

	INSTITUTO POLITÉCNICO NACIONAL ESCUELA SUPERIOR DE CÓMPUTO	HOJA	1 DE 7
		ID DEL SERVICIO	
		FECHA DE ELABORACIÓN	02/01/2026
	CEDULA DE SERVICIO		

1. Información general del servicio de IT

Nombre de la Empresa:	
Departamento:	Cómputo / TI

Nombre del servicio	Migración e Implementación de Servicios en la Nube (servicios críticos: servidores de aplicaciones, bases de datos, almacenamiento y correo)			
Tipo de servicio	Nuevo: <input checked="" type="checkbox"/>	Cambio: <input type="checkbox"/>	Retiro: <input type="checkbox"/>	Activo: <input type="checkbox"/>
Listado de la(s) variante(s) o sub-servicio(s)	<ul style="list-style-type: none"> • Migración de aplicaciones web críticas (IaaS/PaaS). • Almacenamiento institucional en la nube. • Servicio de autenticación / IAM centralizado. • Monitorización y respaldo (backup/DR). • Red privada virtual (VPC / conexión IPSec/DirectConnect). 			
Descripción y alcance del servicio	Migración y estabilización de servicios críticos on-prem a una plataforma en la nube pública o híbrida, la cual Incluye: evaluación y levantamiento, planeación de arquitectura, migración de aplicaciones y datos, configuración de VPC y conectividad, implementación IAM, monitorización y backups, pruebas de recuperación ante desastres, capacitación operacional y entrega de documentación			

Objetivo del servicio	Migrar y estabilizar los servicios críticos a la nube en un periodo de 6 meses, garantizando disponibilidad $\geq 99.9\%$ para servicios productivos y reduciendo el tiempo de aprovisionamiento de entornos de semanas a ≤ 2 días
Usuarios a quienes se brinda el servicio	<ul style="list-style-type: none"> • Comunidad académica (alumnos y docentes que usan plataformas educativas). • Personal administrativo y de gestión. • Personal de soporte y TI interno.
Beneficios del servicio	<ul style="list-style-type: none"> • Escalabilidad bajo demanda y elasticidad. • Mejora en disponibilidad y continuidad de negocio (DR).

	INSTITUTO POLITÉCNICO NACIONAL ESCUELA SUPERIOR DE CÓMPUTO	HOJA	2 DE 7
		ID DEL SERVICIO	
		FECHA DE ELABORACIÓN	02/01/2026
	CEDULA DE SERVICIO		

	<ul style="list-style-type: none"> Reducción de deuda técnica e incremento en velocidad de despliegues (CI/CD). Incremento en controles de seguridad nativos y cumplimiento. Mejora en experiencia de usuarios remotos.
Demanda del servicio	Carga actual limitada en infraestructura on-prem y demanda creciente por accesos remotos, enseñanza a distancia y servicios administrativos. Se espera incremento de consumo en picos de semestre.

2. Responsables del servicio (Matriz RACI)

Actividad/ROL	Project Maganer	Cloud Architect	Ingeniero Sistemas/Cloud	Ingeniero DevOps	Especialista Seguridad	Coordinador Cambio / Formación	Soporte Mesa Ayuda
Levantamiento y evaluación	A	R	C	I	C	I	I
Diseño arquitectura (VPC/IAM/DR)	I	R	C	C	C	I	I
Migración de aplicaciones	C	A	R	R	C	I	I
Implementación CI/CD e Infra como Código	I	C	R	A	I	I	I
Configuración de seguridad (IAM, cifrado)	I	C	C	C	R	I	I
Pruebas DR y validación	A	R	R	C	C	I	I
Capacitación y transferencia	I	I	C	C	I	R	I
Soporte y operación post-migración	I	I	A	R	I	I	R

Legenda: R = Responsible, A = Accountable, C = Consulted, I = Informed.

Rol	Nombre	Correo electrónico	Teléfono/ extensión	Horario de atención
Project Manager	Juan Carlos González González	jgonzalezg1805@alumno.ipn.mx	(55) 2559-2668	L-V 09:00 - 18:00 hrs
Cloud Architect	Carlos David González Sánchez	cgonzalezs1901@alumno.ipn.mx	(55) 7484-4406	L-V 09:00 - 18:00 hrs
Ingeniero Sistemas / Cloud	Juan Pablo Chávez Lacaud	jchavezl1600@alumno.ipn.mx	(55) 1949-6924	L-V 08:00 - 17:00 hrs
Ingeniero DevOps	Jorge Ramírez Castillo	jorge.ramirez@instituto.edu.mx	(55) 4567-8901	L-V 10:00 - 19:00 hrs
Especialista Seguridad	María López Estrada	maria.lopez@instituto.edu.mx	(55) 5678-9012	L-V 09:00 - 18:00 hrs
Coordinador Cambio / Formación	Pedro Sánchez Ruiz	pedro.sanchez@instituto.edu.mx	(55) 6789-0123	L-V 09:00 - 18:00 hrs

	INSTITUTO POLITÉCNICO NACIONAL ESCUELA SUPERIOR DE CÓMPUTO	HOJA	3 DE 7
		ID DEL SERVICIO	
		FECHA DE ELABORACIÓN	02/01/2026
	CEDULA DE SERVICIO		

Soporte Mesa de Ayuda	Equipo Helpdesk	soporte@instituto.edu.mx	(55) 7890-1234	L-V 07:00 - 21:00 hrs

3. Condiciones generales o requisitos para proporcionar el servicio

- Enlace institucional de banda suficiente y redundancia de internet.
- Procedimientos de autorización para cambios (CAB).
- Accesos administrativos, inventario de aplicaciones y datos, y acuerdos de confidencialidad con consultores.
- Herramientas de automatización (IaC), repositorio de código y pipeline CI/CD.
- Plan de pruebas y validación (incluyendo pruebas de DR).

4. Identificación de componentes de infraestructura

Anexar el diagrama lógico de todos los componentes (cada rol) que soporta el servicio.

ARQUITECTURA DEL SERVICIO



INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

CEDULA DE SERVICIO

HOJA

4 DE 7

ID DEL
SERVICIO

FECHA DE
ELABORACIÓN

02/01/2026



5. Niveles de servicio (SLA-acuerdos de servicios para los usuarios)

Tipo de nivel de servicio	Compromiso del nivel de servicio
Disponibilidad	<ul style="list-style-type: none">• Métrica / Definición: Disponibilidad del servicio en producción (tiempo en que el servicio está accesible y funcional para usuarios finales).• Fórmula: $(\text{Tiempo operativo del servicio} / \text{Tiempo total del periodo}) \times 100$.• Target: $\geq 99.9\%$ mensual para servicios críticos; $\geq 99.5\%$ para servicios no-críticos.• Medición / Fuente: Monitoreo (agent + synthetic checks) — pings, health checks, URL checks y métricas del proveedor cloud.• Frecuencia de informe: Diario (dashboard) / Reporte consolidado mensual.• Responsable: Operaciones Cloud / DevOps.

	INSTITUTO POLITÉCNICO NACIONAL ESCUELA SUPERIOR DE CÓMPUTO	HOJA	5 DE 7
		ID DEL SERVICIO	
		FECHA DE ELABORACIÓN	02/01/2026
	CEDULA DE SERVICIO		

	<ul style="list-style-type: none"> • Escalamiento: Si disponibilidad mensual < target → notificar a PM y Seguridad en 24 h; plan de corrección en 72 h.
Soporte vía remota y presencial:	<p>Soporte (remoto)</p> <ul style="list-style-type: none"> • Métrica / Definición: Tiempos de <i>acknowledgement</i> y <i>resolución</i> de incidentes atendidos de forma remota. • Niveles de prioridad: P1 (Crítico), P2 (Alta), P3 (Media), P4 (Baja). • Targets por prioridad: <ul style="list-style-type: none"> ○ P1: Acknowledgement ≤ 15 min; solución temporal ≤ 4 h; solución final ≤ 48 h. ○ P2: Acknowledgement ≤ 30 min; resolución ≤ 24 h. ○ P3: Acknowledgement ≤ 4 h; resolución ≤ 72 h. ○ P4: Acknowledgement ≤ 8 h; resolución ≤ 7 días. • Medición / Fuente: Sistema ITSM (tickets), logs de sesión remota, registros de soporte. • Frecuencia: Monitorización continua; KPI report semanal/mensual. • Responsable: Mesa de Ayuda (1er nivel) / Ingenieros Cloud (2do nivel). • Escalamiento: Si no hay ack en tiempos indicados → escalado automático a Ingeniero Cloud y PM; si no resuelto en target → reunión diaria hasta resolución. <p>3) Soporte (presencial)</p> <ul style="list-style-type: none"> • Métrica / Definición: Tiempo entre escalamiento a soporte presencial y llegada/fijación de actividad in-situ; tiempo a solución in-situ. • Targets por prioridad: <ul style="list-style-type: none"> ○ P1: Despliegue de técnico in-site ≤ 2 horas desde escalamiento (si la ubicación lo permite) y resolución temporal ≤ 8 h; resolución final ≤ 48 h. ○ P2: Despliegue in-site ≤ 8 horas; resolución ≤ 48 h. ○ P3/P4: Programación según SLA operativo (≤ 5 días). • Medición / Fuente: Tickets con timestamp, sistema de despacho de campo. • Frecuencia: Registro en cada incidente; informe mensual. • Responsable: Soporte de campo / Coordinador de Operaciones. • Escalamiento: Si no hay desplazamiento en target → escalado al jefe de soporte y PM; activación de contrato de proveedor si aplica.
Confidencialidad Seguridad	<ul style="list-style-type: none"> • Métrica / Definición: Incidentes de confidencialidad/violación de datos, cumplimiento de controles (cifrado en reposo y tránsito), auditorías/controles. • Indicadores y Targets: • Número de incidentes de confidencialidad por mes: Target = 0. • Porcentaje de datos cifrados (en tránsito y reposo): Target = 100% para datos sensibles; ≥ 95% para resto. • Cumplimiento auditorías de configuración/roles (IAM): Revisiones periódicas completadas → 100% de cuentas revisadas mensualmente para accesos administrativos.

	INSTITUTO POLITÉCNICO NACIONAL ESCUELA SUPERIOR DE CÓMPUTO	HOJA	6 DE 8
		ID DEL SERVICIO	
		FECHA DE ELABORACIÓN	02/01/2026
	CEDULA DE SERVICIO		

	<ul style="list-style-type: none"> • Parches críticos aplicados: Target ≤ 72 h desde publicación. • Medición / Fuente: SIEM, logs de auditoría, escaneos de configuración, reportes de vulnerabilidades. • Frecuencia: Alertas en tiempo real; reporte de cumplimiento semanal/mensual. • Responsable: Equipo de Seguridad / CISO. • Escalamiento: Cualquier incidente de confidencialidad → Escalado inmediato (0–1 h) a CISO, PM y comité de crisis; activación plan de respuesta a incidentes (IRP).
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

6. Niveles de servicio (OLA-acuerdos de servicios respecto a elementos de configuración de infraestructura, aplicaciones, etc.)

Elementos de configuración	Tipo de nivel de servicio y compromiso del nivel de servicio	Métricas de los niveles de servicio
APLICACIONES	Capacidad: Asegurar recursos suficientes para soportar la carga operativa del servicio.	<ul style="list-style-type: none"> • Uso promedio de CPU $\leq 70\%$ • Uso de memoria $\leq 75\%$ • Uso de almacenamiento $\leq 80\%$ • Escalamiento automático ejecutado ≤ 10 min
	Disponibilidad: Mantener operativos los componentes de infraestructura.	<ul style="list-style-type: none"> • Disponibilidad de infraestructura $\geq 99.95\%$ • Tiempo de recuperación ante fallas (RTO) ≤ 4 hrs • Fallas críticas de infraestructura ≤ 1 por mes
	Seguridad: Proteger la infraestructura y los accesos administrativos.	<ul style="list-style-type: none"> • Parcheo de seguridad aplicado ≤ 72 hrs • Accesos administrativos auditados $\geq 100\%$ • Incidentes de seguridad en infraestructura = 0
	Respaldos: Garantizar la recuperación de información ante fallas o incidentes.	<ul style="list-style-type: none"> • Respaldos exitosos $\geq 99\%$ • Frecuencia de respaldo: diaria • RPO ≤ 1 hr • Pruebas de restauración ≥ 1 por trimestre
	Mantenimiento: Ejecutar mantenimientos preventivos y correctivos de forma controlada.	<ul style="list-style-type: none"> • Mantenimientos planificados cumplidos $\geq 95\%$ • Ventanas de mantenimiento notificadas ≥ 72 hrs antes • Incidentes post-mantenimiento $\leq 2\%$



INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

HOJA

7 DE 7

ID DEL
SERVICIO

FECHA DE
ELABORACIÓN

02/01/2026

CEDULA DE SERVICIO

	Mantenibilidad: Facilitar la rápida recuperación y modificación de la infraestructura.	<ul style="list-style-type: none">• Tiempo promedio de reparación (MTTR) ≤ 4 hrs• Cambios exitosos $\geq 95\%$• Documentación técnica actualizada $\geq 100\%$
	Soporte al cliente Proveer apoyo operativo interno para la atención del servicio.	<ul style="list-style-type: none">• Escalamiento interno ≤ 30 min• Incidentes correctamente canalizados $\geq 98\%$• Cumplimiento de OLA $\geq 95\%$
Niveles de servicio para software/aplicación (bases de datos, plataformas, sistemas, etc.):		
	Capacidad: Asegurar que las aplicaciones soporten la demanda de usuarios.	<ul style="list-style-type: none">• Tiempo de respuesta promedio ≤ 2 seg• Usuarios concurrentes soportados $\geq 100\%$ de la demanda prevista• Consumo de recursos por aplicación $\leq 70\%$
	Disponibilidad: Mantener operativas las aplicaciones y sistemas.	<ul style="list-style-type: none">• Disponibilidad del software $\geq 99.9\%$• Caídas críticas ≤ 1 por mes• Tiempo de recuperación de aplicación ≤ 2 hrs
	Seguridad: Proteger el software contra vulnerabilidades y accesos indebidos.	<ul style="list-style-type: none">• Vulnerabilidades críticas corregidas ≤ 72 hrs• Pruebas de seguridad realizadas ≥ 1 por trimestre• Incidentes de seguridad en software = 0
	Respaldos: Garantizar la recuperación de datos y configuraciones del software.	<ul style="list-style-type: none">• Respaldos de bases de datos diarios $\geq 99\%$ exitosos• RPO ≤ 1 hr• Restauraciones exitosas $\geq 95\%$
	Mantenimiento: Actualizar y corregir el software de forma controlada.	<ul style="list-style-type: none">• Actualizaciones aplicadas según plan $\geq 95\%$• Incidentes derivados de cambios $\leq 2\%$• Ventanas de mantenimiento cumplidas $\geq 100\%$
	Mantenibilidad: Facilitar la corrección y mejora del software.	<ul style="list-style-type: none">• MTTR de fallas de software ≤ 4 hrs• Cambios exitosos $\geq 95\%$• Documentación técnica actualizada $\geq 100\%$