	INSTITUTO POLITÉCNICO NACIONAL
	Plan de continuidad

1. Fecha de elaboración

0	3	1	2	2	0	2	6

2. Introducción

El Plan de Continuidad del Negocio tiene como objetivo garantizar la operación del servicio de Consultoría e Implementación de Soluciones de Inteligencia Artificial (EmpresIA) ante eventos disruptivos que puedan afectar la disponibilidad, integridad o confidencialidad de los activos de información.
Este plan se apoya en el análisis de impacto al negocio (BIA), la matriz de riesgos y el inventario de activos, con el fin de establecer estrategias de respuesta, recuperación y continuidad que permitan minimizar interrupciones y asegurar la prestación del servicio a los clientes.

2. Objetivo del Plan de Continuidad

Garantizar la continuidad operativa del servicio EmpresIA ante incidentes tecnológicos, de seguridad o infraestructura, estableciendo acciones claras de respuesta y recuperación que permitan mantener los niveles de servicio acordados y reducir el impacto al negocio.

3. Alcance del Plan

Este plan aplica a los procesos críticos del servicio EmpresIA, incluyendo:

- Diagnóstico y análisis de procesos empresariales.
- Desarrollo y entrenamiento de modelos de IA.
- Integración de soluciones de IA con sistemas del cliente.
- Monitoreo, soporte y atención a incidentes.
- Gestión de datos, modelos y plataformas de IA.

El plan cubre incidentes relacionados con infraestructura, software, seguridad de la información, fallas operativas y eventos externos.

4. Procesos Críticos Identificados (del BIA)

Proceso	Nivel de criticidad
Evaluación de riesgos y vulnerabilidades	Alto

Gestión de identidades y accesos (IAM)	Crítico
Cifrado de datos sensibles	Crítico
Monitoreo y respuesta a incidentes	Alto

5. Escenarios de Interrupción

Escenario 1: Falla en infraestructura Cloud

- Impacto: Interrupción del entrenamiento y despliegue de modelos.
- Procesos afectados: Desarrollo de IA, monitoreo.
- Activos involucrados: Servidores, bases de datos, plataformas Cloud.

Escenario 2: Incidente de seguridad / fuga de información

- Impacto: Riesgo legal y reputacional.
- Procesos afectados: Gestión de datos, cifrado.
- Activos involucrados: Bases de datos, modelos de IA.

Escenario 3: Indisponibilidad del personal clave

- Impacto: Retrasos en soporte y respuesta a incidentes.
- Procesos afectados: Monitoreo, atención a clientes.
- Activos involucrados: Personal especializado.

6. Estrategias de Continuidad y Recuperación

Escenario	Estrategia de continuidad
Falla de infraestructura	Uso de respaldo en la nube y virtualización

Incidente de seguridad	Activación del plan de respuesta a incidentes y aislamiento
Pérdida de datos	Restauración desde respaldos cifrados
Falta de personal	Redistribución de roles y personal capacitado

7. Tiempos de Recuperación (RTO / RPO)

Proceso	RTO	RPO
Monitoreo de incidentes	1 hora	15 minutos
Gestión de accesos (IAM)	30 minutos	0
Cifrado y protección de datos	1 hora	15 minutos
Plataforma de IA	4 horas	1 hora

8. Tiempos de Recuperación (RTO / RPO)

Rol	Responsabilidad
Responsable de TI	Activar el plan de continuidad
Especialista IA/ML	Recuperación de modelos
Soporte técnico	Restauración de servicios
Seguridad	Contención y análisis del incidente

9. Pruebas y Actualización del Plan

El Plan de Continuidad será probado al menos una vez al año mediante simulacros de interrupción controlados. Cualquier cambio en los procesos, infraestructura o riesgos identificados deberá reflejarse en una actualización del plan.

	INSTITUTO POLITÉCNICO NACIONAL
	Plan de continuidad