UNIVERSIDAD NACIONAL AGRARIA LA MOLINA

PLAN DE RESPALDO DE LA INFORMACIÓN – OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Elaborado por:	Revisado por:	Aprobado por:
Christian Alfredo Zacarias Casas Unidad de Tecnología y Operaciones	**Ing. Raul Sacsa Fernandez** Jefe - Unidad de Tecnología y Operaciones	Firmado digitalmente por: MALPARTIDA ZUBIZARRETA Geison Arturo FAU 20147897406 soft Motivo: Soy el autor del documento Fecha: 01/10/2025 09:18:02-0500 **Ing. Geison Arturo Malpartida Zubizarreta** Jefe - Oficina de Tecnología de Información y Comunicaciones

TABLERO DE CONTROL DE CAMBIOS

Versión	Fecha	Sección	Descripción del cambio	Responsables
01	03.12.24	Todas	Creación del documento	**Christian Alfredo Zacarias Casas** Unidad de Tecnología y Operaciones

ÍNDICE

I. INTRODUCCIÓN

El respaldo de información es un proceso crítico para la Universidad Nacional Agraria La Molina (UNALM), ya que garantiza la protección y recuperación de los datos institucionales frente a incidentes de diversa índole, ya sean fallos humanos, errores técnicos, desastres naturales o ataques cibernéticos. La información almacenada en los servidores y demás activos digitales de la universidad constituye un recurso estratégico cuya integridad, disponibilidad y confidencialidad deben asegurarse para la continuidad de las operaciones académicas y administrativas.

El Plan de Respaldo de Información tiene como objetivo establecer medidas y procedimientos que garanticen la seguridad de la información sensible de la UNALM, asegurando su disponibilidad en caso de incidentes. Su propósito fundamental es garantizar la recuperación efectiva de los datos críticos alojados en los servidores institucionales, ya que estos contienen información clave para la gestión académica, administrativa y de investigación. Estos datos no solo son esenciales para la operatividad de las unidades organizacionales, sino que también inciden directamente en la toma de decisiones estratégicas y en la capacidad de respuesta de la universidad ante contingencias.

La implementación de este plan permitirá minimizar los riesgos asociados a la pérdida de información, contribuyendo a la resiliencia institucional ante eventos adversos, ya sean de origen tecnológico, humano o natural. De este modo, se fortalece la continuidad operativa de la UNALM y se sientan las bases para una gestión eficiente y segura de los activos digitales.

II. PROPÓSITOS Y POLÍTICA

El presente Plan tiene como propósito establecer los lineamientos y procedimientos para la gestión del respaldo y recuperación de la información institucional, asegurando la disponibilidad, integridad y confidencialidad de los datos críticos de la universidad. Se orienta a garantizar la continuidad operativa de los sistemas de información, prevenir la pérdida de datos por fallos técnicos, errores humanos o incidentes de seguridad, y cumplir con los estándares nacionales e internacionales de gestión de la información.

III. ALCANCE

El Plan de Respaldo de Información abarca todos los sistemas de información, bases de datos, documentos electrónicos y demás activos digitales críticos de la universidad, incluyendo servidores, estaciones de trabajo, almacenamiento en la nube y dispositivos móviles con acceso a información institucional. Se aplicará a todas las unidades académicas y administrativas, asegurando que los procesos de respaldo se realicen de manera regular y controlada, de acuerdo con las necesidades y riesgos identificados.

IV. BASE LEGAL

El plan se fundamenta en la legislación nacional sobre protección de datos personales, transparencia y acceso a la información pública, y normativas de seguridad de la información aplicables al sector educativo.

Entre los principales marcos normativos se incluyen:

a. Ley N° 27933, Ley de Protección de Datos Personales.
b. Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 27933, Ley de Protección de Datos Personales
c. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
d. Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento de la Ley de Gobierno Digital
e. Directrices de la Autoridad Nacional de Protección de Datos Personales.
f. Estándares internacionales de seguridad de la información: ISO 27001, ISO 27002 y ISO 27032.

V. TÉRMINOS Y DEFINICIONES

5.1. Confidencialidad:
Protección de la información para evitar su acceso por parte de personas no autorizadas.

5.2. Disponibilidad:
Garantía de acceso oportuno a la información cuando se requiera.

5.3. Integridad:
Protección de la información contra modificaciones no autorizadas o corrupción de datos.

5.4. Plan de Respaldo:
Conjunto de actividades automáticas programadas que permite salvaguardar la información producida por todos los usuarios de las diferentes unidades que las componen.

El respaldo de información es la copia de los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra una catástrofe informática, natural o de cualquier índole, sea posible contar con la mayor parte de la información necesaria para el usuario final.

5.5. Respaldo de información:
Copia de seguridad de los datos almacenados en medios físicos o digitales para su recuperación en caso de pérdida o corrupción.

5.6. Recuperación de datos:

Proceso mediante el cual se restauran los datos desde un respaldo ante un incidente.

VI. NORMATIVA ASOCIADA

El Plan de Respaldo de Información se articula con las políticas y normativas internas de la universidad, tales como:

a. Política de Seguridad de la Información.
b. Reglamento de Uso de Tecnologías de la Información y Comunicaciones.
c. Plan de Continuidad Operativa y Recuperación ante Desastres.
d. Directrices internas de gestión documental y administración de bases de datos.

Este marco orienta la correcta implementación del Plan de Respaldo, asegurando su alineamiento con las estrategias institucionales de transformación digital y gestión de la información.

VII. ANÁLISIS SITUACIONAL

Se procederá a detallar el equipamiento tecnológico físico, virtual y nube que posee la UNALM para generar los respaldos de información; asimismo, se detalla la información de los servidores que son respaldados por el mencionado equipamiento tecnológico.

a. Equipamiento tecnológico físico (Hardware):

   - Servidores.

b. Equipamiento tecnológico virtual (Software):

   - Servidores virtuales (VMWare)

c. Equipamiento tecnológico Nube:

   - Amazon Simple Storage Service–S3

d. Detalle del uso del equipamiento tecnológico físico, virtual y nube:

   - Servidor y Unidad de almacenamiento (Físico), se utiliza para respaldar la información de forma local, las cuales se generan de acuerdo al Cronograma de Respaldo de Información.

   - Tape Backup (físico) se utiliza para respaldar la información en cintas magnéticas.

   - Veeam Backup & Replication (Virtual), se utiliza para respaldar las imágenes de los servidores, las cuales se generan cada fin de semana de acuerdo al Cronograma de Respaldo de Información.

- Amazon S3 (Nube), se utiliza para almacenar la información temporal (imagen de los últimos 7 días) de los servidores de aula virtual, y la información de moodledata se genera semestralmente de acuerdo con el Cronograma de Respaldo de Información.

e. Detalle de información respaldada:

- Los servidores y la información a respaldar se detallan en el Anexo 03 (F01-PS06.1.01 Cronograma de Respaldo de Información).

VIII. OBJETIVOS

8.1. Objetivo General

Garantizar la integridad, disponibilidad y confiabilidad de toda la información generada y almacenada en los servidores institucionales, mediante la implementación de estrategias y procedimientos de respaldo que aseguren la protección de los datos frente a fallos tecnológicos, errores humanos, ciberataques y desastres, permitiendo su recuperación oportuna y efectiva en caso de incidentes.

Para cumplir con este objetivo, el plan establece directrices para la ejecución de copias de seguridad, su almacenamiento seguro, la verificación de su integridad y la definición de protocolos de restauración, asegurando la continuidad de las operaciones académicas, administrativas y de investigación en la universidad.

IX. ESTRATEGIAS

9.1. Acciones estratégicas

9.1.1. Revisión y Actualización del Inventario de Equipamiento Tecnológico

Para poder ejecutar el Plan de Respaldo de la Información, es necesario contar con un inventario actualizado de los servidores.

El inventario de equipamiento tecnológico deberá contener la totalidad de servidores, así como su ubicación física y virtual.

9.1.2. Normas de Operación

La Unidad de Tecnologías y Operaciones / Redes – UTO, ha establecido normas para la obtención de restauraciones de información tomando como base el inventario actualizado del equipamiento tecnológico (servidores) para ello, se han definido aspectos que se detallan a continuación:

a. La información a respaldar de los servidores (imagen).
b. Se deberá establecer un cronograma de respaldo de información, donde se describa la periodicidad y horario de ejecución de los respaldos para los servidores.
c. Los respaldos deberán ser registrados en una Bitácora de Respaldo de Información (F02-PS06.1.01).
d. La información de servidores (bases de datos, configuraciones) se ejecuta de forma automática.
e. Los colaboradores internos deberán realizar la copia de respaldo de su información crítica.
f. La relevancia de la información a ser respaldada ha sido establecida como todo el servidor, la cual deberá ser resguardada de forma prioritaria por contener información valiosa para la institución.

9.1.3. Lineamiento de Respaldo:

La Unidad de Tecnologías y Operaciones/Redes - UTO, ha establecido lineamientos que deben ser respetadas para el correcto funcionamiento del procedimiento establecido; para ello, a continuación, se presentan las políticas definidas:

9.1.3.1. Consideraciones Generales:

a. La institución mantiene en sus registros información de distintos niveles de importancia (Alta, Media, Baja). El mecanismo, periodicidad y tecnología de respaldo utilizada para resguardar la información en el tiempo dependerá de la importancia la institución le asigne.
b. Cada respaldo que se realice (automático), deberá quedar registrado en las bitácoras respectivas (respaldo o restauración).
c. Los medios de respaldos removibles (cintas magnéticas) deberán ser retirados del recinto donde se realicen los respaldos y llevados a otro que garantice la fiabilidad, seguridad y disponibilidad de los mismos.
d. Las contraseñas de usuario NO deberán ser respaldadas.
e. La información que NO es relevante/valiosa para la institución, NO será respaldada.

9.1.3.2. Frecuencia y tipo de respaldo:

a. La periodicidad con que se realizarán los respaldos será de acuerdo al Cronograma de Respaldo de Información.

b. La Unidad de Tecnologías y Operaciones deberá definir los tipos de respaldos a utilizar como estándar para la institución. Cada estándar debe considerar la frecuencia del respaldo, los medios de almacenamiento, tipos de contenido, tiempo de almacenamiento y borrado de la información.
c. Las solicitudes especiales de respaldo protegido deberán ser autorizadas por el responsable de la Unidad de Tecnologías y Operaciones o el responsable Encargado de acuerdo a su designación.

9.1.3.3. Protección de la información en medios de respaldo:

a. La criticidad de respaldo como nivel mínimo debe ser almacenado en una ubicación diferente a donde se saca el backup; ello, debe permitir que la información sea salvaguardada y escape de un daño producto de un desastre en el centro de datos principal de la institución.
b. Los registros que se generen deben ser exactos y completos de las copias y procedimientos documentados para la restauración.
c. Para prevenir pérdidas accidentales, todas las copias de seguridad deben almacenarse en un lugar protegido, con acceso controlado.
d. El área de Redes de la Unidad de Tecnologías y Operaciones debe mantener un inventario actualizado de la información almacenada externamente.

9.1.3.4. Eliminación de la información:

a. Todo equipo computacional o medio de almacenamiento que sea dado de baja, deberá ser examinado por la Unidad de Tecnologías y Operaciones, con el fin de comprobar que la información ha sido borrada.

9.2. Ruta Estratégica

a. Elaboración del Plan:
b. Ejecución:
c. Reporte

9.3. Planificación

9.3.1. Etapas

El Plan de Respaldo de Información, considera las siguientes etapas:

a. Elaboración del Plan, donde se incluye el anexo correspondiente (F01-PS06.1.01 Cronograma de Respaldo de Información).
b. Revisión y aprobación del Plan.

9.3.2. Ámbito de ejecución

La ejecución se llevará a cabo en el centro de datos principal y secundario de la UNALM.

9.3.3. Seguimiento y monitoreo

El desarrollo del respaldo de información se efectuará, según el cronograma establecido en el (Anexo 03). Éste cronograma detalla el horario, tipo, origen, elemento respaldado y destino.

Asimismo, el seguimiento y monitoreo a los respaldos de información que hayan sido generados será realizado por los Administradores de Redes, si existen anomalías en la ejecución de respaldos de información deberá ser reportar al responsable de la Unidad de Tecnologías y Operaciones para tomar las acciones correctivas del caso.

X. INDICADORES Y EVALUACIÓN DEL DESEMPEÑO

10.1. Indicadores

Para medir el éxito del Plan de Respaldo de la Información y evaluar el desempeño en la implementación de las acciones y la consecución de los logros esperados, se establecerán indicadores clave de rendimiento (KPI) que permitan evaluar el impacto de las estrategias adoptadas. A continuación, se detallan los logros que se esperan alcanzar junto con sus indicadores asociados:

a. Proteger la información institucional de todos los sistemas académicos y administrativos almacenada en los servidores.
    - Porcentaje de sistemas respaldados regularmente: Proporción de sistemas académicos y administrativos que tienen respaldo automatizado, medido mensualmente. Se espera alcanzar un 100% de respaldo en todos los sistemas críticos.

- Tasa de éxito en restauraciones de respaldo: Proporción de intentos de restauración exitosos frente a intentos fallidos. Se espera mantener una tasa de éxito del 100% en las pruebas de restauración.

b. Mantener la información disponible para el uso de los usuarios, así como la continuidad de todos los servicios.

- Tiempo promedio de recuperación: Tiempo promedio que se tarda en restaurar los datos y poner en funcionamiento los servicios críticos después de un fallo. El objetivo es mantener este tiempo dentro de las 2 horas posteriores al incidente.
- Tasa de disponibilidad de los servicios: Porcentaje de tiempo en que los sistemas y servicios académicos y administrativos están operativos y accesibles para los usuarios, medido mensualmente. Se espera alcanzar una disponibilidad superior al 99.9%.
- Número de interrupciones no programadas: Cantidad de fallos en los sistemas debido a la falta de un respaldo efectivo o fallas en la infraestructura de respaldo. Se busca reducir este número a cero o mínimas incidencias.

10.2. Evaluación del Desempeño

La evaluación del desempeño se realizará de manera periódica, utilizando los indicadores mencionados anteriormente para medir los avances hacia los logros establecidos. Los resultados obtenidos se analizarán de la siguiente manera:

a. Monitoreo mensual: Se revisarán los indicadores clave de manera mensual para asegurar que los respaldos se estén ejecutando de acuerdo con el plan establecido. Esto incluirá una revisión de los tiempos de recuperación y la disponibilidad de los sistemas.
b. Análisis de incidentes: En caso de que se presenten incidentes de pérdida de datos o interrupciones en los servicios, se analizarán las causas subyacentes y se implementarán medidas correctivas inmediatas para evitar que se repitan.
c. Informe de progreso: Se generará un informe semestral sobre el estado del plan de respaldo, donde se destacarán tanto los logros alcanzados como las áreas de mejora. Este informe será presentado a la alta dirección de la universidad para garantizar la alineación de los esfuerzos con los objetivos institucionales.

Estas acciones asegurarán que el plan de respaldo no solo se implemente de manera efectiva, sino que también se mantenga

actualizado y funcione de manera continua, protegiendo la integridad, disponibilidad y confiabilidad de la información institucional.

XI. RIESGOS

11.1. Riesgos Potenciales en el Respaldo de la Información

La implementación de un plan de respaldo de información en la universidad enfrenta diversos riesgos que pueden comprometer la efectividad del proceso y la seguridad de los datos. Entre los principales riesgos se identifican:

a. Fallas en los medios de almacenamiento: La degradación de discos duros, servidores o unidades de respaldo puede generar pérdida o corrupción de los datos almacenados.
b. Errores en la ejecución de respaldos: Fallos en la configuración, interrupciones inesperadas o falta de monitoreo pueden provocar copias incompletas o inexistentes.
c. Ataques cibernéticos y ransomware: Malware, accesos no autorizados o secuestro de datos pueden afectar tanto la información en producción como los respaldos almacenados.
d. Almacenamiento en ubicaciones vulnerables: Si los respaldos no se encuentran en entornos seguros, pueden ser afectados por desastres naturales, incendios, robos o accesos indebidos.
e. Falta de pruebas de restauración: Respaldos defectuosos o incompatibles con los sistemas actuales pueden volverse inutilizables en situaciones críticas.
f. Errores humanos: Eliminación accidental de copias, uso incorrecto de credenciales o mala gestión de los procedimientos pueden comprometer la recuperación de la información.

11.2. Riesgos Potenciales en el Respaldo de la Información

Para minimizar los riesgos asociados al respaldo de la información y garantizar su confiabilidad, se implementarán las siguientes estrategias:

a. Estrategia de respaldo 3-2-1: Mantener tres copias de la información (una principal y dos de respaldo) en al menos dos tipos de almacenamiento diferentes, con una copia externa o en la nube.
b. Automatización y monitoreo continuo: Implementación de herramientas de respaldo automatizadas con alertas y reportes en tiempo real para detectar fallos en la ejecución de copias.

c. Pruebas periódicas de restauración: Ejecución de simulaciones de recuperación de datos para validar la integridad y disponibilidad de los respaldos almacenados.
d. Seguridad en el almacenamiento de respaldos: Uso de cifrado en los datos de respaldo, controles de acceso estrictos y almacenamiento en entornos protegidos contra desastres y accesos no autorizados.
e. Protección contra ciberataques: Implementación de soluciones de ciberseguridad como firewalls avanzados, autenticación multifactor y monitoreo proactivo de vulnerabilidades.
f. Capacitación del personal: Formación en gestión de respaldos, recuperación de información y protocolos de seguridad para reducir errores humanos.
g. Políticas de acceso y auditoría: Control estricto de usuarios con permisos sobre los respaldos, auditorías regulares de accesos y modificaciones en los datos respaldados.

Estas estrategias permitirán asegurar la protección y disponibilidad de la información institucional, garantizando que el plan de respaldo sea eficaz ante cualquier contingencia.

XII. RECURSOS

Para la ejecución de restauración de información de los equipos servidores se procedió a elaborar un cronograma donde se secciona a detalle el horario, tipo, origen, elemento respaldado y destino de la información que será respaldada. Ello se detalla en el Anexo 03.

a. Ejecución
La restauración de información estará programada de acuerdo al cronograma adjunto (Anexo 03).
b. Financiamiento
Se financia a través del presupuesto asignado a la Unidad de Tecnologías y Operaciones.
c. Recursos Humanos
El recurso humano es el personal CAS de la Unidad de Tecnologías y Operaciones/Redes-UTO

XIII. ANEXOS

- Anexo 01 Formato F02-PS06.1.01 Bitácora de Respaldo de Información
- Anexo 02 Inventario de Equipamiento/Servicios Tecnológicos
- Anexo 03 Formato F01-PS06.1.01 Cronograma de Respaldo de Información

ANEXO 01

F02-PS06.1.01 Bitácora de Respaldo de Información

	FORMATO	F02-PS06.1.01	
	BITÁCORA DE RESPALDO DE INFORMACIÓN	Versión: 02 Fecha: 10-02-25	Página 1

N°	ORIGEN								DESTINO	
	Nombre_Grupo	Elementos del grupo	Elementos Respaldados	Tamaño de Respaldo	Tipo_Respaldo	Estado	Fecha_Hora_Inicio	Fecha_Hora_Fin	Ubicación_Respaldo	Observaciones
01										
02										
03										
04										
05										

LEYENDA:

Tipo_Respaldo Existen 02 tipos de respaldo, tales como Incremental y Full
Estado Existen 02 estados para la realización de respaldo, tales como Correcta e Incorrecta.

ANEXO 02

Inventario de Equipamiento/Servicios Tecnológicos

Dispositivos	Total
Servidores (Virtualizados)	110
Servidores (Físico)	18
Servidores (Nube)	02

ANEXO 03

F01-PS06.1.01 Cronograma de Respaldo de Información

	FORMATO	F01-PS06.1.01	
	CRONOGRAMA DE RESPALDO DE INFORMACIÓN	Versión: 01 Fecha: 10-02-25	Página 1

CRONOGRAMA DE RESPALDO DE INFORMACIÓN (AÑO)

Respaldo Diario (de Lunes a Sábado) Tipo Incremental				
Origen	Elemento Respaldado	Destino	Horario	
(Órgano / Unidad Orgánica)				
(Órgano / Unidad Orgánica)				