



UNIVERSIDAD NACIONAL DE EDUCACIÓN

Enrique Guzmán y Valle
"Alma Máter del Magisterio Nacional"

RECTORADO

RESOLUCIÓN N° 1956-2026-R-UNE

Chosica, 02 de julio del 2026

VISTO el Oficio N° 318-2026-OPyP-UNE, del 03 de junio del 2026, de la Oficina de Planeamiento y Presupuesto de la Universidad Nacional de Educación Enrique Guzmán y Valle.

CONSIDERANDO:

Que, a través del Oficio N° 154-2026-OTI-UNE, el Director de la Oficina de Tecnologías de la Información remite la propuesta del Plan de Continuidad Operativa de los Servicios Informáticos de la UNE EGYV, a fin de que se adopten las acciones correspondientes;

Que mediante Oficio N° 0236-2026-UM/OPyP-UNE, del 01 de junio del 2026, la Jefa de la Unidad de Modernización eleva al Director de la Oficina de Planeamiento y Presupuesto el PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS;

Que con el documento del visto, el Director de la Oficina de Planeamiento y Presupuesto remite al Rectorado el expediente en mención, a fin de que el Consejo Universitario se pronuncie al respecto;

Estando a lo acordado por el Consejo Universitario, en su sesión ordinaria virtual realizada el 30 de junio del 2026; y,

En uso de las atribuciones conferidas por los artículos 59° y 60° de la Ley N° 30220 - Ley Universitaria, concordante con los artículos 19°, 20° y 23° del Estatuto de la UNE, y los alcances de la Resolución N° 1436-2026-R-UNE;

SE RESUELVE:

ARTÍCULO 1°.- APROBAR el PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS DE LA UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE, suscrito por la instancia pertinente y la oficina técnica respectiva, dando conformidad al contenido que se adjunta en cuarenta y nueve (49) folios.

ARTÍCULO 2°.- DAR A CONOCER a las dependencias correspondientes los alcances de la presente resolución, a fin de que se adopten las acciones complementarias que resulten pertinentes.

Regístrese, comuníquese y cúmplase.



Abg. Anita Laz Chacón Ayala
Secretaría General



Dr. Tito Doroteo Acosta Castro
Rector



**UNIVERSIDAD NACIONAL DE EDUCACIÓN
ENRIQUE GUZMÁN Y VALLE**
Alma Máter del Magisterio Nacional

**PLAN DE CONTINUIDAD OPERATIVA DE
LOS SERVICIOS INFORMÁTICOS**



Versión: 1.0

 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 2 / 49

CUADRO DE RESPONSABLES

Etapa	Responsable	Firma y sello
Propuesto por:	Lic. Victor Walter Gallegos Ferrel	  Lic. Victor Walter Gallegos Ferrel Director Oficina de Tecnologías de la Información
Cargo:	Director de la Oficina de Tecnologías de la Información.	
Revisado por: (Revisión Técnica)	Lic. Adm. Julia Achahui Huayhua	  Lic. Adm. Julia Achahui Huayhua Jefa de la Unidad de Modernización
Cargo:	Jefa de la Unidad de Modernización.	
Validado por:	C.P.C. Alejandro Juan Mayhuire Gallegos.	  C.P.C. Alejandro Juan Mayhuire Gallegos DIRECTOR Oficina de Planeamiento y Presupuesto
Cargo:	Director de la Oficina de Planeamiento y Presupuesto.	



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 3 / 49

HOJA DE CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Responsable



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 4 / 49

INDICE

1. INFORMACIÓN GENERAL.....	6
2. BASE LEGAL	8
2.1. Marco legal.....	8
2.2. Normas Internacionales Aplicadas.....	9
3. OBJETIVOS	10
3.1. Objetivo General.....	10
3.2. Objetivo Específicos	10
4. TERMINOS Y DEFINICIONES	11
5. ALCANCE	14
6. EXCLUSIONES	15
7. EVALUACIÓN Y GESTIÓN DE RIESGOS.....	15
7.1. Metodología de Evaluación de Riesgos.....	15
7.2. Matriz de Riesgos Identificados.....	16
7.3. Controles de Mitigación Propuestos	17
8. ANÁLISIS DE IMPACTO AL NEGOCIO (BIA)	18
8.1. Metodología del BIA.....	18
8.2. Parámetros Críticos de Recuperación	18
8.3. Clasificación de Servicios	20
8.4. Dependencias Críticas Identificadas	20
9. CONTINUIDAD DEL NEGOCIO	21
9.1. Principios de la Continuidad del Negocio Universitario	21
9.2. Procesos Críticos del Negocio y sus Requerimientos	21
9.3. Procedimientos de Operación en Modo Emergencia.....	22
9.4. Roles de Continuidad por Proceso	24
9.5. Proveedores Críticos y Contratos de Soporte	24
10. ESTRATEGIA DE CONTINUIDAD Y RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS.....	25



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 5 / 49

10.1.	Principios de la Estrategia	25
10.2.	Arquitectura de Alta Disponibilidad Propuesta	25
10.3.	Estrategia de Respaldo y Recuperación de Datos	26
10.4.	Alineación con ISO/IEC 27017 para Servicios Cloud	27
11.	RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS ANTE DESASTRES	27
11.1.	Definición de Escenarios de Interrupción.....	27
11.2.	Procedimiento de Activación para Recuperación de los servicios Informáticos ante Desastres	28
11.3.	Matriz de Clasificación de Incidentes.....	29
11.4.	Procedimientos Específicos de Recuperación.....	29
11.5.	Criterios de Retorno al Sitio Principal.....	32
12.	ESTRUCTURA ORGANIZACIONAL DE RESPUESTA	33
12.1.	Comité de Crisis Institucional	33
12.2.	Equipo de Recuperación Tecnológica (ERT)	34
12.3.	Árbol de Escalamiento y Comunicación	34
13.	PROCEDIMIENTOS DE PRUEBA Y MANTENIMIENTO	35
13.1.	Programa Anual de Pruebas	35
13.2.	Proceso de Mejora Continua	36
13.3.	Criterios de Actualización del Plan	36
14.	INDICADORES Y MÉTRICAS DE DESEMPEÑO	36
14.1.	KPIs del Sistema de Gestión de Continuidad	37
14.2.	Reporte Periódico al Comité de Crisis	38
15.	COMUNICACIONES DE CRISIS	38
15.1.	Principios de Comunicación en Crisis.....	38
15.2.	Públicos y Mensajes Clave.....	38
15.3.	Plantillas de Comunicación de Crisis.....	39
16.	CRONOGRAMA DE IMPLEMENTACIÓN (12 MESES)	40
17.	PRESUPUESTO.....	42
17.1.	Presupuesto Estimado para la Implementación (Primer Año)	42
18.	FACTORES CRÍTICOS DE ÉXITO	43
19.	ANEXOS.....	43



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 6 / 49

PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS

1. INFORMACIÓN GENERAL

En el contexto actual de la transformación digital de la educación superior, la Universidad Nacional de Educación Enrique Guzmán y Valle ha incrementado significativamente su dependencia tecnológica de los sistemas de información para la gestión académica, administrativa y de investigación.

En este entorno digital altamente dependiente de la tecnología, garantizar la continuidad de los servicios de tecnología de la información es fundamental para el correcto funcionamiento de cualquier organización. En este contexto, el Plan de Continuidad Operativa de los Servicios Informáticos de la Universidad Nacional de Educación Enrique Guzmán y Valle, en adelante UNE, establece acciones técnico-operativas para la recuperación eficiente y oportuna de los servicios críticos de tecnologías de la información ante eventos que comprometan su disponibilidad.

Este plan ha sido desarrollado considerando las mejores prácticas en continuidad operativa y seguridad de la información, asegurando la rápida respuesta ante incidentes que puedan afectar la infraestructura tecnológica, los sistemas de información y la disponibilidad de datos esenciales. Su aplicación se activa en situaciones de indisponibilidad severa y prolongada, minimizando el impacto en los procesos institucionales y garantizando la continuidad de las operaciones estratégicas de la UNE.

El documento define la estructura organizativa para asegurar la continuidad operativa, los roles y responsabilidades de los equipos de trabajo, los procedimientos de respaldo y restauración de datos, así como las pruebas y evaluaciones periódicas, en base a un conjunto de actividades necesarias para la recuperación ante desastres y la continuidad de negocio.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 7 / 49

Con la implementación de este plan, UNE refuerza su compromiso con la resiliencia tecnológica y la protección de su infraestructura digital, asegurando que los servicios de tecnologías de la información se mantengan disponibles, confiables y alineados con los objetivos estratégicos de la organización.

Los servicios críticos que dependen de la infraestructura TI incluyen:

- 1) Sistema de Gestión Académica (SIGEAC)
- 2) Sistema Integrado de Gestión Administrativo (SIGA)
- 3) INTRANET – UNE (Alumnos y Administrativos)
- 4) Directorio Activo (AD) y File Server Local
- 5) Campus Virtual y plataforma de educación
- 6) Portales Web Institucionales
- 7) Correo electrónico institucional y comunicaciones
- 8) Sistema de Trámite Documentario
- 9) Sistema de Biblioteca KOHA
- 10) Sistema de Admisión
- 11) Módulo de Mesa de Partes Virtual
- 12) Sistema de Nóminas y Planillas
- 13) Sistema SIAF y File Server SIAF
- 14) Sistema de Backup (VEEAM BACKUP)
- 15) Sistemas CCTV (Video Vigilancia)

La ausencia de una planificación que asegure la Continuidad de Negocio y la Recuperación ante Desastres formalmente documentados y probados expone a la Universidad Nacional de Educación Enrique Guzmán y Valle a riesgos significativos que podrían interrumpir sus actividades académicas, administrativas e investigativas en las tres sedes. La región de Lurigancho-Chosica presenta factores de riesgo particulares que justifican la urgencia de este plan como etapa inicial:

- Riesgo sísmico: La región de Lima se encuentra en una zona de alta actividad sísmica.
- Riesgo hidrológico: La zona de Chosica es vulnerable a huaicos y deslizamientos de tierra.
- Riesgos cibernéticos: Incremento de ataques de ransomware y phishing a universidades públicas.
- Riesgo de falla de infraestructura: envejecimiento de equipos y limitaciones presupuestales.
- Fallas eléctricas: Cortes prolongados de energía eléctrica por más de 6 u 8 horas fuera del horario laboral en las tres sedes.
- Cumplimiento normativo: Resoluciones de la SUNEDU y normativas del Estado Peruano.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 8 / 49

2. BASE LEGAL

2.1. Marco legal

- Decreto Legislativo N.º 1412, que aprueba la Ley de Gobierno Digital.
- Decreto de Urgencia N.º 006-2020, que crea el Sistema Nacional de Transformación Digital.
- Ley Universitaria N.º 30220.
- Ley N.º 27658, Ley Marco de Modernización de la Gestión del Estado
- DS N.º 033-2018-PCM – Plataforma Digital Única del Estado Peruano y disposiciones adicionales para el desarrollo del Gobierno Digital
- DS N.º 003-2013-JUS - Reglamento de la Ley de Protección de Datos Personales.
- Ley N.º 29733 - Ley de Protección de Datos Personales
- Decreto Supremo N.º 038-2021-PCM, que aprueba la Política Nacional de Gestión del Riesgo de Desastres al 2050.
- Resolución Ministerial N.º 320-2021-PCM, que aprueba los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades públicas en los Tres Niveles de Gobierno".
- Resolución Directoral N.º 014-2018-INACAL-DN, que aprueba la Norma Técnica Peruana NTP-ISO 31000:2018 Gestión del Riesgo. Directrices. 2ª Edición
- Resolución Directoral N.º 004-2020-INACAL-DN, que aprueba la Norma Técnica Peruana NTP-ISO 22301:2020 Seguridad y resiliencia. Sistemas de gestión de continuidad del negocio. Requisitos. 1ª Edición.
- Resolución Directoral N.º 022-2022-INACAL/DN, que aprueba la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición. Reemplaza a la NTP-ISO/IEC 27001:2014.
- Decreto Supremo N.º 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N.º 157-2021-PCM, aprueba el Reglamento del Decreto de Urgencia N.º 006- 2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Resolución Ministerial N.º 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 9 / 49

- Resolución N° 1034-2025-R-UNE que reconforma el Comité de Gobierno y Transformación Digital de la Universidad Nacional de Educación Enrique Guzmán y Valle.
- Resolución N° 3566-2023-R-UNE que aprueba el Plan de Gobierno Digital de la Universidad Nacional de Educación Enrique Guzmán y Valle.
- Resolución N° 1943-2024-R-UNE que aprueba el Plan Estratégico Institucional 2025-2030 de la Universidad Nacional de Educación Enrique Guzmán y Valle.
- Resolución Rectoral N°909-2025-R-UNE que designa al Oficial de Seguridad y Confianza Digital.
- Resolución N°3336-2025-R-UNE que conforma el Equipo de Respuestas ante Incidentes de Seguridad Digital de la Universidad Nacional de Educación Enrique Guzmán y Valle (CSIRT-UNE EGYV).
- Resolución Rectoral N°3940-2025-R-UNE que aprueba la Política de Seguridad de la Información de la Universidad Nacional de Educación Enrique Guzmán y Valle.
- Resolución Rectoral N°0392-2026-R-UNE que aprueba la designación del Oficial de Datos Personales de la Universidad Nacional de Educación Enrique Guzmán y Valle.

2.2. Normas Internacionales Aplicadas

El presente plan de continuidad operativa de los servicios informáticos de la UNE EGYV se alinea con las siguientes Normas Internacionales de gestión:

Norma	Título	Aplicación en este Plan
ISO 22301:2019	Seguridad y Resiliencia - SGCN	Marco principal para la continuidad del negocio: contexto, liderazgo, planificación, operación, evaluación y mejora continua del sistema de gestión de continuidad
ISO/IEC 27001:2022	SGSI - Seguridad de la Información	Gestión de activos de información, evaluación de riesgos, controles de seguridad y auditoría del SGSI universitario
ISO/IEC 27031:2011	TIC para Continuidad del Negocio	Guía específica para la preparación de servicios TIC, definición de RTO/RPO y estrategias de recuperación tecnológica



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 10 / 49

Norma	Título	Aplicación en este Plan
ISO/IEC 27017:2015	Controles de Seguridad Cloud	Controles adicionales para servicios en la nube.

3. OBJETIVOS

3.1. Objetivo General

Desarrollar, implementar y mantener un Plan de Continuidad Operativa de Servicios Informáticos para establecer acciones técnico-operativas por realizar ante eventos que comprometan su disponibilidad, integridad y continuidad, bajo los parámetros, cláusulas y recomendaciones que sustenta la planificación de actividades para la continuidad de negocio y la recuperación ante desastres, para la Universidad Nacional de Educación Enrique Guzmán y Valle, alineados con las normas ISO 22301, NTP ISO/IEC 27001:2022, ISO/IEC 27031 e ISO/IEC 27017.

3.2. Objetivo Específicos

- Identificar y clasificar todos los procesos, sistemas y servicios críticos de la universidad que dependen de la infraestructura TIC.
- Realizar un análisis de impacto al negocio (BIA) que determine los tiempos máximos tolerables de interrupción para cada servicio crítico.
- Evaluar los riesgos tecnológicos, físicos y humanos que podrían provocar interrupciones en los servicios institucionales.
- Definir acciones técnicas operativas que incluyan sitios alternos, respaldos, redundancia y servicios en la nube.
- Establecer procedimientos detallados para la respuesta, recuperación y restauración de los servicios TIC ante distintos escenarios de desastre.
- Constituir una estructura organizacional de crisis con roles, responsabilidades y cadena de mando claramente definidos.
- Minimizar el impacto académico, administrativo y reputacional.
- Definir responsabilidades claras durante una crisis tecnológica.
- Establecer tiempos objetivos de recuperación (RTO) y puntos objetivos de recuperación (RPO).
- Implementar un programa de pruebas, capacitación y mejora continua del plan.
- Garantizar el cumplimiento de la normativa legal peruana y las normas internacionales de referencia.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 11 / 49

4. TERMINOS Y DEFINICIONES

SIGLAS	DEFINICIÓN
UNE	Universidad Nacional de Educación Enrique Guzmán y Valle
BIA	Análisis de Impacto al Negocio - Evaluación de las consecuencias de la interrupción de procesos críticos
RTO	Tiempo Objetivo de Recuperación - Tiempo máximo aceptable para restaurar un servicio después de una interrupción
RPO	Punto Objetivo de Recuperación - punto máximo de pérdida de datos tolerable
OTI	Oficina de Tecnología de la Información
USTyR	Unidad de Soporte Técnico y Redes
HA	Alta Disponibilidad - Arquitectura de sistemas diseñada para minimizar el tiempo de inactividad
UPS	Sistemas de alimentación ininterrumpida (SAI), en inglés Uninterruptible Power Supply.
MTTD	Tiempo Medio de Detección - Tiempo promedio entre el inicio de un incidente y su detección
ERT	Equipo de Recuperación de Emergencia - Grupo técnico especializado que ejecuta el DRP
NOC	Centro de Operaciones de Red - Centro de monitoreo y gestión de la infraestructura TI
SLA	Acuerdo de Nivel de Servicio - Contrato que define los niveles de servicio y tiempos de respuesta acordados con proveedores
SGCN	Sistema de Gestión de Continuidad del Negocio - Marco sistemático bajo ISO 22301 para gestionar la continuidad
VM	Máquina Virtual.
ETR	Tiempo Estimado de Reparación

- a) **Base de Datos:** Conjunto estructurado de datos relacionados, almacenados de manera sistemática para su uso y consulta eficiente.
- b) **Centro de Datos (data center) Principal:** Infraestructura centralizada donde se concentran los recursos tecnológicos esenciales para el procesamiento y almacenamiento de la información de la entidad.
- c) **Centro de Datos (data center) Alternativo:** Infraestructura de contingencia diseñada para asumir el procesamiento y almacenamiento de la información en caso de fallas en el centro de datos principal.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 12 / 49

- d) **Copia de Seguridad (Backup):** Réplica de los datos originales realizada con el propósito de garantizar su recuperación en caso de pérdida o falla del sistema.
- e) **Confidencialidad:** Principio de seguridad que asegura que la información solo sea accesible y manipulada por personal autorizado, evitando su divulgación no autorizada.
- f) **Disponibilidad:** Garantía de que los usuarios autorizados puedan acceder a la información y recursos tecnológicos cuando los necesiten, asegurando la continuidad de los servicios.
- g) **Desastre:** Conjunto de daños y pérdidas, en la salud, fuentes de sustento, hábitat físico, infraestructura, actividad económica y medio ambiente, que ocurre a consecuencia del impacto de un peligro o amenaza cuya intensidad genera graves alteraciones en el funcionamiento de las unidades sociales, sobrepasando la capacidad de respuesta local para atender eficazmente sus consecuencias, pudiendo ser de origen natural o inducido por la acción humana.
- h) **Evento:** Suceso o cambio en un conjunto específico de circunstancias que puede tener múltiples causas y consecuencias.
- i) **Impacto:** Conjunto de efectos negativos que se generan cuando un riesgo se materializa, afectando los procesos, la infraestructura o los servicios de la entidad.
- j) **Incidente:** Cualquier interrupción o alteración en los servicios tecnológicos de la organización que afecta desde un usuario individual hasta toda la entidad, comprometiendo la continuidad operativa.
- k) **Infraestructura Tecnológica:** Conjunto de componentes tecnológicos, incluyendo hardware, software, redes y servicios, que soportan y permiten el funcionamiento de las operaciones institucionales.
- l) **Integridad:** Propiedad de la información que garantiza su precisión, fiabilidad y protección contra modificaciones no autorizadas o errores involuntarios.
- m) **Mitigación del Riesgo:** Conjunto de acciones y estrategias implementadas para reducir la probabilidad de ocurrencia o el impacto negativo de un evento adverso sobre la infraestructura y los servicios tecnológicos.
- n) **Ransomware:** También llamado "secuestro de datos", es un tipo de software malicioso que restringe el acceso a archivos o sistemas operativos y exige un



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 13 / 49

pago (rescate) para liberarlos. Generalmente cifra la información, inutilizando el dispositivo, y solicita pagos mediante criptomonedas no rastreables para revertir el daño.

- o) **Peligro o Amenaza:** Probabilidad de que un fenómeno físico, potencialmente dañino, de origen natural o inducido por la acción humana, se presente en un lugar específico, con una cierta intensidad y en un periodo de tiempo y frecuencia definidos.
- p) **Probabilidad:** Posibilidad de que un evento ocurra. Puede expresarse de manera cualitativa o cuantitativa, utilizando términos generales o modelos matemáticos, como frecuencias en un período determinado.
- q) **Proceso Crítico:** Conjunto de actividad esenciales para la continuidad operativa de la institución, cuya interrupción o ejecución deficiente puede generar un impacto negativo en la operatividad, así como el incumplimiento de metas y objetivos institucionales.
- r) **Riesgo:** Probabilidad de que un evento, ya sea perjudicial (no deseado) o beneficioso (deseado), impacte en un proceso o proyecto, afectando su desarrollo y resultados.
- s) **Seguridad de la Información:** Conjunto de medidas organizativas, normativas y tecnológicas destinadas a garantizar que la información cumpla con los principios de confidencialidad, integridad y disponibilidad.
- t) **Sistema de Información:** Conjunto organizado de elementos que interactúan entre sí para tratar los datos y la información (incluyendo procesos manuales y automáticos). Estos elementos son de 4 tipos: personas, datos, actividades o técnicas de trabajo y recursos materiales en general (típicamente recursos informáticos y de comunicación, aunque no tienen por qué ser de este tipo obligatoriamente).
- u) **Tethering:** Función que permite compartir la conexión de datos móviles de un teléfono (3G/4G/5G) con otros dispositivos
- v) **Vulnerabilidad:** Debilidad o falla en un activo, sistema o proceso que puede ser utilizada para comprometer la seguridad, afectando la confidencialidad, integridad o disponibilidad de la información.
- w) **Emergencia:** Situación de peligro o desastre que requiere una acción inmediata.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 14 / 49

- x) **Crisis:** Situación con alto nivel de incertidumbre que interrumpe las actividades principales de la Institución y/o credibilidad y requiere acción urgente.
- y) **Activación:** Hacer que se ponga en funcionamiento un mecanismo, por ejemplo, un plan, proceso o procedimiento.
- z) **Recuperación ante Desastres:** Procedimientos técnicos para restaurar sistemas TIC tras un evento disruptivo.
- aa) **Continuidad del Negocio:** Conjunto de procedimientos y estrategias para mantener las operaciones críticas durante y después de una interrupción.

5. ALCANCE

El presente Plan de Continuidad Operativa de los Servicios Informáticos de la UNE cubre los siguientes ámbitos:

Dimensión	Descripción del Alcance
Geográfico	Campus principal de La Universidad Nacional de Educación "Enrique Guzmán y Valle" ubicado en el distrito de Lurigancho-Chosica; el data center (02 servidores físicos localmente virtualizados) y el servicio contratado en nube.
Organizacional	Todas las unidades académicas, administrativas y de servicios de la universidad que dependen de servicios TIC, incluidas las sedes del Rímac y La Molina.
Tecnológico	Infraestructura de servidores, redes LAN/WAN, sistemas de información críticos, almacenamiento de datos, comunicaciones y servicios en la nube
Temporal	Plan diseñado para 12 meses de implementación con revisión anual y actualización cada 24 meses o ante cambios significativos



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 15 / 49

Dimensión	Descripción del Alcance
Normativo	ISO 22301:2019, ISO/IEC 27001:2022, ISO/IEC 27031:2011, ISO/IEC 27017:2015.

6. EXCLUSIONES

- Planes de seguridad física de las instalaciones (responsabilidad de la oficina de seguridad institucional)
- Gestión del Riesgo del Estado de la Infraestructura física
- Continuidad de actividades de investigación que no dependan de sistemas administrados por la OTI centrales.
- Sistemas de terceros no administrados por la OTI que operen de manera independiente.
- Gestión de seguros externos y aspectos financieros de recuperación que tenga contratado la UNE.

7. EVALUACIÓN Y GESTIÓN DE RIESGOS

7.1. Metodología de Evaluación de Riesgos

La evaluación de riesgos se realizó siguiendo el proceso establecido en la ISO/IEC 27001:2022 (cláusulas 6.1 y 8.2) y en el Anexo A de la misma norma, complementado con las directrices específicas para TIC de la ISO/IEC 27031:2011. Se utilizó la metodología MAGERIT, adaptada al contexto universitario, para identificar las amenazas, vulnerabilidades e impactos de cada activo crítico de TIC.

La probabilidad se evalúa en una escala del 1 al 5 (1=Raro, 5=Casi cierto) y el impacto, también, en una escala del 1 al 5 (1=Insignificante, 5=Catastrófico). El nivel de riesgo resulta del producto: riesgo = probabilidad x impacto.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 16 / 49

7.2. Matriz de Riesgos Identificados

Amenaza / Riesgo Identificado	Probabilidad (1-5)	Impacto (1-5)	Nivel de Riesgo
Ataque de ransomware a sistemas institucionales	4	5	ALTO
Falla de conectividad a internet (ISP)	4	4	ALTO
Sismo de gran magnitud con daño a data center	3	5	ALTO
Huaico o inundación (riesgo local Chosica)	4	4	ALTO
Falla crítica de servidores locales	3	5	ALTO
Corte prolongado de energía eléctrica (> 8 horas)	3	4	ALTO
Incendio en el data center o sala de servidores	2	5	MEDIO
Phishing y robo de credenciales de usuarios	5	3	MEDIO
Falla de almacenamiento y pérdida de datos	3	4	MEDIO



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 17 / 49

Amenaza / Riesgo Identificado	Probabilidad (1-5)	Impacto (1-5)	Nivel de Riesgo
Sabotaje interno por personal no autorizado o autorizado	2	4	MEDIO
Falla de sistema de backups (copias de seguridad incompletas)	3	4	MEDIO
Indisponibilidad de proveedor de NUBE	2	4	MEDIO
Vulnerabilidad en software no actualizado	4	3	MEDIO
Falla de equipos de red (switches/routers)	3	3	BAJO
Error humano en administración de sistemas	4	3	BAJO

7.3. Controles de Mitigación Propuestos

Riesgo	Control de mitigación	Norma Referencia	Prioridad
Ransomware / Ataque Cibernético	Segmentación de red, backups inmutables, EDR/XDR en endpoints, actualizaciones automáticas. Compra de nuevos servidores, para upgrade de sistemas desfasados sin soporte por el fabricante (Al comprar los nuevos servidores se puede tener a los	ISO 27001 A.8	Alta



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 18 / 49

	servidores antiguos como servidores de backup.)		
Sismo / Huaico	Sitio alternativo de recuperación en Lima (para huaicos) y sitios alternos de replicación de servidores en otro departamento del Perú (para sismos de gran magnitud) copia de seguridad offsite diarios, infraestructura antisísmica.	ISO 27031 Sec.7.4	Alta
Falla servidores	Virtualización con alta disponibilidad (HA), clustering de servidores críticos	ISO 27031 Sec.7.3	Alta
Corte energía	UPS de alta capacidad, grupo electrógeno, acuerdo con empresa distribuidora.	ISO 22301 Sec.8.4	Alta
Falla Internet	Contratar segundo ISP como enlace redundante de copia de seguridad, u otra empresa que brinde el servicio de Internet como respaldo.	ISO 27031 Sec.7.2	Alta
Phishing/Robo credenciales	Autenticación multifactor (MFA), capacitación usuarios, filtro de correo antispam/antiphishing	ISO 27001 A.6	Media

8. ANÁLISIS DE IMPACTO AL NEGOCIO (BIA)

8.1. Metodología del BIA

El análisis de impacto al negocio (business impact analysis) se realizó mediante entrevistas estructuradas con directivos y personal clave de cada unidad funcional de la universidad, complementadas con revisión de documentación de procesos existentes, análisis de registros de incidentes tecnológicos previos, y talleres de trabajo con el equipo de la OTI.

Se evaluaron los impactos en cuatro dimensiones: académica, administrativa, reputacional y económica, utilizando una escala de 1 (mínimo) a 5 (catastrófico).

8.2. Parámetros Críticos de Recuperación

Sistema / Servicio	Descripción	RTO (horas)	RPO (horas)	Nivel Criticidad
Red e Internet	Conectividad LAN/WAN y acceso a internet en campus	4	N/A	CRÍTICO



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 19 / 49

SIGEAC	Sistema integrado de gestión universitaria (matrícula, notas, horarios)	8	12	CRÍTICO
INTRANET	Plataforma de módulos de web intranet para estudiantes y administrativos	8	12	CRÍTICO
ADMISIÓN	Sistema de admisión	8	12	CRÍTICO
Correo Institucional	Google para comunicaciones oficiales	2	4	CRÍTICO
Active Directory (AD)	Directorio activo y file server (carpetas compartidas)	4	8	CRÍTICO
Campus Virtual	Plataforma moodle para educación a distancia e híbrida	8	12	CRÍTICO
Sistemas Nóminas	Gestión de planillas y pagos al personal docente y administrativo	4	8	CRÍTICO
Portal Web Inst.	Sitio web institucional y portales de información pública	8	12	ALTO
SIGA	Sistema integrado de gestión administrativo	12	8	ALTO
Trámite Documentario	Sistema de gestión documentaria y expedientes electrónicos	12	8	ALTO
Sistema SIAF	Sistema SIAF para registros, gestión y control de procesos administrativos	12	8	ALTO
Sistema de Backup	Administración, control y monitoreo de los Backups	24	12	MEDIO
Sistema de Biblioteca KOHA	Gestión integral de forma digital de repositorios y acceso a información académica de investigación.	48	24	MEDIO



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 20 / 49

Sistema de Mesa de Partes	Registro, recepción y seguimiento de documentos digitales	48	8	MEDIO
Sistemas CCTV	Videovigilancia del campus universitario	48	N/A	MEDIO

Nota:

N/A = No aplica (servicio sin datos almacenados propios).

8.3. Clasificación de Servicios

Nivel de criticidad	Ventana Máxima de Interrupción	Servicios Incluidos
CRÍTICO (Nivel 1)	0 - 8 horas	Red e internet, SIGEAC, INTRANET, ADMISIÓN, correo institucional, AD y campus virtual, sistema de nóminas.
ALTO (Nivel 2)	8 - 24 horas	Portal web, SIGA, trámite documentario y sistema SIAF,
MEDIO (Nivel 3)	24 - 72 horas	Sistema de backup, sistema de biblioteca KOHA, mesa de partes y sistemas CCTV.
BAJO (Nivel 4)	72 horas - 7 días	Sistemas de soporte, impresión centralizada, aplicaciones secundarias, etc.

8.4. Dependencias Críticas Identificadas

- El BIA identificó las siguientes dependencias críticas que deben ser consideradas en las acciones técnicas operativas de recuperación:
- Red e internet depende de la conectividad, estabilidad y disponibilidad del servicio del proveedor.
- EL SIGEAC depende del servidor de base de datos Oracle y del servidor local de aplicaciones en la red interna.
- La intranet depende de la disponibilidad del proveedor de nube y de la conectividad a internet.
- Admisión depende de la disponibilidad del proveedor de nube y de la conectividad a internet.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 21 / 49

- Los servicios en la nube de correos (Google WorkSpace) dependen de la disponibilidad del proveedor y de la conectividad a internet.
- Los equipos de cómputo que estén dentro del AD dependen del Active Directory / LDAP para autenticación de usuarios que está configurado en el servidor local.
- El campus virtual (moodle) depende del servicio de internet y la disponibilidad del proveedor en nube para acceso externo y del servidor de almacenamiento para contenidos.
- El sistema de nóminas y planillas depende del servidor de base de datos Oracle y del servidor de aplicaciones en la red interna
- El portal web depende del servicio de internet y la disponibilidad del proveedor en nube para acceso externo y del servidor de almacenamiento para contenidos.

9. CONTINUIDAD DEL NEGOCIO

9.1. Principios de la Continuidad del Negocio Universitario

La planificación de la continuidad del negocio de la Universidad Nacional de Educación Enrique Guzmán y Valle tiene como objetivo garantizar que los procesos críticos institucionales puedan continuar operando durante una emergencia, aunque sea en modo degradado o con procedimientos alternativos. Este plan va más allá de la recuperación tecnológica para abordar la continuidad de los procesos académicos, administrativos y de gobierno institucional.

9.2. Procesos Críticos del Negocio y sus Requerimientos

Proceso Crítico	Área Responsable	Dependencia TI	Alternativa Manual/Digital
Matrícula y registro académico	Secretaría General	SIGEAC-UNE (crítico)	Formularios físicos, registro centralizado temporal
Desarrollo de clases presenciales	Vicerrectorado Académico	Campus Virtual (alto)	Clases 100% presenciales, materiales impresos



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 22 / 49

Proceso Crítico	Área Responsable	Dependencia TI	Alternativa Manual/Digital
Clases a distancia / híbridas	Vicerrectorado Académico	Campus Virtual + Internet (crítico)	Reubicación a otra plataforma (Teams, Zoom u otros)
Evaluaciones y calificaciones	Facultades	SIGA-UNE (crítico)	Actas físicas y digitalización posterior
Pago de haberes al personal	RRHH / Finanzas	Sistema Nóminas (crítico)	Proceso manual con planillas impresas previas
Trámite documentario	Secretaría General	SIGA Trámites (crítico)	Trámite físico con numeración manual
Comunicaciones institucionales	Rectorado / OTI	Correo + Web (crítico)	SMS institucional, redes sociales y comunicados físicos
Investigación y posgrado	Vicerrectorado Investigación	Repositorio + Internet (MEDIO)	Acceso offline a bases de datos locales

9.3. Procedimientos de Operación en Modo Emergencia

BCP-01: Continuidad Académica ante Falla del Campus Virtual

Activación: el sistema Moodle está inoperable desde hace más de 4 horas.

- ✓ Notificar a decanos y coordinadores académicos vía correo electrónico o whatsapp institucional.
- ✓ Activar cuenta institucional de Google Workspace For Education (ClassRoom) como plataforma alternativa de emergencia.
- ✓ Publicar en portal web y redes sociales institucionales la plataforma alterna y credenciales.
- ✓ Habilitar repositorio de materiales de emergencia en OneDrive de Google Workspace For Education.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 23 / 49

- ✓ Docentes migran sus materiales de urgencia al OneDrive asignado como repositorio de materiales para las siguientes 48 horas.
- ✓ Mantener registro de asistencia y actividades en formato alternativo para posterior migración.
- ✓ Comunicar cronograma de restauración de Moodle cada 4 horas a la comunidad universitaria.

BCP-02: Continuidad Administrativa ante Falla del SIGA-UNE

Activación: SIGEAC-UNE inoperable por más de 4 horas durante el periodo de matrícula o de evaluaciones.

- ✓ Activar el protocolo de registro manual con formularios preimpresos (mantener stock de 2000 unidades aproximadamente).
- ✓ Asignar personal adicional de las áreas afectadas a la atención presencial.
- ✓ Activar el último reporte impreso del estado de matrículas para consulta.
- ✓ Registrar todas las transacciones en bitácoras físicas para posterior conciliación digital.
- ✓ El área de OTI informa cada 2 horas el estado de restauración del SIGEAC-UNE
- ✓ Al restablecer el SIGEAC-UNE, ingresar todos los registros manuales dentro de las siguientes 24 horas.

BCP-03: Continuidad ante Falla de Comunicaciones

Activación: caída del correo institucional y/o del portal web durante más de 2 horas.

- ✓ Activar el grupo de WhatsApp de emergencias institucionales (Rectoría - Vicerrectorías - Decanos).
- ✓ Publicar avisos físicos en las principales instalaciones del campus.
- ✓ Usar líneas telefónicas directas de las oficinas como medio de comunicación oficial.
- ✓ Activar cuentas de redes sociales institucionales (Facebook, Twitter/X, Instagram u otras) para comunicados.
- ✓ Usar el sistema de SMS masivo de emergencias para mensajes críticos (contratar servicio).



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 24 / 49

9.4. Roles de Continuidad por Proceso

Proceso	Coordinador BCP	Suplente	Recursos Mínimos
Continuidad Académica	Vicerrector Académico	Director de Estudios	Laptops, acceso teams y materiales impresos
Continuidad Administrativa	Director Administrativo	Jefe de Sistemas	Formularios físicos, sellos y archivos impresos
Continuidad TIC	Jefe de OTI	Coordinador de Redes/Sistemas	Kits de emergencia TIC y acceso a backups
Comunicaciones	Director de Comunicaciones	Asistente de Com.	Megáfonos, whatsapp y redes sociales
Financiero/RRHH	Director de RRHH	Contador Principal	Nóminas impresas y acceso al banco

9.5. Proveedores Críticos y Contratos de Soporte

Se deben establecer contratos de soporte prioritario (SLA) con los siguientes proveedores críticos:

- Proveedor principal de internet: SLA de 4 horas para restauración, contacto 24/7.
- Proveedor ISP de respaldo: Activación en menos de 30 minutos.
- Proveedor de data center alternativo: Acceso garantizado en 4 horas.
- Proveedor de UPS y grupo electrógeno: Soporte técnico 24/7 con repuestos en almacén.
- Proveedor de la plataforma SIGEAC -UNE: SLA crítico con soporte en menos de 2 horas.
- Google Workspace For Education: Soporte premium con SLA de disponibilidad del 99.9%
- Proveedor de soluciones de backup: soporte técnico con respuesta de 4 horas.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 25 / 49

10. ESTRATEGIA DE CONTINUIDAD Y RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS

10.1. Principios de la Estrategia

La estrategia de continuidad y recuperación de la Universidad Nacional de Educación se sustenta en los siguientes principios fundamentales derivados de la ISO 22301:2019 y la ISO/IEC 27031:2011:

- Resiliencia proactiva: Implementar medidas preventivas para reducir la probabilidad e impacto de interrupciones
- Redundancia crítica: Duplicar componentes tecnológicos críticos para eliminar puntos únicos de falla.
- Recuperabilidad: Asegurar que todos los sistemas críticos puedan ser restaurados dentro del RTO/RPO definido.
- Mejora continua: Revisar, probar y mejorar el plan periódicamente.
- Continuidad de operaciones: Mantener servicios mínimos esenciales durante una contingencia mediante alternativas manuales o digitales.

10.2. Arquitectura de Alta Disponibilidad Propuesta

La estrategia tecnológica contempla tres niveles de resiliencia:

Nivel 1: Alta Disponibilidad Local (Campus Principal)

- Virtualización de servidores con Proxmox VE en cluster de mínimo 3 nodos.
- Storage Area Network (SAN) con RAID 6 y replicación local.
- Switches de red en configuración redundante (Stacking o VSS).
- Dos enlaces de internet de diferentes ISP con failover automático.
- UPS de doble conversión (online) para toda la sala de servidores.
- Grupo electrógeno con autonomía de 16 horas aprox. (combustible).
- Sistema de detección y extinción de incendios (FM-200 o similar).
- Control de acceso biométrico a sala de servidores.

Nota: La arquitectura descrita representa el estado objetivo tras la migración. Los procedimientos operativos actuales basados en la plataforma VMware se mantendrán vigentes y se actualizarán formalmente en este plan inmediatamente después de completada la migración a Proxmox.

Nivel 2: Sitio Alterno de Recuperación (Lima Metropolitana)

- Contratación de espacio en data center certificado Tier III en Lima (ej. Entel, Telefónica, Americatel) o sobre Cloud AWS/Azure.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 26 / 49

- Replicación asincrónica de datos críticos (SIGEAC, INTRANET, admisión, correos de google Workspace, Campus Virtual, BD Moodle, sistema de nóminas, AD) con RPO de 1-4 horas.
- Equipamiento preconfigurado para activación en menos de 4 horas (Warm Site).
- VPN dedicada entre campus principal y sitio alterno.
- Pruebas semestrales de failover al sitio alterno.

Nivel 3: Nube Pública (Servicios Cloud)

- Suite de Google para correo, colaboración y almacenamiento de documentos (ya contratado).
- Copia de seguridad adicional en la nube usando servicios como Azure Backup o AWS S3 Glacier.
- Campus virtual (moodle) con opción de despliegue en cloud como contingencia.
- Cumplimiento de ISO/IEC 27017:2015 en todos los contratos con proveedores cloud (nube).

10.3.Estrategia de Respaldo y Recuperación de Datos



Sistema	Tipo de Backup	Frecuencia	Retención	Destino
SIGEAC-UNE (BD Oracle)	Completo + Incremental	Completo diario / Incremental c/24 horas	1 año	Local + Offsite + Cloud
INTRANET	Completo + Incremental	Completo diario / Incremental c/24 horas	1 año	Local + Offsite + Cloud
Admisión	Completo + Incremental	Completo diario / Incremental c/24 horas	1 año	Local + Offsite + Cloud
Campus Virtual	Completo + Incremental	Completo diario / Incremental c/12 horas	180 días	Local + Offsite





 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 27 / 49

Sistema	Tipo de Backup	Frecuencia	Retención	Destino
Correo Institucional	Continuo (Google)	Continuo	1 año (Google)	Cloud Google
Active Directory (AD) y File Server	Completo + Incremental	Completo diario / Incremental c/12 horas	1 año	Local + Offsite + Cloud
Sistemas de nóminas	Completo	Completo diario / Incremental c/24 horas	1 año	Local + Offsite + Cloud
Configuraciones Equipos	Snapshot	Semanal	3 meses	Local + Offsite + Cloud

10.4. Alineación con ISO/IEC 27017 para Servicios Cloud

Para todos los servicios en la nube, se implementarán los siguientes controles adicionales según ISO/IEC 27017:2015:

- CLD.6.3.1: Acuerdo de responsabilidad compartida documentado con cada proveedor Cloud.
- CLD.8.1.5: Eliminación y devolución de activos al terminar contrato con proveedores.
- CLD.9.5.1: Segregación en entornos virtuales del proveedor Cloud.
- CLD.12.1.5: Seguridad operacional del administrador.
- CLD.12.4.5: Seguimiento de los servicios en la nube.
- CLD.13.1.4: Seguridad en redes virtuales en la nube (VPC, NSG, firewalls de aplicación).

11. RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS ANTE DESASTRES

11.1. Definición de Escenarios de Interrupción

Contempla procedimientos específicos para los siguientes escenarios de desastre, priorizados según el análisis de riesgos:

Escenario A: Fallo Total del Data Center Principal



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 28 / 49

- **Causas posibles:** Sismo mayor, incendio, inundación por huaico, falla eléctrica masiva y prolongada.
- **Criterio de activación:** Data center inoperable durante más de 2 horas, sin perspectiva de recuperación rápida.

Escenario B: Ciberataque Crítico (Ransomware/DDoS)

- **Causas posibles:** Infección por ransomware que afecte servidores críticos; ataque DDoS que deshabilite los servicios en línea.
- **Criterio de activación:** Detección de cifrado masivo de archivos o de indisponibilidad total de los servicios debido a un ciberataque.

Escenario C: Falla de Sistema Crítico Específico

- **Causas posibles:** Falla de hardware del servidor, corrupción de la base de datos, error en una actualización crítica.
- **Criterio de activación:** Sistema crítico inoperable durante más de 2 horas, sin solución en curso.

Escenario D: Pérdida de Conectividad Total

- **Causas posibles:** Falla de ambos ISP, daño físico a infraestructura de red, falla de equipos core de red.
- **Criterio de activación:** Pérdida total de internet y/o red interna por más de 30 minutos.

11.2. Procedimiento de Activación para Recuperación de los servicios Informáticos ante Desastres

La activación sigue el siguiente flujo de decisión:

- DETECCIÓN:** El equipo de monitoreo (NOC/SOC) por parte del proveedor, detecta un evento de interrupción a través del sistema de monitoreo del servicio de seguridad gestionada.
- NOTIFICACION INICIAL:** El especialista a cargo notifica al coordinador de TI dentro de los primeros 15 minutos de detectado el evento.
- EVALUACIÓN:** El Coordinador evalúa el incidente siguiendo la matriz de clasificación (ver cuadro 10.3)
- DECISIÓN DE ACTIVACIÓN:** El jefe de la Oficina de Tecnología de la Información, en coordinación con el Director General de Administración, deciden la activación dentro de los primeros 30 minutos.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 29 / 49

- e) **NOTIFICACIÓN AL COMITÉ:** Se convoca al comité de crisis siguiendo el árbol de llamadas establecido (ver Anexo A)
- f) **ACTIVACIÓN FORMAL:** El Rector o su delegado emite la declaración formal de emergencia tecnológica.
- g) **EJECUCIÓN DEL PLAN:** Se ejecutan los procedimientos específicos según el escenario identificado

11.3. Matriz de Clasificación de Incidentes

Nivel	Descripción	Criterio	Tiempo	Escalamiento
P1 - CRÍTICO	Servicio o sistema crítico completamente inoperable	RTO amenazado en < 2h	15 min	Jefe OTI + Comité de crisis
P2 - ALTO	Servicio crítico degradado o sistema no crítico caído	Impacto en > 50% usuarios	1 hora	Jefe OTI
P3 - MEDIO	Impacto parcial, workaround disponible	Impacto en < 50% usuarios	4 horas	Coordinador OTI
P4 - BAJO	Incidente menor sin impacto significativo	Usuarios individuales afectados	8 horas	Técnico OTI

11.4. Procedimientos Específicos de Recuperación

Procedimiento-01: Recuperación por Escenario A (Fallo Total Data Center)

T+0h: Confirmar inoperatividad del data center y activar Comité de Crisis.

T+0.5h: Notificar a proveedor de sitio alternativo e iniciar transferencia de operaciones.

T+1h: Activar VPN al sitio alternativo y verificar integridad de últimas copias de seguridad.

T+2h: Restaurar Active Directory y DNS en sitio alternativo.

T+3h: Restaurar (los sistemas críticos) usando último backup (RPO 8h) y verificar integridad de datos.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 30 / 49

T+4h: Restaurar servidor de correo / confirmar disponibilidad del proveedor de Google Workspace.

T+6h: Restaurar Campus Virtual (Moodle) y verificar acceso de estudiantes.

T+8h: Comunicar restablecimiento de servicios críticos a la comunidad universitaria.

T+24h: Restaurar sistemas de nivel 2 y 3 progresivamente.

T+72h: Evaluación postincidente y documentación de lecciones aprendidas.

Procedimiento-02: Recuperación por Escenario B (Ciberataque Crítico Ransomware)

T+0h: Aislar inmediatamente los sistemas afectados de la red (segmentar VLAN).

T+0.5h: Activar comité de crisis y notificar al área de seguridad informática.

T+1h: Realizar análisis forense inicial para identificar alcance de la infección.

T+1h: Reportar al Centro Nacional de Seguridad Digital (incidentes@cnsd.gob.pe) y autoridades competentes según normativa.

T+2h: Identificar último backup limpio (pre-infección) y verificar integridad.

T+3h: Preparar ambiente limpio para restauración (VMs nuevas o formateadas).

T+4h: Iniciar restauración desde los backups de respaldo en entorno aislado.

T+6h: Verificar ausencia de malware antes de reconectar a la red.

T+8h: Restablecer servicios críticos de forma progresiva con monitoreo intensivo.

T+24h: Aplicar parches de seguridad y fortalecer controles para evitar reinfección.

T+72h: Informe completo del incidente para rectoría y comité de crisis.

Procedimiento-03: Recuperación por Escenario C (Falla de Sistema Crítico)

T+0h: Confirmar fallo del sistema crítico y activar comité de crisis.

T+0.5h: Notificar a proveedor de sitio alternativo e iniciar transferencia de operaciones.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Mater del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 31 / 49

T+1h: Activar VPN al sitio alternativo y verificar integridad de últimas copias de seguridad.

T+3h: Restaurar (los sistemas críticos) usando último backup (RPO 8h) y verificar integridad de datos.

T+8h: Comunicar restablecimiento del servicio crítico a la comunidad universitaria.

T+72h: Evaluación postincidente y documentación de lecciones aprendidas.

Procedimiento-04: Recuperación por Escenario D (Pérdida de Conectividad Total)

T+0h: Confirmar la inoperatividad simultánea del enlace de internet principal y del enlace de respaldo, verificar que la red local (LAN) y los servicios internos alojados en los servidores locales sigan operativos y activar comité de crisis.

T+0.5h: Generar tickets de soporte de máxima prioridad (Nivel 1 / Crítico) con ambos proveedores de internet (ISP), solicitar el tiempo estimado de reparación (ETR) inicial y habilitar red de contingencia móvil (routers 4G/5G /tethering) exclusiva para la comunicación entre las áreas críticas administrativas y el servidor de los sistemas más críticos.

Nota: El éxito de este paso depende del cumplimiento de la verificación mensual de saldo y cobertura asignada a la USTyR, garantizando que los equipos estén listos para su uso inmediato.

T+1h: Emitir un primer comunicado oficial a la alta dirección y a la comunidad universitaria informando acerca de la indisponibilidad temporal de servicios expuestos hacia el exterior como (campus virtual moodle y/o acceso externo a sistemas académicos) y la desconexión con Google Workspace. Para ello, se utiliza canales alternos (redes sociales gestionadas por datos móviles, grupos de whatsapp o intranet local).

T+2h: Activar enlace de emergencia de contingencia (si el SGSI contempla un router 4G/5G de respaldo para servicios mínimos) para enrutamiento exclusivo de tráfico altamente crítico y monitorear que la infraestructura local (clúster de servidores Dell PowerEdge y entorno de la plataforma de virtualización) mantenga la integridad de sus procesos y respaldos internos sin alteraciones.

Actualmente, estas tareas se ejecutan sobre el entorno VMware existente; este procedimiento técnico será actualizado en la siguiente revisión del plan para reflejar los cambios operativos post-migración al clúster Proxmox.

T+4h: Escalar los tickets de soporte con los ejecutivos de cuenta o gerentes de servicio de ambos proveedores si no hay avances, reevaluar el ETR y



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 32 / 49

preparar un plan de operaciones 100% offline para las áreas administrativas de la universidad.

T+6h: Emitir una segunda actualización de estado a la comunidad universitaria con el nuevo ETR y verificar que las reglas de firewall perimetral estén preparadas para gestionar la reconexión de manera segura.

T+8h / Momento de Restablecimiento: Confirmar el restablecimiento de los enlaces. Además, realizar failback asegurando que el tráfico retorne al proveedor principal y el proveedor de respaldo vuelva a su estado de standby o balanceo.

T+12h: Verificar la correcta sincronización de los servicios locales y sistemas en general.

T+24h: Confirmar el restablecimiento total de todos los servicios al 100% y enviar el comunicado de cierre de incidente a la alta dirección y usuarios.

T+72h: Solicitar a ambos proveedores de internet su informe de análisis de causa raíz, realizar evaluación postincidente, documentar lecciones aprendidas y evaluar penalidades por incumplimiento de SLA para integrarlo en la revisión del SGSI.

11.5. Criterios de Retorno al Sitio Principal

El retorno de operaciones al sitio principal se ejecutará cuando se cumplan todos los siguientes criterios:

- El sitio principal ha sido verificado como estructuralmente seguro por ingenieros certificados.
- La infraestructura tecnológica del sitio principal ha sido restaurada y probada satisfactoriamente.
- Se han resuelto las causas raíz que originaron la activación de la recuperación ante Desastres.
- Los sistemas han sido probados durante un mínimo de 4 horas continuas sin incidentes.
- El comité de crisis ha dado aprobación formal para el retorno.
- Se ha notificado a toda la comunidad universitaria sobre el cronograma de retorno.

El proceso de retorno debe ser gradual: primero, los servicios críticos (Nivel 1); luego, los de nivel 2; y, finalmente, los de nivel 3 y 4.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 33 / 49

12. ESTRUCTURA ORGANIZACIONAL DE RESPUESTA

12.1. Comité de Crisis Institucional

Se establece el comité de crisis institucional como el órgano máximo de decisión durante la activación de recuperación ante desastres/ continuidad del negocio. Su composición es la siguiente:

Rol en el Comité	Cargo Institucional	Responsabilidades Principales
Director del Comité	Rector de la Universidad	Decisión máxima para activar/desactivar el plan. Vocero institucional principal
Director Alterno	Vicerrector Académico	Asume la dirección en ausencia del rector. Coordina continuidad académica
Líder TI	Director de la Oficina de Tecnología de la Información (OTI)	Coordinación técnica de recuperación ante desastres. Liderazgo del equipo de recuperación TI
Líder Administrativo	Director General de Administración (DIGA)	Aprobación para gestión logística de recuperación
Líder de Planeamiento y Presupuesto	Jefe de la Oficina de Planeamiento y Presupuesto (OPP)	Aprobación de presupuesto de emergencia
Líder de Recursos Humanos	Jefe de la Unidad de Recursos Humanos	Aprobación de procesos de Recursos Humanos
Asesor Legal	Jefe de Asesoría Jurídica	Cumplimiento legal y manejo de responsabilidades ante terceros
Líder Seguridad Ocupacional	Jefe de Seguridad Inst.	Seguridad física de instalaciones y personal durante la emergencia
Coordinador de la Unidad Funcional de Transformación Digital	Responsable de la Unidad Funcional de Transformación Digital	Organizar, convocar y documentar las reuniones



El Equipo de Recuperación Tecnológica es el grupo técnico especializado que ejecuta la recuperación ante desastres bajo la coordinación del director de la OTI:

- 

El siguiente esquema define la cadena de comunicación durante una emergencia:

-



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 35 / 49

13. PROCEDIMIENTOS DE PRUEBA Y MANTENIMIENTO

13.1. Programa Anual de Pruebas

Un plan de continuidad que no se prueba con regularidad no es confiable. La ISO 22301:2019 (cláusula 8.5) y la ISO/IEC 27031:2011 (sección 9) requieren que los planes se prueben periódicamente para verificar su efectividad. El programa de pruebas de la Universidad Nacional de Educación Enrique Guzmán y Valle contempla:

Tipo de Prueba	Descripción	Frecuencia	Participantes
Prueba de escritorio (Tabletop)	Simulación teórica de escenarios ante el comité de crisis	Semestral	Comité de Crisis completo
Prueba de recuperación de backups	Restauración completa en ambiente de pruebas de todos los sistemas críticos	Anual	Equipo ERT - Área Backups
Simulacro de falla de servicio	Simulación real de caída de un sistema crítico sin previo aviso	Semestral	ERT + Usuarios clave
Prueba de failover al sitio alternativo	Activación real del sitio alternativo de recuperación	Anual	ERT completo + Comité
Simulacro de ciberincidente	Ejercicio de respuesta ante ransomware o brecha de seguridad	Anual	ERT + Seguridad + Comité
Prueba de comunicaciones de crisis	Activación del árbol de llamadas y canales alternativos	Anual	Comité de Crisis
Verificación de enlaces de contingencia móvil (4G/5G)	Comprobar vigencia de la línea, saldo de datos, nivel de cobertura y configuración perimetral de los routers de emergencia	Mensual	USTyR/ Coordinador de Redes



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 36 / 49

13.2. Proceso de Mejora Continua

Posterior a cada prueba y a cada activación real del plan, se ejecutará el siguiente proceso de mejora continua (ciclo PDCA de ISO 22301:2019):

- **PLAN:** Definir objetivos de la prueba, escenario, participantes y criterios de éxito.
- **DO:** Ejecutar la prueba según el plan establecido documentando todas las acciones y tiempos.
- **CHECK:** Realizar una sesión de retroalimentación (hotwash) inmediatamente después de la prueba y evaluar el desempeño frente a los objetivos. Documentar brechas y áreas de mejora.
- **ACT:** Actualizar el plan, los procedimientos y/o la infraestructura según las lecciones aprendidas y programar prueba de verificación de mejoras.

13.3. Criterios de Actualización del Plan

El presente plan debe ser revisado y actualizado en los siguientes casos:

- Revisión programada: anualmente (cada 12 meses), sin excepción.
- Cambios significativos en la infraestructura TI: incorporación de nuevos sistemas o servidores críticos.
- Finalización del proyecto de migración de virtualización (VMware a Proxmox VE), lo que requerirá la actualización de todos los procedimientos técnicos operativos y capturas de pantalla de respaldo en un plazo no mayor a 30 días tras el cierre del proyecto.
- Cambios organizacionales: cambio de rector, director administrativo o jefe de TIC.
- Postincidente: Dentro de los 30 días posteriores a cualquier activación real de recuperación de servicios informáticos.
- Cambios normativos: Actualización de las normas ISO de referencia o nuevas disposiciones legales.
- Postprueba: Si las pruebas revelan brechas significativas en el plan.

14. INDICADORES Y MÉTRICAS DE DESEMPEÑO



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 37 / 49

14.1. KPIs del Sistema de Gestión de Continuidad

Indicador (KPI)	Formula / Medición	Meta	Frecuencia de medición
Disponibilidad de servicios críticos (Uptime)	Horas disponibles / Total horas x 100	$\geq 99.5\%$ mensual	Mensual / Continuo
Tiempo de recuperación real (RTO real)	Tiempo transcurrido desde el inicio del incidente hasta el restablecimiento del servicio.	$\leq$ RTO definido	Por incidente
Punto de recuperación real (RPO real)	Antigüedad de los datos restaurados en el último incidente	$\leq$ RPO definido	Por incidente
Éxito de pruebas de backup	N° de backups restaurados exitosamente / Total intentos x 100	$\geq 98\%$	Anual
Cumplimiento del programa de pruebas	N° de pruebas ejecutadas / N de pruebas programadas x 100	100%	Anual
Incidentes críticos sin DRP activado	N° de incidentes P1 donde RTO fue superado	0 por Semestre	Semestral
Personal capacitado en DRP/BCP	N° de personas capacitadas / Total personas en roles críticos x 100	$\geq 100\%$	Anual
Tiempo medio de detección (MTTD)	Tiempo promedio entre inicio del incidente y su detección	≤ 15 min	Por incidente

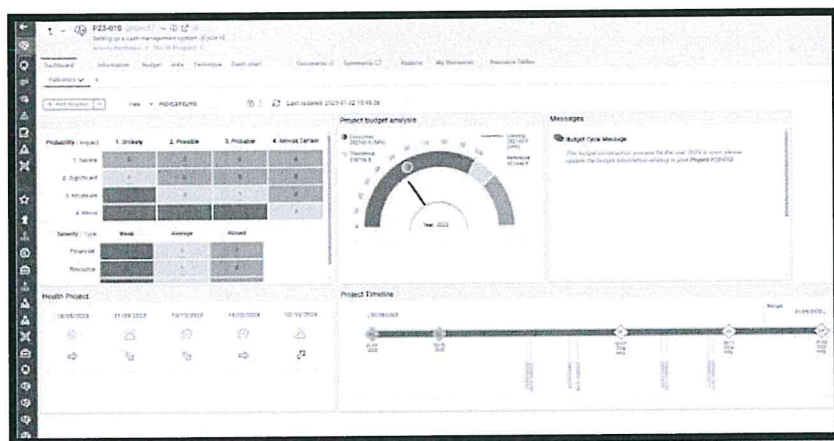


 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 38 / 49

14.2. Reporte Periódico al Comité de Crisis

La OTI presentará al comité de crisis un informe semestral de continuidad que incluya:

- ✓ Dashboard de disponibilidad de todos los servicios críticos.



- ✓ Estado de ejecución del programa de pruebas y backups.
- ✓ Resumen de incidentes ocurridos, tiempos de respuesta y recovery.
- ✓ Estado de implementación de controles y mejoras identificadas en periodos anteriores.
- ✓ Estado de cumplimiento del cronograma de implementación del plan (Gantt).
- ✓ Presupuesto ejecutado vs presupuesto asignado para Oficina de Tecnología de la Información (OTI) en base de continuidad del negocio.

15. COMUNICACIONES DE CRISIS

15.1. Principios de Comunicación en Crisis

Durante una crisis o evento de continuidad, la comunicación debe ser: rápida (dentro de los tiempos establecidos), precisa (sin especulaciones ni información no verificada), clara (lenguaje entendible para todos los públicos), consistente (un solo mensaje oficial emitido por un portavoz designado) y empática (considerando el impacto en la comunidad universitaria).

15.2. Públicos y Mensajes Clave



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 39 / 49

Público Objetivo	Canal Principal	Canal Alternativo	Tiempo Máximo
Autoridades (Rector, VR)	Llamada directa	WhatsApp institucional	30 minutos
Directores y Decanos	Correo + WhatsApp grupo	Llamada telefónica	1 hora
Docentes	Correo institucional	Portal web + redes sociales	2 horas
Estudiantes	Portal web + redes sociales	SMS masivo	2 horas
Personal administrativo	Comunicado interno	Megáfono en campus	2 horas
Medios de comunicación	Comunicado oficial de prensa	Conferencia de prensa	4 horas
MINEDU / SUNEDU	Oficio formal + correo	Llamada directa	8 horas
Proveedores críticos	Correo + llamada	Contacto de emergencia	1 hora

15.3. Plantillas de Comunicación de Crisis

Plantilla 1: Notificación Inicial de Incidente (para comunidad universitaria)

ASUNTO: [EMERGENCIA TI] Interrupción de [nombre del servicio] - Universidad Nacional de Educación "Enrique Guzmán y Valle"

Estimada Comunidad Universitaria:



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 40 / 49

La Oficina de Tecnologías de la Información comunica que actualmente se presenta una interrupción en el servicio [NOMBRE DEL SERVICIO]. El incidente fue detectado a las [HORA] del [FECHA].

Nuestro equipo técnico está trabajando en la restauración del servicio. El tiempo estimado de restablecimiento es de [TIEMPO ESTIMADO].

Durante este periodo, podrán acceder a los servicios alternativos en: [URL/INSTRUCCIONES ALTERNAS].

Les mantendremos informados con actualizaciones cada [FRECUENCIA].
Lamentamos los inconvenientes ocasionados.

Plantilla 2: Comunicado de restablecimiento de servicio

ASUNTO: [SERVICIO RESTAURADO] [NOMBRE DEL SERVICIO]
restablecido - Universidad Nacional de Educación "Enrique Guzmán y Valle"

Estimada Comunidad Universitaria:

Nos complace informar que el servicio de [NOMBRE DEL SERVICIO] ha sido restablecido satisfactoriamente a las [HORA] del [FECHA].

El servicio está nuevamente disponible en: [URL]. Si experimenta alguna dificultad para acceder, por favor, contacte a la Mesa de Ayuda TI al [TELÉFONO] o [CORREO].

Agradecemos su comprensión y paciencia durante este periodo de contingencia.

16. CRONOGRAMA DE IMPLEMENTACIÓN (12 MESES)

El presente cronograma de implementación se desarrolla en cuatro fases durante 12 meses, siguiendo el ciclo PDCA de la ISO 22301:2019:

Fase 1 - Fundación y Diagnóstico (Meses 1-3)

- Mes 1: Constitución del comité de crisis, designación de responsables, kick-off del proyecto.
- Mes 1-2: Inventario completo de activos TIC y documentación de arquitectura actual.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 41 / 49

- Mes 2: Realización del BIA con entrevistas a todas las áreas críticas.
- Mes 2-3: Evaluación de riesgos completa (ISO 27001 - Cláusula 6.1).
- Mes 3: Diagnóstico del estado actual vs ISO 22301 y elaboración del plan de brechas.
- Mes 3: Aprobación de las actividades para la recuperación ante desastres y la continuidad de negocio por el comité de crisis y rectoría.

Fase 2 - Implementación Tecnológica (Meses 3-7)

- Mes 3-4: Adquisición de UPS de alta capacidad y mejora del grupo electrógeno.
- Mes 4-5: Implementación de virtualización y clúster de alta disponibilidad.
- Mes 4-6: Configuración del sitio alternativo de recuperación en data center externo.
- Mes 5: Implementación de segundo enlace de internet (ISP redundante).
- Mes 5-6: Implementación de sistema de respaldo automatizado con verificación.
- Mes 6-7: Implementación de herramientas de monitoreo 24/7 (por ejemplo, Zabbix/Wazuh).
- Mes 6-7: Implementación de controles de seguridad (MFA, EDR, SIEM básico).

Fase 3 - Documentación, Capacitación y Pruebas (Meses 7-10)

- Mes 7-8: Documentación detallada de todos los procedimientos de la recuperación ante desastres y la continuidad de negocio.
- Mes 8: Primer programa de capacitación para el comité de crisis y el ERT.
- Mes 8-9: Primera prueba de escritorio (Tabletop) con escenarios de desastre.
- Mes 9: Primera prueba real de restauración de backups en ambiente de pruebas.
- Mes 9-10: Primera prueba de failover al sitio alternativo.
- Mes 10: Capacitación a usuarios finales sobre procedimientos alternativos.

Fase 4 - Consolidación y Mejora Continua (Meses 10-12)

- Mes 10-11: Corrección de brechas identificadas en las pruebas.
- Mes 11: Primer simulacro completo de ciberincidente.
- Mes 11: Auditoría interna del sistema de gestión de continuidad.
- Mes 12: Revisión y actualización del plan basada en los resultados del año.



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 42 / 49

- Mes 12: Presentación del informe anual de continuidad al Comité de Crisis y Rectoría.
- Mes 12: Planificación del ciclo de mejora del siguiente periodo.

NOTA: La implementación eficiente de la fase requiere la adquisición de los nuevos servidores, servicio de migración de VMware a PROXMOX, upgrade de licencia Oracle 19C (evaluación) y el grupo electrógeno (fuente de energía).

Por tal motivo, la fase 2 que corresponde a implementación tecnológica, considera los siguientes puntos que serán ejecutados temporalmente:

- Mes 4-5: Implementación de virtualización y clúster de alta disponibilidad.
- Mes 4-6: Configuración del sitio alternativo de recuperación en data center externo.

En caso se logre realizar la adquisición, estos 2 puntos serán reemplazados por el traslado de los backups físicos a otra sede u oficinas que estén fuera de la sede central de la UNE para que estén resguardados, ante cualquier incidente.

17. PRESUPUESTO

De acuerdo con el anexo B-5 del Plan Operativo Institucional de la Unidad de Soporte Técnico y Redes, hay dos actividades operativas que se relacionan con los objetivos del presente plan:

- Atención de servicio, que cuenta con presupuesto de S/ 1,205,720.00.
- Implementación de la Gestión de la Contingencia ante Desastres Informáticos, cuyo presupuesto es S/ 30,083.34.

Los costos relacionados con la implementación del plan serán cubiertos por el presupuesto disponible que asciende a S/ 1,235,803.34.

17.1. Presupuesto Estimado para la Implementación (Primer Año)

Los siguientes son costos referenciales para la implementación de las actividades del plan de continuidad operativa de los servicios informáticos en la UNE. Los valores deben ser validados con cotizaciones reales en el contexto del mercado peruano de TI:

Rubro de Inversión	Tipo de Gasto	Costo Est. (S/)	Prioridad
Storage SAN/NAS de alta capacidad	Compra	80,000	Alta



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 43 / 49

Rubro de Inversión	Tipo de Gasto	Costo Est. (S/)	Prioridad
UPS de doble conversión (sala servidores) con mayor autonomía que se tiene actualmente.	Compra	120,000	Alta
Sitio alternativo (data center externo, anual)	Servicio	50,000	Alta
Software de backup y replicación (licencias Veeam backup)	Mantener Renovación	30,000	Alta
Consultoría e implementación (servicios)	Servicio	120,000	Media
TOTAL, ESTIMADO		S/ 400,000	

Nota: Los montos son referenciales y deben ser validados con procesos de licitación según la Ley General de Contrataciones Públicas (Ley N.º 32069). La fuente de financiamiento puede ser el presupuesto ordinario, los recursos recaudados directamente o la gestión de proyectos de inversión pública (SNIP/INVIERTE.PE).

18. FACTORES CRÍTICOS DE ÉXITO

1. Compromiso de alta dirección
2. Inventario TI actualizado
3. Políticas formales de backup
4. Presupuesto asignado
5. Integración con el SGSI
6. Pruebas periódicas reales
7. Gestión de proveedores tecnológicos

19. ANEXOS

- ✓ Anexo A: Formato de Registro de Incidentes
- ✓ Anexo B: Cronograma de Actividades de Implementación de la Continuidad Operativa de OTI
- ✓ Anexo C: Entregables del Plan de Continuidad Operativa OTI



Código: PLA-OTI-002

PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS

Página 44 / 49

Anexo A: Formato de Registro de Incidentes

[illegible]

 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE Alma Máter del Magisterio Nacional	Código: PLA-OTI-002	
	VERSIÓN: 1.0	
	Página 45 / 49	

Anexo B: Cronograma de Actividades de Implementación de la Continuidad Operativa de OTI

UNIVERSIDAD NACIONAL DE EDUCACION ENRIQUE GUZMAN Y VALLE															
Plan de Continuidad Operativa de los Servicios Informáticos - CRONOGRAMA DE IMPLEMENTACION 12 MESES Alineado a ISO 22301 · ISO/IEC 27001 · ISO/IEC 27031 · ISO/IEC 27017															
N°	ACTIVIDAD / ENTREGABLE	RESPONSABLE	PRIORIDAD	Mes 1 Ene-Feb	Mes 2 Feb-Mar	Mes 3 Mar-Abr	Mes 4 Abr-May	Mes 5 May-Jun	Mes 6 Jun-Jul	Mes 7 Jul-Ago	Mes 8 Ago-Sep	Mes 9 Sep-Oct	Mes 10 Oct-Nov	Mes 11 Nov-Dic	Mes 12 Dic-Ene
FASE 1: FUNDACION, DIAGNOSTICO Y PLANIFICACION															
1	Constitución formal del Comité de Crisis Institucional	Rector / Administración	Alta	■											
2	Designación del Equipo de Recuperación Tecnológica (ERT)	Director OTI	Alta	■											
3	Sesión de kick-off del proyecto DRP/BCP con autoridades	Director OTI + Rector	Alta	■											
4	Inventario completo de activos TIC (ISO 27001 - A.8.1)	OTI	Alta	■	■										
5	Documentación de arquitectura de red y sistemas actuales	Coordinador Redes	Alta	■	■										
6	Realización del BIA - Entrevistas con áreas críticas	Director OTI + Consultor	Alta		■										
7	Análisis y documentación del BIA (RTO/RPO por sistema)	Director OTI	Alta		■										
8	Evaluación de riesgos TIC (metodología MAGERT/ISO 27001)	OTI + Seguridad	Alta		■	■									
9	Diagnostico GAP vs ISO 22301, 27001, 27031, 27017	Consultor externo	Alta			■	■								
10	Elaboración del Plan de Tratamiento de Riesgos	Director OTI	Alta			■	■								
11	Aprobación formal del Plan DRP/BCP por Rectoría	Rector	Alta			■	■								



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	
	Código: PLA-OTI-002	
	VERSIÓN: 1.0	Página 46 / 49

UNIVERSIDAD NACIONAL DE EDUCACION ENRIQUE GUZMAN Y VALLE															
Plan de Continuidad Operativa de los Servicios Informáticos - CRONOGRAMA DE IMPLEMENTACION 12 MESES Alineado a ISO 22301 · ISO/IEC 27001 · ISO/IEC 27031 · ISO/IEC 27017															
N°	ACTIVIDAD / ENTREGABLE	RESPONSABLE	PRIORIDAD	Mes 1 Ene-Feb	Mes 2 Feb-Mar	Mes 3 Mar-Abr	Mes 4 Abr-May	Mes 5 May-Jun	Mes 6 Jun-Jul	Mes 7 Jul-Ago	Mes 8 Ago-Sep	Mes 9 Sep-Oct	Mes 10 Oct-Nov	Mes 11 Nov-Dic	Mes 12 Dic-Ene
FASE 1: FUNDACION, DIAGNOSTICO Y PLANIFICACION															
FASE 2: IMPLEMENTACION TECNOLÓGICA E INFRAESTRUCTURA															
12	Adquisición UPS doble conversión y mejora grupo electrógeno	Dir. Admvo. / OTI	Alta												
13	Implementación cluster virtualización HA (VMware/Proxmox)	Adm. Servidores	Alta												
14	Migración de servidores críticos a entorno virtualizado	Adm. Servidores	Alta												
15	Contratación y configuración del sitio alternativo (DR Site)	Jefe OTI	Alta												
16	Configuración de replicación de datos al sitio alternativo	Adm. BD / Jefe de Desarrollo y Sistemas	Alta												
17	Contratación del segundo enlace ISP (redundancia internet)	Director OTI	Alta												
18	Configuración de failover automático de enlace ISP	Coord. Redes	Alta												
19	Implementación de sistema de backup automatizado	Coord. Backups	Alta												
20	Configuración de respaldo en cloud (Azure/AWS)	OTI	Alta												
21	Implementación de herramientas de monitoreo 24/7 (Zabbix)	OTI	Media												
22	Implementación MFA para sistemas críticos (ISO 27001)	Seguridad / OTI	Alta												
23	Implementación EDR/XDR en endpoints críticos	Proveedor de Seguridad Informática	Alta												
24	Segmentación de red y VLANs de seguridad (ISO 27001 A.13)	Coord. Redes	Alta												



[illegible]

 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 48 / 49

UNIVERSIDAD NACIONAL DE EDUCACION ENRIQUE GUZMAN Y VALLE															
Plan de Continuidad Operativa de los Servicios Informáticos - CRONOGRAMA DE IMPLEMENTACION 12 MESES Alineado a ISO 22301 - ISO/IEC 27001 - ISO/IEC 27031 - ISO/IEC 27017															
N°	ACTIVIDAD / ENTREGABLE	RESPONSABLE	PRIORIDAD	Mes 1 Ene-Feb	Mes 2 Feb-Mar	Mes 3 Mar-Abr	Mes 4 Abr-May	Mes 5 May-Jun	Mes 6 Jun-Jul	Mes 7 Jul-Ago	Mes 8 Ago-Sep	Mes 9 Sep-Oct	Mes 10 Oct-Nov	Mes 11 Nov-Dic	Mes 12 Dic-Ene
FASE 4: CONSOLIDACION, MEJORA CONTINUA Y AUDITORIA															
37	Implementación de mejoras pospruebas (brechas identificadas)	ERT / OTI	Alta												
38	Primer simulacro completo de ciber incidente (ransomware)	ERT + Seguridad + Comité	Alta												
39	Prueba de comunicaciones internas y externas de crisis	Comité de Crisis	Media												
40	Auditoría interna del SGCN (ISO 22301 - Clausula 9.2)	Auditor Interno/Externo	Alta												
41	Revisión gerencial del SGCN (ISO 22301 - Clausula 9.3)	Rector + Comité	Alta												
42	Actualización del plan basada en resultados del año	Director OTI	Alta												
43	Informe anual de continuidad presentado a Rectoría	Director OTI	Media												
44	Planificación del ciclo de mejora - Año 2 (Certificación ISO)	Director OTI + Rector	Media												



 UNIVERSIDAD NACIONAL DE EDUCACIÓN ENRIQUE GUZMÁN Y VALLE <i>Alma Máter del Magisterio Nacional</i>	PLAN DE CONTINUIDAD OPERATIVA DE LOS SERVICIOS INFORMÁTICOS	Código: PLA-OTI-002
		VERSIÓN: 1.0
		Página 49 / 49

Anexo C: Entregables del Plan de Continuidad Operativa OTI

ID	Entregables
1	Acta de constitución del proyecto Política de continuidad TIC Estructura de gobierno y roles (RACI) Cronograma aprobado
2	Informe BIA formal Matriz de criticidad de servicios Tabla oficial de RTO y RPO Mapa de dependencias tecnológicas
3	Matriz de riesgos TIC (Excel automatizado) Mapa de calor institucional Informe de riesgos priorizados Plan de tratamiento
4	Documento de estrategia de recuperación Arquitectura objetivo (diagramas) Plan de inversión tecnológica Modelo de sitio alterno
5	Documento PRSI oficial (aprobado por Consejo) Procedimientos técnicos detallados Directorio de contactos críticos Formatos de registro de incidentes
6	Infraestructura configurada Evidencias técnicas Reporte de pruebas técnicas
7	Informe de resultados Planificación de mejoras Actualización del PRSI
8	Planificación anual de pruebas Indicadores KPI Informe anual al Consejo

