



Universidad Nacional de Juliaca

"Año de la Esperanza y el Fortalecimiento de la Democracia"

RESOLUCIÓN DE CONSEJO UNIVERSITARIO **Nº 636 - 2026-CU-UNAJ**

Juliaca, 04 de agosto de 2026.

VISTOS:

La Carta N° 000136-2026-UNAJ/OTI, de fecha 23 de abril de 2026; Informe N° 000025-2026-UNAJ/UPM, de fecha 07 de mayo de 2026; Informe Legal N° 000271-2026-UNAJ/OAJ, de fecha 11 de mayo de 2026; Acuerdo de Sesión Extraordinaria de Consejo Universitario, de fecha 24 de julio de 2026; y,

CONSIDERANDO:

Que, conforme a lo dispuesto por el Art. 18°, 4to párrafo de la Constitución Política del Estado, cada Universidad es autónoma en su régimen normativo de gobierno, académico, administrativo y económico. Las Universidades se rigen por sus propios estatutos en el marco de la constitución y las leyes;

Que, la Ley Universitaria Ley N° 30220, en su Art. 8°, 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, mediante Resolución de Consejo Universitario N° 001-2025-CU/UNAJ, se oficializa la elección de la Dra. Vilma Sarmiento Mamani como Rectora de la Universidad Nacional de Juliaca; 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 establecidos por la Ley Universitaria N° 30220 y del Estatuto;

Que, mediante Carta N° 000136-2026-UNAJ/OTI, de fecha 23 de abril de 2026, la Oficina de Tecnologías de la Información, solicita la APROBACIÓN DE LA POLÍTICA Y EL MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD NACIONAL DE JULIACA, precisa además que estos documentos han sido elaborados con el objetivo de establecer lineamientos claros que permitan proteger la confidencialidad, integridad y disponibilidad de la información institucional. Asimismo, buscan fortalecer las buenas prácticas en el manejo de la información, reducir riesgos y asegurar el cumplimiento de las normativas vigentes. La implementación de esta política y su respectivo manual contribuirá significativamente a mejorar la gestión de la seguridad de la información en la universidad, promoviendo una cultura organizacional basada en la protección de los activos de información;

Que, mediante Informe N° 000025-2026-UNAJ/UPM, de fecha 07 de mayo de 2026, la Unidad de Planeamiento y Modernización emite opinión técnica de la POLÍTICA Y EL MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD NACIONAL DE JULIACA, y concluye indicando que la Política y el Manual de Gestión de Seguridad de la Información para la Universidad Nacional de Juliaca, elaborado por la Oficina de Tecnología de Información se encuentra en el marco de sus competencias según el Reglamento de Organización y Funciones (ROF), se encuentra alineado al Plan Estratégico Institucional (PEI) 2025-2030; representa un instrumento que facilita su uso, por tanto, resulta viable continuar con el trámite administrativo para su aprobación;

Que, mediante Informe Legal N° 000271-2026-UNAJ/OAJ, de fecha 11 de mayo de 2026, la Oficina de Asesoría Jurídica, realizando la revisión y análisis de los actuados, concluye indicando que resulta viable la aprobación del "MANUAL GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN VERSIÓN 1.0" y "POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD", estando acorde a la autonomía universitaria en su régimen normativo;

Que, en Sesión Extraordinaria de Consejo Universitario de fecha 24 de julio de 2026, el Consejo Universitario, acuerdan por **UNANIMIDAD: APROBAR** la Política de Seguridad de la Información y del Manual de Gestión de Seguridad de la Información de la Universidad Nacional de Juliaca;

En uso de las facultades y atribuciones conferidas por el artículo 18° de la Constitución Política del Perú, el artículo 59° de la Ley N° 30220-Ley Universitaria; Art. 27 del Estatuto Universitario;

SE RESUELVE:

Artículo Primero. - APROBAR la POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD y el MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN de la Universidad Nacional de Juliaca, los cuales como anexo forman parte del presente acto resolutivo.

Artículo Segundo. - DISPONER que la Oficina de Tecnologías de la Información, publique el presente acto resolutivo en el portal web de la institución (www.unaj.edu.pe).

Regístrese, comuníquese y cúmplase.



DISTRIBUCIÓN:
RDO.
VRAC.
VRIN.
DGA.
URH.
OTI.
Arch. /2026.



MANUAL GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Versión 1.0



Firmado digitalmente por VARGAS
CANCINO Henry FAU 20448261272
soft
Motivo: Soy el autor del documento
Fecha: 23.04.2026 17:27:49 -05:00

OFICINA DE TECNOLOGÍA
DE LA INFORMACIÓN



 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 2 de 51

ÍNDICE GENERAL

I.	OBJETO Y CAMPO DE APLICACIÓN	3
II.	REFERENCIAS NORMATIVAS	3
III.	TÉRMINOS Y DEFINICIONES	5
IV.	RESPONSABLES.....	6
V.	CONTENIDO.....	6
VI.	ANEXOS.....	35
	ANEXO N° 01	
	MAPA DE PROCESOS.....	36
	ANEXO N°02	
	MATRIZ DE NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	37
	ANEXO N°03	
	ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	38
	ANEXO N°04	
	PARTICIPACIÓN DE LOS PROCESOS ESTRATÉGICOS Y DE SOPORTE EN EL SGSI.....	39
	ANEXO N°05	
	FICHA TÉCNICA DE PROCESO	40
	ANEXO N° 06	
	FICHA TÉCNICA DEL INDICADOR	41
	ANEXO N° 07	
	ACUERDO DE PARTES.....	42
	ANEXO N°08	
	MATRIZ DE PLANIFICACIÓN DE OBJETIVOS E INDICADORES	43
	ANEXO N°09	
	SOLICITUD DE CAMBIO	44
	ANEXO N°10	
	MATRIZ DE REQUISITOS DE COMPETENCIAS POR ROLES	45
	ANEXO N°12	
	LISTA MAESTRA DE DOCUMENTOS	47
	ANEXO N°13	
	LISTA DE DISTRIBUCIÓN DE DOCUMENTOS	48
	ANEXO N°14	
	ACTA DE ELIMINACIÓN	49
	ANEXO N°15	
	RESULTADO DEL INDICADOR	50
	ANEXO N°16	
	CUADRO DE MANDO OPERATIVO	51

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 3 de 51

I. OBJETO Y CAMPO DE APLICACIÓN

Especificar los elementos principales del **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** (SGSI) de la Universidad Nacional de Juliaca en adelante UNAJ, con el fin de que los procesos incluidos en su alcance cumplan los requisitos establecidos en la norma internacional ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información. Requisitos.

II. REFERENCIAS NORMATIVAS

- 2.1 Constitución Política del Perú**, del 30 de diciembre de 1993.
- 2.2 Ley N° 29074**, Ley de Creación de la Universidad Nacional de Juliaca.
- 2.3 Ley N° 29733**, Ley de Protección de Datos Personales, del 03 de julio de 2011 y sus modificatorias.
- 2.4 Ley N° 27269**, Ley de Firmas y Certificados Digitales, del 28 de mayo de 2000 y sus modificatorias.
- 2.5 Decreto de Urgencia N° 006-2020**, crea el Sistema Nacional de Transformación Digital, del 09 de enero de 2020.
- 2.6 Decreto Legislativo N° 1412**, aprueba la Ley de Gobierno Digital, del 13 de setiembre de 2018.
- 2.7 Decreto Supremo N° 052-2008-PCM**, aprueba el Reglamento de la Ley N° 27269 - Ley de Firmas y Certificados Digitales, del 19 de julio de 2008, y modificatoria.
- 2.8 Decreto Supremo N° 070-2011-PCM**, modifica el Reglamento de la Ley N° 27269 – Ley de Firmas y Certificados Digitales, y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo N° 681 y ampliatorias, del 27 de julio de 2011.
- 2.9 Decreto Supremo N° 105-2012-PCM**, establecen disposiciones para facilitar la puesta en marcha de la firma digital y modifica el Decreto Supremo N° 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales, del 21 de octubre de 2012.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 4 de 51

- 2.10 Decreto Supremo N° 003-2023-JUS**, aprueba el Reglamento de la Ley de Protección de Datos Personales, del 22 de marzo de 2013.
- 2.11 Decreto Supremo N° 026-2016-PCM**, aprueban medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado, del 29 de abril de 2016.
- 2.12 Decreto Supremo N° 004-2019-JUS**, Texto Único Ordenado de la Ley N° 27444, Ley de Procedimiento Administrativo General, del 25 enero de 2019.
- 2.13 Decreto Supremo N° 029-2021-PCM**, aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de tecnologías de medios electrónicos en el procedimiento administrativo, del 19 de febrero de 2021.
- 2.14 Decreto Supremo N° 157-2021-PMC**, aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, del 25 de setiembre de 2021.
- 2.15 Resolución Ministerial N° 119-2018-PCM**, aprueba la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública, del 08 de mayo de 2018, modificada mediante Resolución Ministerial N°087-2019-PCM, del 19 de marzo de 2019.
- 2.16 Resolución Directoral N° 014-2018-INACAL/DN**, aprueba la Norma Técnica Peruana NTP-ISO 31000:2018 Gestión del Riesgo – Directrices 2a Edición, del 02 de Julio de 2018.
- 2.17 Resolución Directoral N° 047-2018-INACAL/DN**, aprueba la Norma Técnica Peruana NTP-ISO 19011:2018 Directrices para la Auditoría de los Sistemas de Gestión. 3ªEdición, del 16 de enero de 2019.
- 2.18 Resolución Directoral N° 022-2022-INACAL/DN**, aprueba la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ªEdición. Reemplaza a la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, del 29 de diciembre de 2022.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 5 de 51

2.19 Resolución Directoral N° 022-2022-INACAL/DN, aprueba la Norma Técnica Peruana NTP-ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición. Reemplaza a la Norma Técnica Peruana NTP-ISO/IEC 27002:2017, del 29 de diciembre de 2022.

2.20 Resolución Directoral N° 022-2022-INACAL/DN, aprueba la Norma Técnica Peruana NTP-ISO/IEC 27005:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición. Reemplaza a la Norma Técnica Peruana NTP-ISO/IEC 27005:2018, del 29 de diciembre de 2022.

2.21 Resolución de Secretaría de Gobierno Digital N° 004-2018-PCM/SEGDI, aprueba los lineamientos del Líder del Gobierno Digital, del 22 de diciembre de 2018.

2.22 Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD, que aprueba la Directiva N°001-2023-PCM/SGTD, donde establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital, del 06 de setiembre de 2023.

2.23 Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que aprueba la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas, 06 de setiembre de 2023.

2.24 Norma Internacional ISO/IEC 27000:2018 “Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Visión general y vocabulario”, de febrero de 2018.

III. TÉRMINOS Y DEFINICIONES

3.1 Las definiciones de los términos relacionados a la gestión de la seguridad de la información utilizadas en este documento se encuentran en la Norma Internacional **ISO/IEC 27000 Sistemas de Gestión de Seguridad de la Información – Términos, Definiciones – Vocabulario**.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión:	1.0
		Fecha:	23/04/2026
		Página:	Página 6 de 51

3.2 Abreviaciones

Dentro del presente manual podrán utilizarse las siguientes abreviaciones:

ABREVIATURA	DESCRIPCIÓN DE LA ABREVIATURA
CGTD	Comité de Gobierno y Transformación Digital
CNSD	Centro Nacional de Seguridad Digital
CSCD	Coordinador de Seguridad y Confianza Digital
GIR	Gestión Integral de Riesgos
GO	Gestión de Oportunidades
ISO	International Organization for Standardization (Organización Internacional de Estandarización)
IEC	International Electrotechnical Commission (Comisión Electrotécnica Internacional)
NTP	Norma Técnica Peruana
PCM	Presidencia de Consejo de Ministros
PGO	Plan de Gestión de Oportunidades
PGIR	Plan de Gestión Integral de Riesgos
ROF	Reglamento de Organización y Funciones
SGSI	Sistema de Gestión de la Seguridad de la Información

IV. RESPONSABLES

El presente manual es gestionado por la Oficina de Tecnologías de Información, a través del Oficial de Seguridad y Confianza Digital y es de aplicación obligatoria a todos los órganos y unidades orgánicas que se encuentran dentro del alcance del SGSI de la UNAJ.

V. CONTENIDO

5.1 CONTEXTO DE LA ORGANIZACIÓN

5.1.1 Comprender la organización y su contexto

La Universidad Nacional de Juliaca (UNAJ) es una universidad pública ubicada en la ciudad de Juliaca, provincia de San Román, departamento de Puno, Perú, creada por la Ley N° 29074 el 25 de julio de 2007.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 7 de 51

La UNAJ desarrolla actividades académicas y de investigación en áreas de ingeniería, procesos industriales, gestión pública y emprendimiento empresarial, entre otras, a través de diversas escuelas profesionales. Como institución universitaria pública, goza de autonomía académica, normativa, administrativa y económica, dentro del marco de la Constitución y la Ley Universitaria.

Esto genera un entorno favorable para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado a ISO/IEC 27001.

CONTEXTO EXTERNO RELEVANTE PARA LA SEGURIDAD DE LA INFORMACIÓN

a) Entorno normativo y regulatorio

La UNAJ está sujeta a la regulación de la SUNEDU en materia de licenciamiento institucional y cumplimiento de Condiciones Básicas de Calidad.

Debe cumplir además con el marco legal peruano en protección de datos personales, transparencia y acceso a la información pública, contrataciones del Estado y normativa de gobierno digital aplicable a entidades públicas.

Como universidad pública, está expuesta al control de entidades como la Contraloría General de la República y otros órganos de supervisión y fiscalización, que pueden requerir información física y digital.

b) Entorno geográfico y tecnológico

Juliaca es el principal centro económico de la región Puno y un nodo de comunicaciones relevante, con alta conectividad en telecomunicaciones e Internet a nivel regional.

Este nivel de conectividad favorece la digitalización de procesos académicos y administrativos, pero también expone a la Universidad a

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 8 de 51

amenazas propias del ciberespacio (ataques a servicios en línea, robo de información, etc.).

La ubicación en la zona altoandina puede generar riesgos físicos específicos (cortes eléctricos, fallas en comunicaciones por condiciones climáticas), que deben considerarse en la continuidad del negocio y en la disponibilidad de los servicios TI.

c) Entorno social y educativo

Juliaca concentra una población estudiantil importante y diversas instituciones de educación superior, lo que intensifica el intercambio de información entre instituciones, estudiantes y proveedores de servicios educativos.

El incremento de servicios educativos virtuales, plataformas de aprendizaje y trámites en línea demanda mayores niveles de protección de datos personales y académicos.

3. Contexto interno

a) Naturaleza de los activos de información

La UNAJ gestiona grandes volúmenes de información, entre ellos:

- Datos personales de postulantes, estudiantes, egresados, docentes y personal administrativo.
- Información académica (notas, historial académico, investigaciones, tesis, contenidos de aula virtual).
- Información administrativa y financiera (presupuesto, logística, recursos humanos, contrataciones, convenios).
- Información de investigación y proyectos, algunos de ellos con resultados sensibles o con propiedad intelectual.
- Estos activos se soportan en sistemas de información institucionales (SIAC, sistemas de matrícula, repositorios digitales, correo institucional, plataformas LMS, sistemas contables y administrativos, etc.).

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 9 de 51

b) Modelo de operación y madurez en gestión

La universidad se encuentra en proceso de consolidación de su modelo educativo, de gestión académica y administrativa.

La gestión de TI y de seguridad de la información se encuentra en etapa de formalización: pueden existir procedimientos y controles aislados (respaldos, control de accesos, uso de antivirus), pero aún no articulados dentro de un SGSI integral.

c) Cultura organizacional y capacidades

El nivel de conocimiento en temas de seguridad de la información es heterogéneo entre docentes, estudiantes y personal administrativo.

Es probable que se utilicen múltiples herramientas y servicios en la nube (correo personal, aplicaciones de mensajería, almacenamiento externo) que no siempre se alinean a las políticas institucionales, generando riesgos adicionales.

La rotación de autoridades universitarias y de responsables de áreas puede impactar la continuidad de las iniciativas de seguridad, si no se formalizan adecuadamente en normas internas.

5.1.2 Comprender las necesidades y expectativas de las partes interesadas.

Los procesos que componen el SGSI de la universidad, identifican y priorizan sus partes interesadas, así como las necesidades y expectativas de estas, según lineamiento establecido por la OPP.

Esta información se registra en el formato que se aprecia en el **Anexo N°02 “Matriz de Necesidades y Expectativas de las Partes Interesadas”**, se prevé revisarla al menos con frecuencia anual y/o cuando sea pertinente.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 10 de 51

5.1.3 Determinar el alcance del Sistema de gestión de seguridad de la información.

Para determinar el alcance del SGSI de la Universidad se utiliza el **Anexo N°03 “Alcance del Sistema de Gestión de Seguridad de la Información”**, el cual es aprobado y difundido por la Alta Dirección.

5.1.4 Sistema de gestión de seguridad de la información

La UNAJ aplica la gestión por procesos, lo cual permite lograr un sistema de trabajo enfocado a la mejora continua del funcionamiento de las actividades de la organización mediante la identificación de procesos y la mejora de los mismos. Actualmente, la UNAJ cuenta con procesos misionales, procesos estratégicos y procesos de soporte, como se aprecia en el Mapa de Procesos que se muestra en el **Anexo N°01 “Mapa de Procesos Niveles 0 – Universidad Nacional de Juliaca”**.

Los procesos estratégicos y de soporte del SGSI son de responsabilidad de los órganos institucionales que se detallan en el **Anexo N°04 “Participación de los Procesos Estratégicos y de Soporte en el SGSI”**.

En el formato **Anexo N°05 “Ficha Técnica de Proceso”**, se detalla las características de los procesos e interacciones. Asimismo, las características de los indicadores son descritas en el **Anexo N°06 “Ficha Técnica de Indicador”**.

Las responsabilidades y autoridades de cada órgano y unidad orgánica se describen en el ROF, así como en documentos propios de cada proceso.

Los riesgos y oportunidades de los procesos son abordados aplicando la **“Metodología de Gestión de Riesgos de Seguridad de la Información”**.

Adicionalmente, con la finalidad de establecer requisitos para el desempeño de los procesos de soporte pueden suscribirse **“Acuerdo**

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 11 de 51

de Partes” con los procesos comprendidos en el SGSI, en el que se describan las especificaciones adicionales y condiciones para la prestación del soporte, cuyo formato se aprecia en el **Anexo N°07**.

5.2 LIDERAZGO

5.2.1 Liderazgo y compromiso

La Alta Dirección evidencia su liderazgo y compromiso con el SGSI, a través de las actividades que se describen:

COMPROMISO	ACTIVIDADES
a) Asegurando que la política de seguridad de la información y los objetivos de seguridad de la información son establecidos y compatibles con la dirección estratégica de la organización.	• Resolución Jefatural que aprueba la Política y Objetivos de Seguridad de la Información. • Actualización de la Política y Objetivos de Seguridad de la Información.
b) Asegurando la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización.	• Promueve la implementación, mantenimiento del SGSI en la institución. • Emisión de comunicaciones orientadas al cumplimiento de los requisitos de la Norma Internacional 27001.
c) Asegurando que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.	• Aprueba la asignación de recursos para el mantenimiento del SGSI, así como para la continuidad de su certificación a través de las auditorías internas y externas.

COMPROMISO	ACTIVIDADES
d) Comunicando la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la información.	• Comunica a toda la institución la importancia de la adecuada gestión de la seguridad de la información.
e) Asegurando que el sistema de gestión de seguridad de la información logre su(s) resultado(s) previsto(s).	• Aprueba la asignación de recursos para el mantenimiento del SGSI. • A través de las Revisiones por la Dirección.
f) Dirigiendo y apoyando a las personas para que contribuyan con la eficacia del sistema de gestión de seguridad de la información.	• A través de las Revisiones por la Dirección. • Asignación de roles en el SGSI
g) Promoviendo la mejora continua.	• Promueve la implementación del SGSI, implica una gestión de mejora continua, basada en el modelo de gestión de procesos de Deming: Planificar-Hacer-Verificar-Actuar (PHVA).
h) Apoyando a otros roles de gestión pertinente para demostrar su liderazgo en lo que respecta a sus	• Aprobando el Reglamento de Organización y Funciones. • Designa a la OTI, la función de conducir la implementación y

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 13 de 51

COMPROMISO	ACTIVIDADES
áreas de responsabilidad.	mantenimiento del SGSI en la institución.

5.2.2 Política

La Alta Dirección aprueba la Política de Seguridad de la Información de la Universidad mediante Resolución, se propone la siguiente política:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Universidad Nacional de Juliaca se compromete a garantizar la confidencialidad, integridad y disponibilidad de la información y de los activos que la soportan a través de la gestión de riesgos, controles, procedimientos y metodologías, personal capacitado, tecnología y la mejora continua en el cumplimiento de la normatividad legal vigente y estándares internacionales, en busca de maximizar la seguridad en la prestación de los servicios a sus grupos de interés.

Objetivos de Seguridad de la Información:

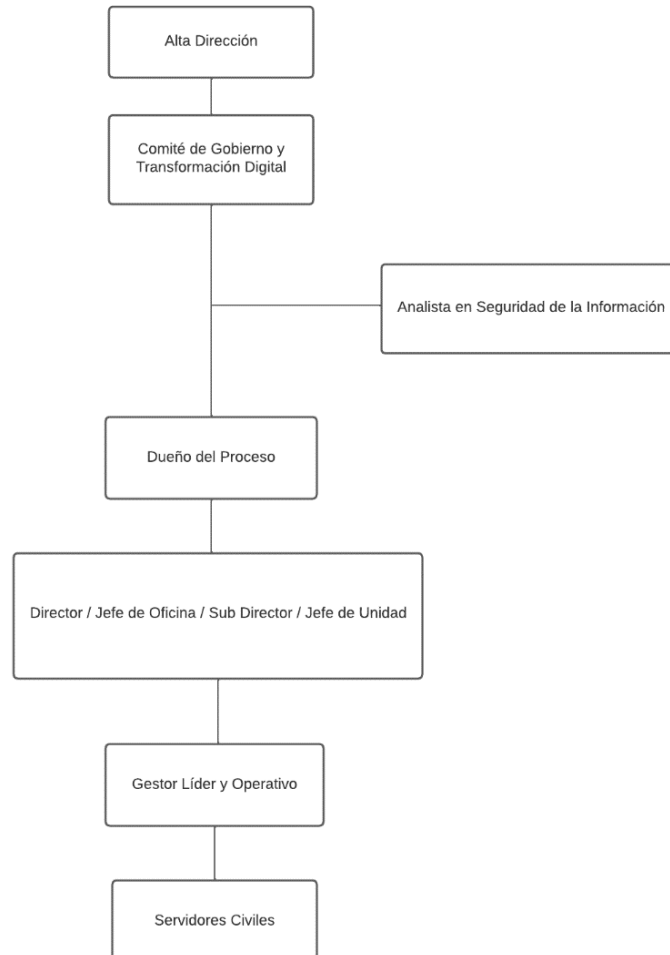
- Garantizar la confidencialidad, integridad y disponibilidad de la información y de los sistemas que soportan sus procesos.
- Contribuir a generar una cultura universitaria de seguridad de la información.
- Asegurar la gestión oportuna de los riesgos e incidentes que afronta la información y los activos que la soportan.

5.2.3 Roles, responsabilidades y autoridades organizacionales

Los roles, responsabilidades y autoridades de la organización para los diferentes Órganos y Unidades Orgánicas del SGSI de los procesos de la UNAJ, están definidos en cada numeral del presente manual. Para la implementación, mantenimiento y mejora del SGSI se tiene la siguiente estructura:

	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 14 de 51

Estructura Organizacional del Sistema de Gestión de Seguridad de la Información – SGSI de la Universidad



5.2.3.1 Alta Dirección

El Rectorado se constituye en la máxima autoridad de la UNAJ, es responsable de dirigir y controlar la institución; asimismo mediante Resolución aprueba la política y objetivos de Seguridad de la Información.

5.2.3.2 Comité de Gobierno y Transformación Digital

Este Comité es la instancia permanente de carácter no técnico y de gobierno para la dirección, evaluación y supervisión del proceso de Transformación y Gobierno Digital en la UNAJ.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 15 de 51

Está constituido mediante Resolución de Consejo de Comisión Organizadora N° 689-2022-CUNAJ.

Dicho comité se encuentra integrado por los siguientes miembros o quien haga sus veces:

- Presidente de la Comisión Organizadora de la UNAJ.
- Director de Administración.
- Jefe de la Oficina de Tecnologías de la Información.
- Responsable del Área de Recursos Humanos.
- Secretario General.
- Especialista en Procesamiento de Datos y Estadística Académica.
- Responsable del Área Legal.
- Jefe de la Unidad de Planeamiento y Modernización.

5.2.3.3 Oficial de Seguridad y Confianza Digital

Mediante Resolución se designa al Oficial de Seguridad y Confianza Digital de la Universidad Nacional de Juliaca, quién tiene las siguientes responsabilidades:

- a. Coordinar la implementación, operación, mantenimiento y mejora continua del SGSI de la entidad, atendiendo las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
- b. Coordinar con las unidades de organización de la entidad las acciones orientadas a implementar y/o mantener el SGSI, de acuerdo con lo establecido por la alta dirección y las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
- c. Formular y proponer políticas, procedimientos y planes en materia de seguridad de la información, gestión de riesgos de seguridad de la información,

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 16 de 51

gestión de incidentes de seguridad de la información, seguridad y confianza digital.

- d. Promover la conformación y adecuada operación del equipo de respuestas ante incidentes de seguridad de la información.
- e. Proponer medidas para la gestión de riesgos e incidentes de seguridad de la información, seguridad digital y ciberseguridad.
- f. Crear y mantener un registro de los eventos e incidentes de seguridad de la información identificados.
- g. Comunicar al CNSD los incidentes de seguridad digital críticos que afecten a los procesos misionales o servicios que brinda la entidad, y de ser el caso, coordinar y/o participar en su atención con el CNSD.
- h. Planificar y coordinar la ejecución de pruebas de evaluación de vulnerabilidades de los aplicativos informáticos, sistemas, infraestructura, datos y redes que soportan los servicios digitales, procesos misionales o relevantes de la entidad.
- i. Elaborar informes de los riesgos e incidentes de seguridad de la información críticos para la entidad pública e informarlos a la máxima autoridad administrativa.
- j. Informar a la máxima autoridad administrativa acerca de los riesgos de seguridad de la información, incidentes de seguridad de la información críticos, avances y dificultades en la implementación u operación del SGSI, resultados de las auditorías de seguridad de la información internas y/o externas realizadas anualmente a la entidad, y sobre la aplicación efectiva de las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 17 de 51

seguridad de la información, seguridad digital y confianza digital.

- k. Coordinar con el CNSD acciones de sensibilización y capacitación para los funcionarios y servidores civiles de la entidad sobre seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
- l. Coordinar con el Oficial de Gobierno de Datos y el Oficial de Datos Personales en todas las cuestiones relativas a la implementación de controles de seguridad de la información relacionados con las materias de gestión de datos y protección de datos personales en la entidad, respectivamente.
- m. Coordinar con el Líder de Gobierno y Transformación Digital, lo concerniente a iniciativas y proyectos en materia de seguridad y confianza digital.
- n. Coordinar con los dueños de procesos, propietarios de riesgos y responsables de las unidades de organización de la entidad su apoyo en la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así como en la gestión de incidentes de seguridad de la información.
- o. Liderar a los CSCD designados en la entidad pública para la adecuada implementación del SGSI.
- p. Asegurar y supervisar la adopción y uso de estándares, normas técnicas y mejores prácticas de seguridad de la información ampliamente reconocidos por parte de la unidad de organización de tecnologías de la información cuando ésta adquiera, tercerice o desarrolle software o implemente otro tipo de soluciones tecnológicas.
- q. Coordinar con la unidad de organización responsable de las tecnologías de la información o la que haga sus

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 18 de 51

veces en la entidad, cuando corresponda, en los temas relativos a sus responsabilidades.

- r. Otras responsabilidades afines que le sean asignadas por el titular de la entidad o la máxima autoridad administrativa.

5.2.3.4 Dueño del Proceso

Es la persona encargada de facilitar o asegurar la disponibilidad de los recursos para la implementación de la Gestión por Procesos. Asume responsabilidad respecto al desarrollo de las actividades propias del proceso, en permanente coordinación y acuerdo con los responsables o Jefes involucrados en el alcance.

El Dueño del proceso tiene la autoridad y responsabilidad para:

- a. Asegurar que el Sistema de Gestión de Seguridad de la Información se ejecute conforme a los requisitos de la normativa vigente.
- b. Asegurar la integración de los requisitos de la norma ISO/IEC 27001:2022 en su proceso.
- c. Revisar y aprobar la información correspondiente a su proceso en el marco del Sistema de Gestión de Seguridad de la Información, como las competencias necesarias para los roles previstos, los indicadores para la medición de la eficacia, entre otros.
- d. Gestionar la disponibilidad de recursos para implementar, monitorear, mantener y mejorar el Sistema de Gestión de Seguridad de la Información.
- e. Comunicar al personal de su proceso la importancia de cumplir con los objetivos y política de seguridad de la información, sus responsabilidades y la necesidad de la mejora continua.
- f. Proponer, comunicar e informar al Oficial de Seguridad y Confianza Digital, las acciones relevantes del SGSI.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 19 de 51

- g. Informar respecto a los compromisos de su responsabilidad asumidos en reuniones del CGTD.
- h. Aprobar el Plan de Gestión Integral del Riesgo y Oportunidades de Seguridad de la Información.
- i. Comunicar al personal de su proceso que los documentos normativos y técnicos que desarrollen deben incluir el cumplimiento a los requerimientos de confidencialidad, integridad y disponibilidad.
- j. Tomar las decisiones que permitan mejorar de manera continua la conveniencia, suficiencia y efectividad del Sistema de Gestión de Seguridad de la Información.

5.2.3.5 Director, Jefe de Oficina, Sub Director o Jefe de Unidad

Empleado de confianza titular (Director o Jefe de Oficina/Unidad) de un órgano que forma parte de un proceso comprendido en el Sistema de Gestión de Seguridad de la Información. Tiene la autoridad y responsabilidad para:

- a. Asegurar que el Sistema de Gestión de Seguridad de la Información se ejecute conforme a los requisitos de la normatividad vigente.
- b. Gestionar la disponibilidad de recursos suficientes para desarrollar, implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información, a través de la formulación del Plan Operativo Institucional.
- c. Participar en la elaboración de la información correspondiente a su proceso en el marco del Sistema de Gestión de Seguridad de la Información, como las competencias necesarias para los roles previstos, los indicadores para la medición de la eficacia, entre otros.
- d. Proporcionar información oportuna al Dueño del Proceso para la elaboración de la información

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 20 de 51

correspondiente al Sistema de Gestión de Seguridad de la Información.

- e. Comunicar al personal de su proceso, la importancia de cumplir los objetivos y políticas de Seguridad de la Información, sus responsabilidades y la necesidad de la mejora continua.
- f. Alertar al Dueño del Proceso respecto a las modificaciones al Sistema de Gestión de Seguridad de la Información que puedan afectar su integridad, disponibilidad y confidencialidad de la información.
- g. Tomar las decisiones que permitan mejorar de manera continua la conveniencia, suficiencia y efectividad del Sistema de Gestión de Seguridad de la Información.

5.2.3.6 Analista de Seguridad de la Información

El Analista de seguridad de la información, tiene la responsabilidad y la autoridad para:

- a. Proporcionar asistencia técnica a los procesos misionales, estratégicos o de soporte en el mantenimiento del Sistema de Gestión de Seguridad de la Información.
- b. Evaluar propuestas de modificaciones a la normatividad del Sistema de Gestión de Seguridad de la Información.
- c. Hacer seguimiento de los indicadores definidos en el marco del Sistema de Gestión de Seguridad de la Información, informando al Oficial de Seguridad y Confianza Digital para el trámite o de las acciones correctivas necesarias.
- d. Identificar y proponer oportunidades de mejora en los procesos misionales que conforman el Sistema de Gestión de Seguridad de la Información, informando al Oficial de Seguridad y Confianza Digital.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 21 de 51

- e. Evaluar el desempeño trimestral del Sistema de Gestión de Seguridad de la Información, informando al Oficial de Seguridad y Confianza Digital.
- f. Promover y difundir la cultura de seguridad de la información.
- g. Monitorear e informar el estado de los hallazgos identificados en auditorías, revisiones y análisis de datos.
- h. Otras funciones que se le asignen en el ámbito de sus competencias.

5.2.3.7 Gestor Líder

Servidor Civil que labora en el proceso, tiene la responsabilidad y la autoridad para:

- a. Velar por el cumplimiento de la Política de Seguridad de la Información, documentos, directivas y normas relacionadas.
- b. Conservar la información documentada de su proceso necesaria para el SGSI.
- c. Coordinar la ejecución de las actividades de sensibilización/concientización en seguridad de la información.
- d. Informar al Oficial de Seguridad y Confianza Digital sobre el desempeño y las oportunidades de mejoras del SGSI.
- e. Mantener comunicación y coordinación con los analistas en seguridad de la información de la OTI.
- f. Monitorear el cierre de las no conformidades y las acciones correctivas; asimismo, reportará al Oficial de Seguridad y Confianza Digital el estado de las acciones correctivas.
- g. Reportar las acciones para la clasificación de la información, etiquetado y uso adecuado de los activos de seguridad de la información, así como liderar el equipo de riesgos de seguridad de la información.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 22 de 51

- h. Reportar la atención de vulnerabilidades, eventos e incidentes de seguridad de la información.
- i. Alertar al dueño del Proceso respecto a las modificaciones al SGSI que puedan afectar su integridad.
- j. Otras funciones que se le asigne en el ámbito de su competencia.

5.2.3.8 Gestor Operativo

Es el servidor civil de cada órgano/unidad orgánica institucional que conforma un proceso, comprendido en el alcance del SGSI, tiene la responsabilidad y la autoridad para:

- a. Integrar el Equipo de Riesgos y ejecutar las actividades que demande la Gestión Integral de Riesgos.
- b. Realizar la evaluación de desempeño del SGSI a través de los indicadores de gestión.
- c. Mantener comunicación y coordinación con los analistas en seguridad de la información de la OTI.
- d. Ejecutar y/o gestionar las actividades que demanden el cierre de las no conformidades y las acciones correctivas.
- e. Velar que los activos de información estén debidamente inventariados y etiquetados según su clasificación, y sean utilizados de acuerdo a los procedimientos establecidos que garantizan su uso aceptable.
- f. Reportar y gestionar la ejecución de los controles para mitigar las vulnerabilidades, eventos e incidentes de seguridad de la información.
- g. Mantener comunicación constante con el gestor líder y responsable del proceso en el ámbito de la Seguridad de la información.
- h. Otras funciones que se le asigne en el ámbito de su competencia.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 23 de 51

5.2.3.9 Servidores Civiles

Personal que presta servicios en los procesos comprendidos en el alcance del SGSI y cuyo trabajo impacta en la conformidad del producto o servicio y tienen las siguientes responsabilidades:

- Cumplir con las políticas y objetivos, lineamientos y procedimientos del SGSI.
- Mantener la confidencialidad, integridad y disponibilidad de la información accedida para el cumplimiento de sus funciones.
- Participar activamente en las acciones de capacitación, en temas de seguridad de la información.
- Reportar cualquier vulnerabilidad, evento, incidente u oportunidades de mejora de seguridad de la información.
- Otras funciones que se le asigne en el ámbito de su competencia.

5.3 PLANIFICACIÓN

5.3.1 Acciones para abordar riesgos y oportunidades

5.3.1.1 General

En el marco de la aplicación de la Metodología de Gestión de Riesgos de Seguridad de la Información que establece la metodología y estandarización para la implementación y sostenibilidad a la Gestión Integral del Riesgo a nivel institucional, a fin de brindar un nivel de seguridad razonable en el logro de los objetivos estratégicos institucionales y el cumplimiento de las disposiciones legales y normativas del Estado.

La referida metodología prevé la identificación, análisis, valoración, tratamiento, seguimiento y revisión de las oportunidades y riesgos de seguridad de la información a los que se encuentran expuestos los procesos.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 24 de 51

Los Dueños de los Procesos comprendidos en el alcance del SGSI, informan con frecuencia mensual los Planes de Gestión Integral del Riesgos (PGIR) y Plan de Gestión de Oportunidades (PGO) al Oficial de Seguridad y Confianza Digital para seguimiento, evaluación y validación de las medidas de control con copia a OIR, de acuerdo a lo establecido por Oficina de Integridad y Riesgos.

5.3.1.2 Evaluación del riesgo de seguridad de la información

Las actividades de evaluación de riesgos de seguridad de la información se encuentran definidas en la Metodología de Gestión de Riesgos de Seguridad de la Información, que establecen los criterios contra los cuales se evalúan los riesgos de seguridad de la información, los lineamientos para identificar, analizar, evaluar, y tratar los riesgos de seguridad de la información a los que se encuentran expuesto los procesos hasta obtener un nivel aceptable del riesgo y garantizar la seguridad de la información en los órganos que cuenten o implementen un SGSI.

El Oficial de Seguridad y Confianza Digital en coordinación con los gestores líderes y operativos; además, de los analistas en seguridad de la información de la OTI: identifican las amenazas, vulnerabilidades y riesgos; para que a posterior se generen un Plan de Gestión Integral de Riesgos (PGIR) y Plan de Gestión de Oportunidades (PGO), bajo los criterios de confidencialidad, integridad y disponibilidad de la información. Se mantiene información documentada de este proceso.

5.3.1.3 Tratamiento de riesgos de seguridad de la información

Los lineamientos para tratar los riesgos del SGSI se encuentran definidos en la Metodología de Gestión de Riesgos de Seguridad de la Información, para lo cual los dueños de los procesos en coordinación con el Oficial de

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 25 de 51

Seguridad y Confianza Digital, establecen estrategias, responsabilidades y tiempo estimado, para el tratamiento del riesgo, estableciendo y/o seleccionando los controles que sean necesarios hasta obtener un nivel aceptable del riesgo.

5.3.2 Objetivos de seguridad de la información y planificación

La Alta Dirección ha definido y aprobado los objetivos de seguridad de la información de la Universidad, mediante Resolución, y son:

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

1. Garantizar la confidencialidad, integridad y disponibilidad de la información y de los sistemas que soportan sus procesos.
2. Contribuir a generar una cultura universitaria de seguridad de la información.
3. Asegurar la gestión oportuna de los riesgos e incidentes que afronta la información y los activos que la soportan.

El Oficial de Seguridad y Confianza Digital propone los objetivos específicos de seguridad de la información haciendo uso del **Anexo N°08 “Matriz de Planificación de los Objetivos e Indicadores”** a la Alta Dirección, quien lo aprueba y difunde a los procesos comprendidos en el alcance, así como al CGTD.

5.3.3 Planificación de cambios

Cuando se determina la necesidad de cambios en el SGSI, estos se ejecutan de manera planificada y sistemática, los cuales podrían darse cuando hay:

- a. Cambios de los procesos, actividades que causan impactos al SGSI
- b. Inclusión de nueva tecnología, equipos, herramientas, entre otros
- c. Inclusión de nueva normativa legal asociada a los procesos.
- d. Riesgos significativos.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 26 de 51

- e. Como resultado de las revisiones por la dirección, resultados de auditorías, revisión de no conformidades, análisis de desempeño de los procesos, cambios en el contexto o de las necesidades de las partes interesadas).

Esta necesidad de cambio se registra en el **Anexo N°09 “Solicitud de Cambio”**, la cual es remitida al Oficial de Seguridad y Confianza Digital y se mantiene información documentada de la revisión de cambios, el personal que autoriza el cambio y de cualquier acción necesaria en la revisión de los cambios.

Los Dueños de los Procesos remiten el formato de **“Solicitud de Cambio”** al Oficial de Seguridad y Confianza Digital con la propuesta del plan de implementación del cambio.

El Oficial de Seguridad y Confianza Digital evalúa la solicitud y consecuencia del cambio sobre el SGSI, propone un cronograma detallado de trabajo y de corresponder eleva la solicitud y cronograma de trabajo al Presidente del CGTD, quien acepta o deniega la solicitud.

Cuando los cambios son identificados por el CGTD o la Alta Dirección, el Oficial de Seguridad y Confianza Digital registra los cambios en el **Anexo N°09 “Solicitud de Cambio”**.

El Oficial de Seguridad y Confianza Digital hace seguimiento del cumplimiento de las actividades planificadas. Cuando identifica desviaciones, esto es comunicado a la Gerencia General en su rol de Alta Dirección y con copia al CGTD para las acciones que estime pertinentes.

5.4 SOPORTE

5.4.1 Recursos

Los Directores y Jefes de las Unidades encargados de conducir los órganos institucionales comprendidos en el alcance del SGSI elaboran anualmente el **Plan Operativo Institucional y Cuadro Multianual de**

	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 27 de 51

Necesidades en base al presupuesto asignado, dentro del cual incluyen las necesidades de recursos humanos, infraestructura, equipos, sistemas y otros que apoyen a la implementación, mantenimiento y la mejora continua del SGSI.

5.4.2 Competencia

El Oficial de Seguridad y Confianza Digital en coordinación con la OPH y los dueños de los procesos comprendidos en el alcance del SGSI, determinan la necesidad de las competencias de los servidores que realizan las actividades que afectan la conformidad de los requisitos del SGSI.

Las acciones de capacitación son ejecutadas conforme a los lineamientos descritos en la DI-141-2016-SERVIR-PE “**Normas para la Gestión del Proceso de Capacitación en las entidades públicas**”.

Asimismo; mediante el formato del **Anexo N°10 “Matriz de Requisitos de Competencia para Roles”**, se detallan las competencias de los servidores civiles que forman parte del alcance del SGSI, el mismo que es aprobado por el dueño del proceso.

5.4.3 Toma de conciencia

El Oficial de Seguridad y Confianza Digital, atenderá las necesidades de formación y sensibilización en seguridad de la información de los servidores civiles de la UNAJ, coordina con recursos humanos su programación y realización, definiéndose. Asimismo; cada Dueño de Proceso a través de los Gestores del SGSI realiza sensibilizaciones en temas de seguridad de la información.

5.4.4 Comunicación

La UNAJ cuenta con una estructura de comunicación interna que facilita la comunicación entre las partes interesadas y entre todos los niveles de la organización, conforme a lo descrito en las directivas pertinentes.

	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 28 de 51

El SGSI cuenta con el formato **Anexo N°11 “Gestión de las Comunicaciones”**, con el fin de que los Dueños de los Procesos comprendidos en el alcance se aseguren de que la comunicación se canalice adecuadamente a las partes interesadas.

5.4.5 Información documentada

5.4.5.1 Generalidades

El SGSI incluye:

- La información documentada requerida por la Norma Internacional ISO/IEC 27001:2022.
- Información documentada establecida como necesaria para la eficacia del mismo.

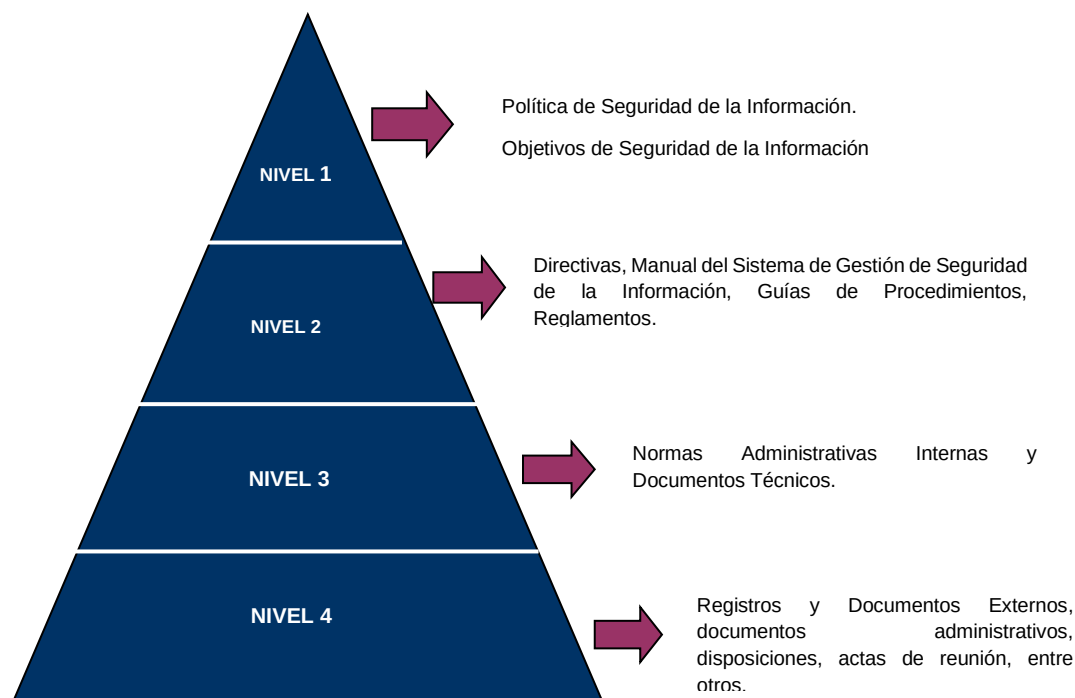
5.4.5.2 Creación y actualización

Para la formulación, revisión, aprobación, publicación, difusión, actualización y derogación de los documentos normativos, se debe establecer procedimientos adecuados.

5.4.5.3 Control de la información documentada

Los documentos que apoyan el SGSI, garantizan que éste cuente con los procedimientos necesarios para asegurar la mejora continua. Estos documentos se encuentran jerarquizados y clasificados según la estructura general que se muestra:

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 29 de 51



Los órganos comprendidos en el alcance del SGSI promueven, actualizan y difunden la información documentada relacionada al cumplimiento del SGSI, velando por su adecuada conservación, almacenamiento, retención y disposición, cuando sea necesario y según corresponda.

Adicionalmente, los documentos referidos en el numeral 5.4.52 son registrados por el Gestor Operativo, en el **Anexo N°12 “Lista Maestra de Documentos”**.

Para asegurar que los documentos normativos vigentes aplicables estén disponibles para todo el personal, se cuenta con los siguientes medios:

- Link en la web/intranet.
- Copia física controlada (cuando se requiera)

Las versiones vigentes de los documentos normativos se exhiben en la Intranet. Las copias impresas de documentos normativos que no tengan sello “**Copia Controlada**”, se consideran “**Copia no controlada**”.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 30 de 51

A fin de asegurar que los documentos normativos vigentes aplicables a los procesos se encuentren disponibles para el personal que no cuente con equipos informáticos, se identificará un punto de uso. Para ello o cuando se requiera, el gestor operativo dispone de copias físicas debidamente identificadas con el sello “**Copia Controlada**”, registrándola en el **Anexo N°13 “Lista de Distribución de Documentos”**.

Al aprobarse nuevas versiones de los documentos normativos, se elaboran controles de cambios, en los que se detallan los cambios en los procedimientos.

Cuando se actualiza un documento normativo, las copias controladas de la versión anterior son recuperadas por el Gestor Operativo, para su eliminación, cuya ejecución se registrará en el **Anexo N°14 “Acta de Eliminación”**.

5.5 OPERACIÓN

5.5.1 Planificación y control operacional

Los Directores, Sub Directores, Jefes de Oficina y Jefes de Unidad encargados de conducir órganos y/o unidades orgánicas institucionales comprendidas en el alcance del SGSI planifican, hacen seguimiento y evalúan sus actividades a través del Plan Operativo Institucional con frecuencia anual.

Con base al presupuesto aprobado, en cada proceso se elaboran los Cuadros multianual de necesidades de bienes y servicios, de acuerdo a los lineamientos para la Contratación de bienes y servicios.

Posteriormente, se formula el requerimiento de bien o servicio a la Oficina de Administración y Finanzas, la cual procede de acuerdo a los lineamientos descritos en el D.L. 30225 “**Ley de Contrataciones del Estado**” y su Reglamento, D.S 350-2015-EF, y sus modificaciones incorporadas mediante D.L. N° 1341 y el Decreto Supremo N° 056-2017-EF y Anexos. Cuando resulte necesario, se solicita apoyo a las

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 31 de 51

áreas técnicas especializadas para identificar los datos técnicos del bien o servicio que se van a requerir.

El desempeño de los proveedores externos es evaluado verificando lo establecido en los contratos a fin de emitir la conformidad del servicio a través de “**Actas de Conformidad**”.

En relación a los procedimientos o lineamientos para la realización de los productos y servicios, sus registros y controles, estos se encuentran descritos en Directivas y Guías de Procedimientos.

El Gestor Líder o el Analista en seguridad de la información de la OTI registran la información en el **Anexo N°16 “Cuadro de Mando Operativo”**, donde se detallan los indicadores del SGSI.

5.5.2 Evaluación de riesgos de seguridad de la información

Los Dueños de los procesos comprendidos en el alcance del SGSI, realizan evaluaciones de riesgos de Seguridad de la Información a intervalos planificados, en el que indica que la periodicidad de la actualización de los documentos del análisis, evaluación y tratamiento de riesgos de Seguridad de la Información, será de un año, contando a partir de la aprobación del Plan de Gestión Integral del Riesgo de Seguridad de la Información o cuando se produzcan cambios significativos que impacten los procesos del alcance el cual es registrado en la Matriz de Riesgo de Seguridad de la Información.

5.5.3 Tratamiento de riesgos de seguridad de la información

Los Dueños de los Procesos comprendidos en el alcance del SGSI, planifica las actividades, responsables, fechas, entre otros para tratar los riesgos de acuerdo al nivel de clasificación y realiza seguimiento mediante el Plan de Gestión Integral del Riesgo del Seguridad de la Información de acuerdo a la Metodología de Gestión de Riesgos de Seguridad de la Información.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 32 de 51

5.6 EVALUACIÓN DEL DESEMPEÑO

5.6.1 Monitoreo, medición, análisis y evaluación

El SGSI ha establecido indicadores para seguimiento y medición:

- Los resultados de los indicadores correspondientes a los objetivos de seguridad de la información se miden con la frecuencia prevista en el **Anexo N°08 “Matriz de Planificación de los Objetivos e Indicadores”**.
- Cada Gestor Operativo y Analista en seguridad de la información, actualiza los datos que corresponden en el **Anexo N°15 “Resultado del indicador”**.
- El Gestor Líder actualiza la información del **Anexo N°16 “Cuadro de Mando Operativo”**. Adicionalmente, con frecuencia trimestral, los Dueños de los Procesos y analistas en seguridad de la información de la OTI/UGTI comprendidos en el alcance del SGSI informan estos resultados al Oficial de Seguridad y Confianza Digital.
- Los Gestores del SGSI medirán los indicadores de sus procesos asignados y los Analistas en seguridad de la información de la OTI/UGTI medirán los indicadores del SGSI transversales.
- Los resultados alcanzados respecto al desempeño de los procesos de soporte, se miden y comunican mensualmente al Oficial de Seguridad y Confianza Digital, quien evalúa el resultado obtenido para cada proceso e informa a los procesos de soporte. Asimismo, cada Gestor Líder actualiza el **Anexo N°16 “Cuadro de Mando Operativo”**.

El Oficial de Seguridad y Confianza Digital comunica con frecuencia trimestral los resultados del monitoreo del desempeño del SGSI a la Alta Dirección con copia a los Dueños de los Procesos y al CGTD.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 33 de 51

5.6.2 Auditoría interna

Se planifica y gestiona la ejecución de las auditorías internas a los sistemas de gestión implementados, de conformidad a los lineamientos brindados, en la que se definen entre otras:

- Las responsabilidades y los requisitos para planificar y realizar las auditorías, incluido los criterios para la selección y calificación de auditores.
- Los lineamientos para informar sobre los resultados y mantener los registros asociados.

5.6.3 Revisión por la dirección

5.6.3.1 General

La Alta Dirección y el CGTD, realizan revisiones de gestión de seguridad de la información en los procesos de acuerdo a los requisitos de la norma ISO/IEC 27001, para asegurar su conveniencia, adecuación y efectividad continua.

5.6.3.2 Entradas para la revisión por la dirección

Incluye información relacionada a:

- a. El estado de las acciones de revisiones de gestiones anteriores.
- b. Cambios en cuestiones externas e internas que son relevantes para el SGSI.
- c. Cambios en las necesidades y expectativas de las partes interesadas que sean relevantes al SGSI.
- d. Retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias en:
 1. No conformidades y acciones correctivas.
 2. Resultados de monitoreo y medición.
 3. Resultados de auditoría.
 4. Cumplimiento de los objetivos de seguridad de la información.
- e. Retroalimentación de las partes interesadas.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 34 de 51

- f. Resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos.
- g. Oportunidades de mejora continua.

5.6.3.3 Resultados de la Revisión por la Dirección

Los resultados de la Revisión por la Alta Dirección, incluyen las decisiones relacionadas a las oportunidades de mejora y a cualquier necesidad de cambio, los mismos que son documentados mediante actas de la revisión de gestión, las cuales serán custodiadas por el Oficial de Seguridad y Confianza Digital, el cual mantiene información documentada de los resultados de las revisiones por la dirección.

El Analista de seguridad de la información en coordinación con el Oficial de Seguridad y Confianza Digital y el Gestor Líder de Seguridad de la Información realizan el seguimiento de los acuerdos y de las acciones aprobadas y comunica el estado de los mismos a la Alta Dirección y al CGTD.

5.7 MEJORAS

5.7.1 Mejora continua

El SGSI ha sido implementado conforme a los lineamientos de la Norma Internacional “ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información”. Requisitos, que detalla los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la información.

En tal sentido, los procesos que se encuentran dentro del alcance del SGSI bajo la norma internacional ISO/IEC 27001, generan propuestas de mejora a partir de:

- El análisis de datos.
- Reuniones del Oficial de Seguridad y Confianza Digital, analistas en seguridad de la información y Gestores Líderes y Gestores Operativos.

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	23/04/2026
		Página:	Página 35 de 51

- La identificación, análisis y valoración del riesgo y oportunidades.
- Los resultados de las acciones para tratar riesgos y oportunidades.
- Los resultados de las revisiones por la Dirección.
- Los resultados de las auditorías internas/externas de seguridad de la información.
- Los resultados de las acciones correctivas que incluyen acciones de mejora.

5.7.2 No conformidad y acción correctiva

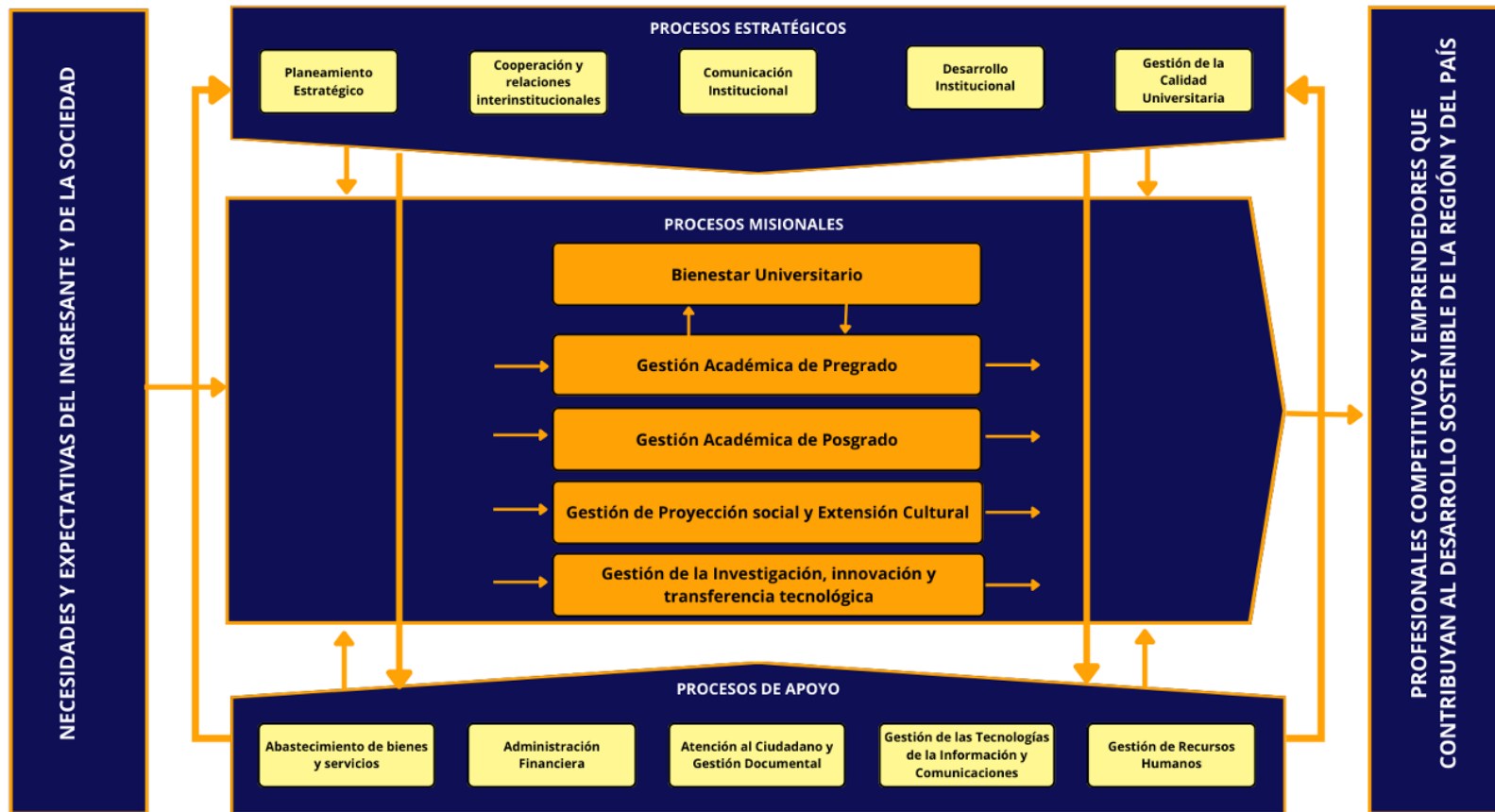
Las No Conformidades identificadas en el alcance del SGSI son tratadas, en cuyo contexto se establecen los lineamientos para el tratamiento de hallazgos que puedan generarse por incumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información, como resultado del análisis de datos, auditorías internas/externas, resultado de la revisión por la Dirección, así también define los lineamientos para controlar y dar seguimiento a las acciones correctivas necesarias para evitar que se repita la no conformidad.

VI. ANEXOS

ANEXO N° 01

MAPA DE PROCESOS

MAPA DE PROCESOS NIVEL 0 - UNIVERSIDAD NACIONAL DE JULIACA



ANEXO N°05

FICHA TÉCNICA DE PROCESO

NOMBRE DEL PROCESO				CÓDIGO	
NIVEL DEL PROCESO					
OBJETIVO DEL PROCESO					
DUEÑO DEL PROCESO				VERSIÓN	
PROCESO DE NIVEL SUPERIOR					
ALCANCE					
PROVEEDOR	ENTRADA	LISTADO DE PROCESOS DE NIVEL INFERIOR		SALIDA	DESTINATARIO
		ACTIVIDADES	EJECUTOR		
1					
2					
3					
4					
5					
6					
7					
8					
9					
CONTROLES					
RECURSOS HUMANOS					
INSTALACIONES					
SISTEMAS INFORMÁTICOS					
EQUIPOS					
REGISTROS					
INDICADORES					

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión	1.0
			Fecha:	21/01/2026
			Página:	Página 41 de 51

ANEXO N° 06
FICHA TÉCNICA DEL INDICADOR

Nombre del proceso			
Tipo de proceso			
Objetivo de proceso			
Nombre del indicador			
Código del indicador			
Objetivo del indicador			
Tipo de indicador			
Responsable del indicador			
Limitaciones del indicador			
Método de cálculo			
Parámetro de medición		Sentido esperado del indicador	
Fuente de datos			
Frecuencia de medición			
Oportunidad de medida			
Meta		Periodo para el cumplimiento de la meta	
Valor de línea base			
Año			
Valor			

ANEXO N° 07

ACUERDO DE PARTES

Acuerdo de partes						FECHA DE SUSCRIPCIÓN	
ÓRGANO INSTITUCIONAL GESTOR							
ÓRGANOS INSTITUCIONALES PARTICIPANTES							
PRODUCTO / SERVICIO SOBRE EL QUE SE APLICA EL ACUERDO		CARACTERÍSTICA DEL PRODUCTO / SERVICIO	REQUISITO	POTENCIAL IMPACTO POR INCUMPLIMIENTO DEL REQUISITO	RESPONSABLE DE CONTROL DE CUMPLIMIENTO DE ACUERDO	INDICADOR	CRITERIO DE CONTROL DEL INDICADOR

ELABORADO POR	SOLICITADO POR	ACEPTADO POR
Firma digital	Firma digital	Firma digital
Cargo	Cargo	Cargo

ACEPTADO POR	ACEPTADO POR	ACEPTADO POR
Firma digital	Firma digital	Firma digital
Cargo	Cargo	Cargo

	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión	1.0
		Fecha:	21/01/2026
		Página:	Página 44 de 51

ANEXO N°09 SOLICITUD DE CAMBIO

SOLICITUD DE CAMBIO

FIRMA DIGITAL DEL DUEÑO DEL PROCESO DE
NIVEL 0 QUIEN SOLICITA EL CAMBIO

Número de la solicitud:		Fecha de la solicitud:	
Nombre del proceso:		Código del proceso:	
Dueño del proceso:		Sistema de gestión afectado:	
IDENTIFICACIÓN DEL CAMBIO			
Propósito del cambio:			
Descripción del cambio:			
Descripción de la consecuencia:			
Tiempo de implementación:	Fecha inicio:	Fecha fin:	
Plan de implementación del cambio			
Actividad	Recurso	Tarea	Responsable
JUSTIFICACIÓN DE LA SOLICITUD DEL CAMBIO			
EVALUACIÓN DE LA SOLICITUD DEL CAMBIO			
Aceptado o rechazado por:	Resultado de la solicitud:	Fecha:	
Comentario en caso de rechazo:			

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión:	1.0
		Fecha:	21/01/2026
		Página:	Página 45 de 51

ANEXO N°10
MATRIZ DE REQUISITOS DE COMPETENCIAS POR ROLES

MATRIZ DE REQUISITOS DE COMPETENCIAS PARA ROLES								FIRMA DIGITAL DEL DUEÑO DEL PROCESO
Código del proceso del N0		Proceso N0				Fecha de aprobación		
						Versión		
N°	Proceso N1	ORGANO	Unidad Orgánica	Rol	Sistema	Conocimientos obligatorios para el rol	Experiencia en el Reniec (en años)	Conocimientos complementarios para el rol

RESPECTO A LA APLICACIÓN:

El alcance del Sistema Integrado de la Calidad del Reniec involucra los siguientes órganos: DRI, DSR, DRE, DRC, DRCD, OTI

Respecto al Proceso de Mejora Continua de los Sistemas de Gestión: De acuerdo a lo previsto en el Alcance del Sistema Integrado de la Calidad del Reniec.

RESPECTO A LA EXPERIENCIA:

No aplicable a los roles "Director ", Sub Director" y "Jefe de Oficina Regional" debido a que son puestos de confianza. En su caso, solo se considera la experiencia laboral requerida para su contratación.

RESPECTO A LA ACREDITACIÓN DE LOS CONOCIMIENTOS OBLIGATORIOS

Se acredita con certificados, constancias o diplomas emitidos por entidades externas o por el Reniec (legajo) o evidencias que proporcione el proceso.

RESPECTO A LA ACREDITACIÓN DE LOS CONOCIMIENTOS COMPLEMENTARIOS:

El Dueño del proceso puede decidir que no se requieren Conocimientos complementarios.

Cuando se declaren Conocimientos complementarios, se acredita la gestión de la capacitación a fin de que el servidor reciba el conocimiento propuesto.

RESPECTO A LA ACREDITACIÓN DE LOS CONOCIMIENTOS COMPLEMENTARIOS:

El Dueño del proceso puede decidir que no se requieren Conocimientos complementarios.

Cuando se declaren Conocimientos complementarios, se acredita la gestión de la capacitación a fin de que el servidor reciba el conocimiento propuesto.

ANEXO N°12

LISTA MAESTRA DE DOCUMENTOS

LISTA MAESTRA DE DOCUMENTOS

FIRMA DIGITAL DEL DUEÑO DEL PROCESO

[illegible]

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código:	M-GSI/OTI
		Versión:	1.0
		Fecha:	21/01/2026
		Página:	Página 48 de 51

ANEXO N°13
LISTA DE DISTRIBUCIÓN DE DOCUMENTOS

LISTA DE DISTRIBUCIÓN DE DOCUMENTOS

CODIGO - NOMBRE DEL DOCUMENTO. VERSIÓN				
Copia controlada N°	Rol del receptor de la copia controlada	Nombre del receptor de la copia controlada	Firma	Fecha de recepción

 UNIVERSIDAD NACIONAL DE JULIACA	MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Código:	M-GSI/OTI
			Versión:	1.0
			Fecha:	21/01/2026
			Página:	Página 49 de 51

ANEXO N°14

ACTA DE ELIMINACIÓN

De acuerdo con lo dispuesto en el Manual de Seguridad de la Información vigente, habiéndose aprobado la _____ versión del documento normativo _____, y con la finalidad de evitar el uso equivocado de documentos obsoletos, se ha recuperado y eliminado la Copia Controlada N° _____ correspondiente a la _____ versión del referido documento normativo, entregada a _____ el ____/____/____.

Fecha: ____/____/____

Responsable del Proceso

Nombre:

DNI N°:

Gestor Operativo de Seguridad de
la Información

Nombre:

DNI N°:

ANEXO N°15
RESULTADO DEL INDICADOR

RESULTADO DEL INDICADOR

Nombre del indicador		Fórmula del indicador		Meta	
----------------------	--	-----------------------	--	------	--

Descripción	Periodo de evaluación											
	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
Resultado del indicador												
Nivel "Malo"												
Nivel "Bueno"												
Numerador												
Denominador												



Periodo en evaluación	Análisis	Acciones a tomar	Responsable	Fecha	Estado
Enero					
Febrero					
Marzo					
Abril					
Mayo					
Junio					
Julio					
Agosto					
Setiembre					
Octubre					
Noviembre					
Diciembre					



POLÍTICA

DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Versión 1.0



Firmado digitalmente por VARGAS
CANCINO Henry FAU 20448261272
soft
Motivo: Soy el autor del documento
Fecha: 23.04.2026 17:32:07 -05:00

OFICINA DE TECNOLOGÍA
DE LA INFORMACIÓN



 UNIVERSIDAD NACIONAL DE JULIACA	POLITICA DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD		Código:	P-SIC/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 2 de 5

1. ALCANCE Y OBJETIVO

Establecer y difundir los lineamientos y compromisos estratégicos y operativos relacionados a la seguridad de la información, para mantener las pérdidas de los activos de información dentro del apetito de riesgo de La UNAJ.

Objetivos específicos

- Garantizar la confidencialidad, integridad y disponibilidad de la información y de los sistemas que soportan sus procesos.
- Contribuir a generar una cultura universitaria de seguridad de la información.
- Asegurar la gestión oportuna de los riesgos e incidentes que afronta la información y los activos que la soportan.

Alcance

- Todos los colaboradores de La UNAJ

2. FINALIDAD

Establecer los lineamientos, principios y responsabilidades para la protección de la información institucional de la Universidad Nacional de Juliaca, asegurando su confidencialidad, integridad y disponibilidad, así como la continuidad de los servicios académicos, administrativos y de investigación.

3. PRINCIPIOS

La Universidad adopta los siguientes principios:

- Confidencialidad:** La información solo será accesible a personas autorizadas.
- Integridad:** La información debe mantenerse exacta, completa y protegida contra modificaciones no autorizadas.
- Disponibilidad:** La información y los sistemas deben estar accesibles cuando se requieran.
- Legalidad:** Cumplimiento de la normativa vigente aplicable.
- Responsabilidad:** Todo usuario es responsable del uso adecuado de la información.
- Mejora continua:** Revisión y fortalecimiento permanente de los controles de seguridad.

4. MATRIZ RACI

Proceso / Actividad clave	Alta Dirección	OTI (TI)	Áreas / Propietarios de información	Usuarios	Terceros
Definición y aprobación de la política	A	R	C	I	I
Implementación del SGSI-C	C	R	C	I	I

 UNIVERSIDAD NACIONAL DE JULIACA	POLITICA DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD		Código:	P-SIC/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 3 de 5

Proceso / Actividad clave	Alta Dirección	OTI (TI)	Áreas / Propietarios de información	Usuarios	Terceros
Monitoreo y mejora continua del SGSI-C	A	R	C	I	I
Gestión de riesgos de SI	A	R	C	I	I
Clasificación de la información	I	C	R/A	I	I
Seguridad en desarrollo/adquisición de sistemas	I	R	C	I	C
Control de accesos	I	R	C	C	I
Gestión de recursos tecnológicos	I	R	C	I	I
Gestión de identidades (altas, bajas, cambios)	I	R	C	C	I
Gestión de incidentes de seguridad	I	R	C	R (reporte)	I
Continuidad del negocio (TI)	A	R	C	I	I
Cumplimiento normativo y auditoría	A	R	C	I	I
Gestión de proveedores (seguridad)	I	R	C	I	R
Concientización y capacitación	A	R	C	R (cumplir)	I

5. BASE LEGAL

- Ley N°29733, Ley de Protección de Datos Personales y su reglamento D.S. N°003-2013-JUS, que regula el tratamiento y protección de datos personales.
- Ley N°30220, Ley que establece las obligaciones de gestión institucional que incluyen el manejo de información.
- Ley N°27269, Ley de Firmas y Certificados Digitales.
- Decreto Legislativo N°1412, establece el marco para la transformación digital y la gestión de seguridad de la información en entidades públicas.
- Decreto Supremo N°029-2021-PCM, Lineamientos de ciberseguridad.
- Resolución Ministerial N°004-2016-PCM, Promueve la implementación de Sistemas de Gestión de Seguridad de la Información.
- Resolución Directoral N°019-2013-JUS-DGPDP, Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales.

6. REFERENCIAS

- Reglamento Interno de Servidores Civiles-RIS.
- Reglamento de Organización y Funciones.

 UNIVERSIDAD NACIONAL DE JULIACA	POLITICA DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD		Código:	P-SIC/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 4 de 5

7. POLÍTICA GENERAL DE SEGURIDAD DE INFORMACIÓN

- a. La Universidad Nacional de Juliaca se compromete a garantizar la confidencialidad, integridad y disponibilidad de la información y de los activos que la soportan a través de la gestión de riesgos, controles, procedimientos y metodologías, personal capacitado, tecnología y la mejora continua en el cumplimiento de la normatividad legal vigente y estándares internacionales, en busca de maximizar la seguridad en la prestación de los servicios a sus grupos de interés.

8. POLÍTICAS ESTRATÉGICAS

- a. La Universidad Nacional de Juliaca (UNAJ) reconoce que la información es un activo que debe ser protegido para evitar pérdidas que le perjudiquen.
- b. La Universidad Nacional de Juliaca (UNAJ) establece que la información física o digital, producida, transmitida, y/o almacenada en sus activos, es de su propiedad. Esto implica que, sin importar el mecanismo de comunicación (oral, escrito, digital, etc.) la información que se recibe para algún proceso de La UNAJ es propiedad de esta.
- c. La Universidad Nacional de Juliaca (UNAJ) dispone la participación obligatoria de todos sus colaboradores en la protección de los activos de información.
- d. La Universidad Nacional de Juliaca (UNAJ) establece que la protección de sus activos de información se extiende, pero no se limita, a salvaguardar su confidencialidad, integridad y disponibilidad. Para tal efecto, también se deberán considerar aspectos de no repudio, autenticidad y monitoreo.
- e. La Universidad Nacional de Juliaca (UNAJ) establece que las medidas de protección de sus activos de información se deben orientar a mantenerse dentro del apetito de riesgo de la empresa.
- f. La Universidad Nacional de Juliaca (UNAJ) implementa, mantiene y desarrolla un SGSI para la protección de sus activos de información, y para la respuesta y recuperación ante ocurrencia de incidentes de SI.
- g. La Universidad Nacional de Juliaca (UNAJ) establece un SGSI con alcance a:
 - 1) Todos sus procesos, proyectos y/o actividades internas y externas.
 - 2) Las funciones y unidades organizacionales, las ubicaciones físicas existentes, la infraestructura tecnológica y de comunicaciones, así como el perímetro de control asociado a las relaciones con terceros, que estén bajo responsabilidad de La UNAJ, conforme a las disposiciones establecidas sobre subcontratación en el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos.
- h. La Universidad Nacional de Juliaca (UNAJ) considera el riesgo de SI como parte del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos.
- i. La Universidad Nacional de Juliaca (UNAJ) cumple con las leyes y normativas relacionadas a la seguridad de la información en el ámbito de su competencia.
- j. La Universidad Nacional de Juliaca (UNAJ) considera a la SI de suma importancia para el

	POLITICA DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD		Código:	P-SIC/OTI
			Versión	1.0
			Fecha:	23/04/2026
			Página:	Página 5 de 5

cumplimiento de sus objetivos estratégicos.

- k. La Universidad Nacional de Juliaca (UNAJ) establece que el presente documento es una declaración oficial sobre su compromiso por proteger sus activos información, a fin de salvaguardar sus intereses y la de sus clientes.
- l. La Universidad Nacional de Juliaca (UNAJ) establece que todo requerimiento de carácter operativo, técnico, administrativo y/o de negocio que implique una situación no contemplada o contraria a la normativa interna o externa en materia de seguridad de la información, deberá ser previamente evaluado por la Oficina de Tecnologías de la Información (OTI). Dicha evaluación deberá quedar debidamente documentada, incluyendo el análisis de riesgos, las medidas de mitigación y la justificación correspondiente, a fin de emitir la conformidad o, de ser el caso, una excepción formal aprobada por la instancia competente, asegurando su trazabilidad y control.
- m. La implementación, monitoreo y cumplimiento de los controles establecidos en la presente política son responsabilidad de la Oficina de Tecnologías de la Información (OTI), como órgano encargado de la gestión de la seguridad de la información, en coordinación con las unidades orgánicas correspondientes. Cada dependencia es responsable de aplicar los controles en el ámbito de sus funciones, debiendo garantizar su cumplimiento, así como la generación, conservación y disponibilidad de evidencias que permitan su verificación en procesos de supervisión y auditoría.