"Año de la unidad, la paz y el desarrollo"

RESOLUCIÓN RECTORAL
N° 070-2023-UNAJMA/R

Andahuaylas, 12 de diciembre de 2023

VISTOS: El Informe N° 199-2023-UNAJMA-OTI, de fecha 05 de diciembre de 2023; el Proveído N° 1512-2023-R, de fecha 11 de diciembre de 2023; por el que, la rectora (e) dispone la emisión de la presente con cargo a dar cuenta al Consejo Universitario, y;

CONSIDERANDO:

Que, por **Ley N° 28372** del 29 de octubre de 2004, se crea la Universidad Nacional José María Arguedas con sede en la Provincia de Andahuaylas, Región Apurímac; y por Resolución N° 035-2017-SUNEDU/CD del 02 de octubre de 2017, el Consejo Directivo de la SUNEDU, otorga la Licencia Institucional a la Universidad Nacional José María Arguedas;

Que, la Ley Universitaria, **Ley N° 30220, en su artículo 8,** respecto a la autonomía universitaria, establece que *"El Estado reconoce la autonomía universitaria. La autonomía inherente a las universidades se ejerce de conformidad con lo establecido en la Constitución, la presente Ley y demás normativa aplicable. Esta autonomía se manifiesta en los siguientes regímenes: Normativo, De gobierno, Académico, Administrativo y Económico"*;

Que, en el artículo 60 de la Ley Universitaria, Ley N° 30220, respecto al Rector, establece que "*El Rector es el personero y representante legal de la universidad. Tiene a su cargo y a dedicación exclusiva, la dirección, conducción y gestión del gobierno universitario en todos sus ámbitos, dentro de los límites de la presente Ley y del Estatuto*";

Que, mediante Resolución N° 007-2023-CU-UNAJMA, de fecha 26 de junio de 2023, el Comité Electoral Universitario de la UNAJMA, reconoce al **Dr. Edgar Luis Martínez Huamán**, como Rector, **Dra. Cecilia Edith García Rivas Plata**, Vicerrectora Académica y **Dra. Mery Luz Masco Arriola**, Vicerrectora de Investigación de la Universidad Nacional José María Arguedas;

Que, mediante Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, se establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas;

Que, en el artículo 3 de la precitada Resolución de Secretaría de Gobierno y Transformación Digital se define el Plan de implementación del Sistema de Gestión de Seguridad de la Información como el instrumento que establece, como mínimo, los objetivos, actividades, recursos, responsables y plazos para implementar un SGSI en un periodo máximo de tres (03) años. Es aprobado por la máxima autoridad administrativa o la que haga sus veces en la entidad pública; asimismo, el referido plan debe registrarse en la Plataforma Facilita Perú para conocimiento y evaluación del Centro Nacional de Seguridad Digital;

Que, mediante Informe N° 199-2023-UNAJMA-OTI, de fecha 05 de diciembre de 2023, la Ing. Marusia Rodas Vergara, jefe de la Oficina de Tecnologías de la Información remite al rector de la Unajma, Dr. Edgar Luis Martínez Huamán, el informe para la implementación del Sistema de Gestión de Seguridad de la Información - SGSI en la Unajma y demás acciones, en atención al Oficio Múltiple N° D000031-2023-PCM-SGTD, mediante el cual la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros comunica la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, para lo cual solicita la aprobación mediante acto resolutivo de lo siguiente:

a. Aprobación del Plan de Implementación del Sistema de Gestión de la Seguridad de la Información.
b. Aprobación de las Políticas de Seguridad de la Información en la Unajma.
c. Designación del Oficial de Seguridad y Confianza Digital.
d. Conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT).
e. Conformación del Comité de Gestión de Seguridad de la Información;

"Año de la unidad, la paz y el desarrollo"

RESOLUCIÓN RECTORAL
N° 070-2023-UNAJMA/R

Andahuaylas, 12 de diciembre de 2023

Que, mediante Resolución Rectoral N° 068-2023-UNAJMA/R, de fecha 07 de diciembre de 2023, se encargó las funciones de rector de la Universidad Nacional José María Arguedas a la Dra. Cecilia Edith García Rivas Plata, vicerrectora académica de la institución, por los días lunes 11 y martes 12 de diciembre de 2023;

Que, con Proveído N° 1512-2023-R, de fecha 11 de diciembre de 2023, la Dra. Cecilia Edith García Rivas Plata, rectora (e) de la Unajma dispone al secretario general proyectar la presente resolución con cargo a dar cuenta al Consejo Universitario;

Por estos considerandos y en uso de las atribuciones que le confiere la Ley Nº 30220, Ley Universitaria, y el Estatuto de la Unajma, al rector y con cargo a dar cuenta al Consejo Universitario;

SE RESUELVE:

ARTÍCULO PRIMERO: APROBAR el Plan de Implementación del Sistema de Gestión de Seguridad de la Información de la Universidad Nacional José María Arguedas, presentado por la Oficina de Tecnologías de la Información; que en anexo forma parte de la presente resolución.

ARTÍCULO SEGUNDO: DISPONER el registro del Plan aprobado en el artículo primero de la presente resolución, en la Plataforma Integral de Solicitudes Digitales del Estado Peruano (Facilita Perú).

ARTÍCULO TERCERO: DISPONER la publicación de la presente resolución en el portal de transparencia de la Universidad Nacional José María Arguedas.

ARTÍCULO CUARTO: ENCARGAR a la Oficina de Tecnologías de la Información de la Universidad Nacional José María Arguedas, adoptar las acciones correspondientes para el cumplimiento de la presente resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE.

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
Dra. Cecilia E. García Rivas Plata
RECTORA (e)

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
Abog. Rodney Veliz Montesinos
SECRETARIO GENERAL

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

Oficina de Tecnologías de la Información

Aprobado con Resolución N° 070-2023-UNAJMA/R
Versión N° 1.0

DICIEMBRE - 2023
ANDAHUAYLAS

RECTOR:

Dr. Luis Edgar Martínez Huamán

VICERRECTORADO ACADÉMICO:

Dra. Cecilia Edith García Rivas Plata

VICERRECTORADO DE INVESTIGACIÓN:

Dra. Mery Luz Masco Arriola

ELABORADO POR	REVISADO POR	APROBADO POR
Cargo	**Cargo**	**Cargo del encargado de aprobar documento**
Marusia Rodas Vergara	Nombres y apellidos	Nombres y apellidos
Firma: UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS Ing. Marusia Rodas Vergara JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN	*Firma:* UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS Lic. Adm. Rubén Franklin Fonseca Barboza DIRECTOR GENERAL DE ADMINISTRACIÓN	*Firma:* UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS Dr. Edgar Luis Martínez Huamán RECTOR

1. INTRODUCCIÓN

La información es un valioso activo del que depende el buen funcionamiento de una organización. Mantener su integridad, confidencialidad y disponibilidad es esencial para alcanzar los objetivos de negocio. La información debe considerarse como un recurso con el que cuentan las Organizaciones y por lo tanto tiene valor para éstas, al igual que el resto de los activos, debe estar debidamente protegida.

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un sistema que nos permite tener una herramienta de gestión que nos ayuda a conocer, gestionar, y minimizar los posibles riesgos que atenten contra la seguridad de la información en la Organización.

Mediante Resolución Ministerial Nº 004-2016-PCM del 8 de enero del 2016, se aprobó el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001 :2014 2ª. Edición (que reemplaza a la NTP-ISO/IEC 27001 :2008) en todas las entidades integrantes del Sistema Nacional de Informática del Estado Peruano. Esta NTP provee un modelo para implementar los principios en las pautas que gobiernan la evaluación del riesgo, el diseño e implementación de la seguridad, la gestión de seguridad y la reevaluación de la información en una institución.

A través de la implementación del SGSI de la Universidad Nacional José María Arguedas, se mantendrá una adecuada gestión de la seguridad de la información logrando los objetivos de seguridad organizacionales, y por tanto, logrará mantener la integridad, disponibilidad y confidencialidad de la información más crítica de los procesos que forman parte del alcance del SGSI.

2. OBJETIVO GENERAL

Implementar un Sistema de Gestión de Seguridad de la Información – SGSI que permita identificar las vulnerabilidades y amenazas que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información en la Universidad Nacional José María Arguedas.

3. ALCANCE

El presente plan aplica a todas las dependencias de la Universidad Nacional José María Arguedas, involucradas en la implementación del SGSI.

4. BASE LEGAL

4.1 Ley Nº 27658, Ley Marco de la Modernización de la Gestión del Estado.
4.2 Ley Nº 29733, Ley de Protección de Datos Personales y su reglamento, aprobado mediante Decreto Supremo Nº 003-2013.JUS.
4.3 Decreto Legislativo N°1412, Ley de Gobierno Digital
4.4 Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece las tecnologías y medios electrónicos en el procedimiento administrativo.

4.5 Decreto de Urgencia N° 006-2020 que crea el Sistema Nacional De Transformación Digital.

4.6 Decreto de Urgencia N° 007-2020 que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

4.7 Resolución Ministerial Nº 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnologías de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2da Edición. En todas las entidades integrantes del Sistema Nacional de Informática.

4.8 Resolución de Consejo Universitario Nº 067-2023-UNAJMA/CU, que aprueba la designación del Comité de Gobierno Digital de la Universidad Nacional José María Arguedas

5. GLOSARIO DE TÉRMINOS

5.1. Activo 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 comunicaciones, la imagen de la entidad, la Información como activo corporativo, puede existir de muchas formas (impresa, almacenada electrónicamente, transmitida por medios electrónicos, mostrada en videos, suministrada en una conversación, conocimiento de las personas).

5.2. Amenazas: fuentes generadoras de eventos en las que se originan las pérdidas por riesgos de seguridad de la información.

5.3. Análisis de riesgo: método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

5.4. Auditoria: proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permite determinar la extensión en que se cumplen los criterios definidos para la auditoria interna.

5.5. Auditor en seguridad de la información: persona con la competencia para efectuar auditorías internas de seguridad de la información.

5.6. Control: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de la organización.

5.7. Declaración de Aplicabilidad: documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la entidad.

5.8. Disponibilidad: la información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para el uso;

la no disponibilidad de la información puede resultar en pérdidas financieras de imagen y/o credibilidad ante los clientes y/o ciudadanos.

5.9. **Efectividad:** medida de impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.

5.10. **Eficacia:** grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

5.11. **Estimación de riesgo:** proceso de asignación de valores a la probabilidad e impacto de un riesgo.

5.12. **Evento de seguridad de la información**: presencia identificada de una condición de un bien o recurso (sistema, servicio, red, etc), asociada a una posible vulneración de la política de seguridad de la información.

5.13. **Evidencia de auditoria:** registro, declaración de hechos o cualquier otra información que son relevantes para los criterios de auditoria y que son verificables. La evidencia de la auditoria puede ser cuantitativa o cualitativa.

5.14. **Gestión de riesgo**: actividades coordinadas para dirigir y controlar los aspectos asociados al riesgo dentro de una organización.

5.15. **Identificación del riesgo:** proceso para encontrar, numerar y caracterizar los elementos de riesgo asociadas a la seguridad de la información.

5.16. **Impacto:** se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos de la organización.

5.17. **Incidente de seguridad de la información:** un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones de la organización y amenazar la seguridad de la información.

5.18. **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, necesita una protección adecuada.

5.19. **Integridad:** la información de la UNAJMA debe ser clara y completa y solo podrá ser modificada por las personas expresamente autorizadas para ello. La falta de integridad de la información puede exponer a la entidad a toma de decisiones incorrectas..

5.20. **Probabilidad:** es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

5.21. Proceso: conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y cuales transforman elementos de entrada en resultados.

5.22. Propietario de información: es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones de acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. El término "Propietario" no implica que la persona tenga realmente los derechos de propiedad de los activos.

5.23. Reducción de riesgo: acciones que se toman para disminuir la probabilidad y/o el impacto negativo asociado a un riesgo.

5.24. Responsabilidades: compromisos u obligaciones del personal o grupo de trabajo.

5.25. Riesgo: consecuencias que pueden ser generadas por las amenazas asociadas a la seguridad de la Información en los activos de la UNAJMA.

5.26. Riesgo en seguridad de la Información: es la probabilidad de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando daño a la UNAJMA.

5.27. Seguridad de la Información: Preservación de la integridad, la confidencialidad, y la disponibilidad de la Información; además puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad. (Fuente: NTP ISO/IEC 270001:2014).

5.28. SGSI: Sistema de Gestión de Seguridad de la Información.

5.29. Transferencia de riesgo: compartir con otra de las partes la perdida (consecuencias negativas) de un riesgo.

5.30. Tratamiento de la Información: desarrollo de las siguientes actividades sobre la Información, sin limitarse a ellas: creación, acceso, inclusión, exclusión, corrección, comunicación, divulgación, publicación, cesión, eliminación y certificación; por cualquier medio oral, digital y/o escrito, conocido o por conocer.

5.31. Tratamiento del riesgo: proceso de selección e implementación de medidas para modificar el riesgo.

5.32. Usuario: cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice Información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de Información de la UNAJMA, para propósitos propios

de su labor y que tendrá el derecho manifiesto de uso dentro del inventario de Información.

5.33. Vulnerabilidades: debilidad de un activo de Información frente a una amenaza.

5.34. Conformidad: cumplimiento de un requisito.

6. DOCUMENTACIÓN DEL GSI

Durante la implementación del Sistema de Gestión de Seguridad de la Información SGSI, se redactarán los siguientes documentos, sin perjuicio de otros que consideren pertinentes:

Nº	Norma Técnica Peruana NTP ISO/IEC 27001:2014	Documento	Descripción
1	**Clausula 7.5** Información documentada	Procedimiento para la gestión de documentos y registros	Documento que establece los lineamientos para la elaboración, probación, distribución y actualización de los documentos y registros relacionados al SGSI
2	**Clausula 4.1** Comprender la organización y su contexto y la **Cláusula 4.2** Comprender las necesidades y expectativas de las partes interesadas	Análisis de contexto y requerimiento de seguridad de las partes interesadas	Documento que establece el contexto interno y externo de la UNAJMA y para asegurar que el SGSI está alineado con los objetivos institucionales y cumpla con las obligaciones legales y normativas relacionadas a la seguridad de la información.

3	**Clausula 4.3** determinar el alcance del SGSI	Alcance y límites del SGSI	Documento que define en forma precisa la ubicación, la tecnología y los activos que forman parte del alcance de la implementación del SGSI
4	**Clausula 5.1** Liderazgo y compromiso y la **Cláusula 5.2** Política.	Política y objetivos de la seguridad de la información	Documento clave que establece el marco normativo para gestionar la seguridad de la información en la UNAJMA.
5	**Clausula 5.3** Roles, autoridad y responsabilidad organizacionales	Roles y Responsabilidades del SGSI	Documento que define la estructura organizacional para la dirección, gestión y operación de la seguridad de la información en la UNAJMA.
6	**Clausula 6.1** Acciones para tratar los riesgos y las oportunidades	Metodología de la Gestión de Riesgos	Documento que describe los métodos y parámetros para la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la
7	**Clausula 6.1.2** Valoración del Riesgo de Seguridad de la Información.	Cuadro de análisis y evaluación de riesgos	Documentación resultante del análisis y la evaluación de los riesgos de seguridad de la información
8		Cuadro de tratamiento de riesgos	Documentación que establece los controles de seguridad que se deben implementar para
9		Informe sobre el resultado de la gestión de riesgos y el tratamiento de los riesgos	Documento que incluye los documentos generados en el proceso de gestión de riesgos.

10	**Clausula 6.1.3** Tratamiento de riesgos de seguridad de la información.	Declaración de Aplicabilidad	Documento que contiene los controles del Anexo A de la NTP ISO/IEC 27001:2014 y justifica la inclusión o exclusión de su implementación.
11		Plan de tratamiento de riesgos	Documento que especifica un plan de trabajo priorizado de los controles que deben implementarse como resultado de la gestión de riesgos. Además de especificar los otros documentos que requieren para evidenciar la conformidad con la NTP ISO/IEC 27001:2014.
	Clausula 7.3 Concientización	Plan de Concientización en Seguridad de la Información	Documento que especifica un plan de formación en seguridad de la información.
	Clausula 9.1 Monitoreo, medición, análisis y evaluación.	Procedimiento de medición y monitoreo del SGSI	Documento que describe el proceso para evaluar el cumplimiento de los indicadores establecidos para el SGSI.
	Cláusula 9.2 Auditoria interna	Procedimiento de auditoria interna	Documento que describe como se realizara la auditoria interna y se informara el resultado de la misma.
	Clausula 9.3 Revisión de la gerencia.	Procedimiento de la revisión por la gerencia	Documento que describe como se realizara la revisión por la Alta Dirección para asegurar la eficacia y efectividad del SGSI.

	Cláusula 10.1 No conformidades y acción correctiva	Procedimiento de acciones correctivas del SGSI	Documento que describe el proceso de implementación de las acciones correctivas y preventivas, así como los formatos a emplear.

7. ORGANIZACIÓN PARA LA IMPLEMENTACIÓN DEL SGSI

7.1. RESPONSABLE DEL PROYECTO SGSI

Oficial de Seguridad de la Información

7.2. EQUIPO DE TRABAJO

Comité del SGSI, según Resolución Ministerial Nº 166-2017-PCM deberá ser conformado por:

- Titular de la entidad.
- Director General de Administración.
- Director de la Oficina de Planeamiento y Presupuesto.
- Director de la Oficina de Tecnologías de la información.
- Director de la Oficina de Asesoría Legal.
- Oficial de Seguridad de la Información de la UNAJMA.

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS – ANDAHUAYLAS – OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

8. RIESGOS IDENTIFICADOS PARA LA IMPLEMENTACIÓN DEL SGSI

La implementación del SGSI contribuye al cambio de cultura organizacional en todos los niveles de la Institución.

A continuación, se detalla los principales riesgos que se pueden identificar en la implementación del SGSI y las acciones de mitigación, a fin de lograr el éxito del mismo.

Riesgos	Acciones de Mitigación
Cambio de los funcionarios de	• La Alta Dirección dará continuidad a la ejecución de los planes aprobados. • La Alta Dirección establecerá una política y objetivos de Seguridad de la Información que incluya el compromiso de satisfacer los requisitos aplicables relacionados a la seguridad de la información.

Ampliación de plazos de la ejecución del Plan, al no contar con requisitos mínimos para la implementación de la NTP ISO/IEC 27001:2014.	Que el coordinador del plan cuente con las competencias técnicas para la implementación de la NTP ISO/IEC 27001:2014. Así mismo que los miembros del comité promuevan e impulsen los documentos correspondientes.
Falta de compromiso del personal de la Universidad Nacional José María Arguedas respecto a la importancia de la seguridad de la información.	Se deben formular y llevar a cabo actividades de concientización relacionadas a seguridad de la información en la Universidad Nacional José María Arguedas, las cuales deberán ser establecidas en el plan de concientización.
Ampliación de plazos en la presentación y aprobación de documentos oficiales (evidencia legal)	El coordinador de la implementación del SGSI supervisara que todas las actividades sean realizadas dentro de los plazos definidos y solicitara a tiempo la intervención del patrocinador.

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS - ANDAHUAYLAS
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

9. ACCIONES PREVIAS Y PERMANENTES

9.1. Para el inicio de la implementación del SGSI

9.1.1. **Compromiso de la Alta Dirección:** con la finalidad de respaldar al equipo y las medidas aprobadas en el Comité de Gobierno Digital.

9.1.2. **Análisis de brechas de seguridad de la Información:** con la finalidad de determinar la distancia que existe entre la organización actual de la seguridad de la información y lo establecido en la NTP ISO/IEC 27001:2014.

9.1.3. **Fortalecimiento de capacidades del coordinador del plan en los siguientes temas:**

- ISO 27001.
- ISO 31000.
- ISO 22301

9.2. Durante la implementación del SGSI

9.2.1. **Realización de Ethical Hacking:** en intervalos de mínimo de tres meses para determinar vulnerabilidades o intrusión a los sistemas informáticos.

9.2.2. **Auditoría informática especializada:** que permita establecer indicadores de cumplimiento y de gestión.

9.2.3. **Fortalecimiento de capacidades:** de los participantes claves en los siguientes temas:

- Seguridad de la Información.
- Ethical hacking.
- Protección de datos personales

10. HERRAMIENTAS DE APOYO AL SGSI

- El contenedor de los documentos del SGSI: mediante una carpeta compartida (creada en el servidor de archivos de la UNAJMA) o mediante un sistema de gestión documental, se tendrá disponible los archivos generados en cada una de las etapas de implementación.
  Todos los miembros del equipo del proyecto tendrán acceso a esos documentos. Sólo el gerente del proyecto y miembros del equipo del proyecto estarán autorizados a realizar modificaciones y borrado archivos.
- Software ofimático, para elaboración de documentos del SGSI.
- Software para la gestión de riesgos de seguridad de la información, según corresponda.
- Entrevistas en sitio, según corresponda.
- Cuestionarios según corresponda.

11. METODOLOGÍA

Para la implementación del SGSI se empleará la metodología PDCA (Plan-Do-Check-Act), también llamada ciclo de DEMING, que impulsa al mejoramiento continuo de procesos y consiste en los siguientes pasos:

- Planear (PLAN): Reconocer una oportunidad y planificar el cambio.
- Hacer (DO): Probar el cambio.
- Verificar (CHECK): Revisar la prueba, analizar los resultados e identificar lo aprendido.
- Actuar (ACT): tomar acción basada en las lecciones aprendidas. Si el cambio fue exitoso, incorporar lo aprendido, de lo contrario intentar un plan diferente.

12. PRESUPUESTO PARA EJECUTAR

El presupuesto para la ejecución del plan de implementación del SGSI será considerada dentro del Plan Operativo Institucional.

13. CRONOGRAMA DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 2024-2025

FASE/OBJETIVO	ACTIVIDADES	DETALLE DE ACTIVIDADES	2024			2025			
			Abr-Mayo	Jun-Ago	Set-Dic	Ene-Mar	Abr-Jul	Ago-Oct	Nov-Dic
FASE I ORGANIZACIÓN Desarrollar las actividades principales para la dirección e inicio de la implementación del SGSI	Desarrollo o evaluación de documentos requeridos para el Sistema de Gestión de Seguridad de la Información.	1. Procedimiento para la gestión de documentos y registros	X						
FASE II PLANIFICACIÓN (PLANEAR) desarrollar las actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos del SGSI dentro del alcance del mismo.	Evaluación del alcance del sistema de Gestión de Seguridad de la información	2. Reformulación del análisis de contexto y requerimiento de seguridad de las partes interesadas.		X					
		3. Reformulación del alcance y límites del SGSI.		X					
	Declaración de la política y los objetivos de seguridad de la información.	4. Reformulación de la política y objetivos de seguridad de la información.		X					

ISO 9001:2015

ISO 21001:2018

		5. Reformulación de los roles y responsabilidades del SGSI.		X					
	Definición de los criterios para la evaluación y aceptación de riesgos.	6. Metodología de gestión de riesgos		X					
	- Evaluación de riesgos. - Análisis entre los riesgos identificados y las medidas correctivas existentes.	7. Inventario de activos de información.			X				
		8. Cuadro de análisis y evaluación de riesgos.			X				
		9. Cuadro de tratamiento de riesgos.			X				
		10. Informe sobre el resultado de la gestión de riesgos y el tratamiento de los riesgos.			X				
	- Desarrollo de un plan de tratamiento de riesgos	11. Plan de tratamiento de riesgos.			X				

	- Desarrollo de la declaración de aplicabilidad - Elaboración del plan de trabajo priorizado	12. Plan de concientización en seguridad de la información.			X				
		13. Declaración de aplicabilidad			X				
		14. Plan de trabajo priorizado, aprobado por los propietarios de los riesgos.			X				
FASE III DESPLIEGUE (HACER) Desplegar las actividades de implementación del SGSI	- Desarrollo de documentos y registros necesarios. - Implementación de los controles seleccionados del plan de tratamiento de riesgos. - Fortalecimiento de la gestión de incidentes	15. Políticas específicas para la seguridad de la información.				X			
		16. Plan de tratamiento de riesgos implementado.				X			
		17. Procedimiento de gestión de incidentes de seguridad de la información.				X			
		18. Plan de concientización en seguridad de la Información implementado				X			
FASE IV REVISION (VERIFICAR)	Monitoreo del desempeño del SGSI	19. Informe de los resultados de la medición y monitoreo del SGSI.					X		

Realizar actividades de revisión del SGSI evidenciando el cumplimiento de los requisitos de la NTP ISO/IEC 27001:2014.		20. Informe de la revisión de la dirección					X		
	Auditoria interna del SGSI	21. Programa de auditoria interna					X		
		22. Informe de los resultados de la auditoria interna					X		
FASE V CONSOLIDACIÓN (ACTUAR) Implementar las mejoras y correcciones del SGSI a fin de cumplir con los requisitos de la NTP ISO/IEC 27001:2014.	Implementación de acciones correctivas y preventivas	23. Plan de acciones correctivas y preventivas.						X	
	- Desarrollo, corrección y mejora de la documentación del SGSI nueva y existente	24. Informe de resultados de las acciones correctivas implementadas.							X
	- Desarrollo de las actividades para evidenciar la mejora continua del SGSI	25. Planes de mejora continua.							X

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
ANDAHUAYLAS