

	PLAN INTERNO		CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN		Versión: 01 Fecha: 03-12-24	Página 1 de 14

UNIVERSIDAD NACIONAL AGRARIA LA MOLINA



PLAN DE RESTAURACIÓN 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	 Ing. Geison Arturo Malpartida Zubizarreta Jefe - Oficina de Tecnología de Información y Comunicaciones

	PLAN INTERNO		CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN		Versión: 01 Fecha: 03-12-24	Página 2 de 14

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

	PLAN INTERNO		CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN		Versión: 01 Fecha: 03-12-24	Página 3 de 14

ÍNDICE

I.	INTRODUCCIÓN	4
II.	PROPÓSITOS Y POLÍTICA	4
III.	ALCANCE	5
IV.	BASE LEGAL	5
V.	TÉRMINOS Y DEFINICIONES	5
VI.	NORMATIVA ASOCIADA	6
VII.	ANÁLISIS SITUACIONAL	6
VIII.	OBJETIVOS	7
IX.	ESTRATEGIAS	7
9.1.	Acciones estratégicas	7
9.2.	Ruta Estratégica	8
9.3.	Planificación	8
X.	INDICADORES Y EVALUACIÓN DEL DESEMPEÑO	9
10.1.	Indicadores	9
10.2.	Evaluación del Desempeño	9
XI.	RIESGOS	10
XII.	RECURSOS	11
XIII.	ANEXOS	11

	PLAN INTERNO	CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN	Versión: 01 Fecha: 03-12-24	Página 4 de 14

I. INTRODUCCIÓN

En el contexto actual, la gestión de la información en la Universidad Nacional Agraria La Molina (UNALM) es un pilar fundamental para el cumplimiento de sus funciones académicas, administrativas y de investigación. La dependencia de los sistemas digitales hace imprescindible la existencia de mecanismos que garanticen la recuperación de datos en caso de incidentes que comprometan su integridad y disponibilidad. La restauración de información es, por tanto, un proceso clave que asegura la continuidad de las operaciones frente a eventos adversos, ya sean provocados por errores humanos, fallas técnicas, desastres naturales o ataques cibernéticos.

El Plan de Restauración de la Información tiene como propósito principal establecer un marco de actuación que permita recuperar de manera efectiva la información crítica almacenada en los activos tecnológicos de la UNALM, principalmente sus servidores. Estos contienen datos esenciales para la gestión institucional y la toma de decisiones en todos los niveles, desde las unidades académicas hasta las instancias de gobierno universitario. La pérdida o alteración de estos datos podría generar impactos significativos en la operatividad y planificación estratégica de la universidad.

Para ello, el presente Plan define procedimientos y medidas técnicas orientadas a minimizar el tiempo de inactividad y garantizar la integridad de la información restaurada. Asimismo, establece los roles y responsabilidades del personal involucrado en el proceso, asegurando que la respuesta ante incidentes sea eficiente y coordinada. De este modo, la UNALM fortalece su capacidad de resiliencia digital y refuerza su compromiso con la gestión segura y confiable de la información institucional.

II. PROPÓSITOS Y POLÍTICA

El propósito del Plan de Restauración de la Información es establecer un marco de acción que garantice la integridad, disponibilidad y confidencialidad de la información institucional de la UNALM ante incidentes que comprometan su operatividad. Este plan define estrategias y procedimientos que permiten la recuperación eficiente de los datos críticos almacenados en los servidores y demás activos tecnológicos, asegurando la continuidad de las funciones académicas, administrativas y de investigación.

Se basa en principios de seguridad, resiliencia y cumplimiento normativo, priorizando la implementación de medidas preventivas y reactivas que reduzcan el impacto de eventos adversos. Asimismo, se promueve una cultura organizacional que valore la protección y gestión adecuada de la información, estableciendo responsabilidades claras para los actores involucrados en los procesos de respaldo y restauración.

	PLAN INTERNO	CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN	Versión: 01 Fecha: 03-12-24	Página 5 de 14

III. ALCANCE

Este Plan aplica a todos los sistemas de información, servidores, bases de datos y demás activos digitales de la UNALM que contienen información relevante para el desarrollo de sus actividades académicas y administrativas. Involucra a todas las unidades organizacionales que gestionan y utilizan estos recursos, estableciendo lineamientos para la identificación, almacenamiento, respaldo y recuperación de datos ante eventos de pérdida, corrupción o ataque cibernético.

Asimismo, abarca las responsabilidades de los usuarios y del personal técnico encargado de la gestión de TI, incluyendo la planificación, ejecución y monitoreo de los procesos de restauración. También contempla la coordinación con otras áreas estratégicas de la universidad en casos de incidentes de alto impacto que requieran una respuesta institucional integrada.

IV. BASE LEGAL

El presente Plan se sustenta en las normativas nacionales e internacionales en materia de seguridad de la información, gestión de riesgos y continuidad operativa. Entre los marcos regulatorios y normativos que respaldan su implementación se incluyen.

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.
- g. Resolución del Consejo Directivo N° 006-2015-SUNEDU/CD, que aprueba el Modelo de Licenciamiento y su Implementación en el Sistema Universitario Peruano.

V. TÉRMINOS Y DEFINICIONES

- 5.1. Continuidad Operativa:** Capacidad de la universidad para mantener sus funciones esenciales en caso de fallos tecnológicos, desastres naturales o ataques cibernéticos.
- 5.2. Incidente de Seguridad:** Cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información de la UNALM.
- 5.3. Integridad:**

	PLAN INTERNO	CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN	Versión: 01 Fecha: 03-12-24	Página 6 de 14

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

5.4. Restauración de Información: Conjunto de actividades manuales/automáticas programadas como simulacro por mantenibilidad frente a un incidente ocasional o por vulnerabilidad que permite recuperar la información perdida. Los riesgos que corre la información pueden perderse debido a diversas causas como:

- a. Terrorismo/sabotaje.
- b. Desastres naturales (Terremotos, inundaciones, etc.)
- c. Caídas eléctricas.
- d. Errores de software.
- e. Errores de hardware.
- f. Eliminación intencional o accidental.

5.5. Respaldo de Datos: Copia de seguridad de la información institucional almacenada en medios digitales con el fin de garantizar su recuperación en caso de pérdida o corrupción.

VI. NORMATIVA ASOCIADA

El Plan de Restauración de Información se enmarca dentro de la normativa interna de la UNALM y las regulaciones nacionales aplicables a la seguridad de la información, incluyendo:

- a. Reglamento Interno de Seguridad de la Información de la UNALM, que establece los lineamientos para la gestión y protección de los datos institucionales.
- b. Plan de Gestión de Tecnologías de la Información (PETI) de la UNALM, que define las directrices para la gestión de TI en la universidad.
- c. Política de Continuidad del Negocio de la UNALM, que contempla las acciones necesarias para garantizar la operatividad de los servicios ante eventos críticos.
- d. Directivas del Centro Nacional de Seguridad Digital, sobre gestión de incidentes de seguridad de la información en entidades públicas.

Este marco normativo garantiza que la restauración de la información se realice bajo estándares de seguridad, legalidad y eficiencia, asegurando la protección del patrimonio digital de la universidad.

VII. ANÁLISIS SITUACIONAL

Se procederá a detallar el equipamiento tecnológico (Software) que posee la UNALM para generar las restauraciones de información.

- a) Equipamiento tecnológico (Software):

	PLAN INTERNO	CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN	Versión: 01 Fecha: 03-12-24	Página 7 de 14

- Servidores Virtuales, se crea una máquina virtual y se restaura la imagen del servidor, después se verifica el encendido y que la información respaldada se encuentre correcta.

VIII. OBJETIVOS

8.1. Objetivo General

Garantizar la disponibilidad, integridad y seguridad de la información generada por los usuarios internos y externos de la Universidad Nacional Agraria La Molina (UNALM).

Para ello, establece medidas y procedimientos que permitan la protección y recuperación efectiva de los datos almacenados en los servidores y demás activos digitales institucionales. Contar con información íntegra que ha sido elaborada por los usuarios internos y externos de la UNALM.

IX. ESTRATEGIAS

9.1. Acciones estratégicas

9.1.1. Revisión y Actualización del Inventario de Equipamiento Tecnológico

Para poder ejecutar el plan de restauración de 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

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) y toda información alojada por los colaboradores internos y usuario externos en dichos equipos; para ello, se han definido aspectos que se detallan a continuación:

- Los colaboradores internos son responsables de alojar toda información crítica en las herramientas brindadas por la Unidad de Tecnologías y Operaciones.
- La información que se respalda en los servidores corresponde a la imagen total del servidor.
- Se deberá establecer un F03-PS06.1.01 Cronograma de Restauración de Información donde se describan las fechas y horarios de ejecución, logrando obtener las evidencias del

	PLAN INTERNO	CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN	Versión: 01 Fecha: 03-12-24	Página 8 de 14

funcionamiento correcto de recuperación de los respaldos para los diferentes tipos de información del punto precedente.

- d. Las restauraciones de información de usuario deberán ser solicitados a la Unidad de Tecnologías y Operaciones-Redes y serán registradas en la Herramienta de Gestión Requerimientos Incidencias (F05-PS06.1.01).
- e. Las restauraciones en todos sus tipos deberán ser registradas en una Bitácora de Restauración de Información (F04-PS06.1.01).

9.1.3. Frecuencia y tipo de restauraciones:

- a. La periodicidad con que se realizarán las restauraciones de Simulacro por Mantenibilidad será de acuerdo con el F03-PS06.1.01 Cronograma de Restauración de Información.
- b. La periodicidad con que se realizarán las restauraciones de información de colaboradores internos será de acuerdo con la solicitud del mismo.
- c. Las solicitudes de los usuarios respecto a restauración deberán ser autorizadas por el responsable de la Unidad de Tecnologías y Operaciones o el responsable Encargado de acuerdo con su designación.

9.2. Ruta Estratégica

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

9.3. Planificación

9.3.1. Etapas

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

- a. Elaboración del Plan, donde se incluye el anexo correspondiente (F03-PS06.1.01 Cronograma de Restauración 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 (ubicado en OTIC) y secundario (ubicado en BAN 2).

9.3.3. Seguimiento y monitoreo

El desarrollo de la restauración de información se efectuará, según el cronograma establecido en el (Anexo 03). Éste

	PLAN INTERNO	CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN	Versión: 01 Fecha: 03-12-24	Página 9 de 14

cronograma detalla el horario, tipo, origen, elemento respaldado y destino.

Por último, el seguimiento y monitoreo de las restauraciones de información que hayan sido generados será realizado por los Administradores de Redes con la validación del responsable de la Unidad de Tecnologías y Operaciones.

X. INDICADORES Y EVALUACIÓN DEL DESEMPEÑO

10.1. Indicadores

La efectividad del Plan de Restauración de Información será medida a través de indicadores clave que permitan evaluar el cumplimiento de los objetivos planteados y la capacidad de recuperación de la información ante incidentes. Los logros esperados incluyen:

a) Mantener la disponibilidad de la información: Garantizar que los datos estén accesibles para los usuarios autorizados y que los servicios institucionales continúen operativos sin interrupciones críticas.

- Indicador 1: Tasa de disponibilidad de la información (% de tiempo en que los sistemas están accesibles sin fallos).
- Indicador 2: Tiempo medio de recuperación (tiempo requerido para restablecer la información tras un incidente).

b) Proteger la información institucional procesada y almacenada en los servidores: Asegurar la integridad, confidencialidad y seguridad de los datos críticos.

- Indicador 3: Tasa de éxito en la restauración de respaldos (% de restauraciones exitosas frente a intentos fallidos).
- Indicador 4: Frecuencia de auditorías y pruebas de recuperación (número de simulacros de recuperación realizados en un período determinado).
- Indicador 5: Número de incidentes de pérdida o corrupción de datos (cantidad de eventos registrados que comprometan la integridad de la información).

10.2. Evaluación del Desempeño

El desempeño del plan será evaluado periódicamente mediante auditorías de seguridad, pruebas de restauración de respaldos y monitoreo continuo de los indicadores establecidos. Se implementará un sistema de control y reporte que permita analizar tendencias, identificar

	PLAN INTERNO		CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN		Versión: 01 Fecha: 03-12-24	Página 10 de 14

vulnerabilidades y proponer mejoras en los procedimientos de respaldo y recuperación.

Además, se fomentará la capacitación del personal responsable en la ejecución del plan, asegurando que los protocolos sean aplicados de manera eficiente y alineada con las mejores prácticas de gestión de la información. Con ello, se busca optimizar la resiliencia institucional ante fallos o ataques, garantizando la continuidad operativa de la UNALM.

XI. RIESGOS

11.1. Riesgos Potenciales en la Restauración de la Información

La restauración de la información en la universidad enfrenta diversos riesgos que pueden comprometer la integridad, disponibilidad y seguridad de los datos institucionales. Entre los principales riesgos se encuentran:

- a. Fallas en el hardware y almacenamiento: La obsolescencia o mal funcionamiento de los servidores, discos duros y sistemas de respaldo puede ocasionar la pérdida irreversible de información crítica.
- b. Errores humanos: La falta de capacitación o procedimientos inadecuados pueden llevar a la eliminación accidental de datos, configuraciones erróneas o restauraciones incompletas.
- c. Ciberataques y malware: Ransomware, virus y ataques dirigidos pueden cifrar o eliminar información clave, impidiendo su recuperación.
- d. Desastres naturales o siniestros: Inundaciones, incendios o terremotos pueden afectar la infraestructura tecnológica, dañando los servidores y medios de almacenamiento.
- e. Corrupción de datos o fallas en el software: Incompatibilidades de versiones, errores en bases de datos o problemas en sistemas de gestión pueden comprometer la integridad de la información al momento de la restauración.
- f. Pérdida de acceso a respaldos: Falta de controles de acceso o pérdida de credenciales pueden retrasar o impedir la recuperación de la información.

11.2. Estrategias de Mitigación

Para garantizar la restauración efectiva de la información y minimizar el impacto de los riesgos, se implementarán las siguientes estrategias:

- a. Respaldo periódico y redundante: Implementación de copias de seguridad automatizadas con almacenamiento en ubicaciones distintas, incluyendo la nube y servidores físicos seguros.

	PLAN INTERNO	CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN	Versión: 01 Fecha: 03-12-24	Página 11 de 14

- b. Pruebas regulares de restauración: Simulación de procesos de recuperación en entornos controlados para validar la integridad de los respaldos y la eficacia de los procedimientos.
- c. Capacitación del personal: Formación continua en gestión de respaldos, seguridad de la información y protocolos de recuperación para minimizar errores humanos.
- d. Implementación de medidas de ciberseguridad: Uso de firewalls, antivirus, autenticación multifactor y monitoreo continuo para prevenir ataques informáticos.
- e. Planes de contingencia ante desastres: Definición de protocolos de actuación en caso de siniestros, con ubicaciones alternativas para la infraestructura tecnológica y accesos seguros a la información crítica.
- f. Control y auditoría de accesos: Gestión estricta de credenciales, permisos diferenciados y registro de accesos a los sistemas de respaldo para evitar pérdidas o alteraciones no autorizadas.

Estas acciones permitirán a la UNALM asegurar la continuidad operativa y proteger su información institucional, garantizando una restauración efectiva en caso de incidentes.

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 F04-PS06.1.01 Bitácora de Restauración de Información
- Anexo 02 Inventario de Equipamiento/Servicios Tecnológicos
- Anexo 03 Formato F03-PS06.1.01 Cronograma de Restauración de Información
- Anexo 004 Formato F05-PS06.1.01 Herramienta de Gestión Requerimientos Incidencias

	PLAN INTERNO		CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN		Versión: 01 Fecha: 03-12-24	Página 12 de 14

ANEXO 01

F04-PS06.1.01 Bitácora de Restauración de Información

	FORMATO		F04-PS06.1.01	
	BITÁCORA DE RESTAURACIÓN DE INFORMACIÓN		Versión: 01 Fecha: 10-02-25	Página 1

Nº	Tipo_Restauración	SOLICITUD (*)					RESTAURACIÓN		
		Fecha_Solicitud	Hora_Solicitud	Usuario_Solicitante	Unidad_Solicitante	Descripción_Información	Ubicación_Destino	Fecha_Restauración	Responsable
01									
02									
03									
04									
05									

ANEXO 02

Inventario de Equipamiento/Servicios Tecnológicos

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

	PLAN INTERNO		CÓDIGO: PI03-PRRI-OTIC	
	PLAN DE RESTAURACIÓN DE LA INFORMACIÓN		Versión: 01 Fecha: 03-12-24	Página 13 de 14

ANEXO 03

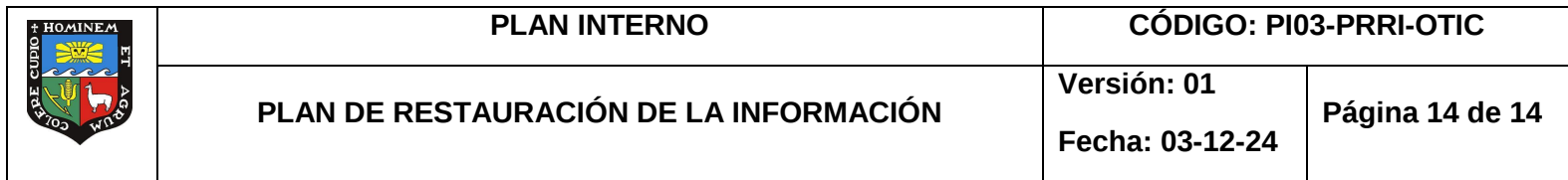
F03-PS06.1.01 Cronograma de Restauración de Información

	FORMATO	F03-PS06.1.01	
	CRONOGRAMA DE RESTAURACIÓN DE INFORMACIÓN	Versión: 02 Fecha: 10-02-25	Página 1

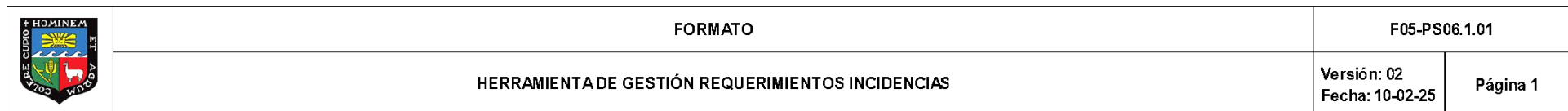
CRONOGRAMA DE RESTAURACIÓN DE INFORMACIÓN (AÑO)

ACTIVIDAD DE RESTAURACIÓN	FECHAS SIMULACRO	HORARIO SIMULACRO	DESCRIPCIÓN RESPALDO	DESTINO RESPALDO

ANEXO 04



F05-PS06.1.01 Herramienta de Gestión Requerimientos Incidencia

[illegible]