UNIVERSIDAD NACIONAL AGRARIA LA MOLINA

PLAN DE GESTIÓN DE LA OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Resolución N.° 0368-2025-R-UNALM

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

Elaborado por:	Revisado por:	Aprobado por:
Ing. Yolanda Cóndor Mori Jefa de la Unidad de Sistema de la Información **Mg. María Teresa Huaita Molero** Coordinadora Oficina de Calidad y Acreditación	**Ing. Geison Arturo Malpartida Zubizarreta** Jefe de la Oficina de Tecnología de la Información y Comunicaciones	**Dr. Américo Guevara Perez** Rector de la UNALM

HOJA DE CONTROL DE CAMBIOS

N°	Texto Modificado	Versión	Fecha	Responsable
1	Creación del documento.	01	31/03/2025	**Ing. Yolanda Cóndor Mori**

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

ÍNDICE

I. INTRODUCCIÓN

La Oficina de Tecnología de Información y Comunicaciones (OTIC) cumple un rol fundamental en la modernización y eficiencia de los procesos institucionales, asegurando el acceso, uso y desarrollo de soluciones tecnológicas alineadas con los objetivos estratégicos de la organización. En un entorno donde la transformación digital es clave para la competitividad y sostenibilidad institucional, la OTIC no solo gestiona la infraestructura y los sistemas de información, sino que también promueve la innovación, la seguridad y la optimización de los recursos tecnológicos.

Este Plan de Gestión establece las directrices, estrategias y acciones necesarias para la gestión eficaz de la OTIC y sus unidades funcionales: la Unidad de Tecnología y Operaciones, responsable del desarrollo, implementación y mantenimiento de plataformas y sistemas; la Unidad de Soporte Tecnológico, encargada de garantizar la operatividad y asistencia a los usuarios; y la Unidad de Sistemas de Información, que vela por la protección de datos, la continuidad operativa y el cumplimiento de normativas en materia de ciberseguridad.

Asimismo, el plan considera la integración de nuevas tecnologías, el fortalecimiento de competencias digitales y el establecimiento de mecanismos de monitoreo y evaluación para asegurar la mejora continua en la gestión de los servicios tecnológicos.

II. ALCANCE

El presente Plan de Gestión abarca las actividades de planificación, desarrollo, operación y mantenimiento de los sistemas de información, infraestructura tecnológica, servicios de soporte y seguridad de la información dentro de la institución. Asimismo, considera la gestión de proyectos de innovación digital, administración de plataformas tecnológicas y garantía de continuidad operativa de los servicios críticos.

III. BASE LEGAL

a. Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
b. Decreto Legislativo N° 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 N° 002-2017-UNALM, Decreto que 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 N° 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley N° 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.
i. Ley N° 27933, Ley de Protección de Datos Personales.
j. Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 27933, Ley de Protección de Datos Personales
k. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
l. Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento de la Ley de Gobierno Digital
m. Directrices de la Autoridad Nacional de Protección de Datos Personales.
n. Estándares internacionales de seguridad de la información: ISO 27001, ISO 27002 y ISO 27032.

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

IV. TÉRMINOS Y DEFINICIONES

4.1. **Ciberseguridad**: Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital.

4.2. **Continuidad Operativa:** Capacidad de la universidad para mantener sus funciones esenciales en caso de fallos tecnológicos, desastres naturales o ataques cibernéticos.

4.3. **Incidente de Seguridad:** Cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información de la UNALM

4.4. **Infraestructura Tecnológica:** Conjunto de recursos, hardware, software y servicios que permiten el funcionamiento de los sistemas informáticos y las comunicaciones de una organización.

4.5. **OTIC**: Oficina de Tecnología de Información y Comunicaciones.

4.6. **Servicios de TIC:** Formas de tecnología que se utilizan para crear, procesar, almacenar, transmitir, compartir, mostrar o intercambiar información.

4.7. **Transformación Digital:** Proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intensivo de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas.

4.8. **UNALM:** Universidad Nacional Agraria La Molina

V. ANÁLISIS SITUACIONAL

Actualmente, la institución enfrenta retos en la gestión de sus recursos tecnológicos, incluyendo la obsolescencia de infraestructura, fragmentación de sistemas de información y brechas en ciberseguridad. La OTIC debe fortalecer su rol estratégico, optimizando la integración de tecnologías y la adopción de herramientas digitales para mejorar la eficiencia y seguridad operativa.

VI. OBJETIVOS

6.1. Objetivo General

Garantizar la gestión eficiente, segura e innovadora de los recursos tecnológicos, contribuyendo a la modernización y optimización de los procesos institucionales.

6.2. Objetivos Específicos

6.2.1. Desarrollar e implementar una infraestructura tecnológica robusta y segura.
6.2.2. Optimizar los servicios de soporte técnico y asistencia tecnológica.
6.2.3. Fortalecer la ciberseguridad y protección de datos institucionales.
6.2.4. Fomentar la transformación digital y la innovación en la institución.
6.2.5. Implementar mecanismos de monitoreo y evaluación continua de los servicios TIC.
6.2.6. Implementar el equipamiento tecnológico para asegurar un mejor control al acceso del personal y vehículos en la universidad.
6.2.7. Fortalecer la seguridad interna del campus de la universidad, unificando la conexión de las cámaras de seguridad para ser monitoreada en el centro de monitoreo.

VII. ESTRATEGIAS

7.1. Acciones estratégicas

7.1.1. Implementación de una arquitectura tecnológica moderna y escalable.
7.1.2. Desarrollo de un plan integral de ciberseguridad.
7.1.3. Fortalecimiento de la capacitación y especialización del personal TIC.
7.1.4. Integración de sistemas de información para la toma de decisiones basada en datos.
7.1.5. Mejorar el control de ingreso y salida del personal y vehículos en la universidad mediante equipamiento tecnológico.
7.1.6. Fortalecer la seguridad de la universidad mediante el monitoreo de las cámaras de seguridad.

7.2. Ruta estratégica

Se establecen etapas progresivas de implementación de tecnologías, evaluación de impacto y ajustes continuos para garantizar la mejora constante de los servicios TIC.

ACCIÓN ESTRATÉGICA	DESCRIPCIÓN	PRIORIDAD	RESPONSABLE
Implementación de una arquitectura tecnológica moderna y escalable.	La transformación digital de la institución requiere una infraestructura tecnológica flexible, segura y preparada para el crecimiento. Esta actividad se centra en la modernización de los entornos tecnológicos mediante la adopción de soluciones en la nube, virtualización, arquitecturas modulares y estándares abiertos que permitan la interoperabilidad y la escalabilidad de los sistemas. Se garantizará un diseño que optimice el rendimiento, la resiliencia y la capacidad de adaptación a nuevas necesidades.	Alta	• Oficina de Tecnología de Información y Comunicaciones. • Dirección General de Administración.
Desarrollo de un plan integral de ciberseguridad.	La creciente digitalización y el incremento de amenazas cibernéticas exigen un enfoque estructurado para la protección de la información y los sistemas institucionales. Este plan establecerá políticas, procedimientos y medidas de seguridad alineadas con estándares internacionales, contemplando la gestión de riesgos, la protección de datos sensibles, la prevención de ataques y la respuesta ante incidentes. También incluirá campañas de concienciación para usuarios y estrategias de cumplimiento normativo.	Crítica	• Oficina de Tecnología de Información y Comunicaciones.
Fortalecimiento de la capacitación y especialización del personal TIC.	La evolución tecnológica exige que el equipo de la OTIC cuente con conocimientos actualizados y especializados en áreas clave como infraestructura digital, ciberseguridad, inteligencia artificial, gestión de datos y desarrollo de software. Se implementará un programa continuo de formación y certificación en tecnologías emergentes, metodologías ágiles y mejores prácticas, promoviendo el aprendizaje colaborativo y la actualización constante.	Alta	• Oficina de Tecnología de Información y Comunicaciones.
Integración de sistemas de información para la toma de decisiones basada en datos.	La dispersión de información en múltiples plataformas dificulta la generación de reportes estratégicos y el análisis de datos en tiempo real. Esta actividad busca consolidar un ecosistema digital integrado que permita la interoperabilidad de los sistemas institucionales, mejorando la accesibilidad, calidad y disponibilidad de los datos. Se implementarán plataformas de analítica avanzada, herramientas de visualización y modelos predictivos que faciliten la toma de decisiones informadas.	Alta	• Oficina de Tecnología de Información y Comunicaciones.
Mejorar el control de ingreso y salida del personal y vehículos en la universidad mediante equipamiento tecnológico	Se implementará el equipamiento tecnológico para mejorar el control de acceso del personal de forma facial y vehicular mediante cámaras que capturan las imágenes de las placas. Se instalarán cámaras internas en los ómnibus para monitorear el traslado del personal y controlar las incidencias. Asimismo, se menciona que la información de las grabaciones de los dispositivos se almacenará en los equipos servidores de la OTIC.	Alta	• Oficina de Tecnología de Información y Comunicaciones.
Fortalecer la seguridad de la universidad mediante el monitoreo de las cámaras de seguridad.	Se realizará la integración de las cámaras de seguridad de la universidad por medio de la fibra óptica, para ser monitoreados por el personal de seguridad. Asimismo, se menciona que la información de las grabaciones de los dispositivos se almacenará en los equipos servidores de la OTIC.	Alta	• Oficina de Tecnología de Información y Comunicaciones.

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

7.3. Planificación

La planificación se estructura en cuatro fases, cada una con plazos específicos y actividades correspondientes que permitan cumplir los objetivos de calidad de la universidad, de esta manera, la implementación de la ruta estratégica se realiza de manera ordenada y eficiente. Las fases se diseñan teniendo en cuenta la prioridad de cada acción y la disponibilidad de recursos.

Esta planificación permite abordar de manera ordenada y escalonada los elementos clave del sistema de calidad, desde el diagnóstico hasta la preparación final para los respectivos procesos de calidad, como son la renovación de licencia institucional y la acreditación de programas, asegurando una implementación eficiente y un monitoreo continuo de los avances.

VIII. INDICADORES Y EVALUACIÓN DE DESEMPEÑO

8.1. Indicadores de desempeño

La matriz de indicadores de desempeño constituye un instrumento fundamental para la gestión de la OTIC, al proporcionar un marco estructurado para el seguimiento y evaluación del cumplimiento de los objetivos estratégicos. Su diseño responde a la necesidad de contar con mecanismos que permitan medir con precisión el impacto de las acciones implementadas, asegurando su alineación con las metas institucionales.

Cada indicador ha sido definido considerando su relevancia en la evaluación del desempeño, estableciendo criterios claros de medición que permitan analizar avances, identificar oportunidades de mejora y fortalecer la toma de decisiones basada en evidencia. La matriz no solo refleja el grado de cumplimiento de los objetivos, sino que también se convierte en una guía para la optimización de procesos, promoviendo una gestión más eficiente y orientada a resultados.

A través de este enfoque sistemático, se busca garantizar la mejora continua, fomentando un ciclo de retroalimentación que facilite la adaptación y fortalecimiento de las estrategias implementadas en el marco de la OTIC.

OBJETIVO GENERAL	OBJETIVO ESPECÍFICO	ACCIÓN ESTRATÉGICA	ACTIVIDADES CLAVE	INDICADOR DE DESEMPEÑO	META	AÑO			RESPONSABLE
						1	2	3	
Garantizar la gestión eficiente, segura e innovadora de los recursos tecnológicos, contribuyendo a la modernización y optimización de los procesos institucionales	Desarrollar e implementar una infraestructura tecnológica robusta y segura.	Implementación de una arquitectura tecnológica moderna y escalable	Actualización y mejora de la infraestructura de redes y servidores	Nivel de disponibilidad de sistemas y servicios TIC	≥ 99.5% de disponibilidad anual	90%	95%	100%	OTIC
			Implementación de sistemas de respaldo y recuperación de datos Nivel de disponibilidad de sistemas y servicios TIC	Nivel de disponibilidad de sistemas y servicios TIC	≥ 99.5% de disponibilidad anual	90%	95%	100%	OTIC
		Mejorar el control de ingreso y salida del personal y vehículos en la universidad mediante equipamiento tecnológico	Implementación de un sistema de control de acceso facial para el ingreso y salida del personal. Adicionalmente, la instalación de las cámaras de reconocimiento de placas de los vehículos al ingreso y salida de la UNALM.	Porcentaje de registro de ingreso y salida de personas y vehículos.	≥ 99.5% de disponibilidad anual	90%	95%	100%	• OTIC responsable de la funcionalidad de la solución tecnológica. Unidad de Seguridad Interna, responsable de la administración y monitoreo de los dispositivos.
		Fortalecer la seguridad de la universidad mediante el monitoreo de las	Integración de todas las cámaras de seguridad para ser monitoreadas en el centro de	Porcentaje de registro de incidencias.	≥ 99.5% de disponibilidad anual	90%	95%	100%	• OTIC responsable de la funcionalidad de la solución tecnológica. • Seguridad Interna, responsable de la

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

		cámaras de seguridad.	monitoreo.						administración y monitoreo de los dispositivos.
	Optimizar los servicios de soporte técnico y asistencia tecnológica.	Fortalecimiento de la capacitación y especialización del personal TIC	Capacitación continua del equipo de soporte en nuevas tecnologías y gestión de incidencias	Tiempo promedio de respuesta y resolución de incidencias	Reducción del tiempo de resolución en un 20% respecto al año anterior	90%	95%	100%	OTIC
			Implementación de un sistema de gestión de incidencias	Tiempo promedio de respuesta y resolución de incidencias	≤ 24 horas en casos críticos	90%	95%	100%	OTIC
	Fortalecer la ciberseguridad y protección de datos institucionales.	Desarrollo de un plan integral de ciberseguridad	Implementación de políticas y procedimientos de seguridad informática	Nivel de cumplimiento de normativas de seguridad de la información	100% de cumplimiento de normativas nacionales e internacionales	90%	95%	100%	OTIC
			Auditorías periódicas de seguridad y pruebas de penetración	Nivel de cumplimiento de normativas de seguridad de la información	Al menos 2 auditorías de seguridad anuales	90%	95%	100%	OTIC
	Fomentar la transformación digital y la innovación en la institución.	Integración de sistemas de información para la toma de decisiones basada en datos	Desarrollo e implementación de un sistema de gestión integral de información	Nivel de satisfacción de usuarios internos con los servicios TIC	≥ 85% de satisfacción en encuestas anuales	90%	95%	100%	OTIC
			Interoperabilidad entre plataformas institucionales para optimizar la gestión de datos	Nivel de satisfacción de usuarios internos con los servicios TIC	Incremento del 15% en la percepción de eficiencia del sistema en comparación con el año anterior	90%	95%	100%	OTIC
	Implementar	Implementación	Desarrollo de	Nivel de	Publicación	90%	95%	100%	OTIC

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

	mecanismos de monitoreo y evaluación continua de los servicios TIC	de un sistema de gestión de calidad TIC	métricas y reportes periódicos de desempeño TIC	satisfacción de usuarios internos con los servicios TIC	trimestral de reportes de desempeño con indicadores clave				
			Aplicación de encuestas de satisfacción y análisis de retroalimentación de usuarios	Nivel de satisfacción de usuarios internos con los servicios TIC	≥ 85% de satisfacción en encuestas anuales	90%	95%	100%	OTIC

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

8.2. Mecanismos de control y seguimiento

Para garantizar la efectividad y el cumplimiento de los objetivos estratégicos del plan, se implementará un sistema integral de monitoreo y evaluación basado en buenas prácticas de gestión tecnológica. Este sistema permitirá identificar oportunidades de mejora, optimizar procesos y fortalecer la toma de decisiones.:

a. Auditorías Periódicas: Programar auditorías tanto internas como externas, con el fin de evaluar la correcta implementación de las estrategias, el uso eficiente de los recursos y el cumplimiento de normativas y estándares tecnológicos. Estas auditorías permitirán detectar riesgos, brechas operativas y necesidades de ajuste en la ejecución del plan.

b. Encuestas de Satisfacción: Realizar encuestas y entrevistas periódicas dirigidas a los usuarios de los servicios tecnológicos, con el objetivo de medir la percepción sobre la calidad, disponibilidad y eficiencia de las soluciones implementadas. Los resultados de estas encuestas servirán para ajustar las estrategias de atención, optimizar la experiencia del usuario y mejorar la alineación de los servicios TIC con las necesidades institucionales.

c. Análisis de Indicadores de Desempeño: Medir el impacto del plan en aspectos como la reducción de incidentes tecnológicos, la mejora en los tiempos de respuesta y resolución, el nivel de adopción de nuevas tecnologías, la seguridad de la información y la eficiencia operativa. Estos indicadores se consolidarán en reportes periódicos que serán presentados a las instancias de gobierno institucional para la toma de decisiones informadas.

d. Retroalimentación y Revisión Continua: Establecer reuniones de seguimiento con las unidades funcionales de la OTIC y los actores clave de la institución. Estas reuniones permitirán ajustar estrategias, atender desafíos emergentes y asegurar que la evolución del plan responda a las necesidades cambiantes del entorno tecnológico y organizacional.

En conjunto, estas acciones conforman un sistema dinámico de control y seguimiento que garantiza la mejora continua, la sostenibilidad de las iniciativas y la alineación del plan con los objetivos estratégicos de la UNALM.

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

IX. RIESGOS

La gestión de riesgos tiene como objetivo anticipar, gestionar y mitigar riesgos potenciales que puedan afectar la implementación efectiva de los procesos y servicios de la OTIC en la universidad.

9.1. Identificación de Riesgos Potenciales

a. Vulnerabilidades en seguridad de la información

La creciente digitalización y el uso intensivo de plataformas tecnológicas exponen a la institución a diversas amenazas cibernéticas, como ataques de malware, phishing, accesos no autorizados y filtraciones de datos. La falta de medidas adecuadas de protección puede comprometer la confidencialidad, integridad y disponibilidad de la información, afectando la operatividad institucional y la confianza de los usuarios. Para mitigar este riesgo, es fundamental implementar estrategias robustas de ciberseguridad, incluyendo políticas de acceso restringido, monitoreo continuo de amenazas, protocolos de respuesta ante incidentes y campañas de concienciación para el personal.

b. Fallas en la infraestructura tecnológica

Una infraestructura desactualizada, con equipos obsoletos o sin mantenimiento adecuado, puede generar interrupciones en los servicios tecnológicos esenciales, afectando la continuidad operativa de la institución. La falta de redundancia y mecanismos de recuperación ante desastres aumenta la vulnerabilidad ante fallos inesperados, impactando la productividad y la calidad de los servicios. Para reducir este riesgo, se requiere una planificación estratégica en la adquisición, mantenimiento y actualización de hardware y software, así como la implementación de soluciones en la nube y esquemas de alta disponibilidad que garanticen la resiliencia de los sistemas.

c. Brechas en la capacitación y especialización del personal OTIC

La rápida evolución de la tecnología demanda que el equipo TIC mantenga un nivel de conocimientos actualizado y alineado con las mejores prácticas del sector. La falta de capacitación continua puede traducirse en errores operativos, configuraciones inadecuadas, baja eficiencia en la gestión tecnológica y una respuesta deficiente ante incidentes. Para abordar este desafío, es necesario desarrollar un programa de formación constante que

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

incluya certificaciones, entrenamientos especializados y acceso a recursos de aprendizaje que fortalezcan las competencias del personal y su capacidad de adaptación a nuevas tecnologías.

d. Falta de integración de sistemas y plataformas digitales

La coexistencia de múltiples sistemas desconectados dificulta la interoperabilidad y el flujo eficiente de la información dentro de la institución, generando redundancias, errores en los datos y limitaciones en la generación de reportes estratégicos. La ausencia de una arquitectura tecnológica integrada restringe la capacidad de análisis de datos y la toma de decisiones basada en información confiable y en tiempo real. Para mitigar este riesgo, es esencial desarrollar una estrategia de integración que contemple la implementación de plataformas de gestión centralizada, estándares abiertos y herramientas de analítica avanzada que permitan optimizar los procesos y mejorar la eficiencia operativa.

TIPO DE RIESGO	RIESGO	PROBABILIDAD	IMPACTO	ESTRATEGIAS DE MITIGACIÓN	RESPONSABLE	INDICADOR DE DESEMPEÑO
Riesgo Estratégico	Falta de integración de sistemas y plataformas digitales	Media	Alto	• Desarrollar una estrategia de integración de sistemas basada en estándares abiertos, interoperabilidad y analítica avanzada. • Implementar plataformas de gestión centralizada.	OTIC	• Número de sistemas integrados en una plataforma única. • Reducción del tiempo de procesamiento de información • Nivel de satisfacción de los usuarios sobre la accesibilidad a datos consolidados.
Riesgo Operativo	Vulnerabilidad en seguridad de la información	Alta	Crítico	• Implementación de un plan integral de ciberseguridad. • Actualización contante de software y hardware. Monitoreo proactivo de amenazas, controles de acceso y protocolos de respuesta ante incidentes.	OTIC	• Número de intentos de acceso no autorizado detectados y bloqueados. • Índice de cumplimiento de normativas de seguridad. Frecuencia de auditorías de ciberseguridad realizadas.
	Fallas en la infraestructura tecnológica	Media	Alto	• Plan de renovación y mantenimiento preventivo de hardware y software. • Implementación de infraestructura en la nube. • Redundancia en sistemas críticos. Estrategias de recuperación ante desastres.	OTIC	• Porcentaje de tiempo de disponibilidad de los servicios de TIC. • Número de fallos críticos reportados y solucionados. Tiempo promedio de recuperación ante fallos.
Riesgo Organizacional	Brechas en la capacitación y especialización del	Alta	Alto	• Desarrollo de un programa de capacitación continua y certificaciones en	OTIC	• Número de horas de capacitación impartidas por año. • Porcentaje de personal OTIC certificado

	personal de OTIC			tecnologías emergentes. • Promoción de aprendizaje colaborativo. • Evaluaciones de competencias periódicas.		en tecnologías clave. • Nivel de satisfacción del equipo OTIC respecto a la formación recibida.

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

9.2. Monitoreo y Evaluación

Para garantizar la eficacia de las estrategias implementadas en la gestión de riesgos tecnológicos, se establecerá un sistema integral de monitoreo y evaluación basado en metodologías de análisis de riesgos, indicadores de desempeño y procesos de mejora continua. Este enfoque permitirá identificar amenazas emergentes, evaluar la efectividad de las medidas adoptadas y optimizar la resiliencia institucional frente a incidentes tecnológicos.

Se aplicarán metodologías de análisis de riesgos para priorizar amenazas y definir estrategias de mitigación, incluyendo la implementación de soluciones de respaldo, capacitación continua y protocolos de respuesta ante incidentes. Este análisis será dinámico, permitiendo ajustes según el contexto tecnológico y las necesidades institucionales.

El monitoreo continuo se basará en el uso de herramientas de gestión de riesgos y ciberseguridad que permitan la detección temprana de vulnerabilidades y la identificación de patrones de actividad sospechosa. Se implementarán tableros de control con indicadores clave para medir la disponibilidad de los servicios, la frecuencia de intentos de intrusión y la respuesta a incidentes, asegurando que las acciones correctivas sean oportunas y efectivas.

Asimismo, se llevarán a cabo auditorías tecnológicas periódicas para evaluar el cumplimiento de políticas de seguridad, el estado de la infraestructura tecnológica y la eficiencia operativa de los sistemas. Estas auditorías serán complementadas con simulaciones de crisis y pruebas de recuperación ante desastres, con el fin de verificar la capacidad de respuesta de la organización frente a contingencias.

El proceso de evaluación incluirá mecanismos de retroalimentación, como encuestas de percepción dirigidas a usuarios y reuniones de análisis con los equipos de trabajo, con el objetivo de detectar oportunidades de mejora en la gestión tecnológica. Además, se fomentará una cultura de seguridad y actualización permanente, donde las mejores prácticas y aprendizajes derivados de incidentes previos se integren en la planificación estratégica.

Con este enfoque, la OTIC garantizará que las medidas adoptadas sean efectivas y se ajusten de manera proactiva a los desafíos del entorno digital, fortaleciendo la seguridad, disponibilidad y eficiencia de los servicios tecnológicos.

9.3. Revisión y Mejora de la Gestión de Riesgos

La gestión de riesgos es un documento dinámico que será revisado y actualizado de manera periódica para garantizar su alineación con los cambios tecnológicos, las necesidades institucionales y la evolución del entorno de riesgos. Se establecerá un proceso de actualización anual, así como revisiones extraordinarias en caso de que se presenten eventos críticos, modificaciones en la infraestructura tecnológica o cambios en las normativas y políticas institucionales.

Este proceso de revisión incluirá un análisis comparativo entre la situación actual y los riesgos inicialmente identificados, permitiendo detectar brechas, ajustar estrategias de mitigación y mejorar los protocolos de respuesta ante incidentes. Para ello, se utilizarán metodologías basadas en la gestión de riesgos, auditorías tecnológicas y el análisis de indicadores clave de desempeño, con el fin de medir la efectividad de las acciones implementadas.

Además, se establecerán mecanismos de retroalimentación que involucren a todos los actores clave, incluyendo al personal OTIC, usuarios finales, autoridades institucionales y expertos en seguridad de la información. La recopilación de información a través de encuestas de satisfacción, reportes de incidentes y sesiones de evaluación permitirá identificar oportunidades de mejora y adaptar el plan a las necesidades emergentes.

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

Otro elemento fundamental será la incorporación de buenas prácticas y tendencias en gestión de riesgos tecnológicos, adoptando estándares internacionales y experiencias exitosas en la mitigación de amenazas digitales. Se promoverá la capacitación constante del equipo OTIC en metodologías actualizadas de análisis y respuesta ante riesgos, asegurando que la organización cuente con los conocimientos y herramientas necesarios para enfrentar nuevos desafíos.

Finalmente, los resultados de cada revisión serán documentados y presentados ante la alta dirección de la UNALM, con recomendaciones concretas para fortalecer la seguridad, resiliencia y eficiencia de la infraestructura tecnológica. Con este enfoque, la OTIC garantizará que la Gestión de Riesgos se mantenga actualizado, adaptable y alineado con la estrategia institucional, contribuyendo a la sostenibilidad y mejora continua de los servicios tecnológicos.