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

RESOLUCIÓN RECTORAL
N° 071-2023-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 de 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, el artículo 4 de la precitada Resolución de Secretaría de Gobierno y Transformación Digital señala al Titular de la entidad pública como responsable de la implementación del Sistema de Gestión de Seguridad de la Información, para lo cual, como mínimo aprueba las políticas y objetivos para implementar, operar, mantener y mejorar el referido sistema;

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;

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;

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

RESOLUCIÓN RECTORAL
N° 071-2023-UNAJMA/R

Andahuaylas, 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 la Política General de Seguridad de la Información en la Universidad Nacional José María Arguedas, presentada por la Oficina de Tecnologías de la Información; que en anexo forma parte de la presente resolución.

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

ARTÍCULO TERCERO: 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

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Oficina de Tecnologías de la Información

Aprobado con Resolución N° 071-2023-UNAJMA/R
Versión N° 1.0

DICIEMBRE - 2023
ANDAHUAYLAS

ISO 9001:2015

ISO 21001:2018

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
Nombres y apellidos	Nombres y apellidos	Nombres y apellidos
Firma:	*Firma:*	*Firma:*
UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS Ing. Marusia Rodas Vergaro JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN	UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS Lic. Adm. Rubén Franklin Ponceca Barboza DIRECTOR GENERAL DE ADMINISTRACIÓN	UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS Dr. Edgar Luis Martínez Huamán RECTOR

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

1. GENERALIDADES

La información y los sistemas de información son activos críticos para las instituciones. Por ello, es necesario protegerlos de las amenazas que pueden poner en riesgo su integridad, confidencialidad y disponibilidad.

La Política General de Seguridad de la Información de la Universidad Nacional José María Arguedas establece un marco para proteger la información de la institución. Esta política se aplica a toda la información y los sistemas de información de la universidad, incluyendo información personal, financiera y académica, información de investigación y desarrollo, información comercial y administrativa, e información tecnológica y de infraestructura.

La responsabilidad de la seguridad de la información recae en todos los miembros de la universidad, pero en particular en la alta dirección. La alta dirección es responsable de establecer y difundir la política, así como de asignar los recursos necesarios para su implementación.

La política establece una serie de medidas de seguridad para proteger la información de la universidad. Estas medidas incluyen controles de acceso, seguridad física, seguridad lógica y educación y formación.

La política se revisa periódicamente para garantizar que siga siendo efectiva.

2. ALCANCE

Esta política se aplica a toda la información y los sistemas de información de la Universidad Nacional José María Arguedas, incluyendo:

- Información personal, financiera y académica de los estudiantes, empleados y socios, tales como nombres, apellidos, direcciones, números de teléfono, números de identificación, datos de salud y datos financieros.
- Información de investigación y desarrollo, incluyendo datos de investigación, prototipos y modelos.
- Información comercial y administrativa, incluyendo datos de clientes, proveedores y contratos.
- Información tecnológica y de infraestructura, incluyendo datos de sistemas informáticos, redes y servicios.

3. OBJETIVOS

a. Establecer los lineamientos para gestionar la seguridad de la información de tal manera que permita proteger los activos de información de la Universidad Nacional José María Arguedas, frente a amenazas internas o externas, deliberadas o accidentales, mediante la implementación de controles de seguridad físicos, lógicos y administrativos.

b. Mantener la Política General de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de la universidad, mediante un proceso de revisión y actualización periódico.

c. Definir las directrices de la Universidad Nacional José María Arguedas para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento, mediante la implementación de un proceso de gestión de riesgos de seguridad de la información.

4. BASE TÉCNICA LEGAL

a. Constitución Política del Perú.
b. Reglamento de Organización y Funciones de la Universidad Nacional José María Arguedas.
c. Resolución Ministerial Nº 246-2007-PCM, que aprueba la "Norma Técnica Peruana NTP ISO/IEC 17799:2007 EDI, Técnicas de Seguridad, Código de Buenas Prácticas para la Gestión de Seguridad de la Información". 2da. Edición.
d. Resolución Ministerial Nº 129-2012-PCM, aprueba el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001 EDI. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información en todas las entidades integrantes del Sistema Nacional de Informática.
e. ISO/IEC 27001: Un estándar internacional para la gestión de la seguridad de la información.
f. NIST Cybersecurity Framework: Un marco desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. para mejorar la ciberseguridad de las infraestructuras críticas.
g. Prácticas de Desarrollo Seguro (Secure SDLC): Estas prácticas se centran en incorporar la seguridad en todas las fases del ciclo de vida del desarrollo de software.

5. RESPONSABILIDADES

La Política General de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Universidad Nacional José María Arguedas, independientemente sea su régimen de contratación y el nivel de tareas que desempeñe.

5.1. El Comité de Gestión de Seguridad de la Información: El Comité de Gestión de Seguridad de la Información es el responsable de establecer la clasificación de la información en la Universidad Nacional José María Arguedas, asimismo efectúa la revisión, aprobación y seguimiento de la política e incidencias de la seguridad de la información. Este Comité debe ser designado mediante Resolución, este comité está compuesto por el Coordinador del Comité de Seguridad de la Información (presidente), el Rector, la Vicerrectora Académica, la Vicerrectora de Investigación y el Director General de Administración.

Funciones Específicas:
Sus funciones específicas son:

a. Revisar los resultados de los análisis de riesgos y aprobar los controles de tratamiento de riesgo que sean necesarios.
b. Evaluar y aprobar las sanciones en caso de incidentes de seguridad sugeridas por el Grupo Operativo de Seguridad de la Información, de conformidad con el reglamento Interno de Trabajo.
c. Definir las estrategias de capacitación en materia de seguridad de la información al interior de la Universidad.
d. Realizar el seguimiento y mejora del Sistema de Gestión de Seguridad de la Institución.

5.2. El Coordinador del Comité de Gestión de Seguridad de la Información: El Coordinador del Comité de Seguridad de la Información será el responsable de coordinar las acciones del Comité de Gestión de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

5.3. El Grupo Operativo de Seguridad de la Información: El Grupo Operativo de Seguridad de la Información será responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación del SGSI y supervisión del cumplimiento. El nivel de supervisión que pueda realizar cada grupo responsable de seguridad, está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el Comité de Gestión de Seguridad de la Información.

- Jefe de la Oficina de Tecnologías de la Información (quien lo preside).
- Especialista en Seguridad de la Información (en caso existiera el personal mencionado).
- Secretario General.
- Jefe de la Oficina de Recursos Humanos.
- Jefe de la Oficina de Abastecimiento.
- Jefe de Asesoría Jurídica.

Sus funciones específicas son:

a. Supervisar la ejecución periódica de análisis de riesgos y proponer controles de tratamiento de riesgos al Comité de Gestión de Seguridad de la Información.
b. Coordinar el inventario periódico de los activos de seguridad de la información de la Universidad Nacional José María Arguedas.
c. Proponer al Comité de Gestión de Seguridad de la Información los niveles de clasificación de la información que se deben de manejar en la Institución.
d. Preparar y recomendar al Comité de Seguridad de la Información la aprobación de planes y programas para la concientización del personal en la seguridad de la información.
e. Revisar las directivas y procedimientos de seguridad de la información verificando su efectividad y correcta implementación, proponiendo oportunamente su modificación o actualización.
f. Revisar y hacer seguimiento de los incidentes de seguridad de la información e informar al Comité de gestión de Seguridad de la Información.
g. Informar al Comité de Gestión de Seguridad de Información el incumplimiento de las directivas y procedimientos de Seguridad de la Información.
h. Proponer al Comité de Gestión de Seguridad de la Información la firma de convenios con instituciones especializadas en seguridad de la información con la finalidad de recibir asesoría permanente.

5.4. La Oficina de Tecnologías de la Información, el Jefe de la Oficina de Tecnologías de la Información es responsable de revisar las políticas específicas de seguridad de información propuestas por el Especialista en Seguridad de la Información. Asimismo, es el encargado de informar al Grupo Operativo de Seguridad de la Información sobre los resultados de la gestión de seguridad de la información.

Las funciones específicas del Especialista en Seguridad de la Información de la Oficina de Tecnologías de la Información son:

a. Ser el nexo entre el Comité de Gestión de Seguridad de la Información, el Grupo Operativo de Seguridad de la Información y la Oficina de Tecnologías de la Información.
b. Evaluar los incidentes de seguridad de la información encargados por el Jefe de la Oficina de Tecnologías de la Información.
c. Registrar los incidentes de seguridad y recomendar acciones de respuesta apropiadas para mitigarlos.
d. Evaluar y desarrollar especificaciones técnicas de seguridad de la información en los proyectos de implementación de nuevas tecnologías informáticas.
e. Gestionar la actualización, mantenimiento y pruebas del Plan de Continuidad de Operaciones de los servicios que administra la Oficina de Tecnologías de la Información.
f. Elaborar con las unidades orgánicas los proyectos de políticas específicas de seguridad de la información que resulten como consecuencia de la Política General de Seguridad de la Información y proponerlos a través del Jefe de la Oficina de Tecnologías de la Información.
g. Apoyar a los usuarios de los sistemas de información de la Universidad Nacional José María Arguedas, en los temas relacionados con la seguridad de su información.

5.5. Los propietarios de activos de información, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado, así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

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

Sus funciones específicas son:

a. Asegurar que el personal a su cargo cumpla con las responsabilidades ya sea como propietario, custodio y/o usuario de la información.
b. Tomar medidas para minimizar el riesgo o pérdida o exposición de los activos de seguridad de la información que se encuentran bajo su responsabilidad.
c. Analizar el impacto de la información en la Institución, es decir valorizar la información y las consecuencias de su uso no adecuado.
d. Clasificar la información de acuerdo con los niveles de clasificación que se establezcan.
e. Realizar el inventario de los activos de seguridad de información y mantenerlo actualizado.
f. Autorizar accesos sobre la información de la que son propietarios, ratificar periódicamente estos accesos e informar inmediatamente a las áreas competentes sobre el personal que no debería tener acceso a la misma.
g. Plantear requerimientos de control y protección de la información.
h. Establecer el nivel crítico de la información y los niveles mínimos de servicio cuando se requiere recuperar información en casos de desastres.

5.6. El órgano de control Institucional es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones

y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

5.7. El Jefe de Recursos Humanos, cumplirá la función de notificar a todo el personal de la Universidad José María Arguedas, de las obligaciones respecto del cumplimiento de la Política General de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal de la Universidad, a través de la suscripción de los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comité de Gestión de Seguridad de la Información.

5.8. Responsabilidades del personal de la Universidad, los jefes de las unidades administrativas y académicas son responsables de la aplicación y control de las políticas de seguridad de la información.

Sus funciones específicas son:

a. Difundir de una manera adecuada la política de seguridad de la información asegurando su correcto entendimiento en el personal a su cargo.
b. Supervisar, controlar y permitir solo el acceso necesario a los activos de seguridad de información en la relación y contratos con terceros.

Todo el personal de la Universidad Nacional José María Arguedas, cualquiera sea su régimen de contrato, la dependencia a la cual pertenece y el nivel de tareas que desempeñe, debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. La Oficina de Tecnologías de la Información debe mantener un directorio completo y actualizado de tales perfiles.

El Comité de Gestión de Seguridad de la Información determina cuales son los atributos que deben definirse para los diferentes perfiles.

La Oficina de Recursos Humanos conjuntamente con la Oficina de Tecnologías de la Información se encargará de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que contribuya al crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

El Comité de Gestión de Seguridad de la Información debe elaborar, mantener, actualizar, mejorar y difundir un documento de responsabilidades personales para la Seguridad de la Información en la Universidad Nacional José María Arguedas.
La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe inmediato; en todo caso el proceso de cambio en la cadena de custodia de la información debe ser parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

5.9. Responsabilidades de los estudiantes, para poder usar los recursos de TI de la Universidad, los estudiantes deben leer y aceptar en cada matrícula de semestre un acuerdo con los términos y condiciones. La Oficina de Tecnologías de la Información debe asegurar los mecanismos para la difusión y aceptación de dichas condiciones por medio de registros y manuales en línea. El estatuto estudiantil debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

5.10. Responsabilidades de Usuarios Externos, todos los usuarios externos y personal de empresas externas deben estar autorizados por un miembro del personal de la Universidad quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales. Los procedimientos para el registro de tales usuarios debe ser creado y mantenido por la Oficina de Asesoría Jurídica, en conjunto con la Oficina de Sistemas y la Oficina de Recursos Humanos.

Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI institucionales. Las cuentas de usuarios externos deben ser de perfiles específicos y tener caducidad no superior a tres (3) meses, renovables de acuerdo a la naturaleza del usuario.

6. SEGURIDAD FÍSICA Y DEL ENTORNO

6.1. ACCESO

El acceso a los cuartos de servidores principales, subsidiarios y a los cuartos de comunicaciones debe estar controlado y restringido. La Oficina de Tecnologías de la Información hará cumplir las normas, controles y registros de acceso a dichas áreas.

6.2. SEGURIDAD EN LOS EQUIPOS

Los servidores que contengan información y servicios institucionales deben encontrarse en un ambiente seguro y protegido por lo menos con los siguientes controles:

- ✓ Controles de acceso y seguridad física, que incluyen una puerta con cerradura que solo puede abrirse con una llave o un código de acceso.
- ✓ Detección de incendios y sistemas de extinción de conflagraciones, que cumplan con las normas vigentes.
- ✓ Controles de humedad y temperatura, que garanticen que los servidores operen en condiciones adecuadas.
- ✓ Bajo riesgo de inundación, por ejemplo, ubicado en un lugar elevado o protegido por muros de contención.
- ✓ Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

a. Toda información institucional en formato digital debe ser mantenida en servidores aprobados por la Oficina de Tecnologías de la Información de la Universidad Nacional José María Arguedas. No se permite el alojamiento de información institucional en servidores externos sin autorización escrita del Comité de Gestión de Seguridad de la Información.
b. Los equipos claves de comunicaciones deben ser alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.

c. Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la institución, el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.
d. Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares, los que serán elaborados y difundidos por el Comité de Gestión de Seguridad en la Información.
e. Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad.

7. IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN

7.1. ELABORACIÓN Y MANTENIMIENTO DEL INVENTARIO

Cada dependencia, bajo la supervisión del Comité de Gestión de Seguridad de la Información, tiene la responsabilidad de elaborar y mantener un inventario exhaustivo de los activos de información que poseen, tanto procesados como producidos. El Comité definirá las características del inventario, incluyendo la clasificación, valoración, ubicación y niveles de acceso de la información.

Responsabilidades:

- ✓ Registrar la ubicación física y lógica de los activos.
- ✓ Mantener actualizado el inventario en tiempo real.
- ✓ Asignar niveles de acceso basados en la clasificación y valoración de la información.

Herramientas de Administración:

La Oficina de Tecnologías de la Información facilitará herramientas a cada dependencia para administrar eficientemente el inventario. Estas herramientas garantizarán la disponibilidad, integridad y confidencialidad de los datos, y serán adaptadas a las necesidades específicas de cada área.

7.2. RESPONSABILIDADES COMPARTIDAS CON LA UNIDAD DE PATRIMONIO Y AMLACEN

La Oficina de Tecnologías de la Información, en colaboración con la Oficina de Patrimonio y Almacén, asume la responsabilidad de mantener un inventario completo y actualizado de los recursos de hardware y software de la institución.

Supervisar el estado y la ubicación física de los activos tecnológicos.

Coordinar con la Oficina de Patrimonio y Almacén para garantizar la integridad del inventario general de activos institucionales.

7.3. PROCESO DE CLASIFICACIÓN Y VALORACIÓN

El proceso de clasificación y valoración de la información será un proceso continuo y adaptativo, revisado periódicamente por el Comité de Gestión de Seguridad de la Información. Este proceso permitirá una asignación precisa de niveles de seguridad a la información en función de su importancia y sensibilidad.

Establecer revisiones periódicas para adaptarse a cambios en la naturaleza de la información.

Incorporar retroalimentación de incidentes de seguridad para ajustar la clasificación y valoración.

7.4. EDUCACIÓN Y CONCIENTIZACIÓN

La Oficina de Tecnologías de la Información coordinará programas de educación y concientización para el personal, enfocados en la importancia de la correcta identificación,

clasificación y valoración de los activos de información. Esto asegurará una comprensión completa de las responsabilidades individuales en la gestión de la información.

Estas mejoras buscan fortalecer el manejo de los activos de información, asegurando una identificación precisa, clasificación adecuada y valoración constante para mantener la integridad y la seguridad de la información institucional.

8. ADMINISTRACIÓN DE LAS COMUNICACIONES Y OPERACIONES

8.1. REPORTE E INVESTIGACIÓN DE INCIDENTES DE SEGURIDAD

El proceso de reporte e investigación de incidentes de seguridad debe ser transparente, eficiente y fomentar la responsabilidad individual. Se implementarán las siguientes mejoras:

8.1.1. Responsabilidades del Personal:

Todo el personal de la Universidad tiene la obligación de reportar posibles violaciones de seguridad de manera diligente y responsable, a través de su jefe inmediato a la Oficina de Tecnologías de la Información.

8.1.2. Canal Directo al Comité:

En situaciones especiales, se permite el reporte directo al Comité de Gestión de Seguridad de la Información, el cual desarrollará herramientas informáticas para formalizar tales denuncias.

8.1.3. Normas y Procesos Claros:

El Comité de Gestión de Seguridad de la Información elaborará, mantendrá y difundirá normas, procesos y guías específicas para el reporte e investigación de incidentes de seguridad. Esto asegurará consistencia y eficacia en el manejo de incidentes.

8.1.4. Privacidad y Autorización:

En cumplimiento con la ley, la Universidad podrá interceptar o realizar seguimiento a las comunicaciones mediante mecanismos autorizados por el Comité de Gestión de Seguridad de la Información. En todo caso, se notificará previamente a los afectados por esta decisión, garantizando la privacidad y la legalidad de dichas acciones.

8.1.5. Educación Continua:

Se establecerán programas de capacitación periódicos para el personal, enfocados en la identificación y reporte adecuado de incidentes de seguridad. Esto fortalecerá la conciencia y comprensión de los protocolos establecidos.

8.1.6. Retroalimentación y Mejora Continua:

Se implementará un sistema de retroalimentación para evaluar la efectividad de las acciones tomadas en respuesta a incidentes. Esta retroalimentación se utilizará para mejorar continuamente los procesos de reporte e investigación.

8.1.7. Protección de Denunciantes:

Se establecerán medidas para proteger a los denunciantes, garantizando que aquellos que reporten incidentes de seguridad no sufran represalias. Esta protección promoverá un entorno seguro y alentador para el reporte de posibles violaciones de seguridad.

8.2. PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y HACKING

8.2.1. CONTROLES DE SEGURIDAD

Los sistemas informáticos deben estar protegidos por los siguientes controles de seguridad:

- ✓ Firewalls: Los firewalls deben estar configurados para bloquear el acceso no autorizado a los sistemas informáticos.

- ✓ Antivirus: Los sistemas informáticos deben estar protegidos por software antivirus con capacidad de actualización automática en cuanto a firmas de virus.
- ✓ Antimalware: Los sistemas informáticos deben estar protegidos por software antimalware para detectar y eliminar malware.
- ✓ Controles de acceso: El acceso a los sistemas informáticos debe estar controlado y restringido para garantizar que solo las personas autorizadas tengan acceso a la información.
- ✓ Cifrado: Las comunicaciones deben estar cifradas para proteger la confidencialidad de la información.

8.2.2. CAPACITACIÓN

Todo el personal que utilice los sistemas informáticos debe recibir capacitación sobre los siguientes temas:

- ✓ Cómo reconocer y evitar software malicioso.
- ✓ Cómo proteger sus cuentas de usuario.
- ✓ Cómo utilizar los sistemas informáticos de manera segura.

8.3. COPIAS DE SEGURIDAD

8.3.1. REQUISITOS PARA LAS COPIAS DE SEGURIDAD

Las copias de seguridad deben cumplir con los siguientes requisitos:

- ✓ Completitud y consistencia: Las copias de seguridad deben ser completas y consistentes, para garantizar que se pueda restaurar toda la información en caso de pérdida o daño.
- ✓ Seguridad: Las copias de seguridad deben ser almacenadas en un sitio seguro, para protegerlas de la pérdida, el daño o el acceso no autorizado.
- ✓ Pruebas: Las copias de seguridad deben ser probadas periódicamente para garantizar que se pueden leer y restaurar correctamente.

8.3.2. RESPONSABILIDADES

- Dependencias administrativas y académicas: Las dependencias administrativas y académicas son responsables de:
  - ✓ Crear copias de seguridad de la información crítica para sus procesos operativos o de misión crítica.
  - ✓ Realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.
  - ✓ Registrar las copias de seguridad en una base de datos creada para tal fin.
- Oficina de Tecnologías de la Información: La Oficina de Tecnologías de la Información es responsable de:
  - ✓ Proporcionar las herramientas para que las dependencias puedan administrar la información y registros de copias de seguridad.
  - ✓ Efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.
- Órgano de control Institucional: El Órgano de control Institucional es responsable de:
  - ✓ Supervisar el cumplimiento de la presente política.

8.3.3. CRONOGRAMAS

Las copias de seguridad de información crítica deben ser mantenidas de acuerdo a cronogramas definidos y publicados por la Oficina de Tecnologías de la Información.

8.3.4. COPIAS DE SEGURIDAD DE ARCHIVOS PERSONALES

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios. Los usuarios deben entregar al respectivo jefe de cada dependencia administrativa y académica las copias de seguridad para su registro y custodia.

8.4. ADMINISTRACIÓN DE CONFIGURACIONES DE RED

8.4.1. REQUISITOS PARA LA ADMINISTRACIÓN DE CONFIGURACIONES DE RED

La configuración de los dispositivos de red debe cumplir con los siguientes requisitos:

- Documentación: La configuración de los dispositivos de red debe ser documentada de forma clara y concisa, para que pueda ser entendida y administrada por el personal autorizado. La documentación debe incluir la siguiente información:
  - ✓ El tipo de dispositivo de red
  - ✓ La versión del firmware
  - ✓ La configuración de los parámetros de seguridad
- Copia de seguridad: La configuración de los dispositivos de red debe ser respaldada por copia de seguridad, para que pueda ser restaurada en caso de pérdida o daño.
- Mantenimiento: La configuración de los dispositivos de red debe ser mantenida actualizada, para garantizar que refleje los cambios en los requisitos de seguridad.

8.4.2. RESPONSABILIDADES

- Oficina de Tecnologías de la Información: La Oficina de Tecnologías de la Información es responsable de:
  - ✓ Desarrollar y mantener los procedimientos para la administración de configuraciones de red.
  - ✓ Proporcionar capacitación al personal sobre los procedimientos para la administración de configuraciones de red.
  - ✓ Supervisar el cumplimiento de la presente política.
- Dependencias administrativas y académicas: Las dependencias administrativas y académicas son responsables de:
  - ✓ Asegurar que los dispositivos de red que utilizan cumplan con los requisitos de la presente política.
  - ✓ Reportar a la Oficina de Tecnologías de la Información cualquier cambio en la configuración de los dispositivos de red que utilizan.

8.4.3. DISPOSITIVOS NO AUTORIZADOS

La Oficina de Tecnologías de la Información debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

8.5. INTERCAMBIO DE INFORMACIÓN CON ORGANIZACIONES EXTERNAS

La gestión del intercambio de información con entidades externas es crucial para mantener la confidencialidad y la integridad de los datos institucionales.

Proceso de Aprobación Formal:

Todas las peticiones de información por parte de entes externos de control deben seguir un proceso formal de aprobación. Este proceso incluirá la aprobación por parte del Consejo universitario, quien evaluará la legitimidad y la necesidad de la solicitud.

- ✓ **Designación de Custodios Responsables:**
  Una vez aprobada la solicitud, los entes externos serán dirigidos a los responsables designados de la custodia de la información solicitada. Estos responsables garantizarán que la información se comparta de manera segura y de acuerdo con las políticas de seguridad de la información.
- ✓ **Registro de Solicitudes:**
  Todas las peticiones de información externa, junto con los detalles de la aprobación y la asignación de custodios, se registrarán de manera sistemática. Este registro servirá como documentación para futuras auditorías y seguimientos.
- ✓ **Protección de Datos Sensibles:**
  Se implementarán medidas específicas para proteger la confidencialidad de datos sensibles al compartir información con entidades externas. Esto incluirá la anonimización de datos cuando sea posible y la aplicación de controles de acceso adecuados.
- ✓ **Comunicación Transparente:**
  La Universidad establecerá una comunicación transparente con las entidades externas sobre las políticas y prácticas de seguridad de la información. Esto incluirá la definición clara de los procedimientos que deben seguirse durante el intercambio de información.
- ✓ **Capacitación del Personal:**
  Se llevará a cabo una capacitación regular del personal involucrado en el intercambio de información con organizaciones externas. Esto garantizará que comprendan las políticas de seguridad y estén equipados para manejar solicitudes de manera segura.

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

8.6. INTERNET Y CORREO ELECTRÓNICO

8.6.1. REQUISITOS PARA EL USO DE INTERNET Y CORREO ELECTRÓNICO

El uso de Internet y correo electrónico debe cumplir con los siguientes requisitos:

- Conformidad con el código de ética institucional: El uso de Internet y correo electrónico debe ser consistente con el código de ética institucional.
- Responsabilidad: El uso de Internet y correo electrónico debe ser responsable y respetuoso de los derechos de los demás.
- Conformidad con las leyes y reglamentos: El uso de Internet y correo electrónico debe ser conforme con las leyes y reglamentos aplicables.

8.6.2. RESPONSABILIDADES

- Oficina de Tecnologías de la Información: La Oficina de Tecnologías de la Información es responsable de:
  - ✓ Elaborar, mantener y actualizar las normas de uso de Internet y correo electrónico.
  - ✓ Proporcionar capacitación al personal sobre las normas de uso de Internet y correo electrónico.
- Dependencias administrativas y académicas: Las dependencias administrativas y académicas son responsables de:
  - ✓ Asegurar que el personal de sus dependencias cumpla con las normas de uso de Internet y correo electrónico.
- Personal: El personal es responsable de:
  - ✓ Usar Internet y correo electrónico de manera segura y responsable.
  - ✓ Cumplir con las normas de uso de Internet y correo electrónico.

8.7. INSTALACIÓN DE SOFTWARE

8.7.1. REQUISITOS PARA LA INSTALACIÓN DE SOFTWARE

Para instalar software en los sistemas informáticos institucionales, se debe cumplir con los siguientes requisitos:

- Solicitud de aprobación: El solicitante debe proporcionar la siguiente información para la aprobación de la instalación de software:
  - ✓ El nombre del software
  - ✓ La versión del software
  - ✓ El propósito de la instalación
  - ✓ Los requisitos del software
- Evaluación de la solicitud: La Oficina de Tecnologías de la Información debe evaluar la solicitud de instalación de software para determinar si cumple con los requisitos de seguridad.
- Aprobación de la solicitud: La Oficina de Tecnologías de la Información debe aprobar las solicitudes de instalación de software que cumplan con los requisitos de seguridad.

8.7.2. RESPONSABILIDADES

- Dependencias administrativas y académicas: Las dependencias administrativas y académicas son responsables de:
  - ✓ Asegurar que las solicitudes de instalación de software cumplan con los requisitos de la presente política.
  - ✓ Informar a la Oficina de Tecnologías de la Información sobre cualquier instalación de software que no cumpla con los requisitos de la presente política.
- Oficina de Tecnologías de la Información: La Oficina de Tecnologías de la Información es responsable de:
  - ✓ Elaborar y mantener los procedimientos para la instalación de software.
  - ✓ Proporcionar capacitación al personal sobre los procedimientos para la instalación de software.
  - ✓ Supervisar el cumplimiento de la presente política.

9. CONTROL DE ACCESO

La implementación de un sólido control de acceso es fundamental para proteger la confidencialidad e integridad de la información institucional.

9.1. POLÍTICA DE ACCESO

Se establecerá una política integral de acceso que defina claramente los procedimientos y requisitos para la gestión de acceso a los sistemas y datos de la Universidad Nacional José María Arguedas. Esta política deberá ser revisada y actualizada periódicamente por el Comité de Gestión de Seguridad de la Información.

9.2. IDENTIFICACIÓN Y AUTENTICACIÓN:

La Universidad implementará un sistema de identificación y autenticación robusto que garantice la verificación adecuada de la identidad de los usuarios. Esto puede incluir la aplicación de autenticación de dos factores para accesos críticos.

9.3. AUTORIZACIONES Y PERMISOS:

Se establecerán procesos claros para la asignación de autorizaciones y permisos de acceso. Estos procesos deben basarse en la jerarquía organizativa y las

responsabilidades laborales para garantizar que los usuarios tengan acceso solo a la información necesaria para llevar a cabo sus funciones.

9.4. MONITOREO CONTINUO:

Se implementarán sistemas de monitoreo continuo para supervisar el acceso a los sistemas y datos. Esto permitirá la detección temprana de actividades inusuales o potencialmente maliciosas.

9.5. AUDITORÍAS REGULARES:

El Órgano de control Institucional llevará a cabo auditorías regulares del control de acceso para evaluar su efectividad y asegurar el cumplimiento de las políticas establecidas. Los resultados de estas auditorías se compartirán con el Comité de Gestión de Seguridad de la Información.

9.6. CAPACITACIÓN EN SEGURIDAD:

Se implementarán programas de capacitación en seguridad para todos los usuarios, destacando la importancia de la gestión responsable del acceso a la información y los sistemas. Esta capacitación debe ser periódica y obligatoria para todo el personal.

9.7. DESVINCULACIÓN DE ACCESO:

Se establecerán procedimientos claros para la desvinculación rápida y segura del acceso cuando un empleado deje la institución o cambie de función. Esto incluirá la revisión y actualización regular de los permisos de acceso.

10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS SOFTWARE

10.1. EVALUACIÓN DE SOFTWARE:

Antes de la adquisición, se llevará a cabo una evaluación exhaustiva de cualquier software propuesto. Esta evaluación incluirá criterios de seguridad, compatibilidad, eficiencia y cumplimiento de licencias.

10.2. DESARROLLO SEGURO:

En el caso de desarrollo interno de software, se seguirán prácticas de desarrollo seguro. Esto incluirá la incorporación de controles de seguridad desde las etapas iniciales del ciclo de vida del desarrollo.

10.3. PRUEBAS RIGUROSAS:

Se implementarán procesos de prueba rigurosos antes de la implementación de cualquier software. Las pruebas incluirán evaluaciones de seguridad para identificar y corregir posibles vulnerabilidades.

10.4. ACTUALIZACIONES Y PARCHES:

La Oficina de Tecnologías de la Información será responsable de gestionar y aplicar actualizaciones y parches de seguridad de manera oportuna. Esto garantizará que los sistemas estén protegidos contra las últimas amenazas conocidas.

10.5. CUMPLIMIENTO NORMATIVO:

Todos los sistemas software adquiridos o desarrollados internamente deben cumplir con las normativas y estándares relevantes de seguridad de la información. El Órgano de control Institucional llevará a cabo auditorías para verificar el cumplimiento.

10.6. CONTROL DE VERSIONES:

Se establecerá un sistema de control de versiones para el software en uso. Esto permitirá rastrear y gestionar cambios, facilitando la reversión a versiones anteriores en caso de problemas o vulnerabilidades descubiertas.

10.7. EVALUACIÓN PERIÓDICA DE SEGURIDAD:

Se realizarán evaluaciones periódicas de seguridad en los sistemas de software en uso. Esto incluirá análisis de vulnerabilidades y pruebas de penetración para identificar y abordar posibles riesgos.

10.8. CAPACITACIÓN EN DESARROLLO SEGURO:

El personal involucrado en el desarrollo de software recibirá capacitación regular sobre mejores prácticas de seguridad. Esto incluirá la concienciación sobre posibles amenazas y la importancia de la seguridad en el ciclo de vida del desarrollo de software.

10.9. GESTIÓN DE CICLO DE VIDA:

Se implementará un enfoque integral de gestión del ciclo de vida del software, que abarcará desde la adquisición hasta el retiro. Esto garantizará una planificación y ejecución adecuadas en todas las fases del software.

11. GLOSARIO DE TÉRMINOS

a. Información

Conjunto organizado de datos procesados con representación física o lógica explícita.

b. Activo de Información

Los activos pueden ser:

- **De información:** archivos, bases de datos, manuales, material de información
- **De software:** software de aplicación, software del sistema, herramientas y programas de desarrollo.
- **Físicos:** instalaciones, equipos de cómputo, de comunicaciones, medios magnéticos (discos y cintas) u otro equipo técnico.
- **De servicios:** servicios informáticos y comunicaciones, servicios generales (energía eléctrica, telefonía, iluminación)
- **Personas:** sus calificaciones, habilidades y experiencia.
- **Intangibles:** como la reputación e imagen institucional.

c. Sistema de Información

Conjunto ordenado de elementos cuyas propiedades se relacionan e interaccionan permitiendo la recopilación, procesamiento, mantenimiento, transmisión y difusión de información utilizando diferentes medios y mecanismos tanto automatizados como manuales.

d. Propietario de Activos de Información

En el contexto de la norma NTC 27001, un propietario de activos de información es cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos.

e. Tecnología de la Información

Conjunto de hardware y software operados por la entidad, que componen la plataforma necesaria para procesar y administrar la información que requiere la entidad para llevar a cabo sus funciones.

f. Evaluación de Riesgos

Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto.

g. Administración de Riesgos

Proceso de identificación, control y reducción o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

h. Comité de Gestión de Seguridad de la Información

El Comité de gestión de Seguridad de la Información, es un cuerpo integrado por diferentes representantes de la Universidad, destinado a garantizar el apoyo manifiesto de las directivas a las iniciativas de seguridad.

Su función principal es definir, estructurar, recomendar, hacer seguimiento y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) de la institución. Depende directamente del Rectorado, y complementa el trabajo del Grupo Operativo de Seguridad de la Información sirviendo como consultor técnico en temas relacionados con la seguridad de la información.

i. Responsable de Seguridad Informática

Coordinador general del Comité de Gestión de Seguridad de la Información. Su función principal es supervisar el cumplimiento de la presente Política y los lineamientos del SGSI.

j. Grupo Operativo de Seguridad de la Información

Grupos de apoyo creado en dependencias de la Universidad que manejan información sensible o crítica y que se encargan de velar por la operación del SGSI. Están conformados por funcionarios o contratistas de la dependencia que tengan formación en temas de seguridad de la información.

k. Incidente de Seguridad Informática

Un incidente de seguridad informática es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad, disponibilidad, legalidad o confiabilidad de la información.

Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

l. Cadena de custodia

En el ámbito de la seguridad de la información La cadena de custodia es la aplicación de una serie de normas y procedimientos tendientes a asegurar, depositar y proteger cada activo de información para evitar la pérdida de integridad, disponibilidad o confidencialidad.