Abg. Marcial Curahua Callañaupa.** | Abg. Marcial Curahua Callañaupa<br>DIRECTOR<br>OFICINA DE ASESORÍA JURÍDICA |
| Cargo: | **Jefe de la Oficina de Asesoría Jurídica** | |
| Validado por: | **C.P.C. Alejandro Juan Mayhuire Gallegos.** | C.P.C. Alejandro Juan Mayhuire Gallegos<br>DIRECTOR<br>Oficina de Planeamiento y Presupuesto |
| Cargo: | **Director de la Oficina de Planeamiento y Presupuesto.** | |

## HOJA DE CONTROL DE CAMBIOS

| Versión | Fecha | Descripción del cambio | Responsable |
|---|---|---|---|
| | | | |

# ÍNDICE


1. INTRODUCCIÓN ..... 5
2. OBJETIVOS DEL PLAN SGSI Y MIEMBROS INVOLUCRADOS ..... 6
   - 2.1. Objetivo general. ..... 6
   - 2.2. Objetivos específicos. ..... 6
   - 2.3. Miembros involucrados. ..... 6
3. MARCO LEGAL ..... 7
4. TÉRMINOS Y DEFINICIONES ..... 8
5. CONTEXTO DE LA ENTIDAD ..... 9
   - 5.1. Alineación con el Marco Estratégico de la Entidad- ..... 9
6. MAPA DE PROCESOS ..... 10
   - 6.1. Planificación de la Implementación progresiva del SGSI ..... 11
7. ALCANCE DEL SGSI ..... 13
8. CRONOGRAMA DE ACTIVIDADES ..... 13
   - 8.1. FASE 1: Diagnóstico Inicial y Planificación Estratégica ..... 14
   - 8.2. FASE 2: Contexto Organizacional y Marco Normativo ..... 16
   - 8.3. FASE 3: Identificación y Evaluación de Riesgos ..... 17
   - 8.4. FASE 4: Implementación de Controles y Documentación del SGSI ..... 19
   - 8.5. FASE 5: Operación, Monitoreo y Medición del SGSI ..... 22
   - 8.6. FASE 6: Auditoría Interna y Revisión por la Dirección ..... 23
   - 8.7. FASE 7: Certificación y Mejora Continua ..... 25
9. RECURSOS Y PRESUPUESTO ..... 25
   - 9.1. Recursos humanos. ..... 25
   - 9.2. Recursos financieros. ..... 27
   - 9.3. Otros recursos. ..... 27
10. MONITOREO Y EVALUACIÓN ..... 27
11. ANEXO: CRONOGRAMA PARA IMPLEMENTACIÓN Y CERTIFICACIÓN SGSI ..... 28

# PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) 1ERA ETAPA

## 1. INTRODUCCIÓN

Las universidades manejan grandes volúmenes de información sensible y crítica, como datos personales de estudiantes y profesores (incluidas identificaciones, calificaciones e historiales académicos), resultados de investigación, propiedad intelectual, información financiera y datos administrativos. Esto, dentro de un contexto actual de digitalización acelerada, amenazas cibernéticas crecientes (como ransomware, phishing y fugas de datos) y regulaciones estrictas sobre la protección de datos (por ejemplo, la LPDP 29733) debido a que la exposición a riesgos es elevada.

En este contexto actual, en el que la información constituye uno de los activos más valiosos de cualquier organización, la Universidad enfrenta un entorno de riesgo particularmente sensible. Maneja datos personales, documentos confidenciales, estrategias, evidencias electrónicas, contratos corporativos. Por tanto, la protección, integridad y confidencialidad de esta información no solo representan una obligación ética y legal, sino también un factor crítico para la reputación y la competitividad.

Por ello, implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma internacional ISO/IEC 27001:2022 permite establecer un marco sistemático y auditable para gestionar los riesgos de seguridad de la información que garantice:

- Cumplimiento normativo y legal (Ley 29733 y DS 016-2024-JUS).
- Reducción del riesgo de incidentes y de brechas de seguridad.
- Crecimiento del prestigio Institucional.
- Complemento base y fundamental para las acreditaciones.

En el caso de la universidad, no solo se busca proteger los datos, sino garantizar la continuidad operativa, el cumplimiento normativo (como la Ley N° 29733 – Ley de Protección de Datos Personales del Perú y su Reglamento) y la confianza de la comunidad universitaria y la sociedad.

Se propone la implementación de la Primera Etapa del Sistema de Gestión de Seguridad de la Información (SGSI), conforme a ISO/IEC 27001:2022, en un plazo máximo de 38 semanas (8 meses aproximadamente), circunscrita al alcance definido para el proceso de Formación Académica, con los siguientes entregables principales:

- Declaración de Aplicabilidad (SoA) completa con 93 controles descritos en el anexo A de la norma ISO/IEC 27001:2022.
- Diagnóstico/Gap Análisis completo
- Política de seguridad y conjunto documental completo (15 políticas y procedimientos)
- Análisis de riesgos y tratamiento de riesgos

- Plan de capacitación y sensibilización
- Simulacro de auditoría interna y preparación para certificación etapa 1.

La culminación de las actividades del plan del SGSI, la evaluación de su implementación y la revisión anual por parte de la Dirección permiten la elaboración de los planes de tratamiento de riesgo, conocer el nivel de cumplimiento de los objetivos, hacer análisis de brecha actualizado y elaboración de informe de auditoría interna.

## 2. OBJETIVOS DEL PLAN SGSI Y MIEMBROS INVOLUCRADOS

### 2.1. Objetivo general.

Establecer el Plan de implementación, mantenimiento y certificación del SGSI, en la etapa 1, en cumplimiento de los requisitos de la Norma Técnica Peruana NTP-ISO/IEC 27001:2022, en la universidad, garantizando la confidencialidad, integridad y disponibilidad de la información.

### 2.2. Objetivos específicos.

a. Definir el proyecto de implementación del Sistema de Gestión de Seguridad de la Información (en adelante, SGSI), así como los documentos que se elaborarán, los plazos, las funciones y las responsabilidades del proyecto en la universidad.

b. Implementar un conjunto de políticas, procedimientos, controles y prácticas que garanticen confidencialidad, integridad y disponibilidad de la información académica, tales como:
   - Datos de estudiantes y docentes.
   - Historial académico.
   - Planes de estudio.
   - Registros de notas y asistencias.
   - Evaluaciones.
   - Contenido educativo.
   - Sistemas académicos (ERP, LMS, plataformas de evaluación).

### 2.3. Miembros involucrados.

Todos los Miembros o actores mencionados trabajan de manera articulada para garantizar una gestión eficiente de la seguridad de la información. El Oficial de Seguridad y Confianza Digital actúa como nexo operativo entre el Comité de Gobierno y Transformación Digital, la Oficina de OTI y el Equipo de respuesta ante incidentes de seguridad digital, asegurando que las decisiones estratégicas se traduzcan en acciones operativas concretas y alineadas con la normativa vigente.

| Miembros/Actores | Rol Principal | Responsabilidades Clave |
|---|---|---|
| **Comité de Gobierno y Transformación Digital (CGTD)** | Dirección estratégica | - Aprobar políticas de seguridad.<br>- Supervisar implementación del SGSI.<br>- Asignar recursos. |
| **Oficial de Seguridad y Confianza Digital (OSCD)** | Responsable operativo del SGSI | - Coordinar y liderar el SGSI<br>- Gestionar riesgos.<br>- Reportar incidencias al CNSD. |
| **Oficina de Tecnologías de la Información (OTI)** | Soporte técnico y ejecución de controles | - Implementar medidas técnicas.<br>- Administrar plataformas seguras.<br>- Colaborar en auditorías. |
| **CSIRT-UNE** | Respuesta ante incidentes de seguridad digital | - Detectar y gestionar incidentes.<br>- Coordinar con otras entidades.<br>- Mejorar ciberresiliencia. |

## 3. MARCO LEGAL

a. Decreto Supremo N° 016– 2024-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.
b. Ley N° 30096, Ley de Delitos Informáticos y sus modificaciones.
c. Decreto Supremo Nº 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
d. Decreto Supremo Nº 157-2021-PCM, aprueba el Reglamento del Decreto de Urgencia N° 006- 2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
e. Resolución Ministerial Nº 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.
f. Resolución Ministerial Nº 087-2019-PCM, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
g. Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
h. Resolución Directoral N° 022-2022- INACAL/DN, que aprueba la Norma Técnica Peruana NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ª Edición.
i. Resolución de Secretaría de Gobierno y Transformación Digital N° 0032023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas.
j. Resolución N° 1034-2025-R-UNE que reconforma el Comité de Gobierno y Transformación Digital de la Universidad Nacional de Educación Enrique Guzmán y Valle.
k. Resolución N° 3566-2023-R-UNE que aprueba el Plan de Gobierno Digital de la Universidad Nacional de Educación Enrique Guzmán y Valle.

l. Resolución N° 1943-2024-R-UNE que aprueba el PLAN ESTRATÉGICO INSTITUCIONAL 2025-2030 de la Universidad Nacional de Educación Enrique Guzmán y Valle.
m. Resolución Rectoral N°909-2025-R-UNE que designa al Oficial de Seguridad y Confianza Digital.
n. Resolución N° 0578-2025-R-UNE que aprueba el Manual de Procedimientos – Proceso de Nivel 0: FORMACIÓN ACADÉMICA de la Universidad Nacional de Educación Enrique Guzmán y Valle.
o. Resolución N°3336-2025-R-UNE que conforma el Equipo de Respuestas ante Incidentes de Seguridad Digital de la Universidad Nacional de Educación Enrique Guzmán y Valle (CSIRT-UNE EGyV)

## 4. TÉRMINOS Y DEFINICIONES

**a. Activos de Información**: Cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa Información y tiene valor para la organización, como base de datos, archivos, programas, manuales, equipos de comunicación, la imagen de la entidad, la Información, etc.
**b. Amenazas**: Fuentes generadoras de eventos que originan pérdidas por riesgos de seguridad de la información.
**c. Confidencialidad:** Propiedad de la información que implica que esta no se pone a disposición ni se divulga a personas, entidades o procesos no autorizados.
**d. Disponibilidad:** La información debe ser accesible en el momento y en el formato que se requieran ahora y en el futuro, así como los recursos necesarios para su uso.
**e. Impacto**: Se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo, lo que genera cambios adversos en los objetivos de la organización.
**f. Incidente**: Evento o serie de eventos no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones de la organización y de amenazar la seguridad de la información.
**g. Información**: Datos relacionados que tienen significado para la organización. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, requiere una protección adecuada.
**h. Integridad:** Condición en que la información es clara, completa y que solo puede ser modificada por las personas expresamente autorizadas para ello.
**i. Probabilidad**: Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
**j. Proceso**: Conjunto de actividades relacionadas entre sí o que interactúan para generar valor y transformar elementos de entrada en resultados.
**k. CISO**: (Chief Information Security Officer u oficial de seguridad de la información) personal asignado como oficial de seguridad y confianza digital.
**l. CSIRT (Computer Security Incident Response Team)**: Equipo de respuesta ante incidentes de seguridad digital.

## 5. CONTEXTO DE LA ENTIDAD

La Universidad Nacional de Educación Enrique Guzmán y Valle, conocida como La Cantuta, es una institución reconocida por la formación de profesionales en diversas áreas académicas. Durante la gestión 2021–2026, enfrenta importantes desafíos derivados del contexto postpandemia, con el compromiso de fortalecer el aseguramiento de la calidad, la mejora continua y la excelencia académica.

Tras obtener el licenciamiento institucional, la universidad proyecta como siguiente objetivo la acreditación de sus programas para consolidar su posicionamiento nacional e internacional. Asimismo, impulsará la planificación estratégica participativa, el gobierno digital, la actualización curricular, el fortalecimiento de la investigación y la publicación científica, promoviendo el trabajo conjunto de toda la comunidad universitaria para contribuir al desarrollo del país.

**Misión:**

Formar profesionales con sentido humanístico, científico, intercultural, tecnológico, con responsabilidad social y principios éticos, a los estudiantes universitarios, enfocada a la mejora continua en la competitividad e innovación, orientada a contribuir al desarrollo sostenible de la educación en la sociedad y en nuestro país.

**Visión**

En la próxima década vemos una universidad renovada en su Licenciamiento y Acreditada, con niveles adecuados de calidad, pluralismo, gobernanza y pertinencia para abordar con conciencia social, critica y de manera éticamente responsable, los desafíos de la enseñanza universitaria, la investigación, la responsabilidad social y la vinculación con el medio, contribuyendo al desarrollo de sus comunidades y del país.

### 5.1. Alineación con el Marco Estratégico de la Entidad-

Mediante Resolución Rectoral N° 1943-2024-R-UNE del 01 de julio del 2024, se aprobó el Plan Estratégico Institucional 2025-2030 de la Universidad Nacional de Educación Enrique Guzmán y Valle, el cual define la dirección estratégica de la UNE y establece las prioridades de sus Objetivos Estratégicos Institucionales (OEI) y Acciones Estratégicas Institucionales (AEI), con vigencia hasta el año 2030, tomando como base el marco normativo de las Políticas Educativas Nacionales, con la finalidad de guiar nuestro accionar en los próximos años.

Los Objetivos Estratégicos Institucionales están articulados con los Objetivos Estratégicos Nacionales del Plan Estratégico de Desarrollo Nacional al 2050, tomando en cuenta la Política General de Gobierno para el periodo 2023-2026 y la Política Nacional de Educación Superior y Técnico-Productiva. En este Plan Estratégico se consideran 6 Objetivos Estratégicos Institucionales:

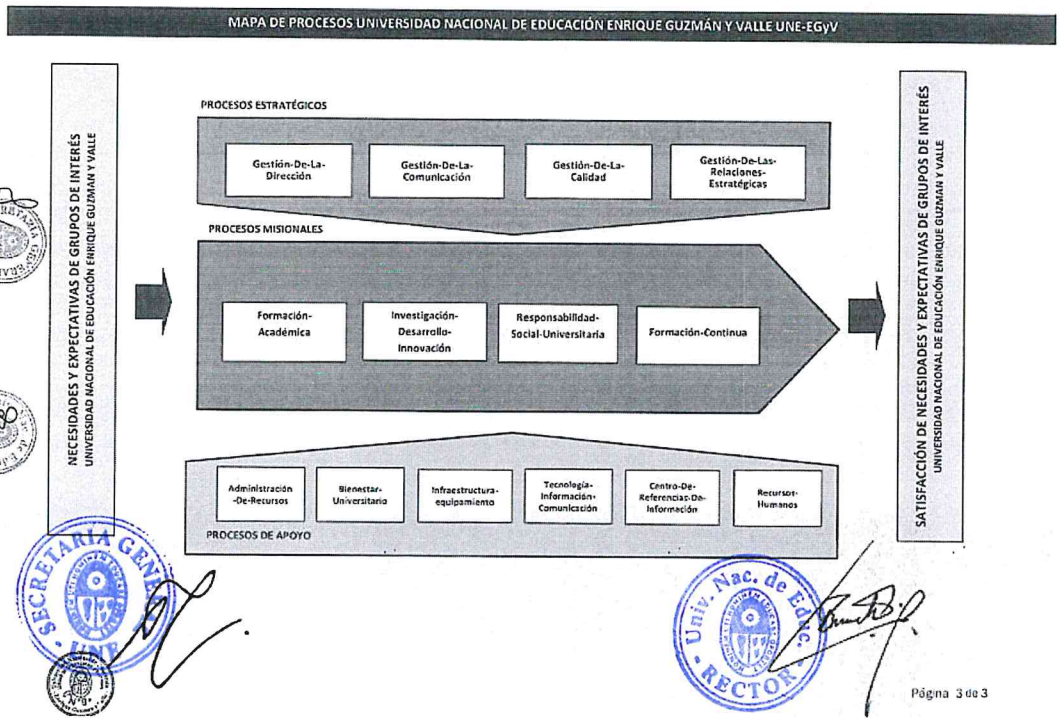
- **OEI.01:** Mejorar la formación académica integral de los estudiantes universitarios.
- **OEI.02:** Promover la investigación científica educativa y tecnológica en la comunidad universitaria.
- **OEI.03:** Fortalecer las actividades de extensión cultural y proyección social aplicado e integrado al conocimiento en la comunidad universitaria y la sociedad.
- **OEI.04:** Fortalecer la gestión institucional.
- **OEI.05:** Implementar la gestión de riesgo de desastres.
- **OEI.06:** Promover la transformación digital implementada en la comunidad universitaria

Asimismo, se estableció una ruta estratégica para cada uno de los objetivos mencionados, incluyendo al **OEI 06 Promover la transformación digital implementada en la comunidad universitaria** al cual se alinea el presente plan:

| *RUTA ESTRATÉGICA INSTITUCIONAL* | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| *OBJETIVO ESTRATÉGICO INSTITUCIONAL* | | | | *ACCIÓN ESTRATÉGICA INSTITUCIONAL* | | | | |
| PRIOR. | CÓDIGO | DESCRIPCIÓN | VINCUL. CON LA PGG | PRIOR. | CÓDIGO | DESCRIPCIÓN | VINCUL. CON LA PGG | UNIDAD ORGÁNICA RESPONSABLE |
| 6 | OEI.06 | *PROMOVER LA TRANSFORMACIÓN DIGITAL EN LA COMUNIDAD UNIVERSITARIA* | *Eje 3: Protección social para el desarrollo* | *1* | *AEI.06.01* | *Implementación de servicios digitales en la comunidad universitaria* | *Eje 3 LIN 3.6* | *DIGA y la Oficina de Tecnologías de la Información* |
| | | | | *2* | *AEI.06.02* | *Seguridad de la información y plataforma de datos abiertos fortalecidos para la comunidad universitaria* | *Eje 3 LIN 3.6* | *DIGA y la Oficina de Tecnologías de la Información* |

## 6. MAPA DE PROCESOS

La Universidad Nacional de Educación Enrique Guzmán y Valle cuenta con 14 procesos de nivel cero conforme a los indicado en la Resolución N° 1069-2021-R-UNE, que aprueba el Mapa de Procesos en su V.1.1.






ANEXO DE LA RESOLUCIÓN N° 1069-2021-R-UNE

## 6.1. Planificación de la Implementación progresiva del SGSI

La implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) en la Universidad Nacional de Educación Enrique Guzmán y Valle se plantea bajo un enfoque progresivo, considerando la naturaleza, complejidad y cantidad de procesos que conforman el Mapa de Procesos institucional. En ese sentido, la presente primera etapa establece como alcance inicial el proceso misional de Formación Académica, priorizando la protección de la información y de los activos asociados a las actividades académicas, conforme al alcance definido en el presente Plan.

La implementación progresiva permitirá que las capacidades, metodologías, controles, políticas, procedimientos y mecanismos de gestión desarrollados durante la primera etapa constituyan una base para la posterior ampliación del SGSI hacia los demás procesos institucionales. Esta estrategia permitirá gestionar de manera ordenada los recursos, riesgos, responsabilidades y requerimientos asociados a cada proceso, procurando asegurar la sostenibilidad y mejora continua del Sistema.

Una vez culminadas las actividades correspondientes a la Primera Etapa, se procederá a realizar la evaluación de los resultados obtenidos, considerando, entre otros aspectos, el nivel de cumplimiento de los objetivos establecidos, los resultados de la gestión y tratamiento de riesgos, los hallazgos identificados durante las auditorías y revisiones, el nivel de madurez alcanzado y la capacidad institucional para continuar con la ampliación del SGSI. El propio Plan contempla la evaluación de la implementación, la revisión por la Dirección, la actualización del análisis de brechas y la elaboración de informes de auditoría interna como elementos para la mejora y continuidad del SGSI.

Con base en dicha evaluación, la Oficina de Tecnologías de la Información (OTI), en coordinación con el Oficial de Seguridad y Confianza Digital (OSCD) y los responsables de los procesos involucrados, elaborará y presentará ante el Comité de Gobierno y Transformación Digital (CGTD) una propuesta para la implementación de la "Segunda Etapa", en la cual se considerará la ampliación del alcance hacia los procesos de apoyo de la Universidad: Administración de Recursos, Bienestar Universitario, Infraestructura-Equipamiento, Tecnología-Información-Comunicación, Centro de Referencias de Información y Recursos Humanos.

La eventual implementación de la Segunda Etapa estará sujeta a la evaluación de sus condiciones técnicas, operativas, organizacionales y presupuestales, así como a la aprobación de las instancias competentes. El Comité de Gobierno y Transformación Digital cumple dentro de la estructura del SGSI un rol de dirección estratégica, incluyendo la supervisión de la implementación del SGSI y la asignación de recursos.

De manera similar, una vez culminada y evaluada la Segunda Etapa, se realizará el análisis correspondiente de los resultados alcanzados y, sobre dicha base, se elaborará y presentará ante el Comité de Gobierno y Transformación Digital la propuesta para la implementación de la última etapa denominada "Tercera Etapa", orientada a incorporar los procesos misionales

pendientes: Investigación-Desarrollo-Innovación, Responsabilidad Social Universitaria y Formación Continua; así como los procesos estratégicos: Gestión de la Dirección, Gestión de la Comunicación, Gestión de la Calidad y Gestión de las Relaciones Estratégicas.

En consecuencia, las tres etapas constituyen una ruta de implementación progresiva y planificada del SGSI, cuya continuidad y ampliación estarán condicionadas a la evaluación de los resultados de cada etapa y a las decisiones institucionales que correspondan. La duración estimada de cada etapa será de seis (6) a ocho (8) meses aproximadamente, pudiendo ser ajustada en función de los resultados de la evaluación, la complejidad de los procesos involucrados, la disponibilidad de recursos y las necesidades institucionales.

La implementación progresiva permitirá que el SGSI evolucione desde un alcance inicial focalizado en el proceso de Formación Académica hacia una cobertura integral de los procesos misionales, de apoyo y estratégicos de la Universidad, fortaleciendo de manera gradual la confidencialidad, integridad y disponibilidad de la información institucional, así como la capacidad de la Universidad para gestionar los riesgos de seguridad de la información y mantener un proceso permanente de mejora continua.

| ETAPA | DURACIÓN | PROCESOS COMPRENDIDOS | FINALIDAD |
|---|---|---|---|
| 1era Etapa | 6 a 8 meses aprox. | **Proceso Misional:** Formación Académica | Implementar el SGSI sobre el proceso de Formación Académica, priorizando la protección de la información y de los activos asociados a los registros y actividades académicas. |
| 2da Etapa | 6 a 8 meses aprox. | **Procesos de Apoyo:** Administración de Recursos; Bienestar Universitario; Infraestructura-Equipamiento; Tecnología-Información-Comunicación; Centro de Referencias de Información; Recursos Humanos | Ampliar progresivamente el alcance del SGSI hacia los procesos de apoyo que sustentan el funcionamiento institucional y que intervienen en la gestión, procesamiento, almacenamiento y disponibilidad de información. |
| 3era Etapa | 6 a 8 meses aprox. | **Procesos Misionales pendientes:** Investigación-Desarrollo-Innovación; Responsabilidad Social Universitaria; Formación Continua.<br><br>**Procesos Estratégicos:** Gestión de la Dirección; Gestión de la Comunicación; Gestión de la Calidad; Gestión de las Relaciones Estratégicas | Completar la extensión del SGSI hacia los procesos misionales pendientes y los procesos estratégicos, culminando la implementación del SGSI a nivel institucional. |

## 7. ALCANCE DEL SGSI

El documento aplica a las actividades de la 1era Etapa que se llevarán a cabo en el marco del Plan de implementación del SGSI que protege la "Integridad y Disponibilidad de los Registros Académicos" correspondientes al proceso de nivel cero Formación Académica, que forma parte del Mapa de Procesos de la UNE EGyV, aprobado mediante Resolución N° 0578-2025-R-UNE y que está conformado por los siguientes procesos de nivel 1:

a. Gestión del Diseño Curricular.
b. Gestión del Proceso de Admisión.
c. Gestión de la Programación Académica.
d. Gestión del Ciclo de Nivelación de Ingresantes de Pregrado.
e. Gestión del Seguimiento a la Enseñanza – Aprendizaje.
f. Gestión de las Prácticas Preprofesionales.
g. Gestión del Seguimiento al Estudiante.
h. Gestión de Grados y Títulos.
i. Gestión del Seguimiento al Egresado.
j. Gestión y Desarrollo Docente.

En consecuencia, el SGSI cubre el proceso completo de formación académica, que incluye actividades como:

- Diseño curricular de cursos.
- Gestión de docentes.
- Ejecución de clases (presencial/virtual).
- Evaluaciones.
- Gestión de notas.
- Certificación y registro académico (grados y títulos).
- Sistemas: Sistema de Gestión Académica SIGEAC, Intranet, Plataforma virtual de cursos, correo institucional, etc.

## 8. CRONOGRAMA DE ACTIVIDADES

La implementación del SGSI se desarrollará en siete fases principales, cada una con objetivos, actividades específicas y entregables definidos

| Fase | Duración estimada |
|---|---|
| **Fase 1:** Diagnóstico Inicial y Planificación Estratégica | 1 mes |
| **Fase 2:** Contexto Organizacional y Marco Normativo | 1 mes |
| **Fase 3:** Identificación y Evaluación de Riesgos | 2 mes |
| **Fase 4:** Implementación de Controles y Documentación del SGSI | 3 meses |
| **Fase 5:** Operación, Monitoreo y Medición del SGSI | 2 meses |
| **Fase 6:** Auditoría Interna y Revisión por la Dirección | 1 mes |
| **Fase 7:** Certificación y Mejora Continua | 1 mes |

Duración total estimada: 8 meses (Ver Anexo).

### 8.1. FASE 1: Diagnóstico Inicial y Planificación Estratégica

**Objetivo**: Evaluar la situación actual de la organización respecto de los requisitos de la norma ISO/IEC 27001:2022 y definir la estrategia de implementación.

**Actividades principales:**

- Reunión de inicio con la alta dirección.
- Definición del alcance preliminar del SGSI.
- Evaluación de madurez y diagnóstico inicial (GAP Analysis).
- Identificación de roles y responsabilidades (RACI).
- Elaboración del plan de trabajo detallado.
- Definición del comité de seguridad de la información.
- Designación oficial del Comité de Seguridad.
- Nombramiento del responsable del SGSI (CISO).
- Elaboración del Acta de Inicio de Proyecto.
- Registro del plan SGSI en Facilita Perú (Cuando el SGSI sea Aprobado).
- Definición del alcance del SGSI.

**Entregables:**

- Informe de diagnóstico GAP ISO 27001:2022.
- Plan maestro para la implementación de la 1era Etapa del SGSI.
- Acta de constitución del comité de seguridad.
- Cronograma general (Gantt).
- Mapa de partes interesadas y de comunicación.
- Acta de constitución del SGSI.
- Alcance documentado.
- Estructura de gobierno del SGSI.
- Definir liderazgo, roles, responsabilidades y alcance.
- Informe diagnóstico de madurez.

**Acciones por desarrollar:**

**Acta de constitución del SGSI (Acta de inicio del proyecto)**

- **Propósito**: Formalizar el proyecto, autorizar los recursos y definir las responsabilidades y el alcance inicial.
- **Contenido típico:** objetivo del proyecto, alcance (procesos y sistemas incluidos), patrocinador, responsable del proyecto (CISO), miembros del comité, presupuesto aprobado, hitos principales, restricciones, riesgos iniciales y firma de aprobación.
- **Formato sugerido:** documento de Word de 2–4 páginas con firmas digitales/escaneadas.

- **Responsable**: Patrocinador + CISO.
- **Criterio de aceptación / evidencia:** Documento firmado por el Rector/Vicerrector, registro en el gestor documental y correo de lanzamiento.

**Alcance documentado**

- **Propósito:** Definir con precisión qué partes de la institución y qué activos cubre el SGSI.
- **Contenido típico:** límites (facultades, sedes), procesos incluidos (inscripción, evaluación, registro académico), sistemas (LMS, ERP académico, correo), exclusiones justificadas, versión y fecha.
- **Formato:** Anexo en Word/PDF + diagrama de alcance (mapeo de procesos y sistemas).
- **Responsables:** Dueño del proceso académico y CISO.
- **Evidencia:** Aprobación en el acta del comité, diagrama publicado en la intranet.

**Estructura de gobierno del SGSI**

- **Propósito:** Mostrar autoridades, los comités y el flujo de toma de decisiones.
- **Contenido:** organigrama, roles (patrocinador, CISO, comité, dueños de procesos, Responsables de TI), responsabilidades y periodicidad de las reuniones.
- **Formato:** Documento + organigrama gráfico.
- **Responsable:** CISO.
- **Evidencia:** Calendario de reuniones, actas de reunión.

**Planificación de trabajo general (Project Plan)**

- **Propósito:** Planificar actividades, recursos, entregables y el cronograma.
- **Contenido:** fases, actividades detalladas, responsables, dependencias, hitos, riesgos y supuestos, entregables y criterios de entrega.
- **Formato:** Gantt (MS Project/Excel) + documento de resumen.
- **Responsable:** Project Manager / CISO.
- **Evidencia:** Archivo Gantt, reporte de avance mensual.

**Informe diagnóstico de madurez (evaluación inicial)**

- **Propósito:** Conocer el punto de partida del SGSI y priorizar las acciones.
- **Contenido:** Resultados de la evaluación de controles, brechas frente a la ISO 27001, recomendaciones priorizadas, puntuación de madurez por dominio (políticas, TI, operaciones, formación).
- **Formato:** Informe con tablas y gráficos (10–20 páginas).
- **Responsable:** Consultor externo / auditor interno.
- **Evidencia:** Informe aprobado por la dirección y plan de tratamiento de gaps.

## 8.2. FASE 2: Contexto Organizacional y Marco Normativo

**Objetivo:** Definir el contexto, el alcance y los lineamientos del SGSI según los requisitos de las cláusulas 4 a 10 de la norma.

**Actividades principales:**

- Identificación de partes interesadas (estudiantes, docentes, SUNEDU, Minedu, TI, proveedores).
- Documentación de necesidades y expectativas.
- Análisis del contexto interno y externo (FODA de seguridad).
- Definición del alcance definitivo del SGSI.
- Revisión de los requisitos legales, normativos y contractuales.
- Elaboración de la política del SGSI.
- Asignación formal de roles (responsable de SGSI, del comité y de las partes interesadas).

**Entregables:**

- Documento de alcance del SGSI.
- Política de Seguridad de la Información.
- Registro de requisitos legales y contractuales.
- Acta de designación de roles y responsabilidades.
- Identificación de requisitos legales (LPDP 29733, DS 016-2024-JUS, derechos de autor, Ley Universitaria).
- Definición de los procesos académicos incluidos.
- Elaboración de criterios para la valoración de la información.
- Matriz de partes interesadas
- Matriz de requisitos legales y contractuales
- Inventario del proceso académico
- Inventario de activos de información (bases de datos, sistemas, equipos, documentos)
- Criterios de clasificación de la información.

**Matriz de partes interesadas**

- **Propósito:** Identificar a los stakeholders y sus necesidades para asegurar el cumplimiento de los requisitos.
- **Contenido:** Listado de actores (estudiantes, docentes, decanos, proveedores, SUNEDU), necesidades y expectativas, impacto en el SGSI, prioridad de comunicación.
- **Formato:** Hoja de Excel o tabla en Word.
- **Responsables:** CISO y responsable de calidad.
- **Evidencia:** Matriz almacenada y uso en el análisis de requisitos.

**Matriz de requisitos legales y contractuales**

- **Propósito:** Registrar las obligaciones jurídicas y contractuales aplicables al proceso académico.

- **Contenido:** Referencia normativa (LPDP, DS 016-2024-JUS, Ley Universitaria, contratos con proveedores de LMS), requisito específico, responsable de cumplimiento, evidencia asociada, estado de cumplimiento.
- **Formato:** Excel con filtros.
- **Responsable:** Protección de Datos + Legal.
- **Evidencia:** Registro con enlaces a la evidencia (contratos, certificados de proveedor, políticas).

**Inventario del proceso académico**

- **Propósito:** Mapear las actividades, las entradas y salidas de información y los puntos de control del proceso de formación.
- **Contenido:** Flujo de proceso (inscripción → dictado de clases → evaluación → registro de calificaciones → titulación), así como los sistemas involucrados y sus responsables.
- **Formato:** Diagrama BPMN o flujograma + tabla descriptiva.
- **Responsable:** Dueño del proceso académico.
- **Evidencia:** Diagrama aprobado y publicado.

**Inventario de activos de información**

- **Propósito:** Conocer y clasificar los activos que respaldan la formación académica.
- **Contenido:** Activo, descripción, propietario, ubicación, categoría (HW, SW, DB, documento), valor/criticidad, clasificación de la información asociada.
- **Formato:** Registro en Excel/CMDB.
- **Responsable:** TI y dueños del activo.
- **Evidencia:** base de datos de CMDB y registros de mantenimiento.

**Criterios de clasificación de información**

- **Propósito:** Definir cómo se clasifica (confidencial, interna, pública) y qué controles aplican.
- **Contenido:** Definiciones, ejemplos, etiquetas, niveles de protección, manejo, retención y destrucción.
- **Formato:** Política/Procedimiento corto.
- **Responsable:** CISO + DPO.
- **Evidencia:** Política aprobada y etiquetas aplicadas en los repositorios.

### 8.3. FASE 3: Identificación y Evaluación de Riesgos

**Objetivo:** Establecer una metodología formal para la gestión de riesgos de seguridad de la información, conforme a la norma ISO/IEC 27005, y evaluar los riesgos actuales. Identificar riesgos en los activos del proceso de formación académica y definir los controles del Anexo A.

**Actividades principales:**

- Definición de criterios de evaluación y apetito de riesgo.
- Inventario y valoración de activos de información.
- Identificación de amenazas y vulnerabilidades.
- Análisis de impacto y de probabilidad.
- Elaboración del mapa de riesgos y de la matriz de tratamiento.
- Determinar criterios de aceptación del riesgo
- Selección de controles ISO 27001 (Anexo A, 93 controles)
- Plan de tratamiento de riesgos

**Entregables:**

- Metodología de gestión de riesgos SGSI.
- Inventario de activos de información.
- Matriz de riesgos del proceso académico.
- Matriz de evaluación de riesgos.
- Plan de tratamiento de riesgos.
- Declaración de aplicabilidad (SoA) inicial.

**Metodología de análisis de riesgos**

- **Propósito:** Establecer un método consistente para identificar, valorar y tratar los riesgos.
- **Contenido:** Criterios de valoración (escala de probabilidad e impacto), fórmula (probabilidad × impacto), niveles de riesgo (bajo, medio, alto, crítico), frecuencia de revisión.
- **Formato:** Documento con un ejemplo de cálculo y plantillas.
- **Responsable:** CISO / Risk Manager.
- **Evidencia:** Metodología aprobada y utilizada en sesiones de riesgo.

**Matriz de riesgos del proceso académico**

- **Propósito:** Registrar los riesgos identificados y su valoración.
- **Contenido:** Riesgo, activo afectado, amenaza, vulnerabilidad, probabilidad, impacto, puntaje, riesgo residual, propietario y fecha de identificación.
- **Formato:** Excel (filtrable) con columnas de tratamiento y de control.
- **Responsable:** Equipo de Riesgos (CISO + dueños de proceso).
- **Evidencia:** Matriz con evidencias de controles implementados y revisiones periódicas.

**Informe de evaluación y aceptación de riesgos**

- **Propósito:** Formalizar la decisión sobre los riesgos residuales y su aceptación o transferencia.
- **Contenido:** Resumen de riesgos críticos, recomendaciones, opciones de mitigación y la decisión de la alta dirección sobre la aceptación/transferencia.

- **Formato:** Informe ejecutivo para la Dirección (3-6 páginas).
- Responsable: CISO + patrocinador.
- **Evidencia:** Acta de aceptación de riesgos por parte de la Dirección.

**Declaración de Aplicabilidad (SoA)**

- **Propósito:** Documentar los controles del Anexo A aplicados, la justificación de inclusiones y exclusiones, y el estado de implementación.
- **Contenido:** lista de controles ISO 27001 (referencia), aplicabilidad (Sí/No), justificativo, fuente de evidencia, estado (planificado/implementado/operando).
- **Formato:** Tabla Excel/Word.
- **Responsable:** CISO + responsable de controles.
- **Evidencia**: SoA aprobado y vinculado a evidencias (procedimientos, registros).
-

**Plan de tratamiento de riesgos**

- **Propósito:** Planificar acciones, responsables y plazos para mitigar riesgos.
- **Contenido:** Riesgo, acción correctiva/mitigadora, responsable, recursos necesarios, fecha de inicio/fin, indicadores y estado.
- **Formato:** Planificación en Excel o en una herramienta de gestión de proyectos.
- **Responsable:** Dueños de riesgos.
- **Evidencia:** Registros de avance y evidencia técnica de los controles implementados.

### 8.4. FASE 4: Implementación de Controles y Documentación del SGSI

**Objetivo:** Implementar los controles de seguridad definidos en el Anexo A (93 controles de ISO/IEC 27001:2022) y elaborar la documentación requerida por la norma.

**Actividades principales:**

- Diseño e implementación de controles técnicos, organizativos y físicos.
- Elaboración y aprobación de políticas, procedimientos y estándares.
- Implementación de medidas de gestión de incidentes, de continuidad y de acceso.
- Concientización y capacitación en seguridad de la información.
- Establecimiento de indicadores de desempeño (KPI y KRI).

**Entregables:**

- Manual del SGSI.
- Registros de capacitación y concientización.
- Declaración de aplicabilidad (SoA) final.
- Planificación de comunicaciones y gestión de cambios.

- Políticas del SGSI (mínimo 13 políticas específicas)
  1. Política de seguridad de la información.
  2. Política de protección de datos personales.
  3. Política de control de acceso.
  4. Política de uso aceptable.
  5. Política de gestión de vulnerabilidades.
  6. Política de continuidad tecnológica.
  7. Política de backup.
  8. Política de gestión de proveedores.
  9. Política de seguridad en el lms y plataformas académicas.
  10. Política de gestión de incidentes.
  11. Política de seguridad física y ambiental.
  12. Política de desarrollo seguro.
  13. Política de clasificación y manejo de la información.

**Procedimientos del SGSI (propuesta)**

- Gestión de incidentes académicos.
- Gestión de cambios en sistemas académicos.
- Gestión de acceso de estudiantes y docentes.
- Procedimiento de registro y custodia de notas.
- Procedimiento de continuidad del servicio del LMS.
- Procedimiento de respaldo y restauración académica.
- Procedimiento de alta/baja de docentes y estudiantes.
- Procedimiento de gestión de proveedores de plataformas educativas.

**Controles tecnológicos (propuesta)**

- Autenticación MFA en el LMS y plataformas.
- Hardening de servidores académicos.
- Encriptación de bases de datos de notas y registros.
- Registro de auditoría de cambios de calificaciones.
- Segmentación de redes académicas.
- Copias de seguridad en nube con retención mínima 1 año.
- Monitoreo de integridad de registros académicos.

**Entregables de esta fase**

- Políticas aprobadas.
- Procedimientos implementados.
- Instructivos operativos.
- Evidencias y registros del SGSI.
- Controles técnicos en operación.

**Políticas del SGSI (conjunto aprobado)**

- **Propósito**: Establecer directrices de alto nivel para el comportamiento y los controles.

- **Contenido**: Para cada política: objetivo, alcance, definiciones, responsabilidades, requisitos mínimos, referencia a procedimientos, revisión y aprobación.
- **Formato**: Documento por política (1-4 páginas) y un índice maestro.
- **Responsable**: CISO (redacción) y comité de seguridad (aprobación).
- **Evidencia**: Políticas publicadas y comunicadas, en versión controlada. (para cada política — por ejemplo, política de control de acceso — incluirá: esquema de gestión de cuentas, requisitos de contraseñas, MFA, roles y privilegios, revocación de accesos.)

**Procedimientos del SGSI**

- **Propósito**: Traducir políticas a pasos operativos reproducibles.
- **Contenido**: Propósito, alcance, responsabilidades, pasos detallados, formularios, registros y criterios de aprobación.
- **Formato**: Documento procedimental con flujogramas y checklists.
- **Responsable**: Propietario del proceso / responsable operativo.
- **Evidencia**: Procedimientos implementados, registros generados (p. ej.: bitácoras de incidentes, registros de backup).

**Instructivos operativos**

- **Propósito**: Guiar tareas técnicas (hardening, backup, restauración) y de usuario (registro de notas).
- **Contenido**: Pasos técnicos paso a paso, comandos, configuraciones, parámetros mínimos y pruebas de verificación.
- **Formato**: Manual técnico (HTML/PDF) o runbook.
- **Responsable**: Equipo TI.

**Evidencias y registros del SGSI**

**Propósito**: Mantener la trazabilidad del cumplimiento y la operatividad.

- **Contenido**: Logs de acceso, registros de backup, resultados de pruebas, informes de antivirus, auditorías, actas de reuniones, capacitación.
- **Formato**: Repositorio central (SIEM/log server/SharePoint).
- **Responsable**: TI + auditor interno.
- **Evidencia**: Retención según las políticas, accesible para la auditoría.

**Controles técnicos en operación**

- **Propósito**: Asegurar que las soluciones tecnológicas estén instaladas y funcionando.
- **Contenido**: Configuración de firewalls, MFA, cifrado de la DB, registros centralizados, sistemas de parches, eliminación de cuentas inactivas.
- **Formato**: Documento de estado / checklist de implementación.
- **Responsable**: Jefe de OTI.
- **Evidencia**: Capturas de pantalla, reportes de herramientas (scanner, SIEM) y registros de pruebas.

## 8.5. FASE 5: Operación, Monitoreo y Medición del SGSI

**Objetivo:** Operar y monitorear el SGSI, asegurando su eficacia y el cumplimiento de los requisitos normativos en base a las directrices de la ISO 27004.

**Actividades principales**:

- Implementación del ciclo PDCA (Plan-Do-Check-Act).
- Monitoreo de eventos, incidentes y cumplimiento de controles.
- Seguimiento de indicadores de seguridad.
- Ejecución de pruebas de continuidad y simulacros.
- Registro y tratamiento de incidentes de seguridad.
- Capacitación general a estudiantes y docentes.
- Capacitación especializada a TI y áreas críticas.
- Campañas de concientización.
- Simulaciones de incidentes (prueba de phishing académico, caída del LMS y fuga de notas).
- Pruebas de restauración y continuidad.
- Auditoría interna.

**Entregables:**

- Registros de incidentes y no conformidades.
- Reportes de desempeño de controles e indicadores.
- Informes de monitoreo de seguridad.

**Formación, concientización y pruebas**

**Plan anual de capacitaciones**

- **Propósito:** Programar formación para los roles (docentes, administrativos, TI, estudiantes) sobre seguridad y protección de datos.
- **Contenido:** Temario por audiencia, frecuencia, modalidad (presencial/online), responsables y KPI (porcentaje de asistencia).
- **Formato:** Planificación en Excel + calendario.
- **Responsable:** Talento Humano + CISO.
- **Evidencia:** Calendario publicado y confirmaciones de inscripción.

**Registros de capacitaciones**

- **Propósito**: Evidenciar el cumplimiento de la formación.
- **Contenido**: Lista de asistentes, materiales entregados, evaluación poscapacitación y certificación interna.
- **Formato**: Excel + certificados.
- **Responsable**: RRHH / Coordinador de Formación.
- **Evidencia**: Registros firmados y resultados de encuestas.

**Informes de pruebas (simulaciones)**

- **Propósito**: Evaluar la efectividad de los controles mediante ejercicios prácticos.

- **Contenido**: Objetivos de la prueba (phishing, RTO de LMS), metodología, resultados, hallazgos, tiempo de recuperación, brechas detectadas y recomendaciones.
- **Formato**: Informe técnico con evidencias (logs y timelines).
- **Responsable**: Equipo TI + DPO (para pruebas relacionadas con datos).
- **Evidencia**: Informe y plan de acción de mitigación.

**Pruebas de restauración y continuidad**

- **Propósito**: Verificar que los backups y los planes de continuidad funcionen y permitan la recuperación.
- **Contenido**: Escenarios de prueba, procedimientos ejecutados, tiempo de recuperación real y fallas detectadas.
- **Formato**: Registro de prueba (runbook) y lecciones aprendidas.
- **Responsable**: TI + responsable de Continuidad.
- **Evidencia**: Restauración de datos de prueba y reporte de verificación.

**Informe de auditoría interna**

- **Propósito**: Comprobar la conformidad con las políticas y el SoA antes de la auditoría externa.
- **Contenido**: Alcance de la auditoría, hallazgos, no conformidades, observaciones, oportunidades de mejora y plan de acciones correctivas.
- **Formato**: Informe estructurado con clasificación de hallazgos (mayor/menor).
- **Responsable**: Auditor interno.
- **Evidencia**: informes y registros de cierre de no conformidades.

**Plan de acciones correctivas**

- **Propósito**: Cerrar las brechas detectadas en auditorías y pruebas.
- **Contenido**: Descripción de la acción, prioridad, responsable, recursos, fecha de cierre y evidencia requerida.
- **Formato**: RACI/tabla en la herramienta de tickets.
- **Responsable**: Dueños de procesos.
- **Evidencia**: tickets resueltos y validación por auditor.

### 8.6. FASE 6: Auditoría Interna y Revisión por la Dirección

**Objetivo:** Evaluar el desempeño del SGSI, verificar su conformidad con la norma y preparar a la organización para la auditoría de certificación.

**Actividades principales:**

- Elaboración del plan de auditoría interna.
- Ejecución de auditorías internas del SGSI.
- Identificación de no conformidades y acciones correctivas.
- Revisión por la Dirección: Análisis del desempeño, de los recursos y de la mejora continua.
- Revisión por la alta dirección.

- Evaluación de indicadores del SGSI.
- Evaluación del cumplimiento legal.
- Cierre de brechas.
- Preparación para certificación ISO 27001 (opcional).

**Entregables:**

- Plan de auditoría interna.
- Informe de auditoría interna.
- Plan de acciones correctivas.
- Acta de revisión por la Dirección.

**Revisión, Mejora Continua y Certificación**

**Informe de revisión por la dirección**

- **Propósito**: Informar a la Alta Dirección sobre el desempeño del SGSI y tomar decisiones estratégicas.
- **Contenido**: estado de riesgos, cumplimiento de indicadores, resultados de auditorías, evidencias de controles, propuestas de mejora y recursos requeridos.
- **Formato**: Informe ejecutivo y presentación en PowerPoint.
- **Responsable**: CISO.
- **Evidencia**: Acta de la reunión de revisión por parte de la dirección, con decisiones y asignaciones.

**Plan de mejora continua**

- **Propósito**: Programar mejoras para incrementar la madurez y reducir los riesgos.
- **Contenido**: Iniciativas, prioridades, indicadores, responsables y cronograma.
- **Formato**: Roadmap en Excel/PowerPoint.
- **Responsable**: CISO + Comité.
- **Evidencia**: Seguimiento en tableros (Jira/Asana) y reportes trimestrales.

**Informe de cumplimiento normativo**

- **Propósito**: Acreditar que el SGSI cumple con las normativas aplicables (protección de datos, acreditaciones académicas).
- **Contenido**: Mapeo legal vs controles, evidencias de cumplimiento, gaps y plan de cierre.
- **Formato**: Informe técnico-legal.
- **Responsable**: DPO + Legal.
- **Evidencia:** Certificados, actas, políticas y evidencia documental.

**Evidencias para auditoría externa / Material para certificación ISO 27001**

- **Propósito**: Reunir toda la documentación y la evidencia necesarias para la auditoría de certificación.

- **Contenido**: Scope, SoA, políticas, procedimientos, registros de auditoría interna, registros de formación, pruebas de operación de controles, informes de continuidad y plan de tratamiento de riesgos.
- **Formato**: Paquete digital organizado (carpetas con índices) y lista de verificación.
- **Responsables**: CISO y Auditor Interno.
- **Evidencia**: Carpeta entregada al organismo certificador y lista de evidencias aprobada.

### 8.7. FASE 7: Certificación y Mejora Continua

**Objetivo:** Obtener la certificación ISO/IEC 27001:2022 y establecer un modelo de mejora continua del SGSI.

**Actividades principales:**

- Selección y coordinación con el organismo certificador.
- Atención a la auditoría de certificación etapa 1.
- Corrección de hallazgos y observaciones.
- Comunicación del logro de la certificación.
- Revisión poscertificación y plan de mejora continua.

**Entregables:**

- Informe de auditoría del organismo certificador.
- Plan de mejora poscertificación.
- Certificado ISO/IEC 27001:2022.
- Informe final de implementación.

## 9. RECURSOS Y PRESUPUESTO

### 9.1. Recursos humanos.

a. Jefe de la OTI.
b. Especialistas que conforman el equipo técnico de la OTI.

Se recomienda un equipo multidisciplinario con roles claros. El equipo total sería de 6 a 12 personas especializadas en TI y/o seguridad de la información que participarán desempeñando las siguientes funciones:

a. **Un líder de SGSI** (CISO): Responsable general, preferiblemente un gerente de TI con certificación CISM o como Lead Implementer ISO 27001. Coordina todas las fases.
b. **Equipo de Implementación** (4-6 personas): Incluye un experto en riesgos (p. ej., analista de seguridad), un especialista en procesos académicos (p. ej., decano o coordinador de formación), un experto legal (para el cumplimiento de datos) y técnicos de TI (para controles en plataformas tecnológicas).
c. **Auditores internos** (2 personas): certificados en ISO 27001 Lead Auditor, independientes del equipo de implementación, para las fases de auditoría.

d. **Consultor Externo** (1-2 personas): Experto en ISO 27001 para asesoría inicial y revisión, contratado durante 6-12 meses.

**Roles y responsables de la implementación**

| Rol | Perfil | Responsabilidades |
|---|---|---|
| CISO / lider SGSI | Experto ISO 27001 | Liderar implementación y coordinar auditorías |
| Jefe de la OTI | Especialista tecnológico | Implementación de controles técnicos |
| Dueño del proceso académico | Decano / Dirección Académica | Aprobar controles e intervenciones |
| Comité de Seguridad | Multidisciplinario | Validar políticas y riesgos |
| Oficial de datos personales | Especialista LPDP | Alineamiento legal |
| Equipo técnico de la OTI | Administradores, ingenieros | Hardening, accesos y monitoreo |
| Auditor interno ISO 27001 | Certificado | Evaluación de cumplimiento |
| Consultor externo (opcional) | ISO 27001 Lead Implementer | Guía metodológica |

La implementación de la primera etapa del SGSI requiere un equipo multidisciplinario con respaldo ejecutivo.

- **Líder del Proyecto / Gestor del SGSI** (CISO o equivalente):
  - **Rol Principal:** Dirigir la implementación, mantener el SGSI y actuar como punto focal para la certificación.
  - **Habilidades Requeridas:** Conocimiento profundo de ISO 27001 y gestión de proyectos.

- **Representante de la Alta Dirección**:
  - **Rol Principal:** Otorgar autoridad, aprobar políticas y asignar recursos.

- **Equipo Técnico de Seguridad y OTI:**
  - **Rol Principal:** Implementar los controles técnicos en redes, servidores y sistemas académicos.
  - Perfil: Personal de TI y administradores de Sistemas.

- **Dueño de proceso:**
  - **Rol Principal:** Documentar flujos de trabajo y asegurar el cumplimiento legal (ej. protección de datos estudiantiles).

- **Auditores Internos (Capacitados en 27001):**
  - **Rol Principal:** Ejecutar las auditorías internas de cumplimiento.

### 9.2. Recursos financieros.

De acuerdo con el anexo B-5 del Plan Operativo Institucional de la Unidad de Soporte Técnico y Redes, hay una actividad operativa que se relaciona con los objetivos del presente plan:

- Gestión para seguridad de la información, que cuenta con presupuesto de S/ 140,000.00.

Los costos relacionados con la implementación del plan, incluyendo hardware, software y asesorías en ISO 27001, serán cubiertos por el presupuesto disponible.

Las actividades programadas para la implementación del **SGSI 1ERA ETAPA** en la UNE EGyV es financiado con cargo al presupuesto institucional de la Oficina de Tecnología de la Información, conforme a lo establecido en el **Plan Operativo Institucional (POI.**
El financiamiento se ejecuta conforme a la normativa vigente y según la **disponibilidad presupuestal**, atendiendo a los requerimientos progresivos que demanda la implementación integral del **SGSI 1ERA ETAPA.**

### 9.3. Otros recursos.

Plataforma de control de versiones de documentos (SharePoint) para la gestión de políticas, procedimientos y registros.

## 10. MONITOREO Y EVALUACIÓN

Para el monitoreo se realizan las actividades descritas en la fase 5 (operación, monitoreo y medición del SGSI) en que se verifican las acciones realizadas durante la implementación de las primeras cuatro fases en base a las directrices de la Norma ISO 27004.

## 11. ANEXO: CRONOGRAMA PARA IMPLEMENTACIÓN Y CERTIFICACIÓN SGSI

| CRONOGRAMA DE IMPLEMENTACIÓN | | | | | MES 1 | | | | MES 2 | | | | MES 3 | | | | MES 4 | | | | MES 5 | | | | MES 6 | | | | MES 7 | | | | MES 8 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| **Descripción del hito** | **Actividades** | **Entregable** | **Días** | **Recursos** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **FASE I: EVALUAR NIVEL DE MADUREZ DE LA ORGANIZACIÓN, RESPECTO A LA EJECUCIÓN DE SUS PROCESOS DENTRO DEL ALCANCE** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Inicio del Proyecto del SGSI – ISO 27001:2022** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Kick off y presentación** | - Reunión inicial del proyecto con el personal involucrado en el proyecto | **Documento de Inicio de Proyecto (Kick off)** | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Entrevistas con el personal** | - Reunión con el personal especialista involucrado en el alcance del SGSI<br>- Presentación del Plan de Proyecto del SGSI de la Organización | **Plan de Proyecto del SGSI aprobado** | 7 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Elaboración del assesment de madurez bajo la norma IS 27001:2022** | - Reunión con el personal especialista involucrado en el alcance del SGSI<br>- Estado Situacional del SGSI en la Organización bajo la ISO 27001/ISO 27002<br>- Análisis de Madurez de las Cláusula y Controles de Seguridad | **Informe de Análisis de Brecha (GAP Analysis) ISO 27001 e ISO 27002** | 60 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| CRONOGRAMA DE IMPLEMENTACIÓN | | | | | MES 1 | | | | MES 2 | | | | MES 3 | | | | MES 4 | | | | MES 5 | | | | MES 6 | | | | MES 7 | | | | MES 8 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| **Descripción del hito** | **Actividades** | **Entregable** | **Días** | **Recursos** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **FASE II: DISEÑO Y ELABORACIÓN DE DOCUMENTOS BASE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE MANERA NTEGRAL** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Implementación estratégica del SGSI – ISO 27001:2022** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **4. Contexto de la Organización** | Análisis de la Matriz FODA, Matriz de Partes interesadas, Mapa de Procesos y Revisión del Alcance del SGSI | **Acta de Alcance del SGSI de la Universidad** | 15 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **5 Liderazgo** | Revisión de Política y Objetivos de Seguridad de la Información, Roles y Responsabilidades, Establecer Comité de Seguridad en la Organización | **Acta de Política del SGSI y Objetivos de Seguridad de la Universidad** | 15 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | **Acta de Comité del SGSI de la Universidad** | 15 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | **Manual de Roles y Responsabilidades de la Universidad** | 15 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE *Alma Máter del Magisterio Nacional* | PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PRIMERA ETAPA | Código: PLA-OTI-003 |
|---|---|---|
| | | VERSIÓN: 1.0 |
| | | Página 30 de 34 |

**CRONOGRAMA DE IMPLEMENTACIÓN**

| Descripción del hito | Actividades | Entregable | Días | Recursos | MES 1 | | | | MES 2 | | | | MES 3 | | | | MES 4 | | | | MES 5 | | | | MES 6 | | | | MES 7 | | | | MES 8 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| **Implementación operativa del SGSI – ISO 27001:2022** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **6 Planificación** | Identificación de Activos de Información, Análisis de Riesgos (Amenazas y Vulnerabilidades), Evaluación de Riesgos (Valoración de Riesgos) y Mapa y Matriz de Riesgos Análisis de Vulnerabilidades y Escaneos Técnicos, Ethical Hacking (Técnicas y Simulación de Phishing) | **Metodología de Gestión de Riesgos de Seguridad de Información de la Universidad** | 30 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | **Informe Técnico de Vulnerabilidades de Seguridad Digital de la Universidad** | 30 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **7 Soporte** | Programa de Capacitación, Matriz de Comunicaciones, Procedimiento de Información Documentada, Lista de registros, Lista de documentos internos y externos | **Plan de Capacitación y Comunicación y Actas de asistencia en SGSI del personal de la Universidad** | 14 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **8 Operación** | Tratamiento de Riesgos (Implementación de Controles) y Declaración de Aplicabilidad (SoA) | **Informe de Gestión de Riesgos y Plan de Tratamiento de Riesgos de Seguridad de Información de la Universidad** | 30 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | **Informe de Declaración de Aplicabilidad (SoA) de la Universidad** | 21 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE *Alma Máter del Magisterio Nacional* | PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PRIMERA ETAPA | Código: PLA-OTI-003 |
|---|---|---|
| | | VERSIÓN: 1.0 |
| | | Página 31 de 34 |

**CRONOGRAMA DE IMPLEMENTACIÓN**

| Descripción del hito | Actividades | Entregable | Días | Recursos | MES 1 | | | | MES 2 | | | | MES 3 | | | | MES 4 | | | | MES 5 | | | | MES 6 | | | | MES 7 | | | | MES 8 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| **Medición y Seguimiento del SGSI – ISO 27001:2022** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **9 Evaluación del desempeño** | Tabla de Indicadores clave de procesos, Procedimiento de Auditoría, Programa de Auditoría, Plan de Auditoría, Revisión por la Dirección | **Informe de Medición del SGSI Plan de Programa y Procedimiento de Auditoría del SGSI** | 36 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **10 Mejora Continua** | Procedimiento de No Conformidades, Formato de tratamiento de no conformidades | **Revisión e Informe de conformidad de la Alta Dirección (Comité del SGSI) de la Universidad** | 14 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE *Alma Máter del Magisterio Nacional* | PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PRIMERA ETAPA | Código: PLA-OTI-003 |
|---|---|---|
| | | VERSIÓN: 1.0 |
| | | Página 32 de 34 |

| CRONOGRAMA DE IMPLEMENTACIÓN | | | | | MES 1 | | | | MES 2 | | | | MES 3 | | | | MES 4 | | | | MES 5 | | | | MES 6 | | | | MES 7 | | | | MES 8 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| **Descripción del hito** | **Actividades** | **Entregable** | **Días** | **Recursos** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **FASE III: DOCUMENTACIÓN, REVISIÓN Y/O ACTUALIZACIÓN DE PROCEDIMIENTOS U OTROS DOCUMENTOS ASOCIADOS AL ANEXO A** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Elaboración o actualización de los documentos relacionados a los controles del anexo A; en base a los objetivos y alcance establecidos. | **Documentos relacionados a: 5 Controles Organizacionales 6 Controles de personal 7 Controles físicos 8 Controles tecnológicos** | **Manual del SGSI Manual de Metodología de Gestión de Riesgos del SGSI** | 60 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE *Alma Máter del Magisterio Nacional* | PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PRIMERA ETAPA | Código: PLA-OTI-003 |
|---|---|---|
| | | VERSIÓN: 1.0 |
| | | Página 33 de 34 |

| CRONOGRAMA DE IMPLEMENTACIÓN | | | | | MES 1 | | | | MES 2 | | | | MES 3 | | | | MES 4 | | | | MES 5 | | | | MES 6 | | | | MES 7 | | | | MES 8 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| **Descripción del hito** | **Actividades** | **Entregable** | **Días** | **Recursos** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **FASE IV: AUDITORÍA INTERNA POR AUDITORES EXTERNOS** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Ejecución de Auditoría Interna | **Informe de Auditoría Interna** | | 7 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Levantamiento de observaciones y no conformidades | **Documentación del SGSI** | | 30 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE *Alma Máter del Magisterio Nacional* | PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PRIMERA ETAPA | Código: PLA-OTI-003 |
|---|---|---|
| | | VERSIÓN: 1.0 |
| | | Página 34 de 34 |

| CRONOGRAMA DE IMPLEMENTACIÓN | | | | | MES 1 | | | | MES 2 | | | | MES 3 | | | | MES 4 | | | | MES 5 | | | | MES 6 | | | | MES 7 | | | | MES 8 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| **Descripción del hito** | **Actividades** | **Entregable** | **Días** | **Recursos** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **FASE V: TRASNFERENCIA DE CONOCIMIENTOS Y ACOMPAÑAMIENTO DURANTE LA AUDITORÍA DE CERTIFICACIÓN (FASE1 Y FASE 2)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Transferencia de conocimiento para el adecuado mantenimiento del SGSI | | **Plan de Capacitación Técnica al personal del SGSI de la Universidad** | 7 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Ejecución de Revisión por la Dirección | | **Acta de Revisión del SGSI por la Alta Dirección (Comité de SGSI) de la Universidad** | 7 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Ejecución de auditoría de certificación | **Auditoría Fase 2 y Fase 3** | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |