RESOLUCION DE CONSEJO UNIVERSITARIO N° 0422-2026

Arequipa, 27 de agosto de 2026

Visto el Oficio N° 462-2026-OTI-UNSA de fecha 05 de agosto de 2026, remitido por la Oficina de Tecnologías de la Información.

CONSIDERANDO:

Que, la Universidad Nacional de San Agustín de Arequipa está constituida conforme a la Ley N° 30220, Ley Universitaria, y se rige por sus respectivos estatutos y reglamentos, siendo una comunidad académica orientada a la investigación y a la docencia, que brinda una formación humanista, ética, científica y tecnológica con una clara conciencia de nuestro país como realidad multicultural.

Que, el artículo 8° de la Ley N° 30220, Ley Universitaria, concordante con el artículo 8° del Estatuto Universitario, referente a la autonomía universitaria establece lo siguiente: *"(...) Esta autonomía se manifiesta en los siguientes regímenes: 8.1* ***Normativo****, implica la potestad autodeterminativa para la creación de normas internas (estatuto y reglamentos) destinadas a regular la institución universitaria. 8.2* ***De gobierno****, implica la potestad autodeterminativa para estructurar, organizar y conducir la institución universitaria, con atención a su naturaleza, características y necesidades. Es formalmente dependiente del régimen normativo (...) 8.4* ***Administrativo****, implica la potestad autodeterminativa para establecer los principios, técnicas y prácticas de sistemas de gestión, tendientes a facilitar la consecución de los fines de la institución universitaria, incluyendo la organización y administración del escalafón de su personal docente y administrativo (...)".*

Que, el artículo 5° del Estatuto Universitario vigente establece que la Universidad tiene entre sus fines el de: *"5.1 Preservar, acrecentar y transmitir de modo permanente, la herencia científica, tecnológica, cultural y artística de la humanidad"*; y el artículo 95° del Reglamento de Organización y Funciones (ROF) de la Universidad, aprobado mediante Resolución de Consejo Universitario N° 0306-2022, prevé que la Oficina de Tecnologías de la Información es el órgano responsable de los procesos de diseño, desarrollo, adquisición, implementación, integración, mantenimiento, documentación y evaluación de los sistemas de información y la infraestructura tecnológica institucional.

Que, mediante Resolución de Consejo Universitario N° 0350-2021 de fecha 23 de julio de 2021, se aprobó el "*Plan de Contingencias de Tecnologías de la Información de la Oficina Universitaria de Informática y Sistemas de la Universidad Nacional de San Agustín de Arequipa*", el cual estableció en su tercera disposición final la obligación de efectuar su actualización con una periodicidad anual.

Que, mediante Informe de Orientación de Oficio N° 003-2026-OCI/0210-SOO, denominado *"Operatividad del Data Center Institucional"*, notificado por el Órgano de Control Institucional, se advirtió en la Situación Adversa N° 2 que la Universidad no contaba con un plan de contingencias de tecnologías de la información actualizado que asegure la consistencia y el uso adecuado de los sistemas de información, infraestructura de hardware y software, lo que podría afectar la continuidad operativa y la oportuna adopción de medidas reactivas y preventivas.

Que, en el marco del plan de acciones adoptadas para la implementación de las medidas correctivas dispuestas por el Rectorado mediante Oficio Circular N° 0061-2026-R-UNSA, la Oficina de Tecnologías de la Información elaboró y remitió a través del documento del visto el **PLAN DE CONTINGENCIA, PLAN DE ATENCIONES SLA PARA DATA CENTER**, con el propósito de garantizar una respuesta técnica estandarizada y oportuna frente a incidentes de infraestructura crítica (eléctrica, climatización/HVAC, enlaces y servidores) del Data Center principal.

Que, en ese contexto, el Consejo Universitario en su **sesión ordinaria de fecha 19 de agosto de 2026**, acordó 1) aprobar el PLAN DE CONTINGENCIA, PLAN DE ATENCIONES SLA PARA DATA CENTER de la Universidad Nacional de San Agustín de Arequipa, precisando que la

Oficina de Tecnologías de la Información deberá remitir la versión final integrando el directorio de emergencia, la identificación de los responsables y suplentes, así como los propietarios funcionales de los servicios, los valores RTO (Recovery Time Objective / Objetivo de Tiempo de Recuperación) y RPO (Recovery Point Objective / Objetivo de Punto de Recuperación) y demás campos pendientes de la Matriz de Servicios Críticos; y, 2) Disponer que la Oficina de Tecnologías de la Información, efectúe la revisión y actualización integral del Plan de Contingencias de Tecnologías de la Información como mínimo una vez al año, y bajo responsabilidad, a fin que comprenda la continuidad de los sistemas de información, infraestructura de hardware y software y demás servicios tecnológicos de la Universidad.

Por estas consideraciones y en uso de las atribuciones que la Ley Universitaria N° 30220 confiere al Consejo Universitario,

SE RESUELVE:

1. **APROBAR** el **PLAN DE CONTINGENCIA, PLAN DE ATENCIONES SLA PARA DATA CENTER** de la Universidad Nacional de San Agustín de Arequipa, elaborado por la Oficina de Tecnologías de la Información, el mismo que en anexo forma parte integrante de la presente resolución.

2. **DISPONER** que la **Oficina de Tecnologías de la Información** remita la versión final del **PLAN DE CONTINGENCIA, PLAN DE ATENCIONES SLA PARA DATA CENTER,** incorporando el directorio de emergencia completo, la identificación nominal de responsables y suplentes, los propietarios funcionales de los servicios, así como los valores de Objetivo de Tiempo de Recuperación (RTO) y Objetivo de Punto de Recuperación (RPO) en la Matriz de Servicios Críticos.

3. **DISPONER** que la **Oficina de Tecnologías de la Información** efectúe, en el más breve plazo y bajo responsabilidad funcional, la revisión y actualización integral del *Plan de Contingencias de Tecnologías de la Información* como mínimo una vez al año y bajo responsabilidad, a fin de que comprenda la continuidad, respaldo y recuperación de los sistemas de información, infraestructura de hardware, software y demás servicios tecnológicos de la Universidad.

4. **ENCARGAR** a la Oficina de Tecnologías de la Información la implementación, ejecución, difusión operativa y estricto cumplimiento de los procedimientos, protocolos de escalamiento y niveles de servicio (SLA) contenidos en el plan aprobado en el punto resolutivo 1.

5. **DISPONER** que la Oficina de Comunicación e Imagen Institucional, en coordinación con la Oficina de Tecnologías de la Información, publique la presente resolución en el Portal Institucional y en el Portal de Transparencia Estándar de la Universidad.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE.

DRA. RUTH MARITZA CHIRINOS LAZO
SECRETARIA GENERAL

DR. HUGO JOSE ROJAS FLORES
RECTOR

C.c.: Dependencias, OTI, OCII, OCI, ARCH (exp.)
Exp. N° 2013489-2026
/fmda

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA
Oficina de Tecnologías de la Información (OTI)

PLAN DE CONTINGENCIA, PLAN DE ATENCIONES SLA PARA DATA CENTER

Versión 1.0 · Julio 2026
Arequipa, Perú

Documento de uso interno — Oficina de Tecnologías de la Información

Tabla de Contenido

PLAN DE CONTIGENCIA

1. Propósito, alcance y supuestos

El propósito es asegurar una respuesta coordinada frente a incidentes de infraestructura crítica, minimizar la interrupción de los servicios institucionales y recuperar la operación de forma segura y verificable.

Alcance

- Seis gabinetes de servidores y comunicaciones, sus equipos activos, cableado de cobre y fibra óptica.
- Alimentación eléctrica, tableros, UPS, banco de baterías, transformador de voltaje y puesta a tierra asociados.
- Sistema aires acondicionados, monitoreo ambiental, ambiente físico y controles operativos del Data Center.
- Servicios académicos, administrativos e institucionales que dependan de los componentes anteriores.

Exclusiones

No sustituye los planes de continuidad de aplicaciones, respaldo y recuperación de datos, ciberseguridad, evacuación institucional ni gestión de emergencias del edificio. Estos deberán coordinarse cuando el incidente lo requiera.

Criterios de activación

Nivel	Criterio de activación	Dirección de respuesta
N1 - Alerta	Evento controlable sin afectación de servicio o con degradación menor a 15 min.	Técnico de turno; informar al Coordinador DC.
N2 - Incidente	Degradación relevante, riesgo térmico/eléctrico o indisponibilidad parcial superior a 15 min.	Activar equipo de contingencia y comunicación interna. Comunicación y escalamiento interno en OTI.
N3 - Emergencia	Indisponibilidad total, riesgo para personas/equipos, incendio, inundación, falla eléctrica mayor o temperatura crítica sostenida.	Activar Comité de Crisis, protocolo de seguridad y continuidad institucional. Escalar incidencia a instancias superiores para informar problemática, mediante canales formales.

2. Contexto de riesgo y prioridades

El informe técnico de evaluación identifica un riesgo global ALTO para el Data Center. No se reporta una falla inminente, pero la exposición aumenta ante incidentes eléctricos, errores de operación o sobretemperatura.

Riesgo base	Evidencia relevante	Prioridad de contingencia
Energía	Deficiencias en documentación eléctrica, acometida eléctrica no apropiada para una continuidad del suministro.	Alta: proteger equipos, aislar fallas y recuperar alimentación segura.
Comunicaciones	Cuatro de seis gabinetes requieren reetiquetado; trazabilidad y documentación incompletas. Considerando que 2 gabinetes son dedicados para el área de investigación.	Alta: evitar desconexiones accidentales y reducir el tiempo de diagnóstico.

Riesgo base	Evidencia relevante	Prioridad de contingencia
HVAC	Recirculación de aire caliente, posibles hot spots y sin extracción dirigida. Ya que se cuenta con aires acondicionados comerciales. Es necesario un sistema de HVAC que se monitoreado.	Alta: detectar temperatura, mantener enfriamiento y apagar cargas no críticas si es necesario.
Gestión	Falta de inventario, planos y procedimientos consolidados. Y publicación de esta información estrategia a las áreas vinculantes.	Alta: mantener bitácoras, escalamiento y control de cambios.

3. Organización para la contingencia

Los nombres, teléfonos y suplentes deben registrarse en el directorio de emergencia del Anexo A antes de aprobar el plan.

Rol	Responsabilidad principal	Suplencia
Director de Crisis (Jefatura OTI)	Autoriza activación N3, prioriza servicios y comunica a la Alta Dirección.	Responsable designado por la OTI
Coordinador del Data Center	Dirige la respuesta técnica, clasifica el incidente y controla la bitácora.	Administrador de infraestructura
Responsable eléctrico	Aísla circuitos, coordina UPS/energía y valida retorno seguro.	Técnico de soporte eléctrico autorizado
Responsable de redes y servidores	Evalúa enlaces, equipos y restauración de servicios.	Administrador de redes/sistemas
Responsable HVAC y ambiente	Verifica climatización, sensores y medidas de mitigación térmica.	Técnico de soporte HVAC autorizado
Seguridad y mantenimiento	Controla acceso, seguridad física y coordinación con emergencias del campus.	Tecnico de sopporte y mantenimiento de turno
Comunicaciones OTI	Emite avisos aprobados a usuarios, autoridades y proveedores.	Representante de OTI

Reglas de operación durante el incidente

- La seguridad de las personas prevalece sobre la continuidad de los servicios.
- Solo personal autorizado interviene tableros, UPS, baterías, climatización y cableado.
- Toda acción, hora, responsable y resultado se registra en la bitácora del incidente.
- No se reconecta un equipo o circuito sin evaluación de causa, riesgo y autorización del Coordinador DC.
- Toda modificación física se realiza bajo control de cambios y se actualiza en planos/inventario.

4. Procedimiento general de respuesta

Fase	Acciones obligatorias	Resultado esperado
1. Detectar y registrar	Registrar alerta, hora, fuente, servicios afectados, condiciones ambientales y eléctricas visibles.	Ticket/bitácora abierta.
2. Clasificar y escalar	Aplicar N1-N3; avisar al Coordinador DC y, en N3, al Director de Crisis. O en su defecto a la jefatura de OTI	Equipo y autoridad activados.
3. Proteger	Restringir acceso; proteger personas; aislar el componente afectado sin agravar la falla.	Riesgo contenido.
4. Mantener servicios	Priorizar cargas y servicios críticos; activar respaldos operativos disponibles.	Impacto reducido.
5. Recuperar	Corregir la causa o aplicar solución temporal controlada; restaurar por etapas.	Servicio estabilizado.
6. Verificar y cerrar	Comprobar disponibilidad, alarmas, temperatura, energía y comunicaciones; emitir informe.	Retorno seguro y lecciones aprendidas.

Fase	Acciones obligatorias	Resultado esperado
7. Informes	Se debe elaborar informes técnicos de los trabajos ejecutados, tanto del personal técnico involucrado en las acciones tomadas frente a nivel de riesgo atentado, también se debe solicitarse informes a contratistas en caso existan terceros atención del vento.	Información adecuada de las acciones tomadas frente a las incidencias o atenciones involucradas.
8. Capacitación	Se debe capacitar de forma constante al personal especializado, tomando como buena práctica de informa las acciones técnicas que se ejecutaron en los incidentes atendidos y corregidos. Y en la nueva infraestructura adquirida por parte de la institución	Se mantiene una buena capacidad de respuesta del personal a cargo y soporte técnico oportuno.

5. Escenarios de contingencia

5.1 Falla eléctrica, UPS o distribución

Aplica ante corte de alimentación, alarma de UPS/baterías, disparo de protección, olor a quemado, calentamiento anormal, sobretensión o falla de puesta a tierra.

Momento	Acciones
Inmediato	No abrir tableros ni intervenir conductores energizados. Restringir acceso. Si existe riesgo eléctrico o humo, activar seguridad y emergencia institucional.
0-15 min	Registrar alarmas UPS, carga, autonomía, voltaje y circuitos afectados. Confirmar si los servicios críticos están en respaldo. Informar N2/N3.
15-60 min	Responsable eléctrico identifica el tramo afectado y aísla solo el circuito necesario. Responsable de sistemas prioriza apagado ordenado de cargas no críticas si la autonomía es insuficiente.
Recuperación	Restaurar energía por etapas: alimentación, UPS, distribución, red, almacenamiento, servidores y aplicaciones. Verificar protecciones, puesta a tierra y parámetros antes de cerrar.
Prohibición	No puentear protecciones, no energizar circuitos sin inspección y no conectar nuevas cargas durante la emergencia.

5.2 Sobretemperatura o falla de climatización

Aplica ante alarma ambiental, temperatura fuera del umbral definido, pérdida de un equipo HVAC, recirculación severa o hot spot identificado.

Disparador	Respuesta
Alerta ambiental	Confirmar lectura con sensor independiente; revisar puertas, obstrucciones, filtros, equipos HVAC y flujo de aire.
Temperatura creciente	Notificar al responsable HVAC; retirar solo obstrucciones permitidas; mantener puertas cerradas y evitar ingreso innecesario.
Riesgo a equipos	Priorizar el restablecimiento del HVAC. De persistir el incremento, aplicar apagado ordenado de cargas no críticas y luego de las críticas según decisión del Director de Crisis.
Retorno	Estabilizar condiciones ambientales durante un periodo definido por OTI antes de recuperar cargas; validar ausencia de alarmas y hot spots.

5.3 Pérdida de enlace, desconexión accidental o falla de comunicación

Paso	Acción
1. Contener	Suspender cambios en el gabinete afectado. No desconectar ni reconectar cables sin identificación y autorización.

Paso	Acción
2. Diagnosticar	Usar matriz de puertos, inventario y monitoreo. Verificar energía, estado de puertos, transceptores, fibra/cobre y rutas redundantes disponibles.
3. Restaurar	Aplicar reconexión o ruta alternativa aprobada; documentar cada cambio y probar conectividad extremo a extremo.
4. Corregir	Actualizar etiquetas, planos y matriz de puertos. Si faltan documentos, generar registro provisional validado por dos técnicos.

5.4 Incendio, humo, agua o daño físico

Ante amenaza a personas, humo, fuego, inundación o ingreso no autorizado, se activa N3 de inmediato.

- Evacuar y activar el protocolo de emergencia del campus. No combatir un incendio salvo personal entrenado y bajo el procedimiento institucional.
- Cortar o aislar energía únicamente si es seguro y conforme al procedimiento eléctrico autorizado.
- No reingresar al ambiente hasta que Seguridad/Mantenimiento declare condiciones seguras.
- Preservar evidencias, evaluar daños y activar la recuperación de servicios desde la alternativa disponible.

6. Priorización de servicios y recuperación

La OTI debe completar y revisar trimestralmente la matriz de servicios críticos. La prioridad final en una emergencia será definida por el Director de Crisis considerando el impacto académico, administrativo y legal.

Prioridad	Criterio	Objetivo de recuperación	Servicios / responsables a completar
P1 - Crítico	Su interrupción paraliza funciones institucionales o compromete seguridad/atención esencial.	Restaurar primero, bajo RTO/RPO aprobados.	[Completar catálogo, RTO, RPO y dueño del servicio]
P2 - Alto	Afecta procesos importantes, con alternativa temporal limitada.	Restaurar después de P1.	[Completar catálogo, RTO, RPO y dueño del servicio]
P3 - Normal	Tiene impacto acotado o alternativa manual disponible.	Restaurar al estabilizar P1 y P2.	[Completar catálogo y dueño del servicio]

RTO: Objetivo de tiempo de recuperación (el tiempo máximo que el sistema puede estar caído tras una falla, antes

que los servicios sufran un impacto inaceptable.

RPO: Objetivo de punto de recuperación (la cantidad máxima de datos que se permite perder, medida en tiempo

desde el ultimo respaldo de datos.

Secuencia mínima de retorno

1. Validar seguridad física, eléctrica y ambiental del ambiente.
2. Validar alimentación, UPS, distribución y monitoreo antes de energizar cargas.
3. Restaurar comunicaciones de gestión y red troncal.
4. Restaurar almacenamiento, virtualización/servidores y dependencias de plataforma.
5. Restaurar servicios P1, validar con sus dueños, y continuar con P2 y P3.
6. Confirmar monitoreo, respaldos, alarmas y documentación actualizada antes del cierre.

7. Comunicaciones, registro y escalamiento

Notificaciones mínimas

Momento	Emisor	Destinatarios	Contenido mínimo
Activación N2/N3	Coordinador DC	Jefatura OTI y equipo de contingencia	Qué ocurrió, hora, alcance, nivel, acción inmediata y próximo reporte.
Actualización	Comunicaciones OTI	Autoridades y dueños de servicios	Estado, servicios afectados, medidas en curso, riesgos y siguiente actualización.
Cierre	Director de Crisis	Partes interesadas	Servicios recuperados, limitaciones, hora de cierre y acciones posteriores.

Bitácora obligatoria

La bitácora debe registrar: identificador del incidente, fecha/hora, detector, nivel, servicios y activos afectados, lecturas de UPS/HVAC, decisiones, autorizaciones, intervenciones, comunicaciones, pruebas de recuperación, causa preliminar, cierre y acciones correctivas.

8. Preparación y mejoras para reducir el riesgo

Horizonte	Acciones
Inmediato	Normalizar puesta a tierra; reetiquetar gabinetes y cableado; optimizar el flujo de aire y eliminar hot spots; establecer directorio y bitácora.
Corto plazo	Implementar monitoreo eléctrico y ambiental; actualizar diagramas unifilares, inventarios, planos y matrices de puertos; ordenar cableado; formalizar control de cambios.
Mediano plazo	Modernizar distribución para una demanda mínima de 78 kVA con crecimiento; evaluar redundancia HVAC y capacidad adicional; realizar ejercicios de contingencia.
Continuo	Mantenimiento preventivo, revisión de UPS/baterías/HVAC, prueba de alarmas, actualización trimestral de contactos y revisión anual del plan.
Capacitación	Mejora la capacidad del personal técnico de soporte para las atenciones inmediatas y criticas que se presenten en el desarrollo y operatividad del Data center.

Indicadores de seguimiento

- Disponibilidad de servicios P1 y duración de incidentes.
- Tiempo de detección, escalamiento y recuperación por tipo de evento.
- Número de alarmas ambientales/eléctricas y tiempo de atención.
- Porcentaje de gabinetes, enlaces y puertos etiquetados y documentados.
- Cumplimiento del mantenimiento preventivo y de los ejercicios programados.

9. Pruebas, mantenimiento y revisión del plan

Actividad	Frecuencia	Evidencia
Validación de directorio de emergencia	Trimestral	Lista de contactos confirmada.
Prueba de notificación y escalamiento	Semestral	Registro de tiempos y oportunidades de mejora.
Ejercicio de mesa: energía/HVAC/comunicaciones	Semestral	Acta, bitácora y plan de acciones.

Actividad	Frecuencia	Evidencia
Simulacro técnico controlado	Anual o tras cambio mayor	Resultados, reversión y aprobación.
Revisión integral del plan	Anual y tras N3	Versión aprobada y distribución controlada.

Toda prueba debe planificarse, evaluarse por riesgo, contar con ventana autorizada y disponer de un plan de reversión. No se efectuarán pruebas que comprometan la producción sin aprobación formal.

10. Aprobación y control de cambios

Rol	Nombre	Firma / fecha
Elaborado por - Coordinación del Data Center	[Completar]	[Completar]
Revisado por - Jefatura OTI	[Completar]	[Completar]
Aprobado por - Autoridad competente	[Completar]	[Completar]

La versión aprobada debe mantenerse disponible para el equipo de contingencia, con copia controlada fuera del ambiente del Data Center y en el repositorio documental institucional.

Anexo A. Directorio de emergencia

Función	Titular	Teléfono	Suplente	Teléfono
Director de Crisis	[Completar]	[Completar]	[Completar]	[Completar]
Coordinador DC	[Completar]	[Completar]	[Completar]	[Completar]
Soporte Electrico / UPS / HVAC	[Completar]	[Completar]	[Completar]	[Completar]
Administrador Infraestructura de Redes de datos	[Completar]	[Completar]	[Completar]	[Completar]
Administrador de Servidores y Ciberseguridad	[Completar]	[Completar]	[Completar]	[Completar]
Soporte / mantenimiento	[Completar]	[Completar]	[Completar]	[Completar]

Anexo B. Lista de verificación de cierre

- La causa fue identificada o se documentó la causa preliminar y el riesgo residual.
- Los servicios recuperados fueron validados por sus dueños.
- No hay alarmas activas eléctricas, de UPS, HVAC o monitoreo.
- Se actualizaron bitácora, ticket, inventario, planos y matriz de puertos si correspondía.
- El Director de Crisis autorizó el cierre y se programaron acciones correctivas.
- Se realizó una revisión posterior al incidente dentro de los cinco días hábiles.

PLAN DE ATENCIONES SLA

1. Objetivo, alcance y principios

El objetivo es estandarizar la atención de incidentes de infraestructura, asignando tiempos y responsabilidades según la criticidad establecida en el Plan de Contingencia. Busca reducir la indisponibilidad, asegurar la comunicación oportuna y dejar evidencia verificable de cada atención.

Alcance

- Energía, UPS, banco de baterías, tableros eléctrico general, de distribución y puesta a tierra vinculados al Data Center.
- Climatización, condiciones ambientales y riesgos de temperatura.
- Gabinetes, conectividad, cableado, enlaces de fibra/cobre y equipos de red del Data Center.
- Monitoreo, alertas, coordinación con proveedores y registro de incidentes.

Principios de servicio

- La seguridad de las personas prevalece sobre cualquier objetivo SLA.
- El SLA mide atención y restauración del servicio; no autoriza intervenciones inseguras ni el puenteo de protecciones.
- Los servicios P1 se atienden 24x7; las demás prioridades se atienden en horario de soporte salvo activación de contingencia.
- El reloj del SLA se detiene únicamente por causas documentadas: espera de acceso autorizado, información indispensable del solicitante, fuerza mayor o proveedor externo sin contrato de atención comprometido.

2. Modelo de criticidad

La clasificación se determina por el impacto en los servicios institucionales, el alcance del componente afectado y la urgencia. Si existen criterios de dos niveles, se aplicará el nivel de mayor criticidad.

Prioridad	Criterios de clasificación	Ejemplos vinculados al Plan de Contingencia
P1 - Crítica	Indisponibilidad total o amenaza inmediata a personas, infraestructura crítica o servicios institucionales P1.	Falla eléctrica mayor; pérdida total del DC; temperatura crítica sostenida; incendio, humo, agua; caída de red troncal.
P2 - Alta	Indisponibilidad parcial relevante, pérdida de redundancia o degradación con riesgo de escalar a P1.	Falla de UPS/HVAC sin impacto total; gabinete o enlace crítico afectado; hot spot localizado; alarma eléctrica relevante.
P3 - Media	Afectación acotada con alternativa operativa, sin riesgo inmediato para continuidad.	Falla no crítica de monitoreo; ordenamiento, etiquetado pendiente; incidencia de puerto no crítico; alerta ambiental estable.
P4 - Baja	Solicitud planificada o mejora que no afecta la operación.	Actualización documental, inventario, consulta técnica, mejora programada o requerimiento de cambio.

3. Catálogo de atención SLA

Los objetivos de restauración representan el tiempo máximo propuesto para recuperar la operación o aplicar una solución temporal aceptada. La solución definitiva puede requerir un plazo adicional con plan de acción y comunicación al solicitante.

Nivel	Cobertura	Acuse	Inicio de diagnóstico	Actualización	Restauración / solución temporal
P1	24x7	15 min	30 min	Cada 30 min	4 horas
P2	24x7 cuando amenace P1; de otro modo horario de soporte	30 min	1 hora	Cada 2 horas	8 horas
P3	Horario de soporte	4 horas hábiles	8 horas hábiles	Diaria o ante cambio material	2 días hábiles
P4	Horario de soporte	1 día hábil	2 días hábiles	Semanal o según acuerdo	5 días hábiles o fecha planificada

Definiciones operativas

Término	Definición
Acuse de recibo	Confirmación al reportante de que el incidente fue registrado, clasificado y asignado.
Inicio de diagnóstico	Inicio documentado de las acciones técnicas para verificar causa, alcance y alternativas.
Restauración	Recuperación comprobada del servicio o componente afectado; puede ser temporal si elimina el impacto inmediato.
Resolución definitiva	Eliminación de la causa raíz o implementación de la corrección permanente, documentada bajo control de cambios.
Cumplimiento SLA	Atención dentro de los objetivos aplicables, descontando pausas válidas registradas.

4. Reglas de priorización por escenario

Escenario	Prioridad inicial	Regla de ajuste
Falla eléctrica, UPS, tableros o puesta a tierra	P1 si afecta servicios críticos o existe riesgo; P2 si es redundante/aislada.	Subir a P1 ante autonomía insuficiente, calentamiento, humo, disparo de protecciones o afectación de varios gabinetes.
HVAC, recirculación o hot spot	P1 ante temperatura crítica o tendencia sostenida; P2 si es localizada y controlada.	Subir a P1 si se requiere apagado de cargas críticas, falla el último equipo HVAC disponible o supera umbral aprobado.
Pérdida de enlace o comunicaciones	P1 si interrumpe red troncal o servicios P1; P2 si afecta segmento crítico; P3 en caso aislado.	Subir por cantidad de usuarios/servicios afectados o pérdida de redundancia.
Documentación, etiquetado y ordenamiento	P3 o P4.	Subir a P2 solo cuando impida recuperar un servicio o incremente un incidente activo.
Incendio, humo, agua, intrusión o daño físico	P1 inmediato.	Aplicar el protocolo de emergencia y seguridad institucional; los objetivos SLA no sustituyen dicho protocolo.

5. Flujo de atención y escalamiento

Paso	Responsable	Acción y evidencia
1. Registrar	Mesa de ayuda / técnico que detecta	Crear ticket: hora, fuente, activos, servicios afectados, prioridad preliminar y evidencias.
2. Clasificar	Coordinador del Data Center	Confirmar prioridad con criterios de impacto y activar el plan de contingencia para P1/P2 cuando corresponda.
3. Atender	Equipo técnico asignado	Diagnosticar, contener y restaurar. Registrar acciones, mediciones, cambios, decisiones y tiempos.
4. Escalar	Coordinador DC / Jefatura OTI	Escalar a responsable eléctrico, HVAC, redes, proveedor o Director de Crisis según el escenario y tiempo consumido.
5. Validar y cerrar	Dueño del servicio / Coordinador DC	Confirmar recuperación, comunicar cierre, documentar causa preliminar y acciones posteriores.

Escalamiento temporal obligatorio

Nivel	Escalamiento técnico	Escalamiento de gestión
P1	Inmediato al Coordinador DC y especialistas; proveedor en los primeros 30 min si se requiere.	Director de Crisis/Jefatura OTI al inicio; aviso institucional según impacto.
P2	Especialista o proveedor al consumir 50% del objetivo de restauración.	Jefatura OTI al consumir 75% del objetivo o si existe riesgo de P1.
P3	Coordinador DC al consumir 75% del objetivo.	Jefatura OTI si supera el objetivo o se repite tres veces en 30 días.
P4	Responsable del servicio según planificación.	Jefatura OTI ante bloqueo, cambio de alcance o incumplimiento planificado.

6. Comunicación y reporte

Prioridad	Primera comunicación	Contenido mínimo	Cierre
P1	Dentro de 30 min de la detección.	Impacto, servicios, acciones de contención, responsable, siguiente actualización y riesgos.	Informe de incidente y revisión posterior en hasta 5 días hábiles.
P2	Dentro de 1 hora.	Impacto, prioridad, acción en curso, ETA o próxima actualización.	Confirmación de recuperación y acciones pendientes.
P3	Dentro de 1 día hábil.	Registro, responsable, diagnóstico inicial y fecha objetivo.	Confirmación mediante ticket.
P4	Según canal de solicitud.	Alcance, responsable y fecha planificada.	Cierre mediante ticket o control de cambios.

Solo la Jefatura OTI o el rol de Comunicaciones OTI emitirá comunicaciones institucionales. Los mensajes técnicos no deben atribuir causas definitivas hasta contar con validación.

7. Indicadores y control del SLA

Indicador	Fórmula / criterio	Meta inicial propuesta	Frecuencia
Cumplimiento de acuse	Tickets con acuse dentro del objetivo / tickets atendidos x 100.	>= 95% mensual	Mensual
Cumplimiento de restauración	Tickets restaurados dentro del objetivo / tickets cerrados x 100.	>= 90% mensual; P1 >= 95% trimestral	Mensual / trimestral
Tiempo medio de restauración	Suma de tiempo de restauración / número de incidentes restaurados.	Tendencia decreciente por prioridad	Mensual

Indicador	Fórmula / criterio	Meta inicial propuesta	Frecuencia
Incidentes repetitivos	Número de incidentes con misma causa o activo en 30 días.	0 P1 repetidos; reducción sostenida P2/P3	Mensual
Calidad de registro	Tickets con bitácora, impacto, causa y validación de cierre completos / tickets cerrados x 100.	>= 95% mensual	Mensual

Tratamiento de incumplimientos

- Todo incumplimiento P1 o P2 requiere análisis de causa, acción correctiva, responsable y fecha compromiso.
- Los incumplimientos por proveedor se consolidan como evidencia para revisar contratos, cobertura y disponibilidad de repuestos.
- Los objetivos podrán revisarse trimestralmente con base en mediciones, capacidad de soporte, resultados de pruebas y cambios de infraestructura.

8. Roles y matriz de responsabilidades

Actividad	Jefatura OTI	Coordinador DC	Especialistas / proveedores	Dueño del servicio
Clasificar P1/P2	A	R	C	C
Atender y restaurar	I	A	R	C
Comunicar impacto	A	R	C	I
Validar recuperación	I	R	C	A
Revisión posterior P1	A	R	C	C
Actualizar SLA y métricas	A	R	C	I

R = Responsable de ejecutar

A = Aprueba / responde por el resultado

C = Consultado

I = Informado

9. Aprobación y anexos

Rol	Nombre	Firma / fecha
Elaborado por - Coordinación del Data Center	[Completar]	[Completar]
Revisado por - Jefatura OTI	[Completar]	[Completar]
Aprobado por - Autoridad competente	[Completar]	[Completar]

ANEXOS RELACIONADOS

Anexo 1: Anexo_1_Matriz_de_Servicios_Criticos_Data_Center_UNSA_v 1.0

Anexo 2: Anexo_2_Dashbord_Cuadro_Control_Tickets_SLA_UNSA

Anexo 3: Anexo_3_control de tickes_SLA_UNSA

Anexo 4: Anexo_4_Resumen mensual de tickes_SLA_UNSA

Anexo 5: Anexo_5_parametros tickes_SLA_UNSA

Anexo 6: Anexo_6_Guia de uso de tickes_SLA_UNSA

Anexo 7: Anexo_7_Informe_Tecnico_EJEMPLO_15.07.2026

Anexo 8: Anexo_8_Formato_Control_Ingreso_Data_Center

MATRIZ DE SERVICIOS CRÍTICOS

Data Center institucional - Sede Facultad de Ingeniería Química

Código	
Versión	1.0
Fecha	22 de julio de 2026
Documento base	Plan_de_Contingencia_Data_Center_UNSA_v 1.0
Propietario	Oficina de Tecnologías de la Información (OTI)
Estado	Matriz propuesta para validación con dueños de servicios

1. Propósito y criterio de uso

La matriz identifica los servicios y componentes que deben priorizarse durante un incidente del Data Center. Se fundamenta en la criticidad alta de energía, comunicaciones y HVAC identificada en el Plan de Contingencia. Los servicios funcionales propuestos deben confirmarse con sus dueños, pues el informe técnico evaluó infraestructura y no aplicaciones o bases de datos.

Escala de prioridad

Prioridad	Definición	Tratamiento en contingencia	RTO objetivo inicial	RPO objetivo inicial
P1	Crítica: paraliza funciones institucionales o compromete la continuidad general.	Restauración prioritaria; atención 24x7 y escalamiento inmediato.	Hasta 4 horas	Según respaldo y validación del dueño
P2	Alta: afecta procesos importantes o elimina redundancia; puede escalar a P1.	Restaurar después de P1; atención acelerada.	Hasta 8 horas	Según respaldo y validación del dueño
P3	Media: afectación limitada con alternativa operativa disponible.	Restaurar al estabilizar P1 y P2.	Hasta 2 días hábiles	Según respaldo y validación del dueño

RTO: tiempo objetivo máximo para restablecer el servicio. RPO: pérdida máxima de datos aceptable; debe ser aprobado por el dueño del servicio y verificarse contra la política de respaldos.

2. Matriz de servicios críticos propuesta

Los campos entre corchetes requieren confirmación institucional. La matriz debe revisarse antes de una contingencia real y cada vez que cambie la arquitectura o el catálogo de servicios.

ID	Servicio / componente	Descripción y alcance	Prioridad	Impacto si falla	Dependencias críticas	Dueño del servicio	RTO	RPO	Estrategia de continuidad / recuperación	Estado de validación
SC-01	Infraestructura eléctrica del Data Center	Alimentación, tableros, UPS, banco de baterías, transformador y distribución hacia gabinetes.	P1	Indisponibilidad parcial o total de todos los servicios tecnológicos alojados.	Red eléctrica, UPS, baterías, protecciones, puesta a tierra, proveedor eléctrico.	OTI / [Responsable eléctrico]	4 h	No aplica	Aislar falla; operar con UPS según autonomía; apagado ordenado de cargas no críticas; restablecer por etapas.	Pendiente
SC-02	Climatización y monitoreo	Equipos HVAC, flujo de aire, sensores de temperatura y humedad del	P1	Sobretemperatura, hot spots,	Energía HVAC, equipos de aire acondicionado,	OTI / [Responsable HVAC]	4 h	No aplica	Restablecer HVAC; eliminar obstrucciones autorizadas;	Pendiente

ID	Servicio / componente	Descripción y alcance	Prioridad	Impacto si falla	Dependencias críticas	Dueño del servicio	RTO	RPO	Estrategia de continuidad / recuperación	Estado de validación
	ambiental	ambiente.		degradación o apagado de equipos de TI.	sensores, proveedor HVAC.				priorizar carga; apagado controlado si persiste riesgo térmico.	
SC-03	Red troncal y conectividad del Data Center	Conmutación/ruteo principal, enlaces de fibra/cobre y conectividad entre gabinetes.	P1	Pérdida de comunicación entre servicios, usuarios y componentes críticos.	Energía, switches/routers, fibra, patch panels, configuración y enlaces de proveedor.	OTI / [Administrador de redes]	4 h	No aplica	Usar rutas redundantes disponibles; restaurar enlaces de gestión y red troncal antes de servicios de aplicación.	Pendiente
SC-04	Plataforma de cómputo y virtualización	Servidores físicos, hipervisores y recursos de cómputo que alojan servicios institucionales.	P1	Indisponibilidad simultánea de múltiples aplicaciones o sistemas institucionales.	Energía, HVAC, red, almacenamiento, respaldos y licencias.	OTI / [Administrador de sistemas]	4 h	[Completar]	Restaurar infraestructura base; iniciar cargas P1 según secuencia aprobada; validar con dueños de servicio.	Pendiente
SC-05	Almacenamiento y repositorios de datos	Cabinas, discos, volúmenes, sistemas de archivos y repositorios institucionales.	P1	Servicios no pueden acceder a datos; posible afectación de integridad o disponibilidad.	Energía, HVAC, red SAN/LAN, respaldos, administración de almacenamiento.	OTI / [Administrador de almacenamiento]	4 h	[Completar]	Verificar integridad; restaurar conectividad y volúmenes; recuperar desde respaldo según RPO aprobado.	Pendiente
SC-06	Servicios de identidad, nombres y direccionamiento	Servicios de directorio, DNS, DHCP, autenticación y sincronización de tiempo, si están alojados en el DC.	P1	Usuarios y sistemas no autentican, resuelven nombres o reciben conectividad.	Red troncal, cómputo, almacenamiento, configuración y respaldos.	OTI / [Administrador de infraestructura]	4 h	[Completar]	Restaurar servicios de soporte antes de aplicaciones dependientes; validar resolución, autenticación y hora.	Pendiente
SC-07	Servicios institucionales académicos y administrativos	Aplicaciones que soportan procesos académicos, administrativos, financieros y de atención institucional.	P1/P2	Interrupción de procesos institucionales; impacto depende del servicio y calendario académico.	Cómputo, almacenamiento, red, identidad, bases de datos, respaldos.	[Dueño funcional] / OTI	[Completar]	[Completar]	Recuperar según catálogo detallado, criticidad funcional, RTO/RPO y secuencia de dependencias.	Pendiente
SC-08	Respaldos y recuperación de datos	Plataforma, repositorios y procedimientos para copias de seguridad y restauración.	P1	Imposibilidad de recuperar información o servicios tras incidente mayor.	Almacenamiento, red, software de respaldo, repositorio externo, credenciales.	OTI / [Responsable de respaldos]	8 h	Según política de respaldo	Verificar último respaldo exitoso; proteger copias; iniciar restauración conforme a RPO y autorización del dueño.	Pendiente
SC-09	Monitoreo, alertas y registros	Monitoreo de infraestructura eléctrica, ambiental, servidores, red y alertas operativas.	P2	Menor capacidad de detección y diagnóstico; aumenta el tiempo de recuperación.	Energía, red, plataforma de monitoreo, sensores y registros.	OTI / [Responsable de monitoreo]	8 h	No aplica	Usar supervisión manual temporal; restablecer alertas, telemetría y umbrales luego de estabilizar P1.	Pendiente
SC-10	Documentación técnica y administración de cableado	Diagramas unifilares, planos, inventarios, matrices de puertos y etiquetado de gabinetes.	P2	Aumenta la probabilidad de error y el tiempo de diagnóstico/recuperación.	Repositorio documental, inventario, personal técnico y etiquetado ANSI/TIA-606.	OTI / [Coordinador DC]	8 h	No aplica	Usar copia controlada fuera del DC; generar registro provisional validado por dos técnicos si falta documentación.	Pendiente

ID	Servicio / componente	Descripción y alcance	Prioridad	Impacto si falla	Dependencias críticas	Dueño del servicio	RTO	RPO	Estrategia de continuidad / recuperación	Estado de validación
SC-11	Acceso físico y seguridad del ambiente	Control de acceso, vigilancia, procedimientos de ingreso y coordinación de seguridad/mantenimiento.	P2	Riesgo de acceso no autorizado, daño físico o demora en la respuesta a emergencia.	Seguridad del campus, energía, cerraduras/controles, personal autorizado.	OTI / Seguridad institucional	8 h	No aplica	Restringir acceso; activar seguridad del campus; registrar ingresos y preservar evidencias.	Pendiente

3. Secuencia de recuperación sugerida

Orden	Componente / servicio	Condición de avance
1	Seguridad física, energía y condiciones ambientales	Ambiente seguro, sin alarmas críticas activas y alimentación validada.
2	Red de gestión y red troncal	Conectividad de administración y enlaces principales operativos.
3	Almacenamiento, cómputo e identidad	Dependencias de plataforma estables y monitoreadas.
4	Servicios institucionales P1	Validación técnica y funcional con el dueño de cada servicio.
5	Servicios P2, monitoreo y documentación	Servicios secundarios restaurados, registros actualizados y acciones pendientes programadas.

4. Validación, control y aprobación

La OTI debe completar el dueño funcional, RTO y RPO de cada servicio; verificar dependencias y respaldos; y realizar una prueba de recuperación de los servicios P1 al menos una vez al año o después de cambios mayores.

Rol	Nombre	Firma / fecha
Elaborado por - Coordinación del Data Center	[Completar]	[Completar]
Revisado por - Jefatura OTI	[Completar]	[Completar]
Validado por - Dueños de servicios críticos	[Completar]	[Completar]
Aprobado por - Autoridad competente	[Completar]	[Completar]

DASHBOARD DE CONTROL DE TICKETS SLA – DATA CENTER UNSA

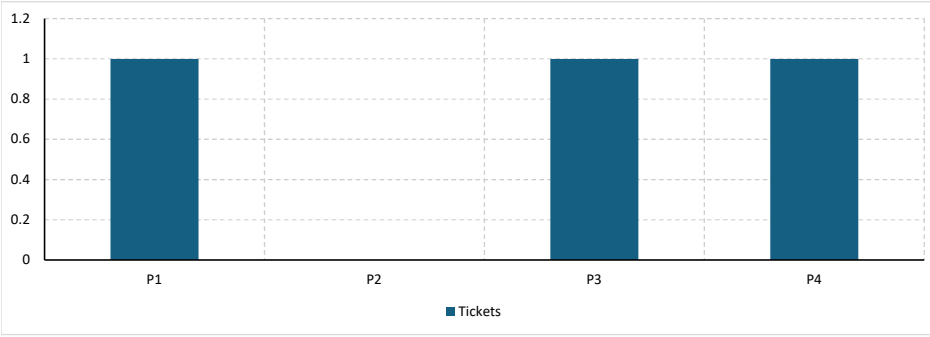
Año	2026	Mes	7	Periodo	Julio 2026

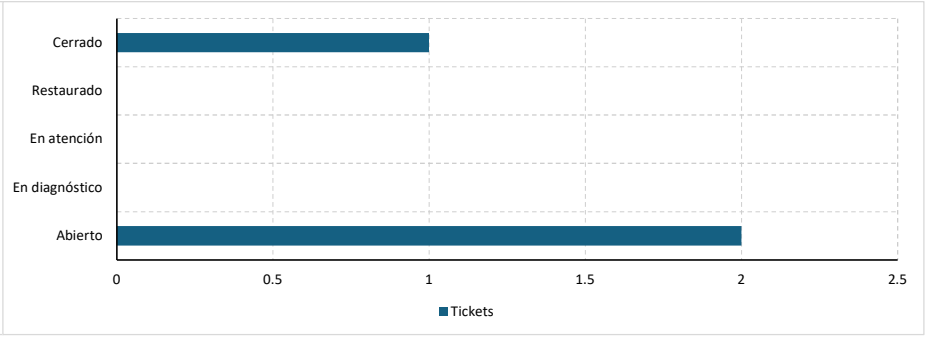
TOTAL DE TICKETS	ABIERTOS / EN ATENCIÓN	TICKETS P1	INCUMPLIMIENTOS SLA
3	2	1	1

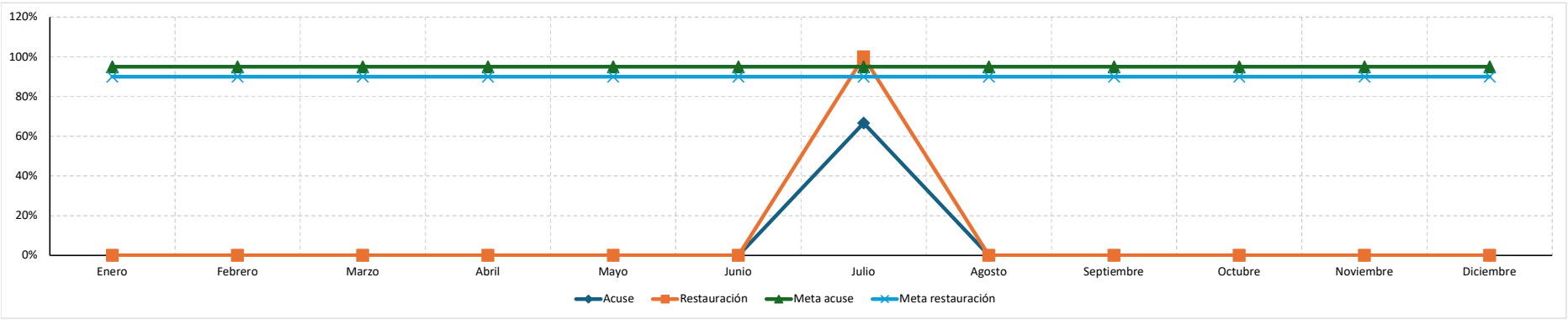
CUMPLIMIENTO DE ACUSE	CUMPLIMIENTO DE RESTAURACIÓN	TIEMPO MEDIO RESTAURACIÓN	CAMPOS MÍNIMOS COMPLETOS
66.7%	100.0%	0.42 h	100.0%

Prioridad	Tickets	Abiertos	% acuse	% restauración	TMR (h)	Incumplimientos
P1	1	1	0.0%			1
P2	0	0				0
P3	1	0	100.0%	100.0%	0.42	0
P4	1	1	100.0%			0

Estado	Tickets
Abierto	2
En diagnóstico	0
En atención	0
Restaurado	0
Cerrado	1







Metas iniciales: acuse ≥95% mensual; restauración ≥90% mensual; calidad de registro ≥95% mensual; restauración P1 ≥95% trimestral.

CUADRO DE CONTROL DE TICKETS DE ATENCIÓN SLA – DATA CENTER UNSA

Complete los campos blancos. Las columnas celestes se calculan automáticamente. Las pausas del SLA deben estar sustentadas y registradas en observaciones.

Código ticket	Estado	Fecha/hora detección	Fecha/hora registro	Mes	Fuente / canal	Reportante	Servicio afectado	Activo	Gabinete / componente	Impacto / usuarios	Prioridad	Alarmas / estado de entrada	Responsable	Proveedor / especialista	Acciones ejecutadas	Autorizaciones	Comunicaciones	Pausa acuse (h)	Pausa diagnóstico (h)	Pausa restauración (h)	Fecha/hora acuse	Inicio diagnóstico	Fecha/hora restauración	Fecha/hora cierre	Validación diseño del servicio	Causa probable/raíz	Acción correctiva	Fecha compromiso	Tiempo acuse real (h)	Tiempo diagnóstico real (h)	Tiempo restauración real (h)	Objetivo acuse (h)	Objetivo diagnóstico (h)	Objetivo restauración (h)	Cumple acuse	Cumple diagnóstico	Cumple restauración	Campos sistemas completos	Semáforo SLA	Observaciones
SLA-1	Cerrado	##########	##########	Julio 2026	Monitoreo	Administrador DC	servidor storage	servidor	gabinete 6	Direccion de adminisiones	P3	caida parcial del servidor	Administrador DC	no aplica	se verifica de forma presencial la causa del problema	Administrador de DC		0.25	0.50	1.00	##########	##########	##########	##########	Validado	se verifica si los equipos HVAC estan en correcta configuracion y operatividad	Se corrige la configuracion de los equipos HVAC para mejorar la temperatura del gabinete	##########	0.42	0.25	0.42	4.00	8.00	16.00	Si	Si	Si	Si	Verde	
SLA-2	Abierto	##########	##########	Julio 2026	Monitoreo	Administrador DC	servidor storage	servidor	gabinete 6	Direccion de adminisiones	P1	caida parcial del servidor	Administrador DC	no aplica	se verifica de forma presencial la causa del problema	Administrador de DC		0.25	0.50	1.00	##########	##########	##########	##########	Validado	se verifica si los equipos HVAC estan en correcta configuracion y operatividad	Se corrige la configuracion de los equipos HVAC para mejorar la temperatura del gabinete	##########	0.42	0.25	0.42	0.25	0.50	4.00	No	Si	Si	Pendiente	Rojo	no se resolvio el problema de temperatura del sistema HVAC
SLA-3	Abierto	##########	##########	Julio 2026	Correo	Administrador DC	switch Core	Switch Core	gabinete 3	Oficina de Tecnologia de Informacion	P4	caida de fuente principal	Administrador DC	proveedor de Switch Core	Se verifica el correcto funcionamiento de la fuente principal	Jefatura de OTI		1.00	1.00	2.00	##########	##########	##########	##########	Pendiente	Se verifica la fuente principal del switch core	se retira la fuente para cambio respectivo con el provesdor, se deja solo con fuente back up	##########	1.67	2.75	2.42	8.00	16.00	40.00	Si	Si	Si	Pendiente	Verde	

RESUMEN MENSUAL DE TICKETS SLA

Los resultados corresponden al año seleccionado en el Dashboard.

Mes	Total	P1	P2	P3	P4	Abiertos	% acuse	% diagnóstico	% restauración	TMR (h)	% campos completos	Incumplimientos	Meta acuse	Meta restauración
Enero	0	0	0	0	0	0						0.0%	95.0%	90.0%
Febrero	0	0	0	0	0	0						0.0%	95.0%	90.0%
Marzo	0	0	0	0	0	0						0.0%	95.0%	90.0%
Abril	0	0	0	0	0	0						0.0%	95.0%	90.0%
Mayo	0	0	0	0	0	0						0.0%	95.0%	90.0%
Junio	0	0	0	0	0	0						0.0%	95.0%	90.0%
Julio	3	1	0	1	1	2	66.7%	100.0%	100.0%	0.42	100.0%	**100.0%**	95.0%	90.0%
Agosto	0	0	0	0	0	0						0.0%	95.0%	90.0%
Septiembre	0	0	0	0	0	0						0.0%	95.0%	90.0%
Octubre	0	0	0	0	0	0						0.0%	95.0%	90.0%
Noviembre	0	0	0	0	0	0						0.0%	95.0%	90.0%
Diciembre	0	0	0	0	0	0						0.0%	95.0%	90.0%

PARÁMETROS DEL PLAN DE ATENCIONES SLA – DATA CENTER UNSA

Prioridad	Cobertura	Acuse (h)	Diagnóstico (h)	Restauración (h)	Objetivo original	Actualización
P1	24x7	0.25	0.50	4.00	4 horas	Cada 30 minutos
P2	24x7 si amenaza P1; de otro modo horario de soporte	0.50	1.00	8.00	8 horas	Cada 2 horas
P3	Horario de soporte	4.00	8.00	16.00	2 días hábiles	Diaria o ante cambio material
P4	Horario de soporte	8.00	16.00	40.00	5 días hábiles o fecha planificada	Semanal o según acuerdo

CONFIGURACIÓN DE JORNADA	Valor
Horas de soporte por día	8
Acuse P4 equivalente (días)	1
Diagnóstico P4 equivalente (días)	2
Restauración P4 equivalente (días)	5

Indicador	Meta	Frecuencia	Criterio
Cumplimiento de acuse	95%	Mensual	Tickets con acuse dentro del objetivo / tickets atendidos
Cumplimiento de restauración	90%	Mensual	Tickets restaurados dentro del objetivo / tickets cerrados
Cumplimiento de restauración P1	95%	Trimestral	Tickets P1 restaurados dentro del objetivo / tickets P1 cerrados
Calidad del registro	95%	Mensual	Tickets cerrados con campos mínimos completos / tickets cerrados
Incidentes repetitivos P1	0	Mensual	Meta: cero P1 repetidos

FUENTE Y CRITERIO DE DISEÑO

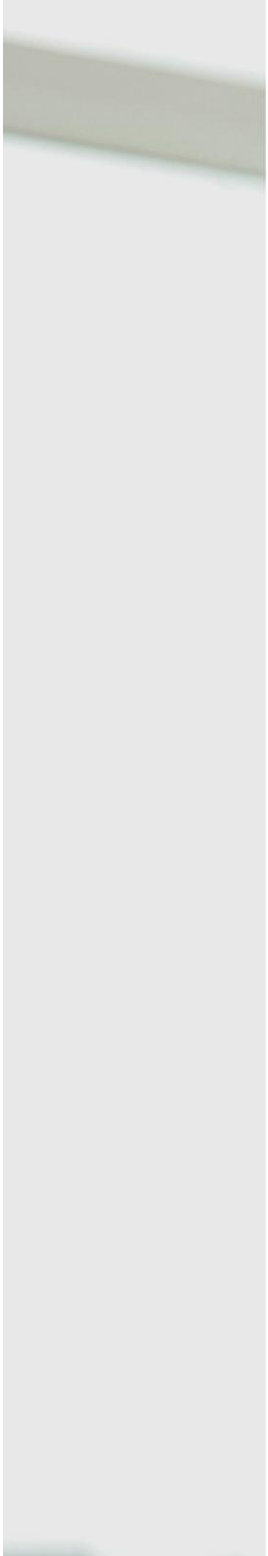
Documento base	Plan de Atenciones SLA del Data Center UNSA
Versión	1.0
Fecha de emisión	22/07/2026
Campos mínimos	Código; detección y registro; servicio/activo/componente; impacto/prioridad; lecturas; responsables; acciones; autorizaciones; comunicaciones; pausas; restauración; validación; causa; acción correctiva.
Nota	Las equivalencias horarias de P3/P4 se calculan con la jornada configurable. La fecha planificada de P4 debe controlarse adicionalmente cuando corresponda.

Estados	Fuente / canal	Prioridad	Validación	Sí / No	Año	Mes
Abierto	Monitoreo	P1	Pendiente	Sí	2026	1
En diagnóstico	Mesa de ayuda	P2	Validado	No	2027	2
En atención	Correo	P3	No validado	N/A	2028	3
Restaurado	Teléfono	P4			2029	4
Cerrado	Proveedor				2030	5
	Otro				2031	6
					2032	7
					2033	8
					2034	9
					2035	10
					2036	11
					2037	12

GUÍA DE USO – CONTROL DE TICKETS SLA

Paso	Instrucción
1	Ingrese cada incidente en la hoja Control Tickets. El código se genera automáticamente cuando se registra la fecha/hora de detección.
2	Complete como mínimo detección, registro, servicio, activo, gabinete/componente, impacto, prioridad, lecturas relevantes, responsable, acciones, autorizaciones, comunicaciones y pausas.
3	Registre acuse, inicio de diagnóstico, restauración y cierre con fecha y hora completas.
4	Las pausas deben corresponder únicamente a causas válidas y quedar sustentadas en Observaciones.
5	Al cerrar el ticket, complete validación del dueño del servicio, causa preliminar, acción correctiva y fecha compromiso.
6	Revise el Semáforo SLA: Verde = dentro de objetivo; Rojo = incumplimiento; Pendiente = ticket aún no evaluable.
7	En Dashboard seleccione año y mes. Los indicadores y gráficos se actualizarán automáticamente.
8	Ajuste en Parámetros SLA las horas de la jornada de soporte si la OTI aprueba una equivalencia distinta.

Campo mínimo del plan	Ubicación en el archivo
Código, detección y registro	Columnas A, C y D
Servicio, activo, gabinete o componente	Columnas H, I y J
Impacto y prioridad	Columnas K y L
Lecturas UPS, temperatura, humedad, alarmas/enlaces	Columnas M a P
Responsables, acciones y autorizaciones	Columnas Q a T
Comunicaciones y pausas SLA	Columnas U a X
Restauración y validación del dueño del servicio	Columnas AA y AC
Causa preliminar y acción correctiva	Columnas AD y AE
Documento base	Plan de Atenciones SLA del Data Center UNSA, versión 1.0.
Fecha de emisión	22/07/2026
Advertencia	Los objetivos propuestos deben validarse con la capacidad real de la OTI, proveedores y dueños de servicios antes de su aprobación.



OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

“TITULO DEL INFORME TECNICA DE MANTENIMIENTO O ATWENCION CORRECTIVA”

FECHA	15/07/2026
LOCAL	
DIRECCION	
BREVE DESCRIPCION DEL TRABAJO	
PERSONAL DE CAMPO	
JEFE DE OFICINA	

Preparado :		No.		
		Nombre del archivo generado con fecha y descripción breve		
Aprobado :	Revisado :	Fecha :	Rev	Referencia
		15/07/2025	Rev A	

1. Generalidades

Ubicación asignada de la atención del usuario final – UNSA.

Fig. 1.- Vista general de la ubicacion.

Preparado :		No. Nombre del archivo generado con fecha y descripción breve		
Aprobado :	Revisado :	Fecha :	Rev	Referencia
		15/07/2025	Rev A	

2. ANTECEDENTES

1.

3. TRABAJOS REALIZADOS

-

4. ANALISIS.

-

Preparado :		No.		
		Nombre del archivo generado con fecha y descripción breve		
Aprobado :	Revisado :	Fecha :	Rev	Referencia
		15/07/2025	Rev A	

5. REPORTE FOTOGRAFICO DE EQUIPOS DE RED DE DATOS ACTUALES

VERIFICACION DE LOS EQUIPOS EXISTENTES	

6. REPORTE FOTOGRAFICO SISTEMA DE PUESTA A TIERRA

VERIFICACION DEL SISTEMA PUESTA A TIERRA	

Preparado :		No.		
		Nombre del archivo generado con fecha y descripción breve		
Aprobado :	Revisado :	Fecha :	Rev	Referencia
		15/07/2025	Rev A	

7. REPORTE FOTOGRAFICO INTERIOR Y EXTERIOR DE CASETA

VERIFICACION DE INTERIOR Y EXTERIOR DE CASETA	

Preparado :		No.		
		Nombre del archivo generado con fecha y descripción breve		
Aprobado :	Revisado :	Fecha :	Rev	Referencia
		15/07/2025	Rev A	

8. REPORTE FOTOGRAFICO VERIFICACION SISTEMA ELECTRICO Y TEMPERATURA DEL AMBIENTE

VERIFICACION DE TOMAS ELECTRICAS COMERCIALES Y TEMPERATURA DE AMBIENTE	

Preparado :		No.		
		Nombre del archivo generado con fecha y descripción breve		
Aprobado :	Revisado :	Fecha :	Rev	Referencia
		15/07/2025	Rev A	

9. CONCLUSIONES

-

10. RECOMENDACIONES

-

REGISTRO DE INGRESO AL DATA CENTER

N°	Fecha	Hora de ingreso	Hora de salida	Nombre completo	DNI	Área / Empresa	Motivo del ingreso	Quién autorizó	Firma del ingresante	Observaciones
001										
002										
003										
004										
005										
006										
007										
008										
009										
010										
011										
012										
013										
014										
015										
016										
017										
018										
019										
020										
021										
022										
023										
024										
025										
026										
027										
028										
029										
030										
031										
032										
033										
034										
035										
036										

Nota: Todo ingreso al Data Center debe contar con autorización previa. Registrar ingreso y salida.