UNIVERSIDAD NACIONAL AGRARIA LA MOLINA

Teléfono 614-7800 Anexos 211-212 Email: secgeneral@lamolina.edu.pe Apartado 12-056 Lima-Perú

La Molina, 21 de abril de 2025
TR. N.° 0198-2025-R-UNALM

Señor:

Presente.-

Con fecha 21 de abril de 2025, se ha expedido la siguiente resolución:
"RESOLUCIÓN N.° 0198-2025-R-UNALM. - La Molina, 21 de abril de 2025. CONSIDERANDO: Que, el artículo 2° de la Ley 28551, Ley que establece la obligación de elaborar y presentar planes de contingencia, define a los planes de contingencia como instrumentos de gestión que definen los objetivos, estrategias y programas que orientan las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres permitiendo disminuir o minimizar los daños, las víctimas u pérdidas que podrían ocurrir a consecuencia de fenómenos naturales, tecnológicos o de la producción industrial, potencialmente dañinos; Que, el artículo 3° de la citada Ley establece que todas las personas naturales y jurídicas de derecho público o privado que conducen o administran empresas, instalaciones, edificaciones y recintos tienen la obligación de elaborar y presentar, para su aprobación ante la autoridad competente, planes de contingencia para cada una de las operaciones que desarrolle; Que, mediante la Resolución de Contraloría N.° 320-2006-CG, la Contraloría General de la República aprueba las Normas de Control Interno, que son aplicables a las Entidades del Estado de conformidad con lo establecido por la citada Ley 28716, señalando en el numeral 3.10 "**Controles para las Tecnologías de la Información y Comunicacione**s" que "*La información de la entidad es provista mediante el uso de Tecnologías de la Información y Comunicaciones (TIC). Las TIC abarcan datos, sistemas de información, tecnología asociada, instalaciones y personal. Las actividades de control de las TIC incluyen controles que garantizan el procesamiento de la información para el cumplimiento misional y de los objetivos de la entidad, debiendo estar diseñados para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas*" Que, asimismo el comentario 07 del numeral 3.10 "**Controles para las Tecnologías de la Información y Comunicacione**s" de la referida norma, dispone que, "*Para el adecuado ambiente de control en los sistemas informáticos, se requiere que éstos sean preparados y programados con anticipación para mantener la continuidad del servicio. Para ello se debe elaborar, mantener y actualizar periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado donde se establezcan procedimientos para la recuperación de datos con el fin de afrontar situaciones de emergencia*"; Que, a través de la Ley 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), se señala que el SINAGERD es el sistema interinstitucional, sinérgico, descentralizado, transversal y participativo, creado a fin de identificar y reducir los riesgos asociados a peligros o minimizar sus efectos, así como evitar la generación de nuevos riesgos, y preparación y atención ante situaciones de desastre, mediante el establecimiento de principios, lineamientos de política, componentes, procesos e instrumentos de la Gestión del Riesgo de Desastres; Que, el Reglamento de la Ley 29664, aprobado por Decreto Supremo N.° 048-2011-PCM, contiene dentro de sus definiciones al Plan de contingencia, señalando que, "Son los procedimientos específicos preestablecidos de coordinación, alerta, movilización y respuesta ante la ocurrencia o inminencia de un evento particular para el cual se tiene escenarios definidos. Se emite a nivel nacional, regional y local";

Que, mediante Resolución Ministerial N.° 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2da. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, precisando en su acápite A.17.1.2 del Anexo A, denominado "**Implementación de continuidad de seguridad de la información**", de la citada Norma Técnica Peruana dispone que "*La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa*"; Que, conforme al literal f) y h) del artículo 57° del Reglamento de Organización y Funciones de la Universidad Nacional Agraria La Molina (UNALM), la Oficina de Tecnología de Información y Comunicaciones (OTIC), tiene entre sus funciones: organizar, supervisar, controlar, desarrollar e implementar los requerimientos y el uso racional de las tecnologías de la información, soporte y comunicaciones; así como aplicar medidas de seguridad informática e implementar soluciones de protección de las redes, equipos y sistemas de información de la UNALM; Que, con Carta N.° 0161-2025-OTIC/RECTORADO, de fecha 15 de abril de 2025, el Ing. Geison Arturo Malpartida Zubizarreta, jefe de la Oficina de Tecnología de Información y Comunicaciones (OTIC), remite al Rectorado el "PLAN DE CONTINGENCIA INFORMÁTICO Y RECUPERACIÓN DE SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN DE LA UNALM", para su respectiva la aprobación; Que, el Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicación de UNALM, tiene como propósito garantizar la continuidad operativa de los servicios tecnológicos institucionales ante incidentes que puedan afectar su disponibilidad, seguridad e integridad, siendo su principal objetivo asegurar que, en caso de una eventualidad que interrumpa el funcionamiento de estos servicios, se implementen medidas efectivas para su restablecimiento en el menor tiempo posible, minimizando el impacto en las actividades académicas, administrativas y de gestión universitaria. Su aplicación se extiende a toda la infraestructura tecnológica de la universidad, incluyendo sistemas críticos como el correo electrónico institucional, plataformas académicas, bases de datos y redes de comunicación; Que, asimismo, la Oficina de Tecnología de Información y Comunicaciones (OTIC) es la responsable de la implementación, supervisión y actualización de este plan, estableciendo procedimientos para la prevención de incidentes, la respuesta inmediata ante fallas o ataques, y la recuperación eficiente de los servicios. Para ello, se contemplan estrategias de monitoreo continuo, respaldo de información, mitigación de riesgos y planes de acción específicos, garantizando que la universidad cuente con protocolos de actuación claros y efectivos. Que, con Carta N.° 444-2025-R-UNALM, de fecha 15 de abril de 2025, el Rectorado autoriza la emisión de la resolución, que aprueba el "PLAN DE CONTINGENCIA INFORMÁTICO Y RECUPERACIÓN DE SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN DE LA UNALM", PROPUESTO por la Oficina de Tecnología de Información y Comunicaciones (OTIC);

La Molina, 21 de abril de 2025
TR. N.° 0198-2025-R-UNALM

Que, de conformidad con lo dispuesto en la Ley 28551, Ley que establece la obligación de elaborar y presentar planes de contingencia; la Ley 28716, Ley de Control Interno de las Entidades del Estado; la Resolución de Contraloría N.º 320-2006- CG, que aprueba las Normas de Control Interno; Ley 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD) y su Reglamento; la Resolución Ministerial N.° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana ISO NTP/IEC 27001:2014; y, el Reglamento de Organización y Funciones de la Universidad Nacional Agraria La Molina, aprobado mediante Resolución N.° 0225-2023-CU-UNALM, y con lo establecido en el literal b) del artículo 314° del Reglamento General de la UNALM y estando a las atribuciones conferidas al señor rector, como titular del pliego; **SE RESUELVE: ARTÍCULO 1.-** Aprobar el "Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicación de la Universidad Nacional Agraria La Molina" y sus anexos contenidos en el mismo, que forma parte integrante de la presente resolución. **ARTÍCULO 2.-** Encargar a la Oficina de Tecnología de la Información la implementación, supervisión y ejecución del Plan aprobado en el artículo 1 de la presente resolución. **ARTÍCULO 3.-** Disponer la publicación de la presente resolución en el Portal Institucional de la UNALM. Regístrese, comuníquese y archívese. Fdo.- Américo Guevara Pérez- Rector- Fdo.- Jorge Pedro Calderón Velásquez. - Secretario General. - Sellos del Rectorado y de la Secretaría General de la Universidad Nacional Agraria La Molina". Lo que cumplo con poner en su conocimiento.

Atentamente,

UNIVERSIDAD NACIONAL AGRARIA Secretaría General LA MOLINA

SECRETARIO GENERAL

c.c.: OCI,R,OAJ,OTIC,DIGA,DEPENDENCIAS

UNIVERSIDAD NACIONAL AGRARIA LA MOLINA

OFICINA DE SERVICIOS INFORMÁTICOS
Vº Bº
U.N.A.L.M.

PLAN DE CONTINGENCIA INFORMÁTICO Y RECUPERACIÓN DE SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN DE LA UNALM – OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Resolución N.° 0198-2025-R-UNALM

Elaborado por:	Revisado por:	Aprobado por:
Ing. Geison Arturo Malpartida Zubizarreta Jefe Oficina de Tecnología de Información y Comunicaciones	**Comité de Gobierno Digital** **Dra. Ethel Rubin de Celis Llanos** Jefa(e) de la Oficina de Calidad y Acreditación	**Dr. Américo Guevara Perez** Rector de la UNALM

TABLERO DE CONTROL DE CAMBIOS

Versión	Fecha	Sección	Descripción del cambio	Responsables
01	03.12.24	Todas	Creación del documento	Ing. Geison Arturo Malpartida Zubizarreta Oficina de Tecnología de Información y Comunicaciones

OFICINA DE SERVICIOS INFORMÁTICOS
V° B°
U.N.A.L.M.

ÍNDICE

OFICINA DE SERVICIOS INFORMÁTICOS
Vº Bº
U.N.A.L.M.

I. INTRODUCCIÓN

El presente documento define el Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones como un proceso continuo de planeación, desarrollo, prueba e implantación de procesos y procedimientos de recuperación en caso de una posible contingencia que pueda presentarse en la Universidad Nacional Agraria La Molina (UNALM). Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de Tecnologías de la Información y Comunicaciones en el menor tiempo e impacto posible.

El Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones cuenta con documentos que en conjunto permiten la gestión, ejecución, pruebas y mantenimiento, esta disgregación de documentos permiten una fácil y ágil operación por los responsables autorizados, ante situaciones de desastres.

II. PROPÓSITOS Y POLÍTICA

El Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicación de la Universidad Nacional Agraria La Molina (UNALM) tiene como propósito garantizar la continuidad operativa de los servicios tecnológicos institucionales ante incidentes que puedan afectar su disponibilidad, seguridad e integridad. Su principal objetivo es asegurar que, en caso de una eventualidad que interrumpa el funcionamiento de estos servicios, se implementen medidas efectivas para su restablecimiento en el menor tiempo posible, minimizando el impacto en las actividades académicas, administrativas y de gestión universitaria.

Este plan se fundamenta en estándares internacionales de seguridad de la información (ISO 27001), gestión de calidad (ISO 9001) y gobernanza de tecnologías de la información (ISO 38500), así como en el marco normativo nacional, incluyendo la Ley N° 29733 de Protección de Datos Personales y el Decreto Legislativo N° 1353 de Ciberseguridad en el Perú. Su aplicación se extiende a toda la infraestructura tecnológica de la universidad, incluyendo sistemas críticos como el correo electrónico institucional, plataformas académicas, bases de datos y redes de comunicación.

La Oficina de Tecnología de Información y Comunicaciones (OTIC) es la responsable de la implementación, supervisión y actualización de este plan, estableciendo procedimientos para la prevención de incidentes, la respuesta inmediata ante fallas o ataques, y la recuperación eficiente de los servicios. Para ello, se contemplan estrategias de monitoreo continuo, respaldo de información, mitigación de riesgos y planes de acción específicos, garantizando que la universidad cuente con protocolos de actuación claros y efectivos.

Este plan es de cumplimiento obligatorio para todas las áreas de la universidad que gestionan o utilizan servicios tecnológicos institucionales. Asimismo, será revisado periódicamente para incorporar mejoras y adaptarse a las nuevas exigencias de seguridad y gestión de la información, asegurando su efectividad y alineación con los objetivos estratégicos de la UNALM.

III. ALCANCE

El Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones, incluye los elementos referidos a los sistemas de información, aplicativos informáticos, bases de datos, equipos e instalaciones tecnológicas, personal, servicios y otros administrados por la Oficina de Tecnologías de la Información y Comunicaciones (OTIC), direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la entidad.

IV. BASE LEGAL

a. Ley Nº 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
b. Decreto Legislativo Nº 1013, Decreto Legislativo que aprueba la Creación, Organización y Funciones de la Universidad Nacional Agraria la Molina.
c. Decreto Supremo N° 018-2017 –PCM, Decreto Supremo que aprueba medidas para fortalecer la planificación y operatividad del Sistema Nacional de Gestión de Riesgos de Desastres mediante la adscripción y transferencia de funciones al Ministerio de Defensa a través del Instituto Nacional de Defensa Civil–INDECI y otras disposiciones.
d. Decreto Supremo Nº 002-2017-UNALM, Aprueban el Reglamento de Organización y Funciones (ROF) de la Universidad Nacional Agraria la Molina - UNALM.
e. Decreto Supremo N° 034-2014-PCM, Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgos de Desastres - PLANAGERD 2014-2021.
f. Decreto Supremo Nº 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
g. Resolución Ministerial N° 004-2016-PCM - Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
h. Resolución Ministerial N° 028-2015-PCM, Aprueban Lineamientos para la gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno.

V. TÉRMINOS Y DEFINICIONES

5.1. Plan de Contingencia Informático

Es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC), cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización.

Este plan permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, establece las acciones a realizarse en las siguientes etapas:

a. Antes, como un plan de prevención para mitigar los incidentes.

b. Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.

c. Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

5.2. Incidente

Circunstancia o suceso que sucede de manera inesperada y que puede afectar al desarrollo de una actividad, aunque no forme parte de él. En nuestro contexto, es una interrupción de las condiciones normales de operación en cualquier proceso informático en la UNALM.

5.3. Método de análisis de riesgos

Los métodos de análisis de riesgos son técnicas que se emplean para evaluar los riesgos de un proyecto o un proceso. Estos métodos ayudan a tomar decisiones que permiten implementar medidas de prevención para evitar peligros potenciales o reducir su impacto.

En el Anexo 1, se detalla la metodología utilizada en el presente Plan.

5.4. Plan de Prevención

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento no deseado, con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en las categorías identificadas en el presente plan. El plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

5.5. Plan de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente y activa la contingencia como un mecanismo alterno

que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible. Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

5.6. Plan de Recuperación

Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

5.7. Plan de Pruebas

Está constituido por un conjunto de pruebas. Cada prueba debe dejar claro qué tipo de propiedades se quieren probar, cómo se mide el resultado, especificar en qué consiste la prueba y definir cuál es el resultado que se espera.

VI. NORMATIVA ASOCIADA

El Plan de Contingencia Informático y Recuperación de Servicios de TIC se enmarca dentro del cumplimiento de normativas nacionales e institucionales que regulan la gestión de tecnologías de la información, la seguridad digital y la continuidad operativa en el sector educativo. A nivel nacional, se consideran las disposiciones establecidas en la Ley N.º 29733, Ley de Protección de Datos Personales, y su reglamento, que obligan a la universidad a garantizar la confidencialidad, integridad y disponibilidad de la información. Asimismo, el Decreto Legislativo N.º 1412, que aprueba la Ley de Gobierno Digital, establece lineamientos para la gestión eficiente de los sistemas de información y la implementación de medidas de ciberseguridad en entidades públicas.

En el ámbito institucional, el plan responde a los compromisos asumidos en el Modelo de Licenciamiento de la SUNEDU, que exige la operatividad de sistemas de gestión académica y administrativa para la transparencia y el acceso oportuno a la información. También se alinea con los estándares del SINEACE en materia de aseguramiento de la calidad, que requieren la implementación de mecanismos de soporte tecnológico para la mejora continua. Adicionalmente, se adopta el marco de referencia de normas internacionales como ISO/IEC 27001 sobre seguridad de la información e ISO 22301 sobre gestión de la continuidad del negocio, con el objetivo de fortalecer la capacidad institucional para prevenir, mitigar y responder ante incidentes tecnológicos que puedan comprometer la operatividad de la universidad.

VII. ANÁLISIS SITUACIONAL

La Universidad enfrenta actualmente una serie de desafíos en la gestión de sus servicios tecnológicos debido a la falta de integración de los sistemas de

información y a la presencia de infraestructuras obsoletas que comprometen la continuidad operativa. Los sistemas críticos, como el de gestión académica, administrativa y financiera, presentan riesgos asociados a caídas inesperadas, vulnerabilidades de seguridad y una limitada capacidad de respuesta ante incidentes. Asimismo, la ausencia de un esquema robusto de respaldo y recuperación de datos incrementa el riesgo de pérdida de información sensible, lo que podría afectar el cumplimiento de los compromisos institucionales y normativos, incluyendo los requerimientos de licenciamiento y acreditación.

En este contexto, es fundamental establecer un Plan de Contingencia Informático y Recuperación de Servicios de TIC que permita garantizar la disponibilidad, integridad y resiliencia de los sistemas. Actualmente, la universidad no cuenta con un protocolo estandarizado de respuesta ante incidentes tecnológicos, lo que dificulta la toma de decisiones en situaciones críticas. Además, se ha identificado que el personal técnico no dispone de capacitaciones actualizadas en manejo de crisis y recuperación de sistemas, lo que retrasa la restauración de servicios ante fallos. La implementación de este plan permitirá reducir la vulnerabilidad institucional frente a interrupciones, fortalecer la capacidad de reacción ante incidentes y asegurar la continuidad de las operaciones académicas y administrativas.

VIII. OBJETIVOS

8.1. Objetivo General

Establecer los principios básicos y el marco necesario para garantizar la operatividad de los servicios y/o procesos de tecnologías de la información y comunicaciones de mayor urgencia de la UNALM, ante la eventual presencia de siniestros que los pueda paralizar parcial o totalmente y garantizar que se continúen prestando de una manera razonable.

8.2. Objetivos Específicos

8.2.1. Identificar y analizar los riesgos posibles que pueden afectar las operaciones, procesos y servicios de tecnologías de la información y comunicaciones de la Entidad.

8.2.2. Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.

8.2.3. Organizar y disponer al personal técnico debidamente capacitado para afrontar adecuadamente las contingencias que puedan presentarse.

8.2.4. Establecer actividades que permitan evaluar los resultados y retroalimentación del presente plan.

IX. ESTRATEGIAS

9.1. Acciones estratégicas

El desarrollo del presente Plan seguirá la siguiente metodología basada en siete (7) fases:

- Fase 1: Planificación
- Fase 2: Determinación de vulnerabilidades y escenarios de contingencia
- Fase 3: Estrategias
- Fase 4: Elaboración del Plan de Contingencia Informático
- Fase 5: Definición y Ejecución del Plan de Pruebas
- Fase 6: Implementación del Plan de Contingencia
- Fase 7: Monitoreo

A continuación, se detalla cada fase:

9.1.1. Fase 1: Planificación

9.1.1.1. Organización

La Oficina de Tecnologías de la Información y Comunicaciones (OTIC) depende directamente de la Oficina General de Administración (OGA), y tiene dentro de sus funciones administra la integridad, confiabilidad, y seguridad en el acceso de la base de datos institucional, así como establecer mecanismos de registro histórico de modificaciones, autenticación de los usuarios, auditoría y control de accesos a la base de datos; además de diseñar, construir, implantar, mantener los sistemas informáticos e infraestructura tecnológica necesaria para el cumplimiento de los objetivos de la UNALM, así como asegurar la disponibilidad y brindar soporte a los mismos.

Para el funcionamiento del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones, se ha establecido la siguiente organización operativa, conformado exclusivamente por personal de la OTIC:

Figura N° 1 - Organización Operativa del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones

El Director de la Oficina de Tecnología de la Información y Comunicaciones debe nombrar un miembro titular y un alterno, por cada integrante de los tres (3) equipos mencionados previamente, detallados en la Figura N° 1. Para tal efecto, se debe contar con la relación del personal de la OTIC que forman estos equipos, quienes serán requeridos en el momento de la contingencia.

Asimismo, los responsables de cada Equipo previamente señalados deben tener operativo el dispositivo móvil asignado por la UNALM para las comunicaciones pertinentes, siendo necesario que el responsable del Equipo de Restauración de TIC cuente con línea abierta disponible, en caso deba comunicarse con proveedores especializados. De igual manera, los correos electrónicos registrados deben estar alojados en plataforma nube, que garantice la disponibilidad de este servicio.

La relación del personal de la OTIC que forma parte del Plan de contingencia debe ser actualizada de manera permanente y socializada al siguiente personal:

a. Personal de la OTIC.
b. Grupo de Comando - Plan de Continuidad Operativa.
c. Personal de la Alta Dirección.
d. Casetas de vigilancia de la entidad.

Las actividades planificadas como parte del presente plan podrán ejecutarse en forma presencial, semipresencial o

en remoto, conforme a los escenarios de prueba que pudieran desprenderse ante los diversos eventos de mayor impacto considerados para el presente Plan de Contingencia Informático; así como, conforme a las disposiciones vigentes.

9.1.1.2. Roles, funciones y responsabilidades dentro del Plan

A continuación, se describen los roles, responsabilidades y funciones que deben desarrollar los distintos equipos del Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones.

9.1.1.3. Coordinador de Continuidad de TIC

Está representado por el/la Director/a de la OTIC de la OTIC y tiene las siguientes funciones:

9.1.1.3.1. Coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.

9.1.1.3.2. Tomar la decisión de activar el Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones.

9.1.1.3.3. Guiar y supervisar a los equipos operativos de contingencia informática, en el desarrollo de sus actividades.

9.1.1.3.4. Evaluar la extensión de la contingencia y sus consecuencias potenciales sobre la infraestructura tecnológica.

9.1.1.3.5. Notificar y mantener informados, a los miembros del Grupo de Comando - Plan de Continuidad Operativa acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.

9.1.1.3.6. Monitorear, supervisar y vigilar la recuperación de infraestructura de Tecnologías de la Información (TI) en el Centro de Datos.

9.1.1.3.7. Contactar a los proveedores para el reemplazo de hardware, software y/o activación de servicios para los sistemas afectados.

9.1.1.3.8. Declarar el evento de término de la ejecución de las operaciones del Plan de Contingencia

Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones, cuando las operaciones del Centro de Datos hayan sido restablecidas.

9.1.1.4. Equipo de Prevención de TIC

Es el equipo encargado de ejecutar las acciones preventivas, antes que ocurra un siniestro o desastre. Su finalidad es evitar la materialización y en caso ocurriese, tener todos los medios requeridos para realizar la recuperación de los servicios de tecnologías de la información y comunicaciones, en el menor tiempo posible.

El responsable del Equipo de Prevención de TIC es el/la Especialista en Seguridad de la Información.

A continuación, se detallan las funciones por cada integrante del equipo de prevención:

Especialista en Seguridad de la Información

a. Establecer y supervisar los procedimientos de seguridad de los servicios de TIC.
b. Coordinar la realización de las pruebas de restauración de hardware y software.
c. Participar en las pruebas y simulacros de desastres.
d. Verificar la realización del mantenimiento preventivo a los equipos componentes del Centro de Datos.
e. Verificar las tareas de copias de respaldo (backup).

Especialista en Redes y Comunicaciones

a. Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
b. Ejecutar y verificar las tareas de copias de respaldo (backup).
c. Programar y/o realizar el mantenimiento preventivo de los equipos de comunicaciones y de los equipos componentes del Centro de Datos, considerando el tiempo de vida útil y garantía de los mismos.
d. Llevar un control detallado del mantenimiento realizado a cada equipo y componentes del Centro de Datos.
e. Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento del Centro de Datos.
f. Verificar que se mantengan actualizados los diagramas de servidores, los diagramas de red, la documentación

de las configuraciones de equipos de comunicaciones, el inventario de software de gestión y otros.

g. Monitorear la red y definir medidas preventivas para minimizar o evitar las contingencias.
h. Realizar las pruebas previas de recuperación.

Técnico en Telecomunicaciones

a. Monitorear el funcionamiento de la Central Telefónica.
b. Verificar que la central telefónica cuenta con las garantías requeridas.
c. Mantener actualizada la lista de anexos y teléfonos.
d. Actualizar el software que utiliza la central telefónica.

Coordinador en Sistemas de Información

a. Coordinar acciones de mantenimiento de sistemas de información existentes asegurando el cumplimiento del ciclo de vida de software
b. Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.
c. Coordinar y verificar que se realicen las copias de respaldo de las fuentes de los aplicativos informáticos existentes en un ambiente adecuado.

Especialista en Sistemas de Información

a. Soporte y mantenimiento de los sistemas y aplicativos instalados en la entidad.
b. Documentación, consolidación y validación de los manuales de los sistemas en producción.
c. Realizar periódicamente las pruebas de restauración de las fuentes de los sistemas de información en producción de la entidad.

Especialista en Administración de Base de Datos

a. Realizar copias de respaldo de las bases de datos de los aplicativos y sistemas de la entidad.
b. Acopiar las copias de respaldo y clasificarlas por tipo de motor de base de datos, aplicativos y sistemas.
c. Realizar las pruebas de restauración de bases de datos en coordinación con el Especialista en Seguridad de la Información.

9.1.1.5. Equipo de Emergencia de TIC

Este equipo es el encargado de ejecutar las acciones requeridas durante la materialización del siniestro o desastre. Su finalidad es mitigar el impacto que puedan tener sobre los equipos tecnológicos y la información del UNALM, procurando salvaguardar su pérdida o deterioro.

A continuación, se citan las acciones que se realizarán durante la contingencia, según los miembros del equipo:

Especialista en Redes y Comunicaciones

a. Notificar el desastre o incidencia al Coordinador de Continuidad de TIC.
b. Ejecutar las acciones de emergencia en los equipos informáticos y componentes instalados en el Centro de Datos del UNALM.
c. Realizar la evaluación de condiciones de los equipos de comunicaciones y los componentes del Centro de Datos del UNALM, durante la emergencia.
d. Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas.

Técnico en Telecomunicaciones

a. Ejecutar las acciones de emergencia en los equipos celulares y central telefónica instalada en el Centro de Datos del UNALM.
b. Realizar la evaluación de condiciones de los equipos de telecomunicaciones, durante la emergencia.
c. Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas.

Coordinador en Sistemas de Información

a. Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
b. Coordinar acciones para verificar el estado de las bases de datos de los sistemas de información.

Especialista en Sistemas de Información

a. Realizar la evaluación de las condiciones de los aplicativos informáticos y sistemas de información durante la emergencia.
b. Solicitar los logs de los aplicativos informáticos afectados durante la emergencia.

Especialista en Administración de Base de Datos

a. Realizar la evaluación de las condiciones de los datos y la información almacenada en las diferentes bases de datos, durante la emergencia.

Técnico de Soporte Informático

a. Realizar la evaluación de la afectación a los equipos informáticos de usuario final (computadoras, teléfonos, impresoras, entre otros).
b. Notificar los casos críticos en cuanto a equipos de usuario final, que afecte la continuidad de operaciones y/o la pérdida de información de los usuarios del UNALM.

Especialista en Seguridad de la Información

a. Apoyar en las labores de verificación y validación de operación de los servicios de TIC.

9.1.1.6. Equipo de Restauración de TIC

Este equipo es el encargado de ejecutar las acciones necesarias luego de que el siniestro o desastre esté controlado. Su finalidad es restituir en el menor tiempo posible el funcionamiento de los equipos tecnológicos y recuperar el estado de los servicios informáticos del UNALM de manera conjunta con los miembros titulares y suplentes del Grupo de Comando - Plan de Continuidad Operativa y especialistas designados por cada órgano del UNALM.

Especialista en Redes y Comunicaciones

a. Es el responsable del equipo de Restauración de TIC
b. Debe iniciar el proceso de recuperación de los servicios de tecnología de la información, realizando las pruebas de funcionamiento en los equipos afectados de la infraestructura informática y los equipos componentes del Centro de Datos del UNALM.
c. Restaurar la información de los equipos afectados de la infraestructura informática que afecten los servicios de TI y los equipos componentes del Centro de Datos del UNALM.
d. Notificar al Coordinador de Continuidad de TIC, las acciones de recuperación ejecutadas.

e. Elaborar *un informe técnico*, que incluya las acciones de recuperación de los equipos de comunicaciones y los equipos componentes del Centro de Datos.

Técnico en Telecomunicaciones

a. Iniciar el proceso de recuperación de los servicios relacionados a la central telefónica instalada en el Centro de Datos del UNALM, así como a los equipos móviles.
b. Realizar la evaluación de condiciones de los equipos de telecomunicaciones, durante la emergencia.
c. Elaborar *un informe técnico*, que incluya las acciones de recuperación de los equipos móviles y la central telefónica ubicada del Centro de Datos.

Coordinador en Sistemas de Información

a. Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
b. Coordinar el estado de las bases de datos de los sistemas de información.
c. Coordinar y monitorear la restauración de aplicativos y ejecución de pruebas para verificación de funcionalidad.

OFICINA DE SERVICIOS INFORMÁTICOS V° B° U.N.A.L.M.

Especialista en Sistemas de Información

a. Verificar el estado de las aplicaciones alojados en los servidores de aplicaciones del UNALM.
b. En caso se quiera desplegar y/o reinstalar los aplicativos informáticos y sistemas de información, de lo contrario verificar que se encuentren funcionando correctamente.
c. Elaborar un informe técnico que incluya la evaluación de condiciones de los aplicativos informáticos y sistemas de información del UNALM.

Especialista en Administración de Base de Datos

a. Verificar el funcionamiento de las bases de datos institucionales.
b. Realizar la creación de bases de datos en servidores alternos, en caso sea requerido.
c. Restaurar las copias de respaldo correspondientes respetando la prioridad establecida para cada escenario.

d. Realizar las pruebas de funcionamiento.
e. Elaborar un informe técnico que incluya la evaluación de condiciones de los datos e información del UNALM luego de efectuado el proceso de recuperación.

Técnico de Soporte

a. Verificar el funcionamiento de los equipos personales en la UNALM afectadas, distribuyendo el trabajo entre los técnicos de soporte.
b. Solucionar los problemas de conexión y funcionamiento de los equipos personales, impresoras, escáner entre otros.
c. Elaborar un informe técnico que incluya la evaluación de condiciones de los equipos personales e información del personal del UNALM, luego de efectuado el proceso de recuperación.

Especialista en Seguridad de la Información

a. Supervisar la restauración de los servicios de TI.
b. Validar la información documentada de los procedimientos de restauración utilizados.

Cabe precisar que los equipos podrían ejecutar sus actividades paralelamente, de acuerdo con el siguiente orden de operación:

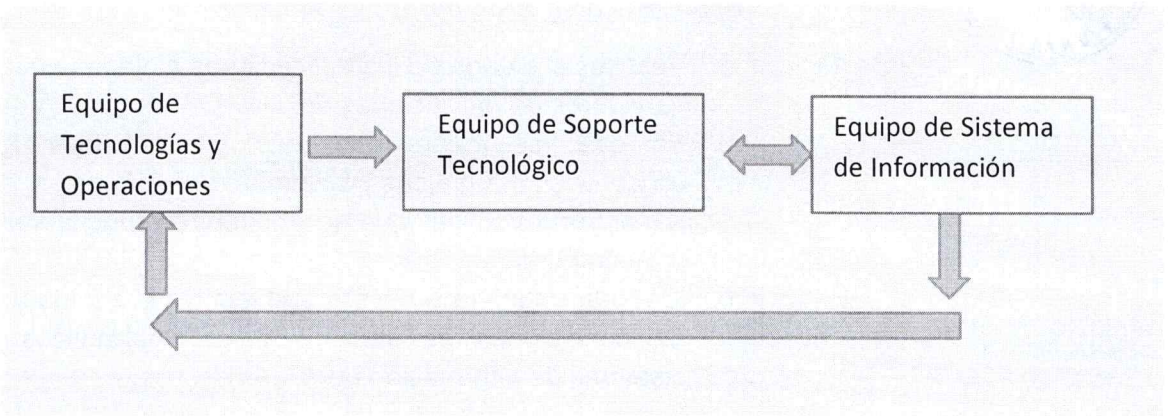

Figura N° 2 – Flujo del orden de operación de los equipos de TI

9.1.2. Fase 2: Determinación de vulnerabilidades y escenarios de contingencia

En esta fase se procederá a la identificación de las aplicaciones críticas, los recursos y el periodo máximo de recuperación de los servicios de tecnologías de la información y comunicaciones, para

los cuales se considerarán todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia.

9.1.2.1. Procesos y recursos críticos

A continuación, se detalla los procesos, aplicaciones y recursos críticos, con su respectiva expectativa del tiempo de recuperación:

Proceso crítico	Aplicaciones y/o recursos críticos	Tiempo de Recuperación (RTO)
Gestión de redes e infraestructura de TI	Equipos de comunicaciones.	12 h
	Equipos de protección eléctrica del centro de datos (UPS)	24 h
	Sistema de aire acondicionado del Centro de Datos	24 h
	Infraestructura del Centro de Datos	24 h
	Cableado de red de datos	24 h
	Enlaces de cobre y fibra óptica para interconexión entre la sede central y el centro de datos	4 h
	Sistema de almacenamiento (storage)	24 h
	Medios de respaldo (cintas de backup)	24 h
	Servidores de red críticos: Directorio Activo, File Server, Base de Datos, Ecodoc.	96h
	Servidores de red en general: Citrix, tomcat, jboss.	98h
	Central Telefónica	24h
Gestión de sistemas de información y bases de datos	Sistemas de información y portales core	48 h
	Sistemas de información administrativos	72 h
	Base de datos y repositorios utilizados por los sistemas y aplicativos.	48 h
Soporte Técnico	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	48 h
Operación y mantenimiento de TICS	Personal crítico responsable de los procesos de TIC.	4 h

Tabla N° 1
Procesos y recursos críticos de TI

*El RTO: Tiempo de Recuperación Objetivo, es determinado por Juicio de Expertos.

9.1.2.2. Identificación de amenazas

Este paso, permite identificar aquellas amenazas que pudieran vulnerar los servicios TIC de la Universidad Nacional Agraria la Molina, considerando la ubicación geográfica, el contexto actual de la sede central y centro de datos, así como la percepción del juicio experto.

N°	Amenaza (Evento)	Tipo
01	Terremoto/Sismo	Siniestros Naturales
02	Inundación y aniego en el Centro de Datos.	
03	Incendio en el Centro de Datos.	
04	Falla en telecomunicaciones.	Tecnológicos
05	Delito informático.	
06	Falla de hardware y software.	
07	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Físico y ambiental
08	Ausencia o no disponibilidad del personal crítico de TI.	Humanos
09	Pandemia y/o Epidemia	Ambiental

Tabla N° 2
Amenazas a los servicios de TI

Una vez determinadas las amenazas que pueden afectar los recursos críticos de TI, se calcula el nivel de probabilidad estimada, a fin de identificar las amenazas que serán consideradas en la evaluación de los riesgos. A continuación, se detalla el resultado obtenido:

N°	Amenaza (Evento)	Ocurrencia	Percepción	Nivel Probabilidad estimada
01	Terremoto.	2	4	Moderado
02	Inundación y aniego en el Centro de Datos.	2	2	Menor
03	Incendio en el Centro de Datos.	1	3	Menor
04	Falla en telecomunicaciones.	3	4	Moderado
05	Delitos informáticos.	2	4	Moderado
06	Falla del suministro eléctrico en el Centro de Datos y gabinetes de Comunicación.	3	3	Moderado
07	Falla del hardware y software.	3	3	Moderado
08	Ausencia o no disponibilidad del Personal crítico de TI.	2	3	Menor

N°	Amenaza (Evento)	Ocurrencia	Percepción	Nivel Probabilidad estimada
09	Pandemia y/o Epidemia	1	2	Menor

Tabla N° 3
Probabilidad estimada de las amenazas a los servicios de TI

9.1.2.3. Identificación de Controles Existentes

La identificación de controles existentes, permiten conocer qué tan protegidos están los recursos de TI de la UNALM frente a cada amenaza.

a. Acuerdos de niveles de servicio con proveedor de enlace de comunicación entre la sede central y la sede donde se encuentra ubicado el Centro de Datos.
b. Cámaras de vigilancia en el interior del Centro de Datos.
c. Grupo electrógeno para el centro de datos.
d. Mantenimiento de generadores eléctricos y UPS. El mantenimiento de generadores (grupo electrógeno está a cargo de Servicios Generales de la Oficina de Abastecimiento) y el mantenimiento de UPS está a cargo de la OTIC).
e. Mantenimiento para equipos de aire acondicionado del Centro de Datos.
f. Redundancia en los enlaces de comunicaciones (fibra óptica) y de internet, pero con el mismo proveedor.
g. Sistema contra incendios en el Centro de Datos.
h. Respaldo de información y custodia externa de medios de respaldo.
i. Solución antivirus instalada en los servidores de red y computadoras.
j. Solución de protección de portales y aplicaciones web publicadas en internet a través de solución en la nube.
k. Póliza de seguro contra todo riesgo.

9.1.2.4. Evaluación del Nivel de Riesgo

Para determinar el Nivel de Riesgo de un recurso de TI crítico de la UNALM, se consideraron los controles existentes que mitigan la afectación de la amenaza descritos en el punto 6.2.2 y de acuerdo con la aplicación

de la metodología de riesgos descrita en el Anexo 1, se obtuvo el siguiente resultado:

N°	Recursos Críticos / Amenazas (Eventos)	Terremoto	Inundación y anegamiento en el Centro de Datos	Incendio en el Centro de Datos	Falla en telecomunicaciones	Delitos informáticos	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	Falla del hardware y software	Ausencia o no disponibilidad del personal crítico de TI	Pandemia y/o Epidemia
1	Equipos de comunicaciones.									
2	Equipos de protección eléctrica del centro de datos (UPS).									
3	Aire acondicionado de precisión del Centro de Datos.									
4	Infraestructura del Centro de Datos.									
5	Cableado de red de datos.									
6	Enlaces de cobre y fibra óptica para interconexión entre la sede central y el Centro de Datos.									
7	Sistema de almacenamiento (storage).									
8	Servidores de red									
9	Medios de respaldo (cintas de backup)									
10	Sistemas de información y portales web									
11	Base de datos utilizados por los sistemas y aplicativos.									
12	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)									
13	Personal crítico responsable de los procesos de TIC.									

Tabla N° 4
Resultado de la evaluación de riesgos de los servicios de TI

9.1.2.5. Escenarios de riesgo

a. Destrucción e indisponibilidad del centro de datos por terremoto.
b. Falla en el funcionamiento de los sistemas de información y portales web por delito informático (ataque cibernético, virus, etc.).
c. Indisponibilidad de los servidores de red por falla de hardware y software.
d. Interrupción de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y/o en los gabinetes de comunicación de la sede central.

A continuación, se presenta el consolidado de los escenarios de riesgo y su impacto, para activar el Plan de Contingencia Informático.

Escenario de Riesgo	Descripción	Impacto
Destrucción e indisponibilidad del centro	Este escenario consiste en que el Centro de Datos deje de funcionar o se destruya, como resultado de un terremoto o incendio, lo cual podría ocasionar caídas de servicios y destrucción de los equipos informáticos alojados en el centro de datos, como también los componentes del mismo.	Extremo
Falla en el funcionamiento de los sistemas de información y portales web	Se refiere a la falla lógica o caída de los sistemas de información, aplicativos y portales web, lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo
Indisponibilidad de los servidores de red por falla de hardware y software.	Se refiere al fallo físico o lógico de los servidores físicos y virtuales, lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo
Interrupción de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y/o en los gabinetes de comunicación de la sede central.	Este escenario consiste en el corte o interrupción de las comunicaciones entre la sede central y el centro de datos, así como los servicios publicados en internet, como resultado de fallas del sistema eléctrico o equipos de suministro eléctrico, así como el corte de energía eléctrica, lo cual ocasionar caídas de servicios informáticos y pérdidas de comunicación en los equipos de infraestructura tecnológica.	Alto

Tabla N° 5
Escenarios de Riesgos

9.1.3. Fase 3: Estrategias del Plan de Contingencia

A continuación, se presentan estrategias para la contingencia operativa en caso de un desastre.

9.1.3.1. Estrategias de prevención de tecnologías de la información

a) Almacenamiento y respaldo de la información (BACKUPS)

- Gestión de copias de respaldo (Backup) de la información almacenada y procesada en el Centro de Datos, de acuerdo a la Directiva N° 009-2018-UNALM/SG, en donde se define la frecuencia de los respaldos de información considerando la criticidad de los datos, así como los criterios de identificación de los medios, la frecuencia de rotación y transporte al sitio externo.
- Realización de copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.
- Verificar la ejecución periódica de las tareas programadas de respaldo de información y comprobación de los medios de respaldo.
- Se utilizan lugares alternativos externos para el almacenamiento de las copias de respaldo a cargo de proveedor externo.

b) Sitios Alternos para el Centro de Datos

El plan incluye una estrategia para recuperar y ejecutar operaciones de sistemas en instalaciones alternativas por un periodo extendido; los sitios alternativos podrán ser:

- Propios de la entidad.
- Instalaciones alquiladas.

Para tal efecto, se debe identificar un ambiente adecuado como lugar alterno para la recuperación de equipos y servicios de tecnologías de la información del Centro de Datos.

c) Evaluación y gestión de proveedores

- Listado de proveedores claves de servicios y recursos de TI, con sus datos de contacto actualizados.
- Mantener listas detalladas de necesidades de equipos y sus especificaciones Técnicas.
- Si es necesario, adquirir o habilitar hardware y software así como transportarlos al sitio alterno de

ser el caso; las estrategias básicas para disponer de equipo de reemplazo serán:

- Acuerdos con proveedores: Establecer acuerdos de nivel de servicios con los proveedores de software, hardware y medios de soporte; se debe especificar el tiempo de respuesta requerido.
- Equipos de respaldo: Los equipos requeridos se compran por adelantado y se almacenan en una instalación segura externa. (*)
- Equipo compatible existente: Equipo existente en sitios alternativos.

(*) Comprar los equipos cuando se necesitan puede ser mejor financieramente, pero puede incrementar de manera significativa el tiempo de recuperación. Asimismo, almacenar un equipo sin ser usado es costoso, pero permite que la recuperación comience más rápidamente.

d) Entrenamiento y personal de reemplazo

- Todo el personal de la OTIC, debe entrenarse en el proceso de recuperación de los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que ha logrado sus objetivos.
- Se debe elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de OTIC, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información.
- Elaboración de una base de datos de conocimiento, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

e) Renovación tecnológica

- Programación de dos revisiones anuales de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.

- Registrar las incidencias de deterioro de los equipos de almacenamiento, procesamiento y comunicaciones, para en base a las estadísticas de este registro adquirir equipos de contingencia.

f) Activación de trabajo remoto

- Verificación y validación de acceso seguro, en remoto, a los sistemas y servicios TICs.
- Activación de redes virtuales VPN, siempre y cuando el equipo a conectarse cuente con los mecanismos de seguridad informáticos necesarios.
- En caso el usuario no cuente con un equipo para realizar su trabajo remoto, se le pueda habilitar el equipo asignado, que se encuentra en la UNALM, para entregársela en su domicilio a fin de que cuente con las herramientas necesarias, siguiendo los protocolos dados por la Oficina de Abastecimiento
- Realizar el Trámite de Certificados Digitales, para instalarlos en los equipos de los usuarios, fuera de la institución.
- Activación del desvío de las llamadas telefónicas a los usuarios asignados encargados de la atención de la central telefónica.
- Verificación de los accesos seguros de los proveedores a cualquier elemento de la plataforma e infraestructura de servicios TICs, a cargo de la OTIC en el Centro de Datos.

OFICINA DE SERVICIOS INFORMÁTICOS Vº Bº U.N.A.L.M.

9.1.3.2. Estrategia frente a emergencias en tecnologías de la información

El alcance de las estrategias frente a emergencias involucra las acciones que deben realizarse durante una emergencia o desastre, a fin de salvaguardar la información de la UNALM y garantizar la continuidad de los servicios informáticos para lo cual se definen las acciones para mitigar las pérdidas que puedan producirse en una emergencia o desastre. A continuación, se citan las acciones que se realizarán durante y después de una contingencia:

Acciones durante la contingencia:

a. Estudiar y evaluar el alcance del desastre en cada área de responsabilidad.

b. Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración de TIC.
c. Informar al responsable del Grupo de Comando - Plan de Continuidad Operativa sobre la situación presentada, para decidir la realización de la Declaración de Contingencia y activación del sitio alterno o de respaldo.
d. Determinar si el área afectada es segura para el personal (en caso de catástrofe).
e. Estudiar y evaluar la dimensión de los daños a los equipos y sus facilidades, y elaborar un informe de los daños producidos.
f. Proveer facilidades al personal encargado de la recuperación, con la finalidad de asegurar que se realicen las tareas asignadas en los procedimientos que forman parte de este plan.

9.1.3.3. Estrategia para la restauración de tecnologías de la información

El alcance de las estrategias para la restauración o recuperación involucra las acciones que deben realizarse luego de suscitada una emergencia o desastre, a fin de recuperar la información y los servicios informáticos de la UNALM para estabilizar la infraestructura tecnológica luego del evento suscitado. Para lo cual se definen las pautas que permitan al personal de la OTIC garantizar la continuidad de las operaciones en la entidad.

El ciclo considerado para la estrategia de recuperación de tecnologías de la información es el siguiente:

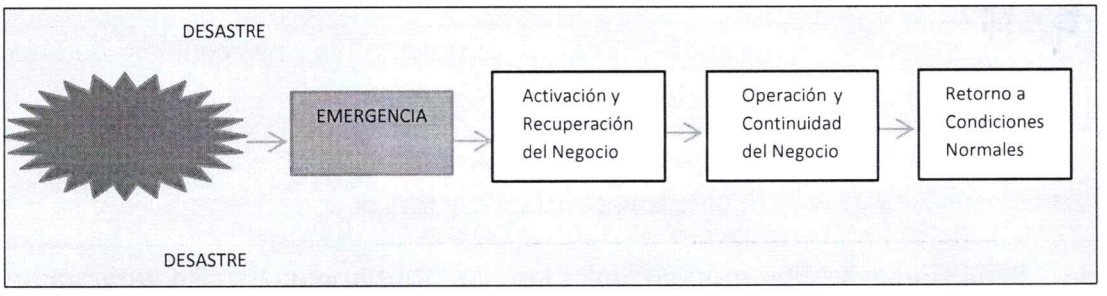

Figura N° 3 – Ciclo de la estrategia de recuperación

La priorización de la restauración de los servicios de tecnologías de información de la UNALM se ejecutará de acuerdo con lo indicado en la siguiente Tabla de información:

Prioridad de Atención	Descripción
1	Atención prioritaria: Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios externos y manejen alto volumen de información. Ejemplo: Trámite documentario, Sistema Administrativo Financiero (SIAF), Sistema de gestión administrativa (SIGFYS), Portal Web institucional, Servidores de bases de datos, gestor documental Alfresco, entre otros.
2	Atención normal: Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. Ejemplo: Sistemas que no requirieran conectividad y/o que cuenten con mayor plazo para la consulta y disponibilidad de información, etc.
3	Atención baja: Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información. Asimismo, equipos de apoyo. Ejemplo: Intranet, CITES, interclima, COP20, etc.

Tabla N° 6
Prioridad de atención durante la restauración de TIC

En el Anexo 2 y Anexo 3 se detallan los sistemas de información y equipos informáticos, con la respectiva prioridad de atención, en caso de activarse la contingencia informática.

Acciones después de la contingencia

a. Evaluar el trabajo de los equipos durante el proceso de recuperación.
b. Evaluar la efectividad del Plan de Contingencia.
c. Evaluar la efectividad del sitio alterno de contingencia y sus facilidades.

9.1.4. Fase 4: Elaboración del Plan de Contingencia y Recuperación de Servicios de TIC

Una vez identificados los eventos de contingencia y los escenarios de riesgos, se desarrollan los Planes de Contingencia agrupados por las categorías indicadas previamente.

El Plan de Contingencia y Recuperación de los Servicios de Tecnología de la Información y Comunicaciones comprenderá los

eventos de mayor impacto, identificados en la Matriz de Riesgo de Contingencia, los cuales serán abordados en formatos independientes, tal como se indica en el siguiente cuadro:

N°	Evento	Exposición al Riesgo
1	Terremoto /Sismo	Extremo
2	Delito informático (ataque)	Extremo
3	Falla de hardware y software	Extremo
4	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Alto

Tabla N° 7
Eventos de mayor impacto para el Plan de Contingencia Informático

En el Anexo 4 se presenta el desarrollo para cada evento.

9.1.5. Fase 5: Definición y Ejecución del Plan de Pruebas

El plan de pruebas está enfocado principalmente a simular situaciones de contingencia en caso de incidencias producidas sobre equipos, información y procesos, manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutados por los equipos operativos de la OTIC, los cuales probarán, verificarán y observarán cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir el plan.

La información que se desarrollará como parte del Plan de Pruebas, tiene el siguiente esquema:

a. Metodología (descripción de la prueba a efectuarse)
b. Alcances (áreas afectadas / personal involucrado)
c. Resultados

Las pruebas relacionadas a este plan se deberán ejecutar semestralmente, en los meses de junio y diciembre, con el fin de evaluar la preparación de la entidad, ante la ocurrencia de un

siniestro y realizar los ajustes necesarios y deberán ser registradas en el formato detallado en el Anexo N° 05.

9.1.6. Fase 6: Implementación del Plan de Contingencia

La implementación del presente plan se realizará a partir del segundo mes de su aprobación.

Para tal efecto, el/la Oficial de Seguridad de la Información, realiza las siguientes funciones:

a. Supervisar las actividades de copias de respaldo y restauración.
b. Establecer procedimientos de seguridad en los sitios de recuperación.
c. Organizar las pruebas de restauración de hardware, software y servicios de Tecnologías de Información (TI).
d. Participar en las pruebas y simulacros de desastres.

9.1.7. Fase 7: Monitoreo

La fase de Monitoreo permite tener la seguridad de que se podrá reaccionar en el tiempo preciso y con la acción correcta. Esta fase es primordialmente de mantenimiento. Cada vez que se da o realiza un cambio en la infraestructura, debemos de realizar la adaptación respectiva.

A continuación, se enumeran las actividades principales a realizar:

a. Realizar mantenimiento de la documentación técnica de operación de los servicios de TI.
b. Revisión continúa de las aplicaciones, sistemas de información y portales web.
c. Revisión continúa del sistema de copias de respaldo (backups).
d. Revisión y mantenimiento de los sistemas de soporte eléctrico del Centro de Datos.

X. ANEXOS

- Anexo 01 Metodología aplicada a la gestión de riesgos
- Anexo 02 Listado de aplicaciones y sistemas de información clasificados por prioridad de atención para la recuperación de TIC
- Anexo 03 Listado de equipos del Centro de Datos y Gabinetes de Comunicación clasificados por prioridad de atención para la recuperación de TIC
- Anexo 04 Registros del Formato del F06-PS06.1.01 Formato de registro y acción ante un evento, del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.

- Anexo 05 Formato F07-PS06.1.01 Formato de Control y certificación de las pruebas, del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones

ANEXO 01

METODOLOGÍA APLICADA A LA GESTIÓN DE RIESGOS

1. **Cálculo de la Probabilidad de Ocurrencia de la Amenaza**

Para realizar este cálculo, se toman en cuenta dos variables: "Ocurrencia" y "Percepción".

Se considera "ocurrencia" a la frecuencia en que se presentan los eventos a evaluar, sobre la base de los registros históricos de incidentes que hayan afectado a la UNALM directamente. Se consideró la siguiente tabla de valores para el cálculo:

N°	Ocurrencia	Descripción
1	Rara Vez	Se presentó al menos una vez en los últimos 20 años / Nunca se presentó
2	No Frecuente	Se presentó al menos una vez en los últimos 10 años
3	Moderada	Se presentó más de una vez en los últimos 5 años
4	Frecuente	Se presentó por lo menos una vez al año en los últimos 5 años
5	Muy Frecuente	Se presentó más de una vez al mes en el último año

La "Percepción" está basada netamente en la sensación de los expertos, de que la amenaza en cuestión podría ocurrir, se consideró la siguiente tabla de valores para el cálculo:

#	Percepción	Descripción
1	Muy Difícil	• <= 1% probabilidad, o • El acontecimiento requiere de circunstancias excepcionales, o • La probabilidad es nula, incluso en un futuro a largo plazo
2	Difícil	• >1% ó <=10% de probabilidad, o • Puede ocurrir, pero no será anticipada
3	Mediana	• >10% ó <=50% de probabilidad, o • Puede ocurrir en el mediano plazo
4	Posible	• >50% ó <=75% de probabilidad, o • Podría ocurrir anualmente
5	Muy Posible	• >75% ó 100% de probabilidad, o • El impacto está ocurriendo ahora, o • Podría ocurrir dentro de unos meses

Los valores definidos para la Ocurrencia y Percepción son promediados y consolidados a fin de obtener una Probabilidad de Ocurrencia consensuada, asociada a cada amenaza en evaluación.

2. **Identificación de las amenazas que se tomarán en cuenta para la evaluación**

De la combinación de las variables descritas se obtiene la Probabilidad Estimada, que sirve como valor discriminatorio para seleccionar que amenazas se deberían evaluar para el alcance. Aquellas que resultan en un nivel de probabilidad estimada insignificante, según la tabla siguiente, no son tomados en cuenta.

Nivel de Probabilidad Estimada	Interpretación
Extrema	Probabilidad de ocurrencia alta (Evaluación de prioridad alta)
Moderado	Probabilidad de ocurrencia intermedia (Evaluación de prioridad baja)
Menor	Probabilidad de ocurrencia muy baja (Evaluación sin prioridad)
Insignificante	No se cree que ocurra (Desestimar evaluación)

3. **Cálculo de la Probabilidad de Afectación del Recurso**

Se utiliza la siguiente tabla de valores para el cálculo:

#	Probabilidad	Descripción
1	Improbable	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento (evaluados y mejorados), se evidencia que han respondido a acontecimientos ocurridos y ejercicios realizados
2	Baja	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas.
3	Moderada	Se cuenta con controles que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas, pero no son suficientes.
4	Alta	Algunos controles se prueban esporádicamente, debido a que no cuentan con un programa definido o de existir no se cumple con el mismo.
5	Muy Alta	Bajo nivel de controles o los controles existentes no son efectivos o eficientes.

4. **Cálculo del Impacto del Recurso**

Se utiliza la siguiente tabla de valores para el cálculo:

#	Impacto	Descripción
1	No significativo	Tiene un efecto nulo o muy pequeño en las operaciones de la sede evaluada.
2	Menor	Afecta hasta en 6 horas las operaciones de la sede evaluada.
3	Moderado	Afecta hasta en 24 horas las operaciones de la sede evaluada.
4	Mayor	Afecta hasta en 48 horas las operaciones de la sede evaluada.

5	Catastrófico	Afecta por más de una semana las operaciones de la sede evaluada.

5. Cálculo del Nivel de Riesgo

Se calcula considerando el mayor Nivel de Riesgo del recurso afectado por la amenaza que se está analizando. Para la identificación del Nivel de Riesgo se considera la siguiente matriz:

Probabilidad de Afectación		Impacto				
		No Significativo (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Muy Alta	(5)	Alto	Alto	Extremo	Extremo	Extremo
Alta	(4)	Moderado	Alto	Alto	Extremo	Extremo
Moderada	(3)	**Bajo**	Moderado	Alto	Extremo	Extremo
Baja	(2)	**Bajo**	**Bajo**	Moderado	Alto	Extremo
Improbable	(1)	**Bajo**	**Bajo**	Moderado	Alto	Alto

Interpretación de cada cuadrante de calor o Nivel de Riesgo de la amenaza en evaluación:

Nivel de Riesgo	Interpretación
Extremo	Riesgo no deseable, se requiere acción correctiva inmediata
Alto	Riesgo no deseable que requiere de una acción correctiva, pero se permite alguna discreción de la gerencia sobre los plazos y compromiso
Moderado	Riesgo aceptable con revisión de la dirección
Bajo	Riesgo aceptable sin revisión

ANEXO 02

LISTADO DE APLICACIONES Y SISTEMAS DE INFORMACIÓN CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Sistema / Aplicativo	Breve descripción	Área Usuaria	Motor de BD	Tipo	Prioridad
1	Portal Web Institucional	Promovemos la conservación y el uso sostenible de los recursos naturales, la puesta en valor de la diversidad biológica y la calidad ambiental en beneficio de las personas y el entorno de manera, descentralizada y articulada con las organizaciones públicas, privadas y la sociedad civil, en el marco del crecimiento verde y la gobernanza ambiental.	OC	MySQL	Web	1
2	Sistema Integrado de Gestión Administrativa Financiera - SIGFYS	Brindar soporte de los procesos administrativos del UNALM (Recursos Humanos, Logística, Contabilidad y Tesorería.	OGA	Oracle	Web	1
3	SIAF	Sistema de Administración Financiera	OGA	FoxPro	Desktop	1
4	Servicios Web - PIDE	Integrar los servicios web de la Plataforma de Interoperabilidad del Estado PIDE, de la ONGEI para consulta de información por parte del personal del UNALM	OTIC	No usa base de datos	Web	1
5	Sistema SIGA GESTOR – Módulo de Planeamiento	Aplicativo para la gestión de las actividades y/o tareas de la elaboración, seguimiento y evaluación del plan operativo institucional.	OGPP	Oracle	Web	1
6	Aula Vea - Aula Virtual	Capacitar virtualmente a docentes, funcionarios de gobiernos locales y regionales, con la finalidad de fortalecer las capacidades y necesidades de formación especializada.	DEGECIA	MySQL	Web	2
7	Módulo de Transparencia	Registro de información de transparencia de la UNALM	OGDAC	SQL Server	Web	2

N°	Sistema / Aplicativo	Breve descripción	Área Usuaria	Motor de BD	Tipo	Prioridad
8	Agenda Alta Dirección	Permite el registro de información de agenda de alta dirección del UNALM y su visualización a través del Portal Institucional	SG	Oracle	Web	2
9	Plataforma Virtual Mesa Verde	Permite el registro de la ayuda de la cooperación internacional que brinda información al UNALM	OGPP	Oracle	Web	3
10	Registro de Eventos	Aplicativo de registro de participantes a Eventos	DGECIA	MySQL	Web	3
11	Biblioteca Virtual / Repositorio Digital / DSPACE	Es un repositorio digital de una colección de más de 500 títulos en formato digital de las publicaciones editadas y auspiciadas por el UNALM, así como las consultorías contratadas por la institución.	OGDAC	PostgreSQL	Web	3
12	Sistema de Secretaría General	Sistema que integra la información de los módulos de comisiones, consultorías y compromisos	OGPP	Oracle	Web	3
13	Intranet	Permite integrar funcionalidades de utilidad para la gestión de información para el personal del UNALM	OGRH	Oracle	Web	3
14	Interface Marcador de Asistencia del Personal	Tiene el fin de capturar los registros de marcación de asistencia para luego enviarlos al Sistema Integrado de Gestión Administrativa del UNALM	OTIC	-------	Interface	3

OFICINA DE SERVICIOS INFORMÁTICOS V°B° U.N.A.L.M.

ANEXO 03

LISTADO DE EQUIPOS DEL CENTRO DE DATOS Y GABINETES DE COMUNICACIÓN CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Tipo de Equipo	Rol	Descripción	Prioridad
1	Equipo de almacenamiento	Almacenamiento	Equipo de almacenamiento de información, donde se configuran las máquinas virtuales.	1
2	Servidor	Controlador de Dominio	Servidor de dominio de red. (Directorio Activo, DNS).	1
2	Servidor	Backup	Servidor donde se encuentra instalado el software de respaldo, para respaldo y restauración de información.	1
3	Librería de Backup	Backup	Equipo donde se realizan las copias de respaldo en medios magnéticos, y es utilizado para la restauración de información.	1
4	Servidor	Base de Datos	Base de Datos Oracle.	1
5	Servidor	Base de Datos	Base de Datos PostgresSQL.	1
6	Servidor	Base de Datos	Base de Datos My SQL.	1
8	Servidor	Repositorio de Información	Fileserver. Servidor de archivos, donde se encuentra la información de las carpetas compartidas de red.	1
11	Servidor	Servidor Web	Servidor del portal web institucional.	1
13	Servidor	Aplicaciones	Servidor SIGA. (SIGFYS)	1
14	Switch	Comunicaciones	Switches Core, swicthes de acceso y DMZ	1
15	UPS	Energía	Equipo de suministro eléctrico para servidores y equipos de comunicaciones	1
16	Transformador	Energía	Equipo de suministro eléctrico para servidores y equipos de comunicaciones	1
17	Aire acondicionado	Acondicionamiento	Aire acondicionado de precisión para el Centro de Datos	1
18	Servidor	Base de Datos	Base de Datos SQL	2
20	Servidor	Servidor Web	Servidor para publicación de portales web ambientales	2
22	Servidor	Telefonía	Servidor de telefonía IP.	2
23	Servidor	Seguridad	Antivirus	2
24	Servidor	Administración de Servicios	PCSistel. Sistema de administración y control de llamadas telefónicas.	3
25	Servidor	Administración de Servicios	Servidor de monitoreo de red	3
27	Servidor	Repositorio de Información	Servidor de Fuentes	3

OFICINA DE SERVICIOS INFORMÁTICOS U.N.A.L.M. V°B°

N°	Tipo de Equipo	Rol	Descripción	Prioridad
28	Servidor	Aplicaciones	Servidor de aplicaciones internas: Intranet, inventario	3
29	Servidor	Almacenamiento	Servidor FTP	3

OFICINA DE SERVICIOS INFORMÁTICOS
V°B°
U.N.A.L.M.

ANEXO 04

FORMATOS DEL PLAN DE CONTINGENCIA INFORMÁTICO Y RESTAURACIÓN DE SERVICIOS DE TIC

	FORMATO	F06-PS06.1.01	
	REGISTRO Y ACCIÓN ANTE UN EVENTO	Versión: 01 Fecha: 10-02-25	Página 1

UNALM	Evento: Terremoto /Sismo

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Los sismos son movimientos en el interior de la tierra, que generan una liberación repentina de energía, que se propaga en forma de ondas provocando el movimiento del terreno.

Este evento incluye los siguientes elementos mínimos identificados por UNALM, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura:

- Oficinas y/o Centro de Datos Principal

Recursos Humanos

- Personal de la entidad.

b) Objetivo

Establecer las acciones que se ejecutarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones del UNALM, sin exponer la seguridad de las personas.

c) Entorno

Este evento puede afectar las instalaciones de la Sede Central y el Centro de Datos, al ubicarse en la misma ciudad y distritos colindantes.

d) Personal Encargado

El Grupo de Comando - Plan de Continuidad Operativa del UNALM, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. Por su parte, el Equipo de Prevención de TIC debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo

- Inspecciones de seguridad realizadas periódicamente.
- Contar con un plan de evacuación de las instalaciones del UNALM, el mismo que debe ser de conocimiento de todo el personal que labora en todas las sedes.
- Realización de simulacros de evacuación con la participación de todo el personal de las distintas sedes.
- Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
- Mantenimiento de las salidas libres de obstáculos.
- Señalización de las zonas seguras y las salidas de emergencia.
- Funcionamiento de las luces de emergencia.
- Definición de los puntos de reunión en caso de evacuación.

f) Acciones del Equipo de Prevención de TIC

- Evaluar en coordinación con el Grupo de Comando - Plan de Continuidad Operativa el ambiente para el Centro de Datos, en el sitio alterno.
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información base de datos, código fuentes y ejecutables.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro de Datos.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos

OFICINA DE SERVICIOS INFORMÁTICOS V° B° U.N.A.L.M.

de la entidad.
- Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia

La contingencia se activará al ocurrir un sismo. El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Procesos Relacionados antes del evento

- Tener la lista actualizada de los servidores por Direcciones y/u Oficinas.
- Mantenimiento del orden y limpieza de los ambientes de la sede central y Centro de Datos.
- Inspecciones trimestrales de seguridad externa.
- Realización de simulacros internos en horarios que no afecten las actividades.

c) Personal que autoriza la contingencia informática

El/La Coordinador/a de Continuidad de TIC.

d) Personal Encargado

Equipo de Emergencia de TIC.

e) Descripción de las actividades después de activar la contingencia

- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.
- Evacuar las oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.
- Verificar que todo el personal del UNALM que labora en el área se encuentre bien.
- Brindar los primeros auxilios al personal afectado si fuese necesario.
- Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo. En todo momento se coordinará con personal de mantenimiento del UNALM, para las acciones que deban ser efectuadas por ellos.

En caso se requiera la habilitación del ambiente provisional alterno para restablecer la función de los ambientes afectados, el/la Director/a de la OTIC deberá coordinar con el Director de la OGA.

f) Duración

Los procesos de evacuación del personal del UNALM deberán ser calmados y demorar 5 minutos como máximo.

La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado es el/la Coordinador/a de Continuidad de TIC y el Equipo de Restauración de TIC, cuyo rol principal es asegurar el normal desarrollo de los servicios y operaciones de TI del UNALM.

b) Descripción de actividades

El plan de recuperación está orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

En caso, el evento haya sido de considerable magnitud, se deberá:

- Verificar la disponibilidad de recursos para la contingencia como: manuales técnicos de

instalación del sistema de información, almacenamiento de datos, sistemas comunicación, hardware, y copias de respaldo.

- Movilizar los equipos de respaldo al sitio alterno de recuperación.
- Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la recuperación de negocio.
- Supervisar el progreso de las operaciones de recuperación y de servicios de TI y mantener informado al Grupo de Comando - Plan de Continuidad Operativa.
- Restauración de los servicios y operaciones de TI en el sitio alterno. El Equipo de restauración de TIC restaurarán el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:
  - Ejecutar los procedimientos de recuperación de la plataforma tecnológica.
  - Verificar que las aplicaciones críticas se hayan recuperado y estén funcionando correctamente.
  - Confirmar los puntos de recuperación de datos de las aplicaciones.
  - Verificar que las funcionalidades de comunicación están funcionando correctamente.
  - Verificar que equipos básicos como escáner, impresora estén disponibles y operacionales para dar soporte a los requisitos de la entidad.
  - Asegurar que el ambiente del área de trabajo, las aplicaciones y las telecomunicaciones están funcionando según lo estimado tanto en el sitio alterno, como al retornar al sitio original, una vez concluida la emergencia o siniestro.
- Registrar todos los gastos operacionales relacionados con la continuidad del negocio.

c) Mecanismos de Comprobación

El/La Coordinador/a de Continuidad de TIC, presentará un informe al Grupo de Comando - Plan de Continuidad Operativa, explicando qué parte de las actividades u operaciones de tecnologías de la información han sido afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

El/La Coordinador/a de Continuidad de TIC desactivará el Plan de Contingencia Informático una vez que se hayan tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica al Grupo de Comando - Plan de Continuidad Operativa.

e) Proceso de Actualización

El proceso de actualización será en base al informe presentado por el/la Coordinador/a de Continuidad de TIC, luego del cual se determinarán las acciones a tomar.

OFICINA DE SERVICIOS INFORMÁTICOS V° B° U.N.A.L.M.

	FORMATO	F06-PS06.1.01	
	REGISTRO Y ACCIÓN ANTE UN EVENTO	Versión: 01 Fecha: 10-02-25	Página 1

UNALM	Evento: Delito Informático

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Alteración de datos de los portales y sistemas de información a través de ataque cibernético (hacking) y/o malware.

El malware es un software malicioso o software malintencionado, que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario, eliminando datos del equipo. Incluye virus, gusanos, troyanos, keyloggers, botnets, ransomwares o secuestradores, spyware, adware, hijackers, keyloggers, rootkits, bootkits, rogues, etc.

Este evento incluye los siguientes elementos mínimos identificados por UNALM, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware
- Servidores
- Estaciones de Trabajo

Software
- Software Base
- Sistemas de información, aplicativos y portales del UNALM

b) Objetivo

Restaurar la operatividad de los equipos y servicios después de eliminar los malware o reinstalar las aplicaciones dañadas.

c) Entorno

Este evento se puede dar en cualquiera de los servidores y estaciones ubicadas en el Centro de Datos y en la sede principal del UNALM.

d) Personal Encargado

El Equipo de Prevención de TIC es el responsable del correcto funcionamiento de los servidores, estaciones de trabajo, sistemas de información y servicios de TI de acuerdo a sus perfiles.

e) Condiciones de Prevención de Riesgo
- Instalación de parches de seguridad en los equipos.
- Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.
- Aplicación de filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus.
- Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado permanentemente.
- Contar con equipos de respaldo ante posibles fallas de las estaciones y servidores, para su reemplazo provisional hasta su desinfección y habilitación.
- Restricción del acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.
- Eliminación o restricción de lectoras y/o quemadores de CD en estaciones de trabajo que no lo requieran.
- Deshabilitación de los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.
- Capacitación al personal de OTIC, sobre Ethical Hacking a las Bases de Datos, Sistemas

Operativos, Servidores y Sistemas Informáticos.
- Ejecución de ataques de Hacking Ético por terceros especializados.

f) Acciones del Equipo de Prevención de TIC
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo de información de la información procesada y almacenada en el Centro de Datos.
- Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.
- Realizar pruebas de restauración de la información almacenada en los repositorios y bases de datos.
- Documentar y validar los manuales de restauración de los sistemas de información en producción.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia
- Mensajes de error durante la ejecución de programas.
- Lentitud en el acceso a las aplicaciones.
- Falla general en el equipo (sistema operativo, aplicaciones).

b) Procesos relacionados antes del evento

Cualquier proceso relacionado con el uso de las aplicaciones en los servidores y en las estaciones de trabajo.

c) Personal que autoriza la contingencia

El/La Coordinador/a de Continuidad de TIC y el/la Oficial de Seguridad de la Información pueden activar la contingencia.

d) Personal Encargado

Equipo de Emergencia de TIC.

e) Descripción de las actividades después de activar la contingencia
- Desconectar o retirar de la red de datos del UNALM, el servidor o la estación infectada o vulnerada.
- Verificar si el equipo se encuentra infectado, utilizando un detector de malware/virus actualizado. En el caso de aplicaciones, verificar si el código o la información de las bases de datos ha sido alterada.
- Rastrear de ser necesario el origen de la infección o ataque (archivo infectado, correo electrónico, hacking, etc.)
- Guardar la muestra del virus detectado y remitir al proveedor del antivirus utilizado. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado, a nivel de software y base de datos.
- Eliminar el agente causante de la infección, es decir, remover el malware/virus del sistema.
- Probar el sistema.
- En caso de no solucionarse el problema, formatear el equipo y restaurar copia de respaldo.

f) Duración

La duración del evento no deberá ser mayor DOS HORAS en caso se confirme la presencia de un virus en estaciones de trabajo y de CUATRO HORAS en servidores de red. Esperar la indicación del personal de soporte técnico para reanudar el trabajo

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El equipo de restauración de TIC, luego de restaurar el correcto funcionamiento del servidor, estación de trabajo (PC, laptop), sistemas de información y portales web, coordinará con el usuario responsable del mismo y/o Director del área para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b) Descripción de actividades

Se informará a el/la Director/a de OTIC del UNALM el tipo de malware/virus, o tipo de ataque

encontrado y el procedimiento usado para removerlo.

Estas actividades deben contemplar como mínimo:

- Instalación y puesta a punto de un cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
- Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.
- Instalación y configuración del sistema de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad.
- Instalación de aplicaciones adicionales necesarias para el funcionamiento del sistema de información.
- Realización de la restauración de la base de datos con la última copia de seguridad disponible (Restore).
- Reinicio del servicio, prueba y afinamiento del sistema de información.
- Conectar el servidor o la estación a la red del UNALM.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información afectados.
- Solicitar la conformidad de la restauración realizada del equipo y o sistema de información afectado.
- Comunicar el restablecimiento del servicio

En función a esto, el/la Oficial de Seguridad de la Información, tomará las medidas preventivas del caso enviando una alerta vía correo al personal del UNALM.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentes de seguridad de la información.

c) Mecanismos de Comprobación

Se llenará el formato de incidentes de seguridad de la información y se informará al Comité de Gestión de Seguridad de la Información.

El personal de Técnico de Soporte y/o Especialista en Redes y Comunicaciones, según sea el caso, presentará un informe a el/la Director/a de OTIC, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

Con el aviso de el/la Coordinador/a de Continuidad de TIC del UNALM, se desactivará el presente Plan.

e) Proceso de Actualización

El problema de infección o alteración presentado en la estación de trabajo y/o servidor de red, en base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar

	FORMATO	F06-PS06.1.01	
	REGISTRO Y ACCIÓN ANTE UN EVENTO	Versión: 01 Fecha: 10-02-25	Página 1

UNALM	Evento: Falla de hardware y software

1. PLAN DE PREVENCIÓN

a) Descripción del evento

El hardware de servidores es el recurso principal para almacenar, procesar y proteger los datos, permitiendo acceso controlado y procesamiento de transacciones rápido para cumplir con los requisitos de las aplicaciones de la entidad.

El software

En ausencia del mismo, los sistemas de información que dependen del mismo no pueden funcionar, siendo la parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores de Base de Datos, Aplicaciones, Archivos
- Storage

Software

- Aplicativos usados por UNALM y de servicio al ciudadano

Información

- Información contenida en base de datos.
- Información contenida en repositorios de información

b) Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados de las imágenes de los servidores o máquinas virtuales en producción.

c) Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a las operaciones del UNALM.

d) Personal Encargado

Equipo de Prevención de TIC.

e) Condiciones de Prevención de Riesgo

- Revisión periódica de los registros (logs) de los servidores, para prevenir mal funcionamiento de los mismos.
- Contar con los backups diarios de datos de las aplicaciones en desarrollo/producción de la entidad, así como de las imágenes de los servidores.
- Contar con servicios de soporte y mantenimiento que contemple actividades de prevención, revisión del sistema y mantenimiento general.
- Disponer de servidores de bases de datos de contingencia, con la instalación del motor de base de datos.
- Disponer de servidores de Aplicaciones de contingencia, con software de instalación tomcat, jboss, wildfly.

f) Acciones del Equipo de Prevención de TIC

Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información.

- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro de Datos.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Realizar monitoreo del funcionamiento de los servidores instalados en el Centro de Datos para su correcto funcionamiento.
- Realizar revisiones de obsolescencia tecnológica de los servidores y componentes internos de forma anual.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia
- Fallas en la conexión. Indisponibilidad del sistema de información y/o aplicativo.
- Identificación de fallas en la pantalla de las estaciones de trabajo y/o servidores de aplicaciones.

b) Procesos Relacionados antes del evento
- Disponibilidad de las copias de respaldo.
- Disponibilidad de instaladores de sistemas operativos y motor de base de datos.

c) Personal que autoriza la contingencia

El/La Coordinador/a de Continuidad de TIC debe activar la contingencia.

d) Descripción de las actividades después de activar la contingencia
- Realizar la revisión del servidor averiado, buscando un recurso de reemplazo verificando que dicho equipo cuente con garantía, de lo contrario se implementará un nuevo servidor virtual configurado de acuerdo a lo requerido.
- Solicitar las cintas de respaldo para poder proceder a la restauración de la información almacenada en el servidor averiado.

e) Duración

El tiempo máximo de la contingencia no debe sobrepasar las cuatro (4) horas.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El Equipo de Restauración de TIC, luego de validar la corrección del problema de acceso a los servidores, y el/la Coordinador/a de Continuidad de TIC informará a los Directores y/o Directores de áreas para la reanudación de las operaciones de los servicios afectados en el servidor averiado.

b) Descripción de actividades

El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio afectado por falla de los servidores. Se debe realizar como mínimo las siguientes actividades:
- Instalación y puesta a punto de un cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
- Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.
- Instalación y configuración del sistema de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad.
- Proceder a la restauración de las copias de respaldo, de la información de los servidores afectados.
- Verificar que la data y los aplicativos se hayan restaurado correctamente.
- Ejecutar pruebas de acceso a los sistemas y aplicaciones.
- Brindar los permisos de acceso a los usuarios finales.
- Remitir un mensaje electrónico a los usuarios del UNALM informando la reanudación de los servicios.
- En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

c) Mecanismos de Comprobación
- Se registrará el incidente en el Sistema de Gestión de Tickets utilizado por la Mesa de Ayuda y Soporte Técnico de la OTIC, precisando las acciones realizadas.
- El/La Especialista en Redes y Comunicaciones, presentará un informe a el/la Director/a de la OTIC, explicando que parte del servicio u operaciones se han visto afectadas, y

cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia
   - Con el aviso de el/la Coordinador/a de Continuidad de TIC, se desactivará el presente Plan.

e) Proceso de Actualización
   - En base al informe presentado por el/la Especialista en Redes y Comunicaciones, quien identifica las causas de la pérdida o fallas de la base de datos institucional, se determinará las acciones preventivas necesarias que deberían incluirse en el presente plan.
   - En caso existiese información pendiente de actualización, el/la Especialista en Redes y Comunicaciones deberá iniciar las labores de actualización de los procedimientos o guías de recuperación de servidores

OFICINA DE SERVICIOS INFORMÁTICOS
V° B°
U.N.A.L.M.

	FORMATO	F06-PS06.1.01	
	REGISTRO Y ACCIÓN ANTE UN EVENTO	Versión: 01 Fecha: 10-02-25	Página 1

UNALM	Evento: Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	FPC - 04

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Falla general del suministro de energía eléctrica en el Centro de Datos o sede principal de la entidad.

Este evento incluye los siguientes elementos mínimos identificados por UNALM, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicios Públicos:

- Suministro de Energía Eléctrica

Hardware

- Servidores y sistema de almacenamiento de información (storage)
- Estaciones de Trabajo
- Equipos de Comunicaciones

Equipos Diversos

- UPS y generador eléctrico
- Aire acondicionado

b) Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

c) Entorno

Este evento puede darse en cualquiera de las instalaciones del UNALM, considerando la Sede Central y la sede donde se ubica el Centro de Datos, por tener cada una de ellas los gabinetes de comunicación y equipos que brinda servicios informáticos a los usuarios a nivel interno y externo.

d) Personal Encargado

El Jefe de la Unidad de Abastecimiento y el/la Coordinador/a de Continuidad de TIC son los responsables de realizar las coordinaciones para restablecer el suministro de energía eléctrica. El Equipo de Prevención de TIC debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicio u operaciones del UNALM se contará con los UPS necesarios para asegurar el suministro eléctrico en los equipos considerados como críticos.
- Los equipos UPS cuentan con mantenimiento preventivo y con suficiente energía para soportar una operación continua de 30 minutos como mínimo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS.
- Realización de pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.
- Capacidad de los UPS para proteger los servidores de archivos, base de datos y aplicaciones, previniendo la pérdida de datos durante las labores. La autonomía del equipo UPS no deberá ser menor a 30 minutos.
- Disponibilidad de UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones del UNALM (puertas, contactos magnéticos, etc.)
- Verificación del cableado eléctrico de todas las sedes de la Universidad Nacional Agraria la Molina, una vez por año.

- Instalación de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.

f) Acciones del Equipo de Prevención de TIC
- Revisar periódicamente y de forma conjunta con el área de Servicios Generales las instalaciones eléctricas del Centro de Datos y Sede principal de la entidad.
- Coordinar y supervisar el mantenimiento preventivo de pozos a tierra, aire acondicionado de precisión del Centro de Datos, UPS, transformador y del gabinete de baterías trimestralmente.
- Verificar que la red eléctrica utilizada en el Centro de Datos y la red de cómputo de la sede principal sea estabilizada. En caso no existan se debe gestionar la implementación de lo requerido con el área respectiva.
- Revisar la presencia de exceso de humedad en la sala de energía del centro de datos de la Universidad Nacional Agraria la Molina.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia
Corte de suministro de energía eléctrica en los ambientes del UNALM.

b) Procesos Relacionados antes del evento
Cualquier actividad de servicio dentro de las instalaciones.

c) Personal que autoriza la contingencia
El/La Director/a de OGA y/o Coordinador de Continuidad de TIC pueden activar la contingencia.

d) Descripción de las actividades después de activar la contingencia
- Informar a el/la Director/a de la Unidad de Abastecimiento del problema presentado.
- Comunicar a la empresa prestadora de servicios de energía eléctrica la falta de energía.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del UNALM y coordinar las acciones necesarias.
- Las actividades afectadas por la falta de uso de aplicaciones deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.
- En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente.
- En caso la interrupción de energía en el Centro de Datos sea mayor a dos (02) horas, se deberán apagar los equipos en forma ordenada mientras funcione el UPS y hasta que regrese el fluido eléctrico.

e) Duración
El tiempo máximo de duración de la contingencia dependerá del proveedor externo de energía eléctrica.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado
El Equipo de Restauración de TIC, quienes se encargarán de realizar las acciones de recuperación necesarias.

b) Descripción de actividades
El evento será evaluado y registrado de ser necesario en el formato de incidentes de seguridad de la información
Se debe realizar como mínimo las siguientes actividades:
- Al retorno de la energía comercial se verificará por el lapso de media hora que no haya interrupciones o fluctuaciones de energía.
- Proceder a encender la plataforma tecnológica ordenadamente de acuerdo con el siguiente detalle:
  - Equipos de Comunicaciones (router, switches core, switches de acceso)
  - Equipos de almacenamiento (storage)
  - Servidores físicos por orden de prioridad

- Servidores virtuales por orden de prioridad

- La contingencia finaliza cuando retorna la energía eléctrica y todos los equipos se encuentran operativos brindando servicio.

c) Mecanismos de Comprobación

El/La Especialista en Redes y Comunicaciones presentará un informe a el/la Director/a de la OTIC, explicando que parte del servicio, equipos u operaciones de tecnología de la información han fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

Este informe deberá ser elevado al Grupo de Comando - Plan de Continuidad Operativa del UNALM.

d) Desactivación del Plan de Contingencia

El/La Coordinador de Continuidad de TIC desactivará el Plan de Contingencia una vez que se recupere la funcionalidad del suministro eléctrico y la operatividad de los sistemas y servicios de tecnología de la información.

e) Proceso de Actualización

En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

OFICINA DE SERVICIOS INFORMÁTICOS
V° B°
U.N.A.L.M.

ANEXO 05

FORMATO DE CONTROL Y CERTIFICACIÓN DE LAS PRUEBAS

	FORMATO	F07-PS06.1.01	
	CONTROL Y CERTIFICACIÓN DE LAS PRUEBAS	Versión: 01 Fecha: 10-02-25	Página 1

CONTROL Y CERTIFICACIÓN DE PRUEBAS DE CONTINGENCIA

PRUEBA N° _____

Escenario de Prueba: (Descripción del escenario a probar/certificar)

Área Responsable: (Área responsable del escenario de prueba a probar/certificar)

INFORMACIÓN DEL PROCESO

Metodología: . (Detallar lo que se va a hacer en la prueba)
.
.

Alcance: . (Definir hasta donde va a abarcar)
.
.

Condiciones de Ejecución

Equipo: Nombre servidor/PC prueba — Aplicación/Software: _____

Ubicación: Lugar de prueba — Fecha de Backup: / /

RESULTADO DE LA PRUEBA

Resultado: Satisfactorio: ☐ Satisfactorio con observaciones: ☐ Deficiente: ☐

Observaciones: . (Detallar lo que se va a hacer en la prueba)
.
.

ACTUALIZACIÓN DEL PLAN DE CONTINGENCIA

Cambios o actualizaciones en el Plan de Contingencia: . (Se indicarán los cambios que se deben realizar en el Plan de contingencia como consecuencia de las observaciones detectadas en las pruebas correspondientes)
.
.

ACTUALIZACIÓN PARTICIPANTES

PARTICIPANTE	CARGO	FIRMA